Parlement francophone bruxellois
(Assemblée de la Commission communautaire française)

7 juin 2024

SESSION ORDINAIRE 2023-2024

PROJET DE DÉCRET ET ORDONNANCE CONJOINTS

**de la Région de Bruxelles-Capitale,
de la Commission communautaire commune et
de la Commission communautaire française
portant le Code de la gouvernance et de la donnée**

SOMMAIRE

EXPOSÉ DES MOTIFS ET COMMENTAIRE DES ARTICLES

TITRE I
Dispositions générales

Article 1er

Cette disposition ne nécessite pas de commentaire particulier.

TITRE II
Code

Article 2

Dans le cadre de la transition numérique, la Région Bruxelloise, la Commission communautaire commune et la Commission communautaire française ont entrepris un travail de compilation et d'approfondissement des questions numériques dans le cadre d'un décret et ordonnance conjoints visant l'adoption d'un Code portant, notamment, sur la gouvernance de la donnée numérique.

Par ailleurs, la mise en place d'une nécessaire gouvernance des données est venue confirmer le fait que la gestion des données est assurément destinée à devenir l'accessoire de toute gestion administrative. Dans cette optique, le Code a également réalisé un même travail de compilation et d'approfondissement au niveau des dispositions légales de droit administratif en lien avec les questions de données numériques. En effet, les questions de publicité administrative et de transparence administrative, sont aujourd'hui, plus que par le passé, intimement liées aux questions de respect des droits sur les données à caractère personnel et accessibilité à l'information. Toutefois, les liens entre les matières, pour évidents qu'ils soient, n'en sont pas moins compliqués à appréhender au sein des Autorités publiques. Le regroupement sous la forme d'un Code complet abordant les questions numériques et les questions administratives porte l'espoir de faciliter le travail des Autorités publiques face à la multiplicité des textes et des matières, bien souvent liées à des législations européennes éparses. De surcroît, le Code vise également à faire prendre conscience aux Autorités publiques de l'importance d'une gestion administrative intégrale.

L'ensemble forme un document d'envergure ambitionnant de codifier dans un même ensemble toutes les questions de gouvernance, administrative ou de la donnée, en tant que document de référence pour toute Autorité publique dans le cadre de son activité quotidienne.

Le Code est divisé selon la structure proposée par les *Principes de technique législative – Guide de rédaction des textes législatifs et réglementaires*, www.conseildetat.be, onglet « Technique législative », recommandation n° 62, à savoir avec les subdivisions suivantes :

Partie
Livre
Titre
Chapitre
Section
Sous-section

Le Code bruxellois de la gouvernance et de la données (CBGD) se structure en trois parties :

– une partie A reprenant l'ensemble des définitions du Code et quelques dispositions communes dans à l'ensemble du Code,

– une partie B portant sur la gouvernance administrative, et reprenant, à ce jour :

  - un livre B.I. consacré à la publicité administrative, qui suppose nécessairement, notamment, des question d'accès à des données numériques,

  - et un livre B.II comprenant le cadre légal organique de la Commission d'accès aux documents administratifs (CADA), renommée Commission d'accès aux documents administratifs et aux données (CADADo) pour souligner le renforcement de ses activités en matière de données.

La structuration du Code en plusieurs parties poursuit notamment le but que cette partie B, relative à la gouvernance administrative, soit, à l'avenir, complétée par d'autres livres en matière de gouvernance administrative présentant un lien avec les questions d'accès à l'information, à la publication et à la transparence administrative, en tant que cadre de gouvernance.

– une partie C relative à la gouvernance de la donnée, regroupant six livres :

  - un livre C.I. exposant le champ d'application ratione personae de la partie C et des dispositions communes à l'ensemble de la partie C,

  - un livre C.II. posant les principes de la gouvernance de la donnée,

- un livre C.III. formulant les obligations de gouvernance des Autorités publiques visées par la partie C;

- un livre C.IV. relatif aux flux de données que sont le partage administratif, la réutilisation et la Communication;

- un livre C.V. portant la Plateforme bruxelloise de la donnée;

- un livre C.VI. portant la structure administrative de la gouvernance.

PARTIE A

DÉFINITIONS

La partie A rassemble l'ensemble des définitions du Code et quelques dispositions communes à l'ensemble du Code rajoutées à la suite de l'avis de l'Autorité de protection des données (APD ci-après).

Un premier livre, A.I., reprend les définitions communes aux parties B et C du Code et les dispositions communes à l'ensemble du Code.

Le livre A.II présente les définitions de la partie B, propres à chaque livre. Une découpe livre par livre a été choisie de manière à permettre que la partie B puisse compter à l'avenir d'autres livres en matière de gouvernance administrative sans que les définitions des actuels livres ne s'imposent à ces futures législations.

Le livre A.III. présente les définitions de l'ensemble de la partie C.

Bien que le Conseil d'État ait formulé la proposition de modifier la structure du Code et d'ajouter les définitions relatives aux parties B et C du Code avant les dites parties, cet avis n'a pas été suivi car l'intention poursuivie par la mise en place d'une partie A, en prélude aux dispositions des autres parties, visait précisément à rassembler en une seule partie l'ensemble des définitions de manière à ce que le lecteur puisse immédiatement avoir à sa disposition, sur un mode lexical, l'ensemble des définitions du Code. Du reste, c'est le mode opératoire généralement retenu pour toute texte législatif : formuler l'ensemble des dispositions en tout premier lieu.

LIVRE A.I.
Définitions communes au Code

Article A.I.1.
Respect intégral du RGPD

L'article A.I.1. contient une référence générale au RGPD conformément à la demande de l'APD, au point 26 de son avis :

« 26. Deuxièmement, compte-tenu des très nombreuses relations existant entre le Projet et les règles de protection des données (le Projet contient des règles sur la classification des données, les recours, les analyses de risque, les responsabilités, la sécurité de l'information, la conformité, la traçabilité et la responsabilités des autorités publiques, la correction des données, etc.), du fait que le Projet soit une lex posterior du rang de loi, et du fait que le RGPD laisse une marge de manœuvre aux États Membres à plusieurs égards, en particulier s'agissant du traitement de données dans le secteur public, l'Autorité est d'avis qu'une disposition générale devrait spécifier que le Projet est sans préjudice du RGPD et ne peut être lu comme limitant les droits des personnes concernées ou les obligations du responsable du traitement ».

Article A.I.2.
Application sauf exception des définitions du RGPD

L'article A.II.2 rend les définitions du RGPD applicables au présent Code sauf définitions spécifiques dans le Code. Ceci a été organisé afin de répondre à une remarque à ce sujet de l'avis de l'APD.

Article A.I.3.
Définitions communes au Code

L'article reprend la définition d'« Autorité publique ».

L'expression « Autorité publique » est transversale à l'ensemble du Code mais le champ d'application de certaines parties, livres ou titres ne vise qu'une partie des Autorités publiques visées par la définition générale. La signification de la notion d'Autorité publique sera donc modulée en fonction de la matière abordée par chaque partie, livre ou titre.

Dans son ensemble, la définition d'Autorité publique proposée se fonde sur les définitions actuelles :

– de la notion d'autorité publique consacrée par l'ordonnance du 27 octobre 2016 visant à l'établissement d'une politique de données ouvertes (Open Data) et portant transposition de la Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la Direc-

tive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public;

– de la notion d'autorité administrative consacrée par le décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française relatifs à la publicité de l'administration dans les institutions bruxelloises.

Ces deux actes législatifs sont la transposition respectivement :

– d'une part, de la directive (UE) 2019/1024 du Parlement et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte),

– d'autre part, de la définition imposée par la directive 2003/4/CE du Parlement européen et du Conseil du 28 janvier 2003 concernant l'accès du public à l'information en matière d'environnement et abrogeant la directive 90/313/CEE du Conseil.

Les exigences relatives à ces deux textes européens ont été reprises dans le cadre d'une définition fusionnée de la notion d'Autorité publique.

Il est important de souligner que certaines Autorités publiques peuvent être visées sous plusieurs tirets.

Pour rappel, l'énumération des Autorités publiques soumises aux livres B.I et B.II est plus explicite que celle des Autorités publiques soumises à la partie C dans la mesure où la législation en matière de publicité administrative contenue dans la partie B dans le but d'être la plus accessible possibles aux citoyens dans le cadre de l'exerce de leur droit à l'information environnementale et d'accès aux documents administratifs.

Les autres définitions de l'article A.I.3. n'appellent pas de commentaire particulier.

LIVRE A.II
Définitions de la partie B

TITRE I
Définitions du livre B.I.

Article A.II.1.
Définitions du livre B.I

Cet article reprend l'article 4 du décret et ordonnance conjoints du 16 mai 2019, en supprimant principalement la notion d'autorité administrative qui est remplacée par la notion d'Autorité publique au sens de l'article A.I.1.

Sont également ajoutées, les définitions des points 9) et 10). Elles proviennent de la circulaire du 16 décembre 2021 précisant les modalités de publication en open data des inventaires des marchés publics et des subventions par les autorités bruxelloises visées par le décret et ordonnance conjoints du 16 mai 2019.

À titre de précision, constituent une subvention les avances de fonds récupérables consenties sans intérêts, octroyées en vue de promouvoir des activités utiles à l'intérêt général ou encore les aides de la Région de Bruxelles-Capitale prévues pour soutenir les entreprises et indépendants Bruxellois en cas de crise majeure.

TITRE II
Définitions du livre B.II.

Article A.II.2.
Définitions du livre B.II

Cet article retranscrit l'article 4 du décret et ordonnance conjoints du 16 mai 2019. Il supprime ce pendant les définitions de « demandeur » (11°) et de « public » (12°) qui ne sont plus pertinentes dans le cadre du livre B.II.

LIVRE A.III.
Définitions de la partie C

Article A.III.1.
Définitions de la partie C

1° « arrêté fixant les seuils numériques » :

Il s'agit de l'arrêté adopté conjointement par le Gouvernement, le Collège réuni et le Collège, qui identifie les Autorités publiques par paliers sur la base de seuils numériques destinés à déterminer l'activité numérique et la maturité numérique de chaque Autorité publique en vue d'établir une proportionnalité par rapport aux obligations de gouvernance de la donnée mise à leur charge.

2° « Règlement sur la gouvernance des données » :

Cette définition n'appelle pas de commentaire.

3° « Règlement eIDAS » :

Cette définition n'appelle pas de commentaire.

4° « Directive SRI 2 (NIS 2) » :

Cette définition n'appelle pas de commentaire.

5° « Autorité publique tierce » :

La définition d'« Autorité publique tierce » permet de viser des pouvoirs publics issus d'un autre niveau de pouvoir, mais qui ne tombent pas sous le champ d'application ratione personae du Code parce qu'elles ne sont pas comprises dans la notion d'Autorité publique.

La notion d'Autorité publique est un terme défini dans le cadre du Code. Or, cette définition vise des organismes publics liés à la Région, à la COCOM et à la COCOF, et ne vise donc pas les organismes publics des autres collectivités publiques dont sont issues les « autorités publiques tierces », comme les autres Régions et Communautés ou le niveau Fédéral ou encore des collectivités de niveau international.

La notion de « pouvoir public » renvoie à un terme générique, non défini dans le cadre du Code, afin de désigner de manière générique tout organisme public défini selon les critères déterminés par les collectivités publiques tierces concernées.

6° « donnée » :

Le Règlement sur la gouvernance des données définit la donnée comme « toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements, sonores, visuels ou audiovisuels ».

La donnée numérique est un type de document tel que défini ci-après. Tant le document que la donnée sont sources d'information. La notion d'information n'est pas définie et est utilisée selon le sens courant de ce terme.

7° « document » :

La définition est reprise de l'article 2, 6), de la Directive (UE) 2019/1024 du Parlement et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte), ci-après la « directive ISP ».

La notion de document est plus large que la notion de donnée. La donnée est exclusivement numérique alors que les documents visent tous les supports possibles. Tant le document que la donnée sont sources d'information. La notion d'information n'est pas définie et est utilisée selon le sens courant de ce terme.

Les notions de donnée et de document restent donc deux notions distinctes vu les régimes différents qui leur sont applicables. Le Règlement sur la gouvernance des données ne vise que les données et la Directive ISP vise les documents.

8° « donnée protégée » :

Cette définition est inspirée de l'article 3, 1), du Règlement sur la gouvernance des données qui définit le champ d'application du Règlement sur la gouvernance des données. Les termes du Règlement sur la gouvernance des données ont été adaptés afin d'obtenir une définition générale de ce type de données.

9° « donnée sensible » :

Une donnée est dite sensible (indépendamment de sa nature protégée, publique …) car sa diffusion pourrait être à l'origine d'un préjudice dont il faut se préserver (ex : les nids de faucons à bxl).

10° « donnée classifiée » :

Définition inspirée de l'article 2, alinéa 1er, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. Elle vise également à couvrir les mentions prévues par l'UE et l'OTAN dans le cadre de leur travail institutionnel ou des accords internationaux.

11° « jeu de données » :

Cette définition est reprise d'initiatives similaires dans des pays limitrophes, comme en France, où l'initiative « Etalab » l'utilise dans le guide destiné à la publication des données (« Publier les données sur data.gouv.fr », https ://guides.etalab.gouv.fr/pdf/guide-data.gouv.fr.pdf).

12° « donnée ouverte » :

Aucune définition n'est disponible en la matière en droit communautaire ou en droit national. Dès lors, il est ici fait appel au droit comparé.

Cette définition est inspirée de la définition reprise au Vocabulaire de l'informatique et du droit en droit français (Texte n° 107, JORF n° 0103 du

3 mai 2014, accessible en ligne https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000028890784)

Les données ouvertes sont accessibles par tous. La notion de données ouvertes recouvre la notion anglaise de « open data » au sens de la Directive ISP. L'accès libre aux données ouvertes ne préjuge cependant pas de leur caractère réutilisable.

13° « donnée acquise » :

Les « données acquises » sont les données qui ne sont pas produites par l'entité qui les détient; elles ne peuvent être définies que par rapport aux données produites.

À titre d'exemple, les tiers mentionnés dans la définition peuvent être, par exemple, des courtiers de données, et les moyens non commerciaux pourraient par exemple être des initiatives gouvernementales ouvertes.

14° « donnée à forte valeur (ensemble de) » :

Cette définition est reprise de l'article 2, 10), de la Directive ISP et de l'ordonnance bruxelloise du 10 décembre 2021.

Ces données devraient être mises à la disposition du public en priorité et selon les modalités de publications et réutilisations énoncées dans le Règlement d'exécution (UE) 2023/138 de la Commission du 21 décembre 2022 établissant une liste d'ensembles de données de forte valeur spécifiques et les modalités de leur publication et de leur réutilisation.

15° « donnée déduite » et « donnée dérivée » :

Cette définition est reprise des « Lignes directrices relatives au droit à la portabilité des données » (Groupe de Travail Article 29, « Lignes directrices relatives au droit à la portabilité des données », WP 242 rev.01, 16/FR) https://www.cnil.fr/sites/default/files/atoms/files/wp242rev01_fr.pdf).

Dans le cadre du présent Code, les notions de « données déduites » et de « données dérivées » sont interchangeables. Ces deux notions peuvent être utilisées par les Autorités publiques en fonction de la finalité qu'elles poursuivent. Néanmoins, nous soulignons que ces deux notions ne se recoupent pas entièrement.

Ainsi, prenons l'exemple relative à la taille d'un oiseau.

D'une part, supposons que nous avons mesuré la longueur de l'aile d'un oiseau et que nous connaissons sa famille d'oiseaux. Nous pouvons déduire la taille approximative de l'oiseau en utilisant des données de référence pour cette famille. La taille de l'oiseau est une donnée déduite.

D'autre part, supposons que nous avons mesuré la longueur et la largeur de l'aile d'un oiseau. Nous pouvons alors calculer la surface de l'aile en multipliant la longueur et la largeur. La surface de l'aile est une donnée dérivée.

16° « donnée d'origine privée » :

Le terme d'entité est choisi à dessein en vue de viser le plus grand éventail de cas de figure (entités avec et sans personnalité juridique, personnes morales ou physiques, etc.). On retrouvera également et notamment, en fonction du contexte, les notions d'opérateur privé, de citoyen ou d'usager, reprises à différents endroits du Code, pour faire référence à des entités privées.

17° « donnée exclusive » :

Aucune définition n'est disponible en la matière en droit communautaire ou en droit national. Dès lors, il est ici fait appel à la doctrine.

Cette définition est reprise de la doctrine, voir notamment S., Gagnon-Turcotte, M. Schulthorp, S. Coutts, Les partenariats de données numériques : mettre les bases d'une gouvernance de données collaborative dans l'intérêt du public, Edition Nord Ouvert, Montréal, 2021.

18° « donnée fermée » :

Aucune définition n'est disponible en la matière en droit communautaire ou en droit national. Dès lors, il est ici fait appel à la doctrine.

Cette définition est reprise de la doctrine, voir notamment S., Gagnon-Turcotte, M. Schulthorp, S. Coutts, *Les partenariats de données numériques : mettre les bases d'une gouvernance de données collaborative dans l'intérêt du public*, Edition Nord Ouvert, Montréal, 2021.

19° « donnée fournie librement » :

Aucune définition n'est disponible en la matière en droit communautaire ou en droit national. Dès lors, il est ici fait appel à la doctrine.

Cette définition est reprise de la doctrine, voir notamment S., Gagnon-Turcotte, M. Schulthorp, S. Coutts, *Les partenariats de données numériques : mettre les bases d'une gouvernance de données collaborative dans l'intérêt du public*, Edition Nord Ouvert, Montréal, 2021.

20° « donnée observée » :

Aucune définition n'est disponible en la matière en droit communautaire ou en droit national. Dès lors, il est ici fait appel à la doctrine.

Cette définition est pour partie reprise de la doctrine, voir notamment S., Gagnon-Turcotte, M. Schulthorp, S. Coutts, Les partenariats de données numériques : mettre les bases d'une gouvernance de données collaborative dans l'intérêt du public, Edition Nord Ouvert, Montréal, 2021.

L'exemple-type de données observées est la récolte de données analytiques sur la base de cookies.

21° « donnée partageable » :

On distinguera les données partageables des données ouvertes en ce que celles-ci sont dites « partageables » moyennant la création d'un cadre légal défini, ce qui n'est pas le cas, par exemple, des données ouvertes.

22° « donnée publique » :

L'attention est attirée sur le fait que toute donnée détenue par une Autorité publique n'est pas forcément et automatiquement une donnée publique dans la mesure où certaines Autorités publiques peuvent avoir des activités qui ne peuvent pas être assimilées à des missions de services publics. Les données récoltées dans le cadre de ces activités ne sont alors pas des données publiques, conformément à ce que précise l'article 1.2, a) de la directive ISP.

Cette situation est notamment celle de personnes morales qui peuvent se voir qualifier d'Autorités publiques conformément au livre C.I. du présent Code et qui se voient confier une SIEG. Par ailleurs, en dehors de leur activité SIEG, ces Autorités publiques restent libre de développer également une activité de nature purement commerciale dans laquelle elles seront assimilées à des opérateurs privés, sans financement public.

23° « donnée d'usage » :

Les données d'usage sont constituées par les traces d'activité des utilisateurs de services numériques, tel l'historique de recherche sur un portail documentaire. Elles permettent de connaître le comportement du public dans les environnements numériques, incluant leurs goûts et préférences en matière de contenus.

24° « donnée de contenu » :

Les données de contenu sont tout audio, vidéo, image, formule arithmétique ou toute autre forme qui contient effectivement les informations visées par la donnée, à la différence des données de référence.

25° « donnée de référence » :

Cette définition s'inspire de la définition du même terme inscrite dans le droit français (voir Article L321-4 du Code des relations entre le public et l'administration). Il s'agit de données indispensables pour lier des bases de données de nature hétérogène et construire tout nouveau service intégré au web des données.

Il s'agit de donnés qui permettent de faire le lien avec d'autres systèmes ou bases de données, telles que le numéro d'identification à la Banque Carrefour des Entreprise ou le numéro de Registre national.

Ces données se distinguent des métadonnées en ce que ces dernières sont des informations qui décrivent les caractéristiques des données, telles que leur format, leur taille, leur auteur, leur date de création, leur emplacement de stockage, …

26° « donnée dynamique » :

Cette définition est reprise de l'article 2, 8), de la Directive ISP.

27° « données de la recherche » :

Cette définition est reprise de l'article 2, 9), de la Directive réutilisation.

28° « métadonnée » :

Cette définition s'inspire du travail réalisé par l'autorité de contrôle française, notamment au travers du *Guide pratique de la publication en ligne et de la réutilisation des données publiques « open data »*, établi par la CNIL et la CADA (Commission d'accès aux documents adminis-

tratifs), et disponible en ligne: https://www.cnil.fr/sites/default/files/atoms/files/guide-open-data.pdf.

29° « donnée issue de source authentique »

Contrairement à la suggestion du Conseil d'État de supprimer cette définition, il a été décidé de la conserver afin de marquer clairement la différence entre :

– les données authentiques, c'est-à-dire les données qui ont pour qualité d'être authentique sans être pour autant des données issues de sources authentiques au sens du Code;

– les données issues de sources authentiques (que cette source authentique soit bruxelloise ou d'un autre niveau de pouvoir).

30° « source authentique » :

Une source authentique est une base de données particulière à laquelle est attribuée une valeur particulière du fait que cette base de données n'est gérée que par une seule Autorité publique, qualifiée de producteur au sens du présent Code. Au niveau fédéral, le Registre national ou la Banque Carrefour des Entreprises sont des exemples de sources authentiques.

Il est important de souligner que la source authentique vise bien la base de données, dans laquelle les Autorités publiques (qui ne sont pas le producteur de la source authentique) iront chercher les données issues de sources authentiques nécessaires à leurs missions de services publics et obligations d'intérêt général. La source authentique ne vise donc pas l'Autorité producteur de la source authentique.

Cette définition est inspirée de la définition fédérale de la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral visant :

– la *« donnée authentique » en tant que « donnée récoltée et gérée par une instance dans une base de données et qui fait foi comme donnée unique et originale concernant la personne ou le fait de droit concerné, de sorte que d'autres instances ne doivent plus collecter cette même donnée »;*

– la *« source authentique » : « banque de données dans laquelle sont conservées des données authentiques »;*

Le fait de s'être aligné sur la formulation de la loi fédérale permet pratiquement que les données authentiques fédérales puissent être assimilées à des données issues de source authentique au sens du présent Code. En effet, l'État fédéral peut qualifier d'authentiques certaines données ou sources dans le cadre de ses compétences propres et ces sources ou données authentiques seront traitées conformément aux dispositions du Code en matière de sources authentiques.

Chaque entité a, dans le cadre de ses compétences, la mission de récolter certaines données. Ces données peuvent intéresser d'autres entités dans le cadre de l'exercice de leurs compétences. Chaque entité peut décider dans son ordre juridique interne d'accorder l'accès de ses sources authentiques à d'autres entités qui ne pourront, nécessairement, en faire usage que dans le cadre de l'exercice de leurs compétences propres. L'utilisation de données n'est qu'une compétence accessoire à une compétence matérielle propre à chaque entité. En utilisant les sources authentiques d'une autre entité, aux conditions légales fixées par cette autre entité, l'entité utilisatrice des sources authentiques reste dans le cadre de ses compétences propres.

Les données issues de source authentique sont une catégorie particulière de données. Ce qui caractérise une donnée authentique n'est pas sa nature (le nom d'une personne peut, par exemple, être tant une donnée « authentique » qu'une donnée à caractère personnel « ordinaire »), mais la façon dont cette donnée est collectée, conservée et rendue accessible dans le cadre de sa gouvernance. En effet, les données issues de sources authentiques ne sont collectées et actualisées que par une Autorité publique ou une Autorité publique tierce – dite Autorité publique producteur de la donnée –, mais peuvent ensuite être consultées par un nombre en principe illimité d'autres Autorités publiques aux conditions fixées par le livre C.V du Code.

Le principe de la donnée issue de source authentique veut qu'une fois collectée par une Autorité publique au sens du présent Code ou par une Autorité publique tierce, toutes les autres Autorités publiques ne soient plus tenues de collecter cette même donnée.

Comme les données issues de sources authentiques ne seront gérées que par un seul service public, elles ont une valeur unique et originale dans l'ensemble de l'écosystème bruxellois.

L'objectif poursuivi est de permettre aux Autorités publiques de travailler autant que possible avec les données issues de sources authentiques.

Il convient de préciser que le concept d'« authentique » a une signification autonome dans le cadre du présent Code. Cette interprétation qui lui est propre est donc indépendante de la signification reprise dans d'autres législations, comme par exemple dans le Code civil.

31° « source authentique bruxelloise » :

Cette notion désigne la source authentique désignée comme tel par arrêté, conjoint ou non, par le gouvernement, le Collège réuni et/ou le Collège, ou par ordonnance ou décret; afin de distinguer ces sources authentiques bruxelloises des sources authentiques reconnues par les autorités publiques tierces.

32° « domaine de données » :

Cette notion est utilisée pour décrire l'étendue et les limites d'un ensemble de données, ainsi que les règles et les structures qui régissent l'accès, l'utilisation et la manipulation de ces données. Une liste de domaines et de sous-domaines de données, en lien avec le thésaurus multilingue, est géré par l'Office des publications de l'Union européenne, EuroVoc.

33° « utilisateur (des données) » :

Le Règlement sur la gouvernance des données définit l'utilisateur (des données) comme « *toute personne physique ou morale qui dispose d'un accès licite à certaines données à caractère personnel ou non personnel et qui a le droit, y compris au titre du règlement (UE) 2016/679 lorsqu'il s'agit de données à caractère personnel, d'utiliser ces données à des fins commerciales ou non commerciales* ».

34° « administrateur de base de données » :

Les administrateurs des données sont les destinataires des données qui s'efforcent généralement de produire de la valeur en analysant et traitant les données partagées de manière à les transformer en information utile.

35° « administrateur de sécurité informatique » :

L'administrateur de sécurité informatique s'assure que les données sont protégées contre l'accès non autorisé, la modification, la destruction ou la divulgation. Il est également chargé de la mise en place et de la surveillance des politiques de sécurité, et de la gestion des incidents de sécurité.

36° « administrateur réseau » :

Cette définition n'appelle pas de commentaire particulier.

37° « administrateur système » :

Cette définition n'appelle pas de commentaire particulier.

38° « organisations altruistes » :

Cette définition n'appelle pas de commentaire particulier.

39° « altruisme en matière de données » :

Le Règlement sur la gouvernance des données définit l'altruisme en matière de données comme « *le partage volontaire de données fondé sur le consentement donné par les personnes concernées au traitement de données à caractère personnel les concernant, ou l'autorisation accordée par des détenteurs de données pour l'utilisation de leurs données à caractère non personnel sans demander ni recevoir de contrepartie qui aille au-delà de la compensation des coûts qu'ils supportent lorsqu'ils mettent à disposition leurs données, pour des objectifs d'intérêt général prévus par le droit national, le cas échéant, par exemple les soins de santé, la lutte contre le changement climatique, l'amélioration de la mobilité, la facilitation du développement, de la production et de la diffusion de statistiques officielles, l'amélioration de la prestation de services publics, l'élaboration des politiques publiques ou la recherche scientifique dans l'intérêt général* ».

Les organisations altruistes réalisent leurs missions en augmentant le volume des données disponibles pour des utilisations à des fins d'intérêt général tels que décrites ci-avant.

40° « prestataire de services de confiance » :

Le Règlement eIDAS définit le *« prestataire de service de confiance » comme « toute personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié »*.

41° « service de confiance » :

Le Règlement eIDAS définit le *« service de confiance » comme « tout service électronique*

normalement fourni contre rémunération qui consiste :

A) en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services; ou

B) en la création, en la vérification et en la validation de certificats pour l'authentification de site internet; ou

C) en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services ».

42° « prestataires de services en nuage » :

Cette définition est reprise de l'article 6, 30) de la Directive « SRI 2 » (dite également « NIS 2 »). Nous notons que la Directive NIS, transposée en Belgique par la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, définissait le service d'informatique en nuage comme *« un service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées ».*

La définition reprise dans la directive NIS 2, qui n'est pas encore transposée en droit national, paraît plus complète.

43° « prestataire de services informatiques de stockage » :

Ces services peuvent inclure des solutions de stockage de données en réseau (dites « nas »), de stockage de données de bloc (dites « san ») ou de stockage de données en objet (dites « object storage »), ainsi que des services de sauvegarde, de récupération et d'archivage de données.

Les prestataires de services de stockage informatique peuvent également offrir des services de migration de données pour aider les organisations à déplacer leurs données d'un système à un autre, et des services de gestion de données pour aider les entreprises à organiser, classer et gérer leurs données. Les prestataires de services de stockage informatique peuvent également offrir des solutions de stockage de données en cloud pour des institutions qui souhaitent bénéficier de la flexibilité, de la scalabilité et de la rentabilité des services de stockage en cloud.

44° « service d'intermédiation de données » :

Le Règlement sur la gouvernance des données définit le service d'intermédiation de données comme : *« tout service qui vise à établir des relations commerciales à des fins de partage de données entre un nombre indéterminé de personnes concernées et de détenteurs de données, d'une part, et d'utilisateurs de données, d'autre part, par des moyens techniques, juridiques ou autres, y compris aux fins de l'exercice des droits des personnes concernées en ce qui concerne les données à caractère personnel, à l'exclusion au minimum de ce qui suit :*

a) des services qui obtiennent des données auprès des détenteurs de données et les agrègent, les enrichissent ou les transforment afin d'en accroître substantiellement la valeur et concèdent une licence d'utilisation des données résultantes aux utilisateurs de données, sans établir de relation commerciale directe entre les détenteurs de données et les utilisateurs de données;

b) des services axés sur l'intermédiation de contenus protégés par le droit d'auteur;

c) des services qui sont utilisés exclusivement par un seul détenteur de données pour lui permettre d'utiliser les données qu'il détient, ou qui sont utilisés par des personnes morales multiples au sein d'un groupe fermé, y compris dans le cadre de relations de fournisseur ou de client ou de collaborations établies par contrat, en particulier ceux qui ont pour principal objectif de garantir les fonctionnalités d'objets et de dispositifs connectés à l'internet des objets;

d) des services pour le partage de données proposés par des organismes du secteur public qui ne cherchent pas à établir des relations commerciales. ».

45° « écosystème numérique bruxellois » :

Cette définition n'appelle pas de commentaire particulier.

46° « Plateforme bruxelloise de la donnée » :

Cette définition n'appelle pas de commentaire particulier.

47° « Centre d'intégration bruxellois » :

Cette définition n'appelle pas de commentaire particulier.

48° « Catalogue des données » :

Cette définition n'appelle pas de commentaire particulier.

49° « Portail ouvert des données publique » :

Cette définition n'appelle pas de commentaire particulier.

50° « Centre d'exploitation et d'analyse des données » :

Cette définition n'appelle pas de commentaire particulier.

51° « Point de contact et d'information » :

Cette définition n'appelle pas de commentaire particulier.

52° « Service d'appui » :

Cette définition n'appelle pas de commentaire particulier.

53° « Secrétariat numérique » :

Cette définition n'appelle pas de commentaire particulier.

54° « Comité de coordination numérique » :

Cette définition n'appelle pas de commentaire particulier.

55° « Bureau de la donnée » :

Cette définition n'appelle pas de commentaire particulier.

56° « Comité de validation de l'architecture numérique » :

Cette définition n'appelle pas de commentaire particulier.

57° « Comité de gouvernance de la donnée » :

Cette définition n'appelle pas de commentaire particulier.

58° « Bureau d'achats numériques » :

Cette définition n'appelle pas de commentaire particulier.

59° « administrateur local de la donnée » :

Cette définition n'appelle pas de commentaire particulier.

60° « responsable de la donnée » :

Cette définition n'appelle pas de commentaire particulier.

61° « conseiller en sécurité de l'information » :

Cette définition n'appelle pas de commentaire particulier.

62° « entreprise publique » :

Cette définition provient de l'article 2, 3 et de l'article 1er, § 1er, b) de la Directive ISP.

63° « université » :

Cette définition provient de l'article 2, 4), de la Directive ISP.

64° « opérateur privé » :

L'opérateur privé vise toute entité qui n'est pas une Autorité publique, par exemple une personne physique ou morale, une association ayant une personnalité juridique ou non. Cet opérateur privé, au sens du présent Livre, porte un intérêt à communiquer à des Autorités publiques des données qu'il possède ou à en recevoir en vue d'une réutilisation. Ce terme a été choisi afin de rassembler tous les acteurs susceptibles de participer à une réutilisation ou une communication, au sens du présent Code et est donc plus large que la notion d'entreprise visée dans le Code de droit économique. En effet, ces flux peuvent intéresser également un citoyen, ou une organisation qui ne relève pas de la définition d'entreprise au sens du Code de droit économique.

65° « Autorité publique producteur (de données) » :

Cette définition n'appelle pas de commentaire particulier.

66° « Autorité publique destinataire » :

Cette définition n'appelle pas de commentaire particulier.

67° « valorisation » :

La valorisation des données vise à organiser, gérer les données de manière à ce que celles-ci acquièrent davantage de valeur numérique et puissent être directement assimilées à un véritable actif numérique qui, dans le chef des Autorités publiques, contribuera à l'amélioration de leurs services ou, dans le chef des opérateurs privés, multipliera les opportunités de réutilisation.

68° « partage de données » :

Le Règlement sur la gouvernance des données définit le partage de données comme suit :

« Fourniture de données à un utilisateur de données par une personne concernée ou un détenteur de données, en vue de l'utilisation conjointe ou individuelle desdites données, sur la base d'accords volontaires ou du droit de l'Union ou du droit national, directement ou via un intermédiaire, par exemple dans le cadre de licences ouvertes ou commerciales, moyennant le paiement d'une redevance ou gratuitement ».

Dans le cadre du Code, le terme de partage est l'appellation générique pour désigner le partage administratif et la réutilisation.

69° « partage administratif » :

Le partage administratif vise opérationnellement deux types de procédés, à savoir la mise à disposition ou la transmission de données publiques entre Autorités publiques aux seules fins de l'exercice de leurs missions de service public ou leurs obligations d'intérêt général.

Les données publiques qui peuvent faire l'objet d'un partage administratif peuvent être des données issues de sources authentiques ou non, être des données à caractère personnel ou non, être transmises à intervalle régulier ou non, pour autant qu'il s'agisse d'un flux de données publiques entre deux Autorités publiques.

Le partage ne vise cependant pas les données ouvertes, à savoir des données librement accessibles, pour autant que ces données soient librement accessibles via le portail ouvert des données publiques de la Plateforme bruxelloise de la donnée, pour les opérateurs privés et pour les Autorités publiques sans besoin de passer par le Centre d'intégration.

Le cas des partages entre une Autorité publique et le gestionnaire de la Plateforme bruxelloise de la donnée, à savoir Paradigm pour alimenter le Catalogue des données n'est pas non plus assimilé à un partage administratif au sens du présent Code dans un souci de simplification administrative.

La définition du partage administratif énonce une condition essentielle au partage administratif, à savoir que le partage ne peut avoir comme base légale que les missions de service public ou les obligations d'intérêt général des Autorités publiques parties au partage administratif.

Cette limite quant aux bases légales pouvant justifier le traitement des données (personnelles et non personnelles) implique par conséquent que :

1° dans un premier temps, les Autorités publiques productrices des données ont collecté ces données dans le cadre de leurs missions de service public et leurs obligations d'intérêt général;

2° dans un second temps, les Autorités publiques destinataires des données ne peuvent accéder à ces données que dans le cadre de leurs missions de service public et leurs obligations d'intérêt général.

Par exemple, ne sont pas visées les données qui auraient été traitées par une Autorité publique agissant en dehors de son mandat de service d'intérêt économique général au sens des aides d'État, à savoir en dehors de ses missions de service public.

70° « réutilisation » :

Cette définition transpose l'article 2, 11), de la Directive ISP.

71° « Communication » :

La Communication désigne le flux de données des opérateurs privés vers les Autorités publiques. Il s'agit donc de données d'origine privée qui seront communiquées à une Autorité publique et deviendront de ce fait des données publiques.

72° « traitement » :

Le Règlement sur la gouvernance des données définit le « traitement » comme *« le traitement au sens de l'article 4, point 2), du Règlement (UE) 2016/679 en ce qui concerne les données à caractère personnel ou de l'article 3, point 2), du*

Règlement (UE) 2018/1807 en ce qui concerne les données à caractère non personnel ».

Ces définitions se lisent comme suit :

a) le traitement au sens du RGPD est *« toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »*;

b) Le traitement au sens du Règlement 2018/1807 est *« toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou à des ensembles de données sous forme électronique, telles que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».*

73° « accès » :

Le Règlement sur la gouvernance des données définit l'« accès » comme *« l'utilisation de données conformément à des exigences techniques, juridiques ou organisationnelles particulières, sans que cela implique nécessairement la transmission ou le téléchargement de données ».*

74° « transmission » (dans le cadre d'un partage administratif) :

La transmission organise l'envoi de la donnée chez son destinataire, de sorte que les données sont transférées d'une source à une destinataire spécifique qui pourra les utiliser, et le cas échéant les altérer ou les modifier. Cette notion telle que définie ne s'applique que dans le cadre de partages administratifs, de sorte que le mot « transmettre » ou « transmission » puisse en dehors de ce cas de figure retrouver une signification courante.

75° « mise à disposition » (dans le cadre d'une partage administratif) :

La mise à disposition permet de rendre les données accessibles à d'autres parties intéressées. Lorsqu'une Autorité publique met les données à disposition, elle permet à d'autres entités d'y accéder et de les utiliser, en fournissant un accès approprié. Cette notion telle que définie ne s'applique que dans le cadre de partages administratifs, de sorte que le mot « mettre à disposition » ou « mise à disposition » puisse en dehors de ce cas de figure retrouver une signification courante.

76° « anonymisation » :

Cette définition est reprise de de l'article 2, 7) de la Directive ISP.

77° « occultation » :

L'objectif de l'occultation est de rendre impossible, en pratique, toute identification de secrets commerciaux ou d'affaires et ce de manière irréversible.

78° « intégration des données » :

L'intégration de données implique de rassembler des données provenant de sources multiples et hétérogènes et de les consolider en un seul ensemble de données cohérent et exploitable. La nouvelle base de données ainsi consolidée est alors considérée comme une base nouvelle dépendante de ses sources d'origine. Il est donc nécessaire que l'auteur de l'intégration les mette à jour en fonction des sources utilisées.

79° « archivage » :

La notion d'archivage est ainsi définie en opposition à la notion d'archivage à titre historique qui implique la conservation des documents et des données à des fins historiques, patrimoniales ou socio-culturelles.

80° « base de données » :

La définition est reprise de l'article 1, 2), de la Directive 96/9/CE du Parlement et du Conseil du 11 mars 1996 concernant la protection juridique des bases de données.

81° « autorisation » :

Le Règlement sur la gouvernance des données définit l'« autorisation » comme *« le fait d'accor-*

der aux utilisateurs de données le droit au traitement de données à caractère non personnel ».

82° « interopérabilité » :

Nous attirons l'attention sur le fait que cette définition doit tenir compte de la proposition de Règlement du Parlement Européen et du Conseil établissant des mesures destinées à assurer un niveau élevé d'interopérabilité du secteur public dans l'ensemble de l'Union, COM(2022) 720 final, adoptée le 18 novembre 2022.

En tous les cas, l'interopérabilité peut être définie à plusieurs niveaux : technique, sémantique, organisationnel, légal et ne se limite pas à des mesures techniques.

83° « (réseau et) système d'information » :

Cette définition est reprise de l'article 6, 1), de la Directive SRI 2 (NIS 2), non encore transposée en droit interne.

84° « cas d'usage ou cas d'utilisation » :

La définition de « cas d'usage » dans le code clarifie les contextes spécifiques dans lesquels les données peuvent être utilisées. Cela aide à comprendre les scénarios réels d'utilisation des données, guidant ainsi leur collecte, traitement et analyse de manière plus ciblée et pertinente.

85° « format ouvert » :

Cette définition provient de l'article 2, 14), de la Directive réutilisation.

86° « informatique en nuage (cloud computing) » :

Ces ressources sont attribuées à la demande et parfois en libre-service. La différence entre un hébergement externe partagé classique et un hébergement de type informatique en nuage réside dans le fait que ce dernier se distingue parfois par la mise à disposition de ressources de manière dynamique ou automatique, sans intervention humaine de l'hébergeur.

87° « modèle opérationnel » :

Le modèle opérationnel (ou « operating model » en anglais) n'a pas de définition réglementaire. Néanmoins, on la retrouve dans la doctrine, et notamment dans M. de Vries, A. van der Merwe, P. Kotze, A. Gerber, « A Method for Identifying Process Reuse Opportunities to Enhance the Operating Model », in *IEEE International Conference on Industrial Engineering and Engineering Management*, pp. 1005-1009.

88° « interface de programmation d'application » :

La définition d'une « API (Interface de Programmation d'Application) » provient de l'ordonnance dite « open data » du 10 décembre 2021 modifiant l'ordonnance du 27 octobre 2016 visant à l'établissement d'une politique de données ouvertes et portant transposition de la Directive 2019/1024/UE du Parlement européen et du Conseil du 20 juin 2019 (refonte) concernant les données ouvertes et la réutilisation des informations du secteur public open data du 10 décembre 2021.

89° « intelligence artificielle » :

Cette définition est reprise de l'article 3, 1), de la proposition de Règlement du Parlement européen et du Conseil du 21 avril 2021 établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union (COM(2021) 206 final). Néanmoins, étant donné le statut de cette réglementation, il n'est pas possible d'uniquement renvoyer à cette définition.

90° « licence type » :

Cette définition provient de l'article 2, 5), de la Directive ISP.

91° « format lisible par machine » :

Cette définition provient de l'article 2, 13), de la Directive ISP.

92° « norme formelle ouverte » :

Cette définition provient de l'article 2, 15), de la Directive ISP.

93° « retour sur investissement raisonnable »

Cette définition provient de l'article 2, 16), de la Directive ISP.

94° « tiers de confiance » :

Le tiers de confiance est une entité indépendante qui dispose des moyens techniques nécessaires à l'anonymisation ou la pseudonymisation des données à caractère personnel dans le cadre des traitements énoncés par l'article 89 du RGPD;

Le tiers de confiance est :

1° soumis au secret professionnel au sens de l'article 458 du Code pénal;

2° indépendant du responsable du traitement initial et du traitement ultérieur.

95° « sécurité de l'information » :

Cette définition provient de l'article 1er, 2°, de l'Arrêté Royal du 17 mars 2013 relatif aux conseillers en sécurité institués par la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral.

96° « Intégrateur de services » :

Cette définition est reprise de l'ordonnance du 8 mai 2014 portant création et organisation d'un intégrateur de services régional (article 2, 1°).

97° « intégration de services » :

Cette définition est reprise de l'ordonnance du 8 mai 2014 portant création et organisation d'un intégrateur de services régional (article 2, 2°) et adaptée avec la terminologie du Code.

98° « Intégrateur de services bruxellois » :

Paradigm désigné en cette qualité conformément à l'article C.V.12.

99° « commande publique numérique mutualisable » :

Cette définition est alignée avec la définition de l'ordonnance relative à Paradigm.

100° « sécurité informatique » :

Inclure cette définition dans le code est nécessaire afin d'établir une base commune de ce qui constitue la protection des infrastructures et des données informatiques. Cela permet une application cohérente des règles et des pratiques de sécurité à travers différentes entités et situations visées par le Code.

101° « état de l'art » :

Définir l'état de l'art dans le code aide à fixer un standard de référence souple pour les technologies et pratiques en matière de sécurité informatique. Cela assure que les mesures de sécurité adoptées sont en ligne avec les développements les plus récents et efficaces du domaine en tenant néanmoins compte des moyens à disposition et des données concernées.

102° « donnée d'usage » :

La définition de la donnée d'usage dans le code clarifie le type de données qui peut être collecté sur l'interaction des utilisateurs avec les services numériques. Cela permet de réglementer adéquatement leur collecte, traitement, et utilisation, en assurant une utilisation responsable et respectueuse de la vie privée.

103° « donnée à caractère personnel non confidentielle » :

Cette définition distingue les informations personnelles qui peuvent être publiées en Open data (ex auteur de livres). Elle oriente les politiques et les pratiques concernant la divulgation des données personnelles, assurant un équilibre entre transparence et protection de la vie privée.

La distinction entre donnée à caractère personnel confidentielle et donnée à caractère personnel non confidentielle a été maintenue malgré l'avis du CE qui postulait de manière erronée que cela revenait à modifier la définition de données à caractère personnel pour l'ensemble du Code et de ne pas appliquer la définition consacrée de donnée à caractère personnel du RGPD. Il n'en est rien, la définition de donnée à caractère personnel au sens du RGPD est bien la définition qui s'applique à l'ensemble du Code en vertu de l'article A.I.2. La distinction entre donnée à caractère personnel confidentielle ou non confidentielle ne modifie pas la définition de données à caractère personnel vu qu'une donnée à caractère personnel peut être confidentielle ou non confidentielle selon le régime légal qui s'y applique. Par exemple certaines données à caractère personnel sont publiées dans le cadre d'obligation de publicité active. En effet, certaines données personnelles peuvent, voire doivent, faire l'objet de publication en open data comme les données d'identification des mandataires de société, les mandataires politiques, les auteurs de livres ou autres personnes qui souhaitent être identifiées en tant qu'auteur en application de leur droit (d'auteur) de paternité. L'importance de cette qualification de données à caractère personnelle est donc de les identifier spécifiquement afin de pouvoir justifier d'une limitation de leur traitement, de minimisation et de liceité dans le cadre de la publication en open data.

Du reste la distinction entre donnée à caractère personnel confidentielle ou non confidentielle a

été introduite à la suite de l'avis de l'APD sur le Code.

104° « donnée à caractère personnel confidentielle » :

Définir ce terme dans le code est nécessaire pour distinction avec la précédente.

105° « individualisation » :

L'inclusion de cette définition dans le code souligne la nécessité de protéger l'identité des individus dans le traitement des données. Le but est de prévenir les risques liés à l'identification personnelle à partir de données ce qui recoupe un aspect central de la protection de la vie privée.

106° « corrélation » :

Définir la corrélation dans le code aide à définir et cerner les limites de l'anonymisation puisqu'il est parfois possible d'identifier/réidentifier une personne à partir de la combinaison de différentes données.

107° « inférence » :

La définition de l'inférence dans le code est importante pour sensibiliser aux implications de l'analyse des données, où des informations sensibles peuvent être déduites. Cela aide à définir les meilleures pratiques d'analyse des données pour protéger la vie privée.

108° « traçabilité » :

Cette définition dans le code met en lumière l'importance de pouvoir suivre l'historique et l'utilisation des données. Cela est essentiel pour la gestion transparente des données et pour des audits éventuels.

109° « réversibilité » :

Cette définition dans le code souligne l'importance de la capacité à restaurer les données à un état antérieur, crucial pour la gestion des erreurs et la protection des données.

110° « randomisation » :

En définissant la randomisation, le code guide l'adoption de méthodes d'anonymisation pour protéger la vie privée. Cela aide à empêcher l'identification directe des individus à partir des ensembles de données.

111° « généralisation » :

Cette technique d'anonymisation dans le code vise à permettre de réduire la précision des données pour les rendre moins identifiables, contribuant à la protection de la confidentialité et ce en fonction des utilisations qui peuvent être faites.

112° « attributs de données » :

Cette expression fournit des éclaircissement sur la nature et le rôle des différentes informations dans un ensemble de données. Cela est fondamental pour structurer et analyser les données de manière appropriée.

113° « Urbis » :

Cette définition a été reprise de l'actuelle ordonnance 8 mai 2014 portant création et organisation d'un intégrateur de services régional.

PARTIE B
GOUVERNANCE ADMINISTRATIVE

LIVRE B.I.
Publicité administrative

TITRE 1
Dispositions générales

Article B.I.1.
Dispositions générales

Cet article reprend en intégralité l'article 2 du décret et ordonnance conjoints de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française relatifs à la publicité de l'administration dans les institutions bruxelloises du 16 mai 2019 (ci-après « décret et ordonnance conjoints du 16 mai 2019 »).

En plus l'article tient compte en son alinéa 3 de l'aspect technologique du contexte dans lequel le présent livre s'intègre, à savoir l'établissement d'un texte codifié sur la donnée et la gouvernance.

Article B.I.2.
Champ d'application ratione personae

Cet article reprend selon le dispositif du Code intégré à la partie A le champ d'application ratione

personae visé à l'article 3 du décret et ordonnance conjoints du 16 mai 2019 :

« Article 3. – Le présent décret et ordonnance conjoints s'applique :

1° aux autorités administratives dépendant de la Région de Bruxelles-Capitale, dénommées ci-après « autorités administratives régionales ». Pour l'application du présent décret et ordonnance conjoints, les organes consultatifs régionaux en matière d'environnement ou d'aménagement du territoire sont assimilés à des autorités administratives régionales;

2° aux autorités administratives qui exercent les compétences dévolues à l'Agglomération bruxelloise.

Pour l'application du présent décret et ordonnance conjoints, ces autorités administratives sont assimilées à des « autorités administratives régionales »;

3° à toute personne physique ou morale :

a) qui exerce des fonctions administratives publiques, y compris des tâches, activités ou services spécifiques en rapport avec l'environnement ou l'aménagement du territoire;

b) ayant des responsabilités ou des fonctions publiques, ou fournissant des services publics, en rapport avec l'environnement ou l'aménagement du territoire sous le contrôle d'un organe ou d'une personne visée au point 1° ou 3°, a)

Pour l'application du présent décret et ordonnance conjoints, ces personnes physiques ou morales sont assimilées à des « autorités administratives régionales »;

4° aux autorités administratives communales, en ce compris les organes consultatifs communaux en matière d'environnement ou d'aménagement du territoire;

5° aux intercommunales régionales et interrégionales soumises à la tutelle administrative de la Région de Bruxelles-Capitale ainsi qu'à leurs filiales, aux ASBL communales et pluricommunales et aux régies communales autonomes, visées par l'ordonnance du 5 juillet 2018 relative aux modes spécifiques de gestion communale et à la coopération intercommunale.

Pour l'application du présent décret et ordonnance conjoints, les intercommunales et leurs filiales, les ASBL communales et pluricommunales, et les régies communales autonomes sont assimilées aux « autorités administratives communales »;

6° aux autorités administratives dépendant de la Commission communautaire commune;

7° aux centres publics d'action sociale;

8° aux associations visées au Chapitre XII et XIIbis de la loi du 8 juillet 1976, organique des centres publics d'action sociale;

9° aux autorités administratives dépendant de la Commission communautaire française.

Le présent décret et ordonnance conjoints s'applique également aux autorités administratives autres que celles visées à l'alinéa 1er, mais seulement dans la mesure où elle prohibe ou restreint la publicité de documents administratifs pour des motifs relevant de la compétence de la Commission communautaire commune, de la Région de Bruxelles-Capitale et de la Commission communautaire française. ».

Ce champ d'application transpose notamment la définition imposée par la directive 2003/4/CE du Parlement européen et du Conseil du 28 janvier 2003 concernant l'accès du public à l'information en matière d'environnement et abrogeant la directive 90/313/CEE du Conseil :

« 2) « autorité publique » :

a) le gouvernement ou toute autre administration publique, y compris les organes consultatifs publics, au niveau national, régional ou local;

b) toute personne physique ou morale qui exerce, en vertu du droit interne, des fonctions administratives publiques, y compris des tâches, activités ou services spécifiques en rapport avec l'environnement, et

c) toute personne physique ou morale ayant des responsabilités ou des fonctions publiques, ou fournissant des services publics, en rapport avec l'environnement, sous le contrôle d'un organe ou d'une personne visé(e) au point a) ou b).

Les États membres peuvent prévoir que la présente définition n'inclut pas les organes ou institutions agissant dans l'exercice de pouvoirs judiciaires ou législatifs. Les États membres peuvent exclure ces organes ou institutions si, à la date d'adoption de la présente directive, leurs dispositions constitutionnelles ne prévoient pas de procédure de recours au sens de l'article 6; ».

Les considérants de la directive mentionnent que :

« (11) Afin de tenir compte du principe énoncé à l'article 6 du traité, selon lequel les exigences de la

protection de l'environnement doivent être intégrées dans la définition et la mise en œuvre des politiques et actions de la Communauté, il convient d'étendre la définition des autorités publiques de manière à englober le gouvernement et les autres administrations publiques aux niveaux national, régional et local, qu'elles aient ou non des responsabilités particulières en matière d'environnement, et d'autres personnes ou organismes assurant des services d'administration publique en rapport avec l'environnement en vertu de la législation nationale, ainsi que les autres personnes ou organismes agissant sous leurs ordres et ayant des responsabilités ou des fonctions publiques en rapport avec l'environnement.

(12) Il convient que les informations environnementales détenues matériellement pour le compte d'autorités publiques par d'autres organismes entrent aussi dans le champ d'application de la présente directive. ».

Le décret et ordonnance conjoints du 16 mai 2019 utilise la notion d'« Autorité administrative » qui est une notion de droit public renvoyant directement à la compétence du Conseil d'État à l'égard des Autorités administratives visées à l'article 14 des lois coordonnées sur le Conseil d'État (LCCE). Mais le décret et ordonnance conjoints du 16 mai 2019 vise avec cette expression, des Autorités administratives au sens de l'article 14 LCCE et toute autre personne physique ou morale qui ne seraient pas *a priori* des Autorités administratives au sens de l'article 14 LCCE. Cette ambiguïté a été supprimée et le terme « Autorité publique » a été préféré pour l'ensemble des Autorités soumises au présent livre. L'expression « Autorité publique » est du reste également celle consacrée par la directive en matière d'information environnementale.

Les autorités visées par le champ d'application du présent livre ont été dénommées Autorités publiques. Toutefois, il s'agit de souligner la différence de signification entre les Autorités publiques au sens de la partie C du Code et les Autorités publiques au sens du présent livre (voir livre C.I)

Les deux définitions ne sont pas identiques dans la mesure où la définition retenue pour les Autorités publiques au sens du présent livre est volontairement très explicite et détaillée quant aux Autorités visées, afin, d'une part, de permettre à tout un chacun de visualiser plus facilement les personnes morales de droit public visées par les obligations de publicité administrative, et, d'autre part, également comprendre les éléments de transpositions provenant de la directive 2003/4/CE du Parlement européen et du Conseil du 28 janvier 2003 concernant l'accès du public à l'information en matière d'environnement et abrogeant la directive 90/313/CEE du Conseil.

Article B.I.3.
Calcul des délais

Cet article reprend l'article 5 du décret et ordonnance conjoints du 16 mai 2019.

TITRE 2
Publicité active

CHAPITRE 1
Dispositions générales

Article B.I.4.
Publications sur les sites internet de chaque Autorité publique

Cet article reprend l'article 6 du décret et ordonnance conjoints du 16 mai 2019.

Conformément au livre C.V, l'ensemble de ces informations vont être reprises dans le Catalogue des données au sein de la Plateforme bruxelloise de la donnée avec un lien vers les mises à disposition de données prévues dans le cadre du Portail ouvert des données publiques.

Ceci est explicitement visé pour ce qui concerne les données des inventaires visés à l'alinéa 2, 2° à 4°. Il est également prévu qu'un arrêté organise que les données relatives aux subsides et aux marchés publics soient traitées visuellement et graphiquement pour une meilleure accessibilité et compréhension de ces données

Certaines modifications ont été introduites au niveau des obligations de publication active imposées aux Autorités publiques.

Ainsi, l'inventaire des études réalisées pour le compte des Autorités publiques comprend également le titre de ces études. Il est également organisé que le contenu de ces études soit également publié dans une démarche d'information citoyenne pour autant que :

– (i) ces études présentent un intérêt économique, social, sanitaire ou environnemental. Cette condition réserve un pouvoir d'appréciation dans le chef des Autorités publiques, qui disposent d'une certaine marge de manœuvre afin de définir ce qui est susceptible de présenter un tel intérêt économique, social, sanitaire ou environnemental. Ce pouvoir d'appréciation est toutefois soumis au contrôle de la CADADo, auprès de laquelle un recours peut être adressé en cas de violation des obligations de publicité active imposées aux Autorités publiques, comme organisé dans le cadre du livre B.II. Saisie de pareil recours, la CADADo pourra le cas

échéant censurer toute erreur manifeste d'appréciation dans le chef de l'Autorité publique qui aurait considéré de manière manifestement déraisonnable que ces études n'étaient pas susceptibles de présenter un intérêt suffisant;

– (ii) le contenu de ces études ne pourra être publié que pour autant que les conditions d'accès visées à l'article B.I.17 sont rencontrées. Par dérogation au paragraphe 1er, alinéa 2, 3°, le titre de l'étude pourra le cas échéant être omis de l'inventaire s'il s'avère que toute publicité à cet égard pourrait être préjudiciable. L'on pense par exemple aux études examinant des questions précises de sécurité publique pour lesquelles la publicité du titre pourrait déjà être problématique. Bien entendu un accès partiel aux études visées reste possible.

Conformément à l'avis de l'APD, l'article B.I.4 est complété afin de :

– mentionner les finalités des traitements que constitue la publication des données à caractère personnel contenues dans les documents ou directement visées par les obligations de publicité active à charge des Autorités publiques;

– de mentionner le temps de publication de ces données. Ce temps est de un an pour ce qui concerne les études et les inventaires des subventions vu que le budget est voté annuellement. Le temps de publication est d'une législature pour ce qui concerne les données à caractère personnel publiées dans le cadre de fonctions ou de mandats politiques (§ 2, alinéas 2 et 3). Le temps de publication est de soixante jours pour les décisions en matière de fonction publique afin de permettre aux agents qui le souhaitent d'introduire un recours contre ces décisions devant le Conseil d'État;

– le droit d'opposition des personnes concernées, conformément à l'article 21 du RGPD dès lors que ces données sont publiées dans le cadre la missions de service public de publicité active imposée par l'article B.I.4.

La publication des données à caractère personnel dans le cadre de la rubrique transparence apparaît le moyen le plus efficace d'assurer l'information adéquate de tout un chacun au regard des finalités poursuivies. La limitation des durées de publication des données à caractère personnel, relativement courtes, assure le caractère proportionné du traitement.

À la suite de l'avis du Conseil d'État, des modifications ont également été introduites au niveau du § 3, 2°. Une exception a été introduite pour ce qui concerne la publication des décisions des exécutifs de portée individuelle afin de préserver la vie privée des personnes physiques visées et dans un souci de cohérence par rapport à l'article B.I.15, § 3. De même, le respect des condition d'accès aux documents administratifs et information environnementale imposée dans le cadre des demandes de publicité passive est également ajouté de manière à ce que ne soient pas publiées des notes et des annexes pouvant compromettre, par exemple, la sécurité publique ou encore le secret des délibérations des pouvoirs publics, ou toute autre obligation de secret telle que visée par l'article B.I.17.

Article B.I.5.
Désignation de la personne en charge de la publicité active

Cet article reprend l'article 7 du décret et ordonnance conjoints du 16 mai 2019.

Article B.I.6.
Indication de la personne disposant de l'information et des modes de saisine du médiateur bruxellois

Cet article reprend l'article 8 du décret et ordonnance conjoints du 16 mai 2019.

Article B.I.7.
La disponibilité des informations publiées

Cet article reprend l'article 9 du décret et ordonnance conjoints du 16 mai 2019.

CHAPITRE 2
Dispositions spécifiques aux informations relatives à l'environnement et l'aménagement du territoire

Article B.I.8.
Publications actives spécifiques à Bruxelles Environnement

Cet article reprend l'article 10 du décret et ordonnance conjoints du 16 mai 2019.

Article B.I.9.
Publication active d'informations environnementales

Cet article reprend l'article 11 du décret et ordonnance conjoints du 16 mai 2019.

Article B.I.10.
Publication active des permis d'urbanisme et de lotir ainsi que des rapports et études jointes

Cet article reprend l'article 12 du décret et ordonnance conjoints du 16 mai 2019.

Article B.I.11.
Publication active des mesures de protection du patrimoine immobilier

Cet article reprend l'article 13 du décret et ordonnance conjoints du 16 mai 2019.

Article B.I.12.
Publication active des permis d'environnement

Cet article reprend l'article 14 du décret et ordonnance conjoints du 16 mai 2019.

Article B.I.13.
Publication active en cas de menace imminente

Cet article reprend l'article 15 du décret et ordonnance conjoints du 16 mai 2019.

Article B.I.14.
Rapport sur l'état de l'environnement bruxellois

Cet article reprend l'article 16 du décret et ordonnance conjoints du 16 mai 2019.

TITRE 3
Publicité passive

Article B.I.15.
Principes

Cet article reprend l'article 17 du décret et ordonnance conjoints du 16 mai 2019.

Dans son avis, l'APD souhaite que les demandeurs de documents administratifs justifient d'un intérêt à disposer de données à caractère personnel dans le cadre des documents administratifs dont l'accès est demandé.

Le législateur rappelle que le livre B.I du Code implémente le droit d'accès aux documents administratifs garanti à l'article 32 de la Constitution :

« Chacun a le droit de consulter chaque document administratif et de s'en faire remettre copie, sauf dans les cas et conditions fixés par la loi, le décret ou la règle visée à l'article 134. ».

Précisément, l'article B.I.17 fixe les conditions dans lesquelles les demandes peuvent être rejetées, notamment :

« § 2. – L'autorité publique rejette la demande de consultation, d'explication ou de communication sous forme de copie d'un document administratif, si elle constate que l'intérêt de la publicité ne l'emporte pas sur la protection de l'un des intérêts suivants :

1° les libertés et les droits fondamentaux des administrés, en ce compris la vie privée;

(…)

Le présent paragraphe n'est pas applicable aux informations environnementales.

§ 3. – L'autorité publique rejette la demande de consultation, d'explication ou de communication sous forme de copie d'une information environnementale si elle constate que l'intérêt du public servi par la publicité ne l'emporte pas sur la protection de l'un des intérêts suivants :

(…)

5° la confidentialité des données à caractère personnel et des dossiers concernant une personne physique si cette personne n'a pas consenti à la divulgation de ces informations au public, lorsque la confidentialité de ce type d'information est prévue par le droit régional ou européen;

(…)

L'autorité publique ne peut, en vertu des points 1°, 4°, 5°, 6°, 7°, rejeter une demande lorsqu'elle concerne des informations relatives à des émissions dans l'environnement. ».

Par conséquent, pour qu'un demandeur puisse avoir accès à un document administratif ou une information environnementale comprenant des données à caractère personnel : la personne concernée doit avoir consenti à la divulgation ou une obligation de publication de ces données à caractère personnel doit exister. Les règles en matière d'accès aux documents administratifs et à l'information environnementale comprennent donc des exceptions afin de protéger la vie privée des personnes concernées. Dans ces hypothèses, comme l'impose le paragraphe 5 de l'article B.I.17, les données à caractère personnel seront anonymisées et le document sera transmis avec un accès partiel à l'information qu'il contient.

La seule hypothèse où l'exception en matière de protection des données à caractère personnel ne pourra pas être invoquée est lorsque la demande d'information portera sur des émissions environnementales, lesquelles ne supposent *a priori* pas, dans la grande majorité des cas, la communication de données à caractère personnel. Cependant, la Conseil d'État a rappelé, après analyse de la directive européenne en matière d'information environnementale, telle que transposée dans le présent livre, que :

« 28.3. Au regard de l'article 4, paragraphe 2, alinéa 3, de la directive 2003/4/CE, il va de soi que, si, ainsi que le prévoit l'article 4, paragraphe 2, alinéa 2, 3e phrase, de la directive 2003/4/CE, la demande ne peut pas être rejetée pour le motif prévu au paragraphe 3, alinéa 1er, 5°, de l'article B.I.18 du Code en projet (« la confidentialité des données à caractère personnel et des dossiers concernant une personne physique si cette personne n'a pas consenti à la divulgation de ces informations au public, lorsque la confidentialité de ce type d'information est prévue par le droit régional ou européen »), les autorités concernées doivent néanmoins veiller, dans l'hypothèse où les informations environnementales concernant des émissions dans l'environnement comporteraient des données à caractère personnel, au respect des exigences du RGPD, et dès lors vérifier concrètement si la communication des données à caractère personnel est indispensable à l'intérêt protégé par la communication des informations relatives aux émissions dans l'environnement. ».

Au surplus, il va de soi bien entendu que lorsque les données à caractère personnel concernent le demandeur, les exceptions ne sont pas applicables vu l'absence de violation de la vie privée du demandeur.

L'Autorité publique se limitera de constater qu'elle ne dispose pas du consentement des personnes concernées pour la communication de leurs données dans le cadre d'une demande d'accès en matière de publicité administrative et d'information environnementale, dans la mesure où l'Autorité publique n'aura pas collecté le consentement des personnes concernées, sauf dans certaines situations particulières où d'autres législations lui imposent de demander le consentement (par exemple en cas d'accès à des plan d'architecte soumis à des droits d'auteur, comme l'impose la législation fédérale).

Par ailleurs, la directive 2000/3/4 du Parlement européen et du Conseil du 28 janvier 2003 concernant l'accès du public à l'information en matière d'environnement et abrogeant la directive 90/310/ CEE du Conseil, précise que :

« Article 3. – Accès sur demande aux informations environnementales

1. Les États membres veillent à ce que les autorités publiques soient tenues, conformément à la présente directive, de mettre à la disposition de tout demandeur, et sans que celui-ci soit obligé de faire valoir un intérêt, les informations environnementales qu'elles détiennent ou qui sont détenues pour leur compte ».

La législation bruxelloise a, du reste, pu estimer utile d'organiser la démonstration d'un intérêt pour ce qui concerne uniquement les documents dans lesquels sont repris une appréciation ou un jugement de valeur relatif à une personne identifiée ou identifiable ou lorsqu'elle se rapporte à un comportement de cette personne dont la divulgation peut manifestement lui causer préjudice, conformément à la liberté que lui laisse l'article 86 du RGPD.

Il s'agit également de rappeler que la demande d'un document administratif ou d'une information environnementale ne sera le plus souvent pas soumise au RGPD dans la mesure où il agira dans le cadre d'une activité domestique.

En réponse, au commentaires 30 de l'avis de l'APD, il est rappelé que la balance des intérêts à réaliser dans le cadre de l'application des §§ 2 et 3 de l'article B.I.17 ne vise pas l'intérêt spécifique du demandeur du document administratif ou de l'information environnementale, comme l'indique l'APD mais vise ce que l'article identifie explicitement comme l'intérêt de la publicité en général, et de manière particulière pour le demandeur, et les autres intérêts listés par la législation justifiant des exceptions à la publicité administrative. Une balance des intérêts doit être réalisée par l'Autorité publique afin de vérifier si l'atteinte à la publicité n'est pas démesurée par rapport à l'intérêt à protéger. En effet, en droit public de la publicité administrative, il convient de rappeler que la publicité est la règle et que le refus d'accès est l'exception. La mise en balance des intérêts est un procédé classique en matière d'examen des libertés publiques et de droits fondamentaux, que chaque Autorité publique applique et motive dans le cadre des décisions qu'elle adopte.

Article B.I.16.
Demande d'accès au document administratif ou à une information environnementale

Cet article reprend l'article 18 du décret et ordonnance conjoints du 16 mai 2019.

Vu les motifs de refus d'accès aux données à caractère personnel contenues dans des documents administratifs ou des informations environnementales formulées dans le cadre de l'article B.I.17, l'accès aux données à caractère personnel est très limité en matière de publicité administrative. Cet accès est logiquement encore plus restrictif plus lorsqu'il s'agit de données sensibles au sens de l'article 9 RGPD vu que l'intérêt de la protection de la vie privée devrait le plus souvent l'emporter dans ces hypothèse avec encore plus d'acuité sur l'intérêt de la publicité.

Les documents administratifs ou les informations environnementales étant communiquées dans le cadre d'une demande formulée sur pied de la législation en matière de publicité administrative n'appellent pas de mesures de sécurité particulière, vu que, si l'information est communiquée, c'est que aucun des motifs de refus de communication n'a trouvé à s'appliquer à l'espèce. Par conséquent, il semble inutile de suivre l'avis de l'APD souhaitant laisser les Autorités publiques libres de décider du mode de communication selon le cas d'espèce dans la mesure où doit être privilégiée l'accessibilité de chacun aux documents administratifs et à l'information environnementale. Un mode de communication simple, tels les courriels, reste à privilégier.

Article B.I.17.
Rejet des demandes

Cet article reprend l'article 19 du décret et ordonnance conjoints du 16 mai 2019.

Un paragraphe 4 est ajouté suite à l'avais de l'APD concernant les consentements visés aux paragraphes 2 et 3.

À la suite de l'avis du Conseil d'État rappelant en ses points 25.1 à 25.3 que les obligations de publicité active pouvaient être limitées également par les condition d'accès en matière de publicité passive, l'article B.I.4 a été modifié mais un paragraphe 6 a également été ajouté à l'article B.I.17 afin de rappeler que chaque entité fédérale et fédérée est compétente pour définir les exceptions à la publicité administrative relevant de ses propres compétences matérielles (comme, par exemple, la défense nationale ou les relations diplomatiques pour ce qui concerne l'État fédéral).

Article B.I.18.
Délais

Cet article reprend l'article 20 du décret et ordonnance conjoints du 16 mai 2019.

Article B.I.19.
Notification de la décision

Cet article reprend l'article 21 du décret et ordonnance conjoints du 16 mai 2019.

TITRE 4
Correction d'informations inexactes ou incomplètes

Article B.I.20.
Principe

Cet article reprend l'article 22 du décret et ordonnance conjoints du 16 mai 2019.

Article B.I.21.
Demande de rectification

Cet article reprend l'article 23 du décret et ordonnance conjoints du 16 mai 2019.

Article B.I.22.
Renvoi vers l'Autorité publique compétente

Cet article reprend l'article 24 du décret et ordonnance conjoints du 16 mai 2019.

TITRE 5
Dispositions finales

Article B.I.23.
Obligations de publicité plus étendues

Cet article reprend l'article 37 du décret et ordonnance conjoints du 16 mai 2019.

1. Le considérant 24 de la directive en matière d'information environnementale transposée dans le livre B.I. prévoit que :

2. *« (24) Les dispositions de la présente directive ne devraient pas porter atteinte au droit d'un État membre de continuer à appliquer ou d'introduire des mesures permettant un accès plus large à l'information que ne le prescrit la présente directive, ».*

L'article B.I.24 du Code organise bien que le régime de publicité prévu par le livre B.I. qu'il met en place n'est qu'un minimum et qu'une publicité plus large est donc possible.

Contrairement à ce que soutient le Conseil d'État dans son avis, le législateur est d'avis qu'il ne se déduit pas que les dispositions qui prévoiraient un

régime de publicité moins large seraient supposées être abrogées. En effet, l'article B.I.17, § 5 fixe que :

« L'Autorité publique rejette la demande de consultation, d'explication ou de communication sous forme de copie d'un document administratif si la publicité porte atteinte à une obligation de secret instaurée par une ordonnance de la Région de Bruxelles-Capitale, une ordonnance de la Commission communautaire commune ou un décret de la Commission communautaire française ».

Par conséquent, si le refus d'accès à un document administratif ou à une information environnementale était justifiée par pareille obligation de secret, il s'agirait d'en déduit que ce régime plus restrictif de publicité serait tout à fait compatible avec les dispositions du livre B.I.

Article B.I.24.
Qualité des informations environnementales

Cet article reprend l'article 38 du décret et ordonnance conjoints du 16 mai 2019.

LIVRE B.II.
La Commission d'accès aux documents administratifs et aux données (CADADo)

TITRE 1
Dispositions générales

Ce livre institue et organise un organe de recours succédant aux droits et aux obligations de la précédente Commission d'accès aux documents administratifs de la Région de Bruxelles-Capitale (CADA). Le livre B.II du présent code en fait l'organe de recours des décisions prises par les Autorités Publiques en cas non seulement, comme auparavant, de demandes d'accès aux documents administratifs mais également de demande de partage administratif et de réutilisation des données et documents. Un nouveau nom a dès lors été donné à la CADA qui devient la Commission d'accès aux documents administratifs et aux données.

La CADADo est compétente à l'égard des décisions prises par les Autorités publiques visés à l'article A.I.3.1) du présent code.

Afin de permettre à la Commission de faire face à l'extension de ses compétences notamment en matière de partage administratif, une réorganisation profonde de la Commission a été imaginée au départ principalement du décret et ordonnance conjoints de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française relatifs à la publicité de l'administration dans les institutions bruxelloise du 16 mai 2019 ainsi que de l'actuel règlement d'ordre intérieur de la CADA, ci-après « le décret et ordonnance conjoints du 16 mai 2019 ».

Ainsi, par exemple le présent livre crée des chambres distinctes selon l'objet du recours, augmente le nombre des membres et organise la fonction de la CADADo en tant que gardienne de la légalité des flux de données au sein de la Région de Bruxelles-Capitale.

Article B.II.1.
Transposition partielle

Cette disposition ne nécessite pas de commentaire particulier.

Article B.II.2.
Calcul des délais

Cet article retranscrit l'article 5 du décret et ordonnance conjoints du 16 mai 2019.

TITRE 2
Composition et organisation de la Commission

Article B.II.3.
Compétences de la Commission et indépendance

Cet article reprend l'article 25 du décret et ordonnance conjoints du 16 mai 2019. Les compétences actuelles de la CADA sont conservées.

Concernant la compétence d'avis de la Commission, le Conseil d'État renvoie au rapport annuel 2023 de la Commission d'accès aux documents administratifs bruxelloise, p. 4 :

« Dans un de ses avis (AI. 22.23 du 6 mars 2023 [lequel se réfère à l'avis interprétatif n° 16.22 du 29 novembre 2022 lequel se réfère aux AI 8.21 du 1er avril 2021, 11.21 du 21 mai 2021 et 13.21 du 16 septembre 2021]), la Commission a réitéré le principe important selon lequel il n'est pas de sa compétence d'émettre un avis à l'intention d'une autorité administrative sur une demande d'accès (individuelle) qui est examinée parallèlement par cette autorité. L'émission d'un avis dans un tel contexte constituerait une entorse aux garanties établies par le législateur bruxellois pour mettre en œuvre l'article 32 de la Constitution. En effet, l'intention ne peut être que la Commission émette un avis dans le cadre d'une demande d'accès individuelle qui pourrait par la suite

être contestée devant la Commission par le biais d'un recours ».

Sont également reprises les compétences visées à l'article 7 de l'ordonnance du 27 octobre 2016 visant à l'établissement d'une politique de données ouvertes (Open Data) et portant transposition de la Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, à savoir :

« Article 7. § 1er. – Dans le cadre de la réutilisation des documents, la Commission d'accès aux documents administratifs visée au Chapitre 5 du décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française relatifs à la publicité de l'administration dans les institutions bruxelloises est compétente pour connaître des recours à l'encontre d'une décision de mise à disposition des documents, en cas de refus d'exécuter une décision, ou en raison de toute autre difficulté qui est rencontrée dans l'exercice des droits que confère la présente ordonnance.

§ 2. – La Commission exerce cette compétence en toute impartialité et neutralité. Lors du traitement des recours, elle ne peut recevoir aucune instruction. ».

Est ajoutée comme nouvelle compétence, celle de contrôler les partages administratifs décrits dans le livre C.IV., titre 2.

L'objectif du présent livre est de réformer la CADA actuelle afin qu'elle puisse intégrer parfaitement les compétences qui lui avaient été confiées en dehors de son cadre organique et les nouvelles compétences en matière de partage administratif.

Le caractère indépendant de la nouvelle CADADo est confirmé vu son caractère essentiel afin que la CADADo, en tant qu'autorité administrative, puisse exercer ses compétences en toute impartialité.

Article B.II.4.
Composition générale

Cette disposition instaure désormais la répartition des compétences de la CADADo en trois chambres distinctes. Chaque chambre sera spécialisée dans un type de recours dont connaît la CADADo : accès aux documents administratifs et informations environnementales, partages administratifs de données, réutilisation de données et de documents.

La division en chambres permet de favoriser l'engagement de profils spécialisés dans chacune des catégories de recours, ce qui est de nature à favoriser l'attrait de ces fonctions pour les futurs candidats.

Comme auparavant, il est désigné un Président magistrat auprès du Conseil d'État ou émanant du monde judiciaire. La possibilité de désigner comme président également un membre de la Cour constitutionnelle a été introduite, sous réserve de l'application de l'article 44 de la loi spéciale du 6 janvier 1989 sur la cour constitutionnelle :

« Article 44. – Les fonctions de juge, de référendaire et de greffier, sont incompatibles avec les fonctions judiciaires, avec l'exercice d'un mandat public conféré par élection, avec toute fonction ou charge publique d'ordre politique ou administratif, avec les charges de notaire et d'huissier de justice, avec la profession d'avocat, avec l'état de militaire et avec la fonction de ministre d'un culte reconnu.

Il peut être dérogé par le Roi, sur avis favorable et motivé de la Cour, à l'alinéa 1er :

1° lorsqu'il s'agit de l'exercice de fonctions de professeur, chargé de cours, maître de conférence ou assistant dans les établissements d'enseignement supérieur, pour autant que ces fonctions ne s'exercent pas pendant plus de cinq heures par semaine ni en plus de deux demi-jours par semaine;

2° lorsqu'il s'agit de l'exercice de fonctions de membre d'un jury d'examen;

3° lorsqu'il s'agit de la participation à une commission, à un conseil ou comité consultatif, pour autant que le nombre de charges ou fonctions rémunérées soit limité à deux et que l'ensemble de leurs rémunérations ne soit pas supérieur au dixième du traitement brut annuel de la fonction principale à la Cour.

Le nombre de membres permanents de la Commission, dont fait partie le Président, augmente de 9 à 13 afin de pourvoir également les nouvelles chambres créées en matière de partage administratif et de réutilisation.

Toutefois, afin d'éviter toute situation de manque de candidats aux mandats de membres de la CADADo, la possibilité est introduite que la Commission soit composée de moins de treize membres si certains membres siègent dans plusieurs chambres et par conséquent occupent deux mandats, comme organisé au niveau de l'article B.II.5, § 4.

Il est également essentiel que la CADADo soit dotée d'un secrétariat propre et permanent afin de

seconder efficacement les membres et son Président dans leurs missions diverses. Le secrétariat est considéré comme un service faisant partie intégrante de la Commission. Les membres statutaires qui exercent la fonction de secrétaire agissent dans le cadre organique de la Commission. ».

Article B.II.5.
Composition des chambres

La composition de la chambre relative à l'accès aux documents administratifs et à l'information environnementale est la plus conséquente : le Président et 8 membres permanents ce qui est identique au nombre de membres actuels de la CADA.

Le secrétariat est commun à l'ensemble des trois chambres mais les secrétaires qui siègent dans chacune des chambres ne sont pas membres délibérants de celles-ci.

La chambre relative au partage administratif et à la réutilisation sont toutes deux composées de trois membres : le Président ainsi que deux membres.

Il est évidemment essentiel que les membres de la Commission présentent des compétences dans les matières liées aux recours spécifiques à chaque chambre. C'est ce que vise le contenu de la présente disposition.

Comme exposé au niveau de l'article B.II.4, les membres de la Commission peuvent le cas échéant siéger dans deux chambres de la Commission et donc bénéficier de deux mandats, au terme de deux désignations différentes par deux arrêtés conjoints conformément à l'article B.II.7, § 1er. Il va de soi que les membres cumulant deux mandats doivent remplir les conditions propres à chacun de leur mandat, à savoir les conditions visées aux paragraphes 1er, 2, ou 3 de l'article B.II.5 selon le mandat qu'ils visent.

Les paragraphes 7 et 8 ne nécessitent pas de commentaire particulier et reprennent, en le modifiant quant au ratio minimum, le contenu actuel de l'article 25, § 3 de l'ordonnance du 16 mai 2019.

Article B.II.6.
Experts

La possibilité de faire appel à des experts en raison de leur expertise spécifique est une nouveauté dans l'organisation de la Commission.

Les experts ne sont pas considérés comme membres de la CADADo. Ils sont désignés pour des dossiers spécifiques et n'ont pas de voix délibérative. Leur mission est de remettre des avis circonstanciés sur les questions soumises à la CADADo.

Les experts sont désignés, par arrêté conjoint pour un mandat de 5 ans renouvelable une fois. Les experts désignés constituent une sorte de réserve dans laquelle le Président peut venir piocher pour attribuer une mission spécifique à un expert.

Article B.II.7.
Mandats des membres

Le mode de désignation est identique à celui choisi pour la CADA actuelle (cfr. L'article 26, § 1er, de l'ordonnance du 16 mai 2019).

De l'indépendance des experts découle l'indépendance de la CADADo elle-même.

En ce sens, un régime de fin de mandat est instauré de même qu'un rappel de l'interdit d'intérêt personnel dans le cadre de toute délibération.

Dans un souci de sécurité juridique, le Conseil d'État souhaitait que les devoirs des membres de la Commission soient définis. Ces devoirs sont en partie définis par le présent livre B.II. Il apparaît au surplus plus opportun de laisser à la Commission le soin de préciser les devoirs de son Président et de ses membres.

Article B.II. 8.
Rémunération

Le choix de la fixation de la rémunération des membres de la CADADo par jeton se justifie par le fait que ses membres ne travaillent pas à temps plein pour la Commission et que l'expérience de l'ancienne CADA démontre qu'il est difficile d'attirer de bons profils et des compétences pointues sur la base d'une rémunération fixe peu élevée.

Les membres seront dès lors désormais rémunérés par dossier traité, ce qui devrait aussi récompenser les membres désireux de particulièrement s'investir. Le terme « dossier traité » vise soit la demande d'avis soit le recours introduit auprès de la Commission.

Article B.II.9.
Fonctionnement

Suite à la crise sanitaire, à l'évolution technologique au sein de la société et afin de permettre le plus de souplesse possible dans l'organisation des réunions, ces dernières peuvent se dérouler tant en distanciel qu'en présentiel.

TITRE 3
Les demandes d'avis

Article B.II.10.
Modalités des demandes d'avis

Cette disposition ne nécessite pas de commentaire particulier.

Article B.II.11.
Information des membres

Cette disposition ne nécessite pas de commentaire particulier.

Article B.II.12.
Délibération de la Commission

Un nombre minimum est requis afin de permettre la délibération des demandes d'avis. Ce choix permet de rendre des avis de la manière la plus objective, transparente et impartiale.

Article B.II.13.
Délai dans lequel la Commission statue

L'article B.II.13 instaure un délai de 60 jours, à compter de la réception de la demande d'avis, endéans lequel la Commission doit rendre son avis. L'objectif de cette disposition est de donner un cadre temporel à la procédure d'avis et de donner plus de prévisibilité aux demandeurs d'avis. Le délai de 60 jours est le même que celui dans lequel la Commission doit statuer pour les recours.

Article B.II.14.
Secrétariat

Cette disposition ne nécessite pas de commentaire particulier.

Article B.II.15.
Publication de l'avis

La Commission publie sur son site internet visés à l'article B.II.26, dans les 20 jours ouvrables de leur adoption, les avis qu'elle adopte.

Sauf consentement préalable de la personne concernée par les données à caractère personnel contenues dans un avis de la Commission, la Commission opère une anonymisation des avis avant leur publication. Elle omet également toute information qu'elle jugera confidentielle.

Le texte a été modifié afin de permettre le cas échéant à la CADADO de limiter la publication des données à caractère personnel également le cas échéant contenues dans ses avis et non uniquement ses décisions.

TITRE 4
Les recours

Article B.II.16.
Délai pour introduire un recours

Les paragraphes 1er et 2 de cet article reprennent l'article 27, § 1er, alinéa 1er, du décret et ordonnance conjoints du 16 mai 2019.

Le paragraphe 3 reprend l'article 27, § 1er, alinéa 2, du décret et ordonnance conjoints du 16 mai 2019.

Le paragraphe 4 reprend l'article 27, § 1er, alinéa 3, du décret et ordonnance conjoints du 16 mai 2019 tout en prévoyant qu'un nouveau délai peut commencer à courir également à l'expiration d'un délai de 4 mois à compter de l'introduction de la réclamation devant le médiateur, si la notification n'est pas intervenue plus tôt.

Article B.II.17.
Modalités d'introduction du recours

Cet article précise les modalités d'introduction des recours devant la CADA. La date certaine de l'envoi et de sa délivrance est importante pour la suite de la procédure de recours. Cela justifie le choix que la requête soit adressée par lettre recommandé ou par tout autre moyen similaire.

Article B.II.18.
Formalités des recours

La demande de recours n'est pas soumise à des exigences de formes importantes. Les conditions de recevabilité telles que mentionnées dans cette disposition visent principalement à permettre à la CADADo de traiter le plus efficacement et rapidement le recours.

Article B.II.19.
Délais d'obtention des documents par la CADADo

Cet article reprend l'article 28 du décret et ordonnance conjoints du 16 mai 2019.

Les articles B.II 18/19/20 ont été modifiés afin de répondre aux points 109 à 111 de l'avis de l'APD pré-

cisant que les données ou documents visés par un partage administratif ou une réutilisation ne devaient pas nécessairement faire l'objet d'une communication de la part de l'Autorité publique vers la CADADo saisie d'un recours à ce sujet mais qu'au contraire, il devait être organisé que la CADADo puisse elle-même décider de demander la communication des données si elle l'estimait nécessaire et ne pas la demander si elle ne l'estimait pas nécessaire.

À l'article B.II.19, les délais ont été adaptés en conséquence des modifications souhaitées par l'APD. La possibilité pour les Autorités publiques de remettre une note justifiant leur refus de donner accès aux documents administratifs, aux informations environnementales ou encore aux données ou documents visés par une demande de partage ou de réutilisation est conservée en toute hypothèse que la CADADo demande ou non de disposer des éléments litigieux.

Article B.II.20.
Délai maximal pour statuer sur le recours

Cet article reprend l'article 29 du décret et ordonnance conjoints du 16 mai 2019.

Article B.II.21.
Délibération de la Commission

Cette disposition ne nécessite pas de commentaire particulier.

Le Conseil d'État rappelle que l'obligation de motivation formelle visée par la loi du 29 juillet 1991 « relative à la motivation formelle des actes administratifs » s'applique aux décisions de la Commission.

Article B.II.22.
Notification de la décision de la Commission

Cette disposition ne nécessite pas de commentaire particulier.

Article B.II.23.
Pouvoirs de réformation de la Commission

Cet article reprend l'article 25 du décret et ordonnance conjoints du 16 mai 2019.

La possibilité pour la CADADo d'accorder elle-même l'accès au document administratif litigieux est déjà prévue pour la CADA à l'article 25, § 1er, de l'ordonnance du 16 mai 2019. Elle a été maintenue dans le présent Code.

L'Autorité publique est alors contrainte de délivrer les documents administratifs demandés, les informations environnementales et également désormais, les données faisant l'objet du partage administratif ou de la réutilisation.

Si l'Autorité publique n'obtempère pas, la Commission peut elle-même, moyennant préavis, mettre les documents, informations et données à disposition.

Article B.II.24.

Publication des décisions, avis et propositions

Cet article reprend l'article 30 du décret et ordonnance conjoints du 16 mai 2019. Toutefois, l'anonymisation plutôt que pseudonymiysation est imposée car les données pseudonyomisées sont encore des données personnelles.

TITRE 5

Rapport annuel et site web

Article B.II.25.

Rapport annuel

La présentation du rapport annuel permet à la Commission de rendre compte de ses activités et de la manière dont elle remplit ses missions. Elle permettra aussi d'avoir une idée de l'importance des flux de données réalisées dans la Région de Bruxelles-Capitale et des difficultés qui freinent leur développement.

Ce rapport contiendra aussi un contenu budgétaire permettant au Parlement de contrôler l'utilisation de la dotation annuelle prévue et d'anticiper les besoins futurs de la CADA.

Article B.II.26.

Site Web

La mise en place d'un site web avec des informations minimales est nécessaire à l'exigence de transparence des activités de la nouvelle Commission.

TITRE 6
Dotation

Article B.II.27.
Dotation

Il est essentiel que la future Commission reçoive les moyens nécessaires à son fonctionnement, sous peine d'enrayer tout le processus de flux de données censé être facilité et régi par la partie C du présent Code. Le système d'une dotation annuelle paraît le plus adapté aux besoins de la CADADo qui devra, dans son rapport annuel, justifier de l'utilisation de la dotation et présenter un budget prévisionnel pour les deux années à venir.

PARTIE C
GOUVERNANCE DE LA DONNÉE

La partie C du Code organise la gouvernance de la donnée au niveau de la Région bruxelloise, de la COCOM et de la COCOF.

L'objectif de gouvernance des données est largement décrit et documenté par la doctrine en la matière :

« Une bonne gestion des données peut en effet assurer plus de 80 % des protections nécessaires, mais surtout, elle permet d'améliorer la qualité des données, donc de mieux exploiter les informations, et donc, in fine d'améliorer la qualité des services fournis. Par exemple, une bonne gouvernance des données et une architecture de données et des systèmes bien pensés permettent de réduire les erreurs et d'augmenter la cohérence. Elles permettent aussi de rationnaliser les coûts en ne stockant plus les données non nécessaires et en ne dupliquant plus les données sur des dizaines de serveurs informatiques différents; de réduire les coûts de maintenance en réduisant le nombre de bases de données et le nombre de serveurs; d'accroître la réactivité par la fluidification de la circulation des données; de simplifier des processus de validation; et, enfin, de mieux contrôler les partages et accès aux données.

La mise en place d'une telle gouvernance est aussi l'occasion de passer d'un modèle « task centric » à un modèle « data centric » afin de fluidifier l'échange de l'information au sein de l'administration et donc de l'ensemble des processus métier. Autrement dit, mettre en œuvre une bonne gouvernance et architecture des données et des systèmes d'information peut être le moyen de faire un saut qualitatif majeur permettant de mieux rendre le service aux usagers, d'améliorer l'efficience en rationalisant les coûts et de se conformer sur l'exigence la plus difficile à rencontrer du RGPD : la privacy by design.

Bien sûr qu'un tel changement ne peut se faire du jour au lendemain. Il faut du temps. Du temps pour que l'organisation comprenne l'intérêt de la démarche. Du temps pour recruter des profils de personnes adéquats pour occuper des fonctions dans ces nouveaux métiers de la donnée. Du temps pour que l'organisation intègre ce nouveau paradigme où la donnée devient centrale. Du temps pour qu'une nouvelle gouvernance de données, et corollairement, de projets se mette en place. Ce changement exige des ressources – pas forcément plus de ressources, mais une redistribution des ressources disponibles.

Une telle approche a bien sûr un coût, mais comme vu plus haut, elle engendre un retour sur investissement non négligeable, contrairement à une approche par la pure conformité qui ne fait que coûter. Une telle démarche a un double avantage : premièrement d'apporter structurellement à l'administration une très grande part de la conformité avec un minimum de dépenses spécifiques pour le RGPD, et deuxièmement, d'amener un changement plus facile à initier puisqu'il se veut positif contrairement à une démarche conformiste qui implique généralement un changement sous contraintes.

Entrer dans une telle démarche systémique alliant agilité, culture de la confiance et gouvernance des données, c'est intégrer totalement le principe qui nous semble plus important du PbD (1) d'Ann Kavoukian : « full fonctionnality – Posistive-Sum, not Zero-sum » » (2).

L'approche « *data centric* » offre une réponse robuste aux défis actuels de la sécurité de l'information, mais elle doit être mise en œuvre dans le cadre d'une stratégie de sécurité globale et intégrée pour être vraiment efficace. L'approche « *data-centric* » peut répondre aux préoccupations de l'APD exprimées aux points 20 à 22 de son avis, mieux qu'une vision décentralisée de la donnée :

1. Adaptabilité aux nouveaux usages :

– Les Autorités publiques d'aujourd'hui ont des agents qui travaillent à distance, utilisent leurs propres appareils (BYOD) et échangent des données avec des tiers. La sécurité périmétrique ne peut pas protéger ces données une fois qu'elles quittent le réseau d'entreprise.

– L'approche data centric garantit que les données sont sécurisées, peu importe où elles se trouvent ou comment elles sont accessibles.

(1) Privacy by design.
(2) A. BEELEN (dir.), *La protection des données pour les institutions publiques*, Anthemis, Limal, 2020, p. 229-230.

2. Sécurisation des données elles-mêmes :

– Au lieu de se concentrer uniquement sur la sécurisation des points d'entrée et de sortie, la sécurité centrée sur les données veille à ce que les données soient protégées depuis leur source jusqu'à leur stockage ou destruction finale.

– Le chiffrement est un exemple clé de cette approche, garantissant que les données restent sécurisées en transit ou au repos.

3. Gestion final des accès :

– Grâce à la classification des données et à la gestion des identités et des accès, seules les personnes autorisées peuvent accéder aux données pertinentes.

– Le modèle Zero Trust renforce cette approche en éliminant la confiance implicite et en requérant des vérifications constantes.

4. Prévention des fuites de données :

– Les solutions DLP (préventives de pertes de données) qui pourraient être implémentées surveillent les flux de données pour éviter les partages accidentels ou malveillants.

5. Conformité aux réglementations :

– Une gouvernance data centric assure une meilleure conformité à diverses réglementations dont notamment le RGPD ne serait-ce notamment que par l'identification et la classification des données à caractère personnel depuis leur collecte jusqu'à leur destruction.

LIVRE C.I.
Champ d'application ratione personae

Article C.I.1.
Champ d'application ratione personae

La partie C du présent Code s'applique aux Autorités publiques visées à l'article A.I.3., a), b), c), i), j).

Ce champ d'application résulte de la transposition de la Directive (UE) 2019/1024 du Parlement et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte) (ci-après la Directive ISP) :

« Aux fins de la présente directive, on entend par :

1) « organismes du secteur public », l'État, les autorités régionales ou locales, les organismes de droit public ou les associations formées par une ou plusieurs de ces autorités ou un ou plusieurs de ces organismes de droit public;

2) « organismes de droit public », les organismes présentant toutes les caractéristiques suivantes :

a) ils ont été créés pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial;

b) ils sont dotés de la personnalité juridique; et

c) soit ils sont financés majoritairement par l'État, les autorités régionales ou locales ou d'autres organismes de droit public, soit leur gestion est soumise à un contrôle de ces autorités ou organismes, soit leur organe d'administration, de direction ou de surveillance est composé de membres dont plus de la moitié sont désignés par l'État, les autorités régionales ou locales ou d'autres organismes de droit public; ».

Cette définition de la directive avait déjà été transposée dans l'ordonnance actuellement en vigueur du 27 octobre 2016 visant à l'établissement d'une politique de données ouvertes (Open Data) et portant transposition de la Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public :

« 1° autorité publique :

a) la Région de Bruxelles-Capitale;

b) les personnes morales de droit public qui dépendent, directement ou indirectement, de la Région de Bruxelles-Capitale;

c) les communes;

d) les personnes, quelles que soient leur forme et leur nature, qui :

– ont été créées pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial;

– sont dotées de la personnalité juridique;

– *et dont soit l'activité est financée majoritairement par les autorités ou organismes mentionnés au a), b) ou c), soit la gestion est soumise à un contrôle de ces autorités ou organismes, soit plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance sont désignés par ces autorités ou organismes;*

e) les associations formées par une ou plusieurs autorités publiques visées au a), b), c) ou d); »

Ce champ d'application a été repris dans le cadre de la partie C du Code en l'adaptant aux compétences de la COCOF et de la COCOM.

Il est proposé de faire correspondre le champ d'application *ratione personae* général de la partie C du Code à la définition d'Autorité publique résultant de la transposition de la directive réutilisation.

Cette définition a été adaptée à la circonstance que le présent Code est adopté sous la forme de décrets et ordonnance conjoints et vise donc les entités de la Région de Bruxelles-Capitale, de la Commission communautaire commune et de la Commission communautaire française.

Le point b) vise tous les organismes d'intérêt public de la Région, COCOM et COCOF, qui sont soumis à l'autorité hiérarchique du Gouvernement, du Collège et du Collège réuni, de même que tous les organismes d'intérêt public qui sont soumis au contrôle (de tutelle) du Gouvernement, du Collège et du Collège réuni.

Le niveau local est également visé par le présent Code.

Le point i) vise la définition des pouvoirs adjudicateurs au sens de la réglementation européenne en matière de marché public. Cette définition étend considérablement le champ d'application du Code à l'ensemble des pouvoirs adjudicateurs au sens du point d) actifs dans la sphère de compétence de la Région, de la COCOM et de la COCOF.

Vu ce champ d'application très étendu directement inspiré du champ d'application de la Directive ISP, telle que transposée dans le cadre des compétences de la COCOM, COCOF et Région et bien que le présent Code ait vocation à s'appliquer aux Autorités publiques visées par l'article C.I.1. dans leur ensemble, certaines des dispositions formulées dans le livre C.III ne sont destinées à s'appliquer qu'à certaines catégories d'Autorités publiques qui seront regroupées en « paliers » par l'arrêté fixant les seuils numériques visés à l'article C.III.1.

Article C.I.2.
Dispositions générales

En réponse à l'avis de l'APD, plus particulièrement les points 24 et 25, l'article C.I.2 expose les finalités des traitements des données à caractère personnel que la partie C du Code occasionnera.

Les finalités de ces traitements sont donc légalement formulées conformément aux prescripts de l'article 8 de la Convention européenne des droits de l'Homme et l'article 22 de la Constitution. Comme le mentionne l'APD, au point 25 de son avis, les autres éléments essentiels du traitement sont fixés par la législation organique de chaque Autorité publique.

LIVRE C.II.
Principes généraux

Le présent Titre affirme et définit l'approche globale du Code.

Premièrement, le texte fournit les clés d'interprétation des dispositions, droits et obligations conférées par le Code. Il s'agit des **principes directeurs** que les Autorités publiques auxquelles s'adresse le Code doivent respecter.

Deuxièmement, le texte présente les **objectifs stratégiques** du Code, à savoir les standards, libellés en termes d'approche et de gouvernance, que les Autorités publiques doivent atteindre à long terme par l'application des dispositions du Code.

Troisièmement, le texte décrit les **objectifs opérationnels** du Code, à savoir les initiatives concrètes que les Autorités publiques doivent adopter en vue d'atteindre les objectifs stratégiques. Certains de ces objectifs opérationnels sont par ailleurs décrits dans les autres livres du Code : dans ce cas, il y est expressément fait référence dans les autres livres.

L'ensemble de ces principes sont appelés à être développés sous forme arborescente dans le Code.

TITRE 1
Les principes directeurs

Article C.II.1.
Les quatre principes directeurs

Les Autorités publiques sont appelées à respecter les quatre principes directeurs qui sont mieux définis dans les articles suivants du livre. Les Autorités publiques sont responsables de la mise en œuvre de ces principes, de telle sorte qu'il leur appartient de prendre les mesures appropriées afin d'en garan-

tir le respect. Le présent Code organise également les moyens par lesquels les Autorités publiques sont amenées à collaborer, ou à être accompagnées concernant les opérations réalisées sur des données.

Comme le précise l'alinéa 2, il doit être tenu compte de ces principes directeurs dès l'origine, à savoir dès la conception, la création ou la collecte d'une donnée par une Autorité publique. Il s'agit d'appliquer ces principes by design.

Les Autorités publiques doivent également garantir le plus haut niveau de respect de ces principes, en évaluant quelles sont les meilleures mesures techniques et organisationnelles disponibles en la matière et les mettre en place en fonction de la nature des données concernées. Les Autorités publiques doivent néanmoins effectuer une balance entre les mesures disponibles et le traitement tel qu'il est appelé à se dérouler *in concreto*. Il s'agit d'appliquer ces principes *by default*, à savoir que les principes directeurs énoncés s'appliquent par principe sauf dispositions contraires ou difficultés concrètes à les mettre œuvre.

Cette approche se fonde notamment sur les sept principes de la « confidentialité programmée » développés par Ann Cavoukian, ancienne Commissaire à l'information et à la protection de la vie privée de l'Ontario (Canada), qui ont été adoptés à fin 2010 par la 32e Conférence internationale des autorités de protection des données à Jérusalem (2010).

Cette approche est volontairement étendue à l'ensemble des données détenues par les Autorités publiques bruxelloises, lorsque cela est pertinent.

Ces sept principes peuvent se résumer comme suit :

1° prendre des mesures proactives et non réactives, préventives et non correctives;

2° assurer la protection implicite des données personnelles;

3° intégrer la protection des données à caractère personnel dans la conception des systèmes et des pratiques;

4° assurer que les systèmes sont fonctionnels pour tous selon un paradigme à somme positive, à savoir que chacun retire un bénéfice des systèmes mis en place;

5° assurer la sécurité de bout en bout, pendant toute la période de conservation des données;

6° assurer la visibilité et la transparence;

7° faciliter les vérifications;

8° assurer les protections des données à caractère personnel dans une approche centrée sur l'utilisateur.

Le respect de ces principes implique le respect de différentes obligations qui en découlent et qui sont notamment décrites dans les autres livres.

Article C.II.2.
Principe de protection et de sécurisation des données

Les Autorités publiques doivent tout mettre en œuvre pour assurer une protection adéquate des droits liés aux données qu'elles détiennent. Les titulaires de droits sur les données protégées doivent avoir la certitude que le partage de leurs données est fait dans le respect de leurs droits et de leurs intérêts.

Le premier paragraphe énonce le principe général de protection; le deuxième paragraphe énonce le principe général de sécurisation des données.

Le principe de sécurisation vise non seulement à garantir la qualité la plus élevée possible des données gérées, mais également à garantir une sécurisation adéquate des données; ces deux principes apparaissent nécessairement imbriqués.

Le paragraphe 3 contextualise le principe en fonction des catégories de données particulières que les Autorités publiques peuvent détenir.

En effet, les Autorités publiques garantissent notamment la protection et la sécurisation des données protégées. Plus particulièrement, les Autorités publiques garantissent que les données à caractère personnel ou faisant l'objet de droits de propriété intellectuelle, ou contenant des secrets d'affaires ou commerciaux, ou encore des secrets statistiques, ne peuvent être partagées qu'aux conditions légales ou réglementaires en vigueur. Les Autorités publiques protègent également la vie privée et les droits des personnes concernées par les données à caractère personnel qu'elles détiennent.

Le partage de ces données est possible moyennant le respect des conditions fixées par le Règlement sur la gouvernance des données et le présent Code.

La protection des données protégées par les Autorités publiques doit être organisée sans préjudice d'autres réglementations particulières éventuelles établissant un niveau supérieur de protection des

données, comme la protection instituée par l'article 26 de la loi du 17 juin 2013 relative à la motivation, à l'information et aux voies de recours en matière de marchés publics, de certains marchés de travaux, de fournitures et de services et de concessions.

Concernant les droits dont les personnes concernées par des données à caractère personnel disposent en vertu de la réglementation applicable en la matière, les Autorités publiques doivent faire du respect des données à caractère personnel qu'elles détiennent une priorité. Il est renvoyé sur ce point à la réglementation applicable en la matière, notamment au travers du RGPD.

De manière générale, les données protégées doivent être traitées dans la seule mesure où elles sont nécessaires à l'exercice des missions de l'Autorité publique et, en tous les cas, ne peuvent l'être que si elles font l'objet d'une sécurisation par l'Autorité publique.

Article C.II.3.
Principe de partage

Le paragraphe 1er énonce le principe du partage, entre les Autorités publiques, des documents ou des données qui peuvent l'être.

Pour rappel, la notion de partage vise à la fois dans le cadre du Code le partage administratifs de données et la réutilisation des documents. Le premier paragraphe de l'article vise cette conception générale du partage.

Le paragraphe 2 de l'article C.II.3 concerne un type de partage de données, à savoir le partage administratif de données, s'opérant entre deux Autorités publiques. Le texte précise bien que le partage administratif est un objectif fixé à chaque Autorité publique afin de rencontrer l'approche développée par le Code mais que toute demande de partage ne débouche pas effectivement sur un partage, en application des dispositions légales et réglementaires applicables, à savoir notamment, pour ce qui concerne spécifiquement les données à caractère personnel, le principe du respect des finalités.

Le paragraphe 3 aborde plus précisément un type de partage administratif, à savoir le partage administratif de données issues de sources authentiques, bruxelloises ou non. Dans ces hypothèses, le partage des données est obligatoire afin de respecter le principe du *once only*. Les conditions de ce type de partage sont détaillées dans le Code, avec l'obligation de récolter le consentement de la personne concernée pour ce qui concerne le partage de données issues de sources authentiques bruxelloises qui seraient des données à caractère personnel.

Enfin, le paragraphe 4 instaure également le principe du partage des données publiques vers l'extérieur dans le cadre de réutilisations. Comme exposé dans le cadre des commentaires des articles du livre C.IV consacrés à la réutilisation, ces articles transposent le plus fidèlement la directive européenne qui règle elle-même les conditions de réutilisation des documents.

L'article C.II.3 vise à développer la culture du partage mais ne cherche pas à maximiser les partages administratifs et la réutilisation, comme évoqué dans le point 75 de l'avis de l'APD, dans la mesure où ces opérations sont strictement encadrées par le Code, et, pour partie par le droit européen. L'expression partage par défaut a été supprimée afin de respecter la notion juridique plus adéquate de principe. Pour rappel, les principes sont appelés à être interprétés largement et les exceptions de manière restrictive. Les exceptions aux hypothèses de partages administratifs et de réutilisations sont exposées dans les livres y étant consacrés du Code ou découlent également de l'application de textes légaux, réglementaires ou statutaires, quant à la compétence des Autorités publiques concernées (les partages administratifs ne pouvant avoir lieu que dans le cadre des missions d'intérêt publics de chaque Autorité), ou, découlent encore de l'application de dispositions internationales ou européenne, telles le RGPD.

Article C.II.4.
Principe de transparence

Le principe de transparence de l'administration signifie que les actions et décisions de l'administration doivent être accessibles au public.

Dans le cadre du présent Code, ce principe est également applicable en matière de données sous la forme de principes spécifiques.

Premièrement – paragraphe 2 – il s'agit de la mise en œuvre d'une politique pour l'innovation et le développement numérique faisant une place prioritaire à la réutilisation des données publiques qui peuvent l'être – dite également politique open data.

Les données ouvertes se réfèrent à des données qui sont librement accessibles, par tous, dont la réutilisation peut le cas échéant se faire sans restriction de propriété intellectuelle ou autre. Les données ouvertes sont généralement utilisées pour une variété de fins, comme la recherche, l'analyse, l'innovation et la transparence.

Les données publiques, détenues par une Autorité publique, sont celles qui sont produites ou collectées dans l'exercice de leurs missions de services publics mais qui peuvent inclure des informations sur les finances, les agents, les politiques et les programmes gouvernementaux, ainsi que des données sur les citoyens et les entreprises. Toutes les données publiques ne sont pas nécessairement librement réutilisables et peuvent être soumises à certaines restrictions d'utilisation et de diffusion.

Les Autorités publiques doivent prioritairement envisager la diffusion sous format ouvert ou assurant le plus haut degré d'ouverture, c'est-à-dire par tout protocole de communication, d'interconnexion ou d'échange et tout format de données interopérable et dont les spécifications techniques sont publiques et sans restriction d'accès, ni de mise en œuvre.

Le paragraphe 3 vise à ce que les Autorités publiques mettent en place une véritable documentation. Ce principe approfondit le principe de transparence ou de publicité en ce qu'il requiert, en matière de données, la mise en place de procédures spécifiques et dédiées, formellement rédigées et accessibles à tous.

Le principe de documentation inclut la mise à disposition, d'initiative, d'informations sur les politiques et les procédures de l'Autorité publique en matière de gouvernance de la donnée lorsque cela est possible (principe de transparence active dans la même logique que celle de la publicité active visée au livre B.I.); cela inclut également que les Autorités publiques soient responsables de transmettre l'information utile en matière de gouvernance de la donnée au sens du présent Code à tout citoyen ou opérateur privé qui en fait la demande ou encore en interne à leurs agents ou services (principe de transparence passive dans la même logique que celle de la publicité passive visée au livre B.I.).

L'obligation d'une documentation active vis-à-vis des données qu'elles détiennent implique une description la plus précise possible des processus mis en œuvre par les Autorités publiques et a pour objectif que les données soient exploitées, tant par les Autorités publiques que le cas échéant des tiers, à la fréquence de leur production et/ou mise à jour.

En tous les cas, la documentation mise en place par l'Autorité publique ne doit pas porter préjudice à la protection de certaines des données – dites « données protégées ».

L'obligation de documentation passive concerne l'obligation qui est faite aux Autorités publiques de répondre aux demandes de ses services ou des tiers qui lui seraient adressées. Cette réponse peut concerner soit une problématique particulière, auquel cas l'Autorité publique endosse une fonction de support – résolution de problème, … –, soit une demande d'information générale ou précise. L'information visée dans le cadre de cette obligation de transparence passive ne peut que concerner la gouvernance des données numériques.

Article C.II.5
Principe de qualité

Les utilisateurs de données doivent avoir l'assurance que les données sont de haute qualité : il s'agit d'une condition nécessaire à ce que tout traitement effectué à partir de ces données soit pertinent et efficient.

Chaque fois qu'il est fait mention de la « qualité des données » dans le présent Code, il s'agit de la vue complémentaire des dimensions citées ci-dessous.

Les différentes dimensions de la qualité ne sont à ce jour pas définies dans un texte réglementaire. Néanmoins, nous faisons le choix de les définir de la manière suivante :

1° consistance

2° exactitude

3° exhaustivité

4° vérifiabilité

5° validité

6° unicité

7° intégrité

8° ponctualité.

1° consistance : mesure dans laquelle les données sont homogènes et cohérentes entre elles. Les données cohérentes présentent des caractéristiques communes ou des relations similaires entre elles.

2° exactitude : mesure dans laquelle les données sont conformes à la réalité ou à la vérité.

3° exhaustivité : mesure dans laquelle toutes les données pertinentes ont été collectées et incluses dans la base de données.

4° vérifiabilité : mesure dans laquelle les données peuvent être validées ou vérifiées pour s'assurer de leur exactitude et de leur intégrité.

5° validité : mesure dans laquelle les données sont conformes aux règles et aux normes spécifiées pour leur utilisation ou leur stockage.

6° unicité : mesure dans laquelle chaque élément de données est unique et ne se répète pas.

7° intégrité : mesure dans laquelle les données sont protégées contre les pertes, les altérations ou les dommages non autorisés.

8° ponctualité : mesure dans laquelle les données sont mises à jour et disponibles dans les délais requis.

TITRE 2
Les objectifs stratégiques

Article C.II.6.
Six objectifs stratégiques

Le présent Titre décrit les objectifs stratégiques que les Autorités publiques sont à la fois appelées à appliquer et à atteindre au travers de l'application du Code.

La mise en place de ces objectifs stratégiques a pour vocation d'assurer la correcte implémentation des principes énoncés précédemment dans le cadre de l'action administrative.

En effet, les Autorités publiques doivent adopter une certaine approche, définie par les objectifs stratégiques, dans la mise en œuvre des obligations de gouvernance du Code. Dans le même temps, l'on peut considérer qu'adopter une telle approche leur permettra, in fine, de mettre en place une gouvernance des données optimale et proportionnelle à l'importance de leur activité numérique.

Article C.II.7.
Approche centrée sur la donnée

L'adoption d'une approche centrée sur les données doit permettre aux Autorités publiques de faire de la gouvernance des données une priorité dans le cadre de l'exercice de leurs missions de services publics et de leurs obligations d'intérêt général, notamment en donnant la priorité à des outils performants et puissants, par exemple pour accéder, stocker ou protéger les données en interne ou de manière externe.

En plaçant les données au cœur de leur stratégie, les Autorités publiques reconnaissent l'importance de la gestion et de l'utilisation efficace des données. Cela permet de maximiser la valeur des données en les utilisant de manière pertinente et stratégique.

Les Autorités publiques gèrent les données comme elles gèrent les autres biens publics : l'inventorisation, la gestion et la valorisation des données font donc partie de leurs plans de gestion.

Article C.II.8.
Définition des rôles et responsabilités

La gouvernance des données est une responsabilité partagée. Pour s'assurer que l'ensemble des acteurs concernés participent à sa mise en œuvre de manière cohérente, les Autorités publiques doivent se baser sur un cadre commun de définition des rôles et responsabilités, tel que décrit au niveau du livre C.III.

Une claire définition des rôles et responsabilités des parties prenantes permet de garantir une meilleure coordination et collaboration dans la gestion des données ce qui facilite la transparence et évite les conflits d'intérêts, en assurant que chacun comprend ses responsabilités et contribue de manière appropriée à l'ensemble du processus.

Ce cadre doit couvrir l'ensemble des responsabilités, des aspects stratégiques jusqu'à la gestion quotidienne et l'utilisation des données par les citoyens.

Ce cadre commun ou modèle opérationnel commun doit pouvoir être décliné dans les Autorités publiques et adapté à leur taille, leur culture et leur maturité en termes de gouvernance des données.

Article C.II.9.
Adoption de standards communs

Le volume grandissant de données et le développement de leur utilisation présentent des risques importants de développement de modèles différents, dont la coexistence génère une baisse de l'efficacité de la gestion et une augmentation substantielle des coûts.

L'utilisation de standards communs pour la gestion des données favorise l'interopérabilité et facilite l'échange de données entre les différentes parties prenantes. Cela garantit également la cohérence, la qualité et la compatibilité des données, ce qui est essentiel pour assurer leur intégrité et leur utilisation efficace.

Pour garantir l'efficacité dans la gestion et optimiser les dépenses liées à la gestion et à l'utilisation des données, les Autorités publiques doivent donc favoriser l'utilisation de solutions mutualisées. Partager les coûts liés aux développements de nouvelles solutions permet de réaliser des économies d'échelles et d'accélérer la transformation « data ». Standardiser les

outils et les échanges de données permettra également d'éviter de dupliquer les données, ce qui facilite le respect des principes de sécurité et le respect des droits individuels. Le partage de solutions et de standards communs d'architecture des données, permet également de travailler ensemble au développement des compétences communes.

Article C.II.10.
Gouvernance évolutive

L'application des obligations du Code permet aux Autorités publiques de structurer leurs activités de gestion des données au travers d'une politique de gouvernance formalisée.

Les processus et politiques de gouvernance des Autorités publiques à mettre en place doivent prendre en considération l'évolution des techniques et des outils. Ainsi, une politique ne devrait être mise en place pour un type d'outil ou de technique unique ou exclusif que dans le cas où il ne peut être fait autrement. En tous les cas, si cet outil ou technique devient obsolète, le processus ou la politique correspondant devrait être amendée ou abrogée.

La gouvernance évolutive implique la mise en place de structures et de processus flexibles qui peuvent s'adapter aux évolutions technologiques, légales et aux besoins changeants des parties prenantes.

Les processus et politiques doivent prendre en considération l'évolution des réglementations applicables. En effet, étant donné l'influence majeure du droit européen sur le domaine du droit des données, les Autorités publiques devraient être en mesure d'appliquer le plus directement possible au regard de l'instrument juridique visé, les dispositions réglementaires européennes. Cette obligation vise aussi bien les dispositions déjà applicables que les dispositions futures qui pourraient être adoptées de manière générale ou spécifiquement pour une ou plusieurs catégories de données ou de traitements.

Article C.II.11.
Éducation des parties prenantes

Dans le cadre de la mise en œuvre des obligations découlant du Code, les Autorités publiques expliquent autant que possible les objectifs et les méthodes d'utilisation, d'analyse et de prise de décisions à partir des données collectées. Ils veillent à promouvoir des formations régulières sur l'importance de l'utilisation éthique des données, du respect de la vie privée et de la confidentialité.

L'ensemble des intervenants doivent être mobilisés, informés, sensibilisés, formés, voire entourés ou aidés de manière plus ou moins spécifique.

Une éducation numérique adéquate permet aux parties prenantes de comprendre les enjeux liés à la gestion des données, y compris les aspects juridiques, éthiques et techniques. Cela favorisera une utilisation responsable des données et renforce la confiance entre les parties prenantes.

Ces mesures doivent permettre, in fine, d'éviter de creuser la fracture numérique et doivent contribuer à ce que chacun et chacune puisse profiter pleinement de la transformation numérique des services publics.

À cet effet, les Autorités publiques adoptent une culture de la donnée qui permet de communiquer de manière pédagogique et critique et d'appréhender comment tenir compte des résultats du traitement des données lors de discussions ou de prises de décisions.

Article C.II.12.
Exploitation éthique, efficiente et responsable

L'éthique a été ajoutée comme principe d'exploitation des données afin de répondre aux préoccupations exprimées par le Centre interfédéral pour l'égalité des chances (Institut pour l'égalité des femmes et des hommes).

Les Autorités publiques privilégient, autant que faire se peut, le recours à des sources d'approvisionnement et l'utilisation de technologies qui limitent leur empreinte environnementale. Cette démarche s'inscrit dans la volonté de bâtir une politique numérique responsable.

L'exploitation efficiente des données implique de les utiliser de manière efficace pour atteindre les objectifs stratégiques de l'organisation.

L'objectif de mise en place d'une politique du numérique responsable, au travers de l'exploitation efficiente et durable des données, engendre également une obligation d'économicité dans le chef des Autorités publiques. Néanmoins, ces objectifs ne peuvent être examinés séparément. En effet, leur examen distinct pourrait aboutir à des priorisations différentes. Cette évaluation doit être menée par chaque Autorité publique *in concreto* au regard du projet qu'elle entend mener, en tenant compte des contraintes légales et réglementaires mais également économiques et d'opportunité. Cette évaluation peut par exemple être menée concernant le développement d'une application, laquelle demanderait également d'être hébergée. Sous l'angle des principes d'éco-

nomicité et de durabilité, l'Autorité publique devrait être en mesure de prioriser les étapes du projet, qu'il s'agisse de l'achat d'un serveur, de sa sécurisation ou du développement de l'application.

Les Autorités publiques appliquent le principe d'économicité également pour les outils utilisés pour la collecte et la conservation des données. Ainsi, les Autorités publiques s'engagent à collecter les seules données nécessaires à l'accomplissement des missions de services publics et des obligations d'intérêt général, et en limitent le stockage.

TITRE 3
Les objectifs opérationnels

Article C.II.13.
Huit objectifs opérationnels

Les Autorités publiques sont appelées, tout au long de la mise en œuvre des obligations découlant du présent Code, à atteindre les objectifs opérationnels mieux définis au présent Titre.

La réalisation de ces objectifs dépend notamment de l'organisation et de la mise en place de moyens humains et techniques adéquats par les Autorités publiques.

Dans ce cadre, les Autorités publiques sont amenées à définir une stratégie à l'égard de leurs données, notamment en ce qui concerne l'ordre de priorité dans lequel elles feront l'objet d'une valorisation.

Les objectifs opérationnels se concentrent sur les activités spécifiques et les mesures tangibles qui permettront d'atteindre les objectifs stratégiques fixés.

Afin d'être pleinement réalisés, certains des objectifs sont mieux définis soit dans la suite du présent Code, soit dans d'autres instruments juridiques (réglementaires ou non).

Article C.II.14.
Valorisation des données

Cet objectif vise à ce que les Autorités publiques soient en mesure d'identifier les données qu'elles détiennent voire d'en réaliser le cadastre. Il s'agit d'une étape préalable indispensable à la mise en œuvre d'une gouvernance efficiente des données.

Cet objectif vise à reconnaître la valeur potentielle des données détenues par une Autorité publique et à déterminer les priorités en termes d'utilisation et de valorisation.

Comme le précise l'alinéa 2, les Autorités publiques doivent également identifier si les données qu'ils détiennent correspondent à des catégories particulières de données au sens de la réglementation européenne.

D'une part, cela concerne les données de forte valeur au sens de la Directive réutilisation.

Selon l'article 2 de la Directive ISP, l'identification d'ensembles de données de forte valeur particuliers en vertu du paragraphe 1er est fondée sur l'évaluation de leur aptitude potentielle à :

1) Générer des avantages socio-économiques ou environnementaux importants et des services innovants;

2) Bénéficier à un grand nombre d'utilisateurs;

3) Contribuer à générer des recettes et;

4) Être associés à d'autres ensembles de données.

La Directive définit actuellement six catégories de données de forte valeur : géospatial, observation de la Terre et environnement, météorologie, statistiques, entreprises et propriété des entreprises, mobilité.

D'autre part, cela concerne les données relatives aux espaces européens communs des données qui relèvent de leurs compétences.

S'appuyant sur l'expérience acquise avec la communauté des chercheurs dans le cadre du nuage européen pour la science ouverte, la Commission européenne appuie, à ce jour, la mise en place des neuf espaces européens communs des données : un espace européen commun des données relatives à l'industrie (manufacturière), un espace européen commun des données relatives au pacte vert, un espace européen commun des données relatives à la mobilité, un espace européen commun des données relatives à la santé, un espace européen commun des données financières, un espace européen commun des données relatives à l'énergie, un espace européen commun des données relatives à l'agriculture, un espace européen commun des données pour l'administration publique, et un espace européen commun des données relatives aux compétences

L'attention des Autorités publiques est attirée sur le fait que la Commission peut envisager de lancer,

de manière séquentielle, d'autres espaces européens communs des données dans d'autres secteurs.

À la suite d'une observation de la section de législation du Conseil d'État, les espaces de données européens communs font référence à des espaces qui permettront de disposer d'un plus grand nombre de données en vue de leur accès et de leur réutilisation. Voy. not. Communication du 19 février 2020 de la Commission européenne au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions, Une stratégie européenne pour les données, COM(2020) 66 final.

Article C.II.15.
Identification du ou des régime(s) juridique(s) applicable(s)

Cet objectif vise à ce que les Autorités publiques puissent identifier le ou les régimes juridiques applicables aux données qu'elles détiennent.

Cette étape est cruciale afin de permettre l'implémentation d'une gouvernance de la donnée efficiente. Sa mise en œuvre ne se suffit pas à elle-même.

L'identification des régimes juridiques applicables aide à déterminer les mesures de sécurité, de consentement/autorisation, de conservation des données, et à évaluer les risques juridiques potentiels liés à la gestion des données.

Il est impératif que les Autorités publiques organisent la protection de ce ou ces régimes dans les relations qu'elles nouent entre elles ou avec des tiers. Cela concerne notamment les contrats, et notamment marchés publics, que les Autorités publiques attribuent à des prestataires externes pour des missions de gestion, d'hébergement, ou de stockage des données. L'ensemble de ces liens juridiques sont repris dans la notion de partenariats numériques visée au livre C.III.

Article C.II.16.
Respect de la confidentialité des données protégées

Cet objectif vise à ce que les Autorités publiques prennent les mesures adéquates pour protéger les données qui devraient l'être avant tout traitement ultérieur.

L'occultation est le processus qui consiste à effacer les données protégées ou remplacer définitivement les données protégées par des données fictives réalistes.

Pour chaque jeu de données à partager, les Autorités publiques procèdent à l'occultation des données identifiées comme confidentielles et non communicables.

Pour chaque jeu de données à rendre accessible, les Autorités publiques procèdent à l'occultation des données identifiées comme confidentielles et non communicables.

L'on renvoie au livre A.III. consacré aux définitions de la partie C en ce qui concerne la notion d'anonymisation.

Cet article a été revu à la suite de l'avis de l'APD afin de s'assurer d'une anonymisation/occultation adéquate des données, essentiellement pour la réutilisation. Rajouter la possibilité de l'intervention d'un tiers de confiance implique que l'Autorité publique concernée puisse faire appel à une entité Tiers de confiance qui procède techniquement à l'anonymisation, à défaut pour l'Autorité de disposer des outils ou des moyens nécessaires.

Article C.II.17.
Interopérabilité

Pour que les données puissent être valorisées, diffusées et échangées, comprises et réutilisées, il est nécessaire qu'elles respectent des règles d'interopérabilité. Il est donc nécessaire que les Autorités publiques mettent en place des systèmes interopérables entre eux en vue d'assurer le plus haut niveau de qualité des données.

Les Autorités publiques peuvent notamment mettre en place une ou plusieurs des techniques suivantes en vue d'assurer l'interopérabilité :

1) L'adoption de standards. Dans le domaine de la donnée, les standards prennent par exemple la forme de schémas de données, c'est-à-dire une liste de champs que l'on doit retrouver dans un fichier et les valeurs autorisées pour chacun de ces champs.

2) Le recours à des librairies ou les référentiels de données, c'est-à-dire de glossaires pour recenser les termes employés dans un métier particulier. Ces glossaires sont nécessaires en vue de disposer d'un vocabulaire commun.

3) La description des flux de données. Les flux de données sont créés entre les outils pour échanger des données. Dans ces flux, les données peuvent circuler en temps réel ou sur des « pas de temps » spécifiques. La description des flux permet de préciser la nature des données qui y transitent, leur

format, leur granularité et leur fréquence. Les flux doivent faire l'objet d'une vigilance particulière en termes de cybersécurité afin d'éviter toute vulnérabilité du système d'information. Il est renvoyé à cet égard aux dispositions du chapitre 2 du titre 4 du livre B.III.

4) L'utilisation d'API, c'est-à-dire de « branchement » qui permet de faire communiquer deux logiciels entre eux. Les données peuvent ainsi circuler de manière automatisée entre plusieurs outils. Certaines API sont dites génériques, c'est-à-dire qu'elles permettent de faire transiter des données dont les formats sont standards.

Cet objectif opérationnel préfigure l'application future du Règlement pour une Europe interopérable (actuellement proposition de Règlement du Parlement Européen et du Conseil établissant des mesures destinées à assurer un niveau élevé d'interopérabilité du secteur public dans l'ensemble de l'Union, COM(2022) 720 final, adoptée le 18 novembre 2022). Outre la question de l'interopérabilité elle-même, les Autorités publiques préparent ainsi leur participation aux « *datas spaces* ». Dans le cadre de la stratégie européenne des données, les « *data spaces* » (ou « espaces de données » en français) font référence à des infrastructures techniques et organisationnelles qui permettent de partager des données entre différents acteurs, tout en assurant leur interopérabilité et leur sécurité.

L'objectif des *data spaces* est de faciliter l'échange de données entre différents acteurs (entreprises, organismes publics, universités, etc.) tout en garantissant la protection de la vie privée, la sécurité des données et la conformité aux réglementations en vigueur.

Les *data spaces* peuvent être spécialisés par domaine (par exemple, les données de santé, les données environnementales, les données de transport) ou être transversaux. Ils peuvent également être organisés à différentes échelles, allant d'un niveau local à un niveau européen.

Article C.II.18.
Traçabilité et réversibilité

La traçabilité des données fait référence à la capacité de suivre l'origine, les transformations et les mouvements des données tout au long de leur cycle de vie. Cela permet de comprendre comment les données ont été collectées, traitées et utilisées, et d'assurer leur intégrité et leur fiabilité. La traçabilité peut être réalisée en enregistrant les métadonnées associées aux données, telles que les informations sur la source, les transformations appliquées, les utilisateurs ayant accédé aux données, etc.

La réversibilité des données, quant à elle, concerne la capacité de récupérer et de migrer les données d'un système à un autre, en préservant leur intégrité, leur structure et leur format. Cela permet de garantir la portabilité des données et d'éviter la dépendance vis-à-vis d'une plate-forme ou d'une technologie spécifique.

En garantissant ces principes, les Autorités publiques peuvent assurer la transparence et la responsabilité dans l'utilisation des données.

Cela permet de garantir l'intégrité des données et de permettre la correction d'erreurs ou la restauration de versions antérieures des données. Finalement, la mise en œuvre de cet objectif permet de garantir la qualité des données.

La mise en œuvre du principe de réversibilité permet également la récupération des données si l'infrastructure et les outils utilisés ne pouvaient plus l'être, par exemple en raison d'un problème technique ou de la fin d'un contrat de prestations de services informatiques.

On précise néanmoins que la mise en place d'une telle garantie de réversibilité et de traçabilité n'est pas souhaitable ni possible à l'égard de tout type de données mais doit faire l'objet d'une application proportionnelle en fonction de la pertinence et de l'importance de la démarche par rapport à l'objectif poursuivi.

En outre, conformément à la demande de l'APD dans le cadre de son avis, la traçabilité et la réversibilité ne trouvent plus à s'appliquer en cas d'anonymisation, fin du traitement ou destruction des données.

Article C.II.19.
Intégration des données

Cet objectif vise à ce que les Autorités publiques soient en mesure de combiner des données provenant de plusieurs sources d'origine afin de fournir aux utilisateurs une vue unifiée unique. L'intégration consiste à regrouper des composants plus petits dans un système unique afin qu'il puisse fonctionner en tant que composant unique. Le cas échéant, une nouvelle base de données intégrées est ainsi créée et l'Autorité publique qui en est à l'origine est considérée comme le producteur.

Article C.II.20.
Génération et gestion des métadonnées et données de référence

Cet objectif vise à ce que les Autorités publiques intègrent pleinement les notions de données de référence et de métadonnées.

Les données de référence sont indispensables pour lier des bases de données de nature hétérogène et construire tout nouveau service intégré au Web des données. Leur production est donc de nature à permettre aux Autorités publiques de remplir de manière efficiente leurs obligations en vertu du présent Code.

Les métadonnées, souvent appelées données des données ou information sur l'information, facilitent la réutilisation des données de référence.

Article C.II.21.
Contrôle des conditions d'hébergement et de stockage des données

Cet objectif vise à permettre aux Autorités publiques à faire face aux enjeux de sécurité et de souveraineté que soulèvent le traitement d'un nombre de plus en plus important de données.

À cet égard, les Autorités publiques doivent imposer des conditions d'hébergement et de stockage des données qui permettent de respecter au plus haut les dispositions réglementaires applicables au regard des données concernées (comme le RGPD dans le cas de données à caractère personnel).

De cette manière, les Autorités publiques seront en mesure de connaître les conditions dans lesquelles sont hébergées ou stockées leurs données.

LIVRE C.III.
Obligations de gouvernance des Autorités publiques

Vu la mise en place d'une véritable politique de gouvernance de la donnée, chaque Autorité publique visée par le présent Code se voit attribuer de nouvelles obligations en lien direct avec la gestion des données, visant à organiser les données et les flux de données, et visant, de manière générale, à poser les conditions de bases à la multiplication des partages au sens du livre C.IV.

Ces obligations légales sont mises à charge de chaque Autorité publique dans le cadre de leurs compétences respectives, selon des degrés divers, conformément au principe de proportionnalité. L'objectif est que les Autorités publiques soient regroupées par paliers, déterminés en fonction de seuils numériques fixés par arrêté conjoint du Gouvernement, du Collège réuni et du Collège.

Ces nouvelles obligations concernent notamment :

a) les partenariats numériques (titre 2);

b) la valorisation des données (titre 3);

c) la gestion des données (titre 4);

d) le contrôle de la conformité, la traçabilité et la responsabilité des Autorités publiques (titre 5).

Actuellement, les Autorités publiques ignorent trop souvent quelles données elles détiennent et de quelle manière le traitement de ces données pourrait, non seulement, leur permettre de réaliser leurs missions de service public ou leurs obligations d'intérêt général avec plus d'efficience, mais également, par ailleurs parvenir à intéresser également les autres Autorités publiques, les collectivités publiques du pays ou encore des opérateurs socio-économiques.

Dans une première phase, une nouvelle notion est introduite, celle de « partenariat numérique ». Cette notion a pour seule ambition de permettre aux Autorités publiques de qualifier les liens juridiques ou administratifs qu'elles entretiennent et dont la finalité est la valorisation de données. Une fois la qualification de partenariat numérique de données posée, certaines obligations précises visant à qualifier, ordonner, catégoriser les données et les qualités de chaque partie au partenariat, s'imposent aux Autorités publiques. La démarche est pragmatique, avant de mettre en place une véritable gouvernance de la donnée, les Autorités publiques vont chercher à partir de leur activité juridique et administrative, et observer quelles données sont concernées. La démarche de qualification en partenariats les liens juridiques et administratifs (i), et ensuite les parties (ii) et les données (iii), est donc reprise en tant que première étape dans le cadre de ce livre. L'objectif n'est pas d'imposer un nouveau régime juridique aux Autorités publiques qui s'appliquerait dès qu'un partenariat numérique de données est identifié, mais simplement d'inviter les Autorités publiques à nommer et catégoriser car, de cette qualification, dépend le régime juridique applicable.

Ensuite, les Autorités publiques vont être amenées, étape par étape, à identifier parmi les données détenues celles qui seront susceptibles de créer de la valeur et de quelle manière ces données peuvent être valorisées. Il s'agit du Titre 3.

Dans le cadre de la gestion de leurs données (Titre 4), les Autorités publiques sont amenées à respecter une série de règles qui visent à garantir la qualité des données qu'elles détiennent.

Les obligations de sécurité sont abordées dans le cadre du titre 5.

Enfin, les diverses obligations décrites dans le présent livre, notamment au niveau des Titres 3 et 4, visent à concrétiser les principes directeurs décrits au titre 2 du livre C.II. Pour rappel, il s'agit des principes de protection et de sécurisation des données, de partage, de transparence et de qualité. Ces obligations sont également mises en place en vue d'atteindre les objectifs stratégiques décrits au titre 3 du livre C.II ou les objectifs opérationnels décrits au titre 4 du livre C.II. Il est fait référence, le cas échéant, dans le présent livre à l'article ou aux articles pertinents du livre C.II auxquels les obligations décrites se rattachent.

TITRE 1
Champ d'application ratione personae

Article C.III.1.
Habilitation du Gouvernement, Collège et Collège réuni de fixer des seuils numériques

Comme exposé dans le cadre du commentaire de l'article C.III.1., l'ensemble du livre C.III n'est pas destiné à s'appliquer à l'ensemble des Autorités publiques visées à l'article C.I.1.

Un arrêté conjoint a pour objet de fixer des seuils numériques identifiant des groupes d'Autorités publiques organisés par palier selon des critères objectifs et pertinents.

TITRE 2
Les partenariats numériques de données

CHAPITRE 1
Principe

Article C.III.2.
La notion de partenariats numériques de données aux fins de valorisation des données

Dans la pratique, les Autorités publiques aménagent des liens juridiques ou administratifs :

a) soit entre elles;

b) soit avec un ou plusieurs opérateurs privés;

c) soit, pour les Autorités publiques les plus importantes, entre leurs différents services (direction générale ou organes consultatifs, …).

Le présent titre s'intéresse à qualifier ces liens pour autant que ceux-ci ont pour finalité ou pour résultat, la valorisation ou le partage de données.

L'intérêt de cette qualification en partenariat numérique de données a pour seul effet d'obliger les Autorités publiques à porter leur attention sur ces relations juridiques et administratives afin de veiller à ce que celles-ci soit correctement appréhendées d'un point de vue numérique, quand à deux aspects principalement : la qualification des parties et la catégorisation des données.

Il ne s'agit donc pas de créer un nouveau régime ou cadre juridique pour ces relations de partenariats numériques de données mais de les conceptualiser, dans leur ensemble de même que dans leurs composantes (à savoir au niveau des parties au partenariat et au niveau des types de données visées).

La nécessité de qualifier les situations juridiques au regard de concepts précis est une démarche courante et, par exemple, déjà présente dans le cadre du RGPD où il s'agit de qualifier les parties concernées soit de responsable de traitement, soit de responsables de traitement conjoints, soit de sous-traitant. La qualification choisie implique l'application d'un régime juridique particulier pour ces parties.

La démarche est identique dans le cadre du présent titre : elle vise à qualifier la relation, en vue de qualifier par la suite les parties au sein de cette relation et les données visées.

La définition du partenariat numérique de données se veut extrêmement large dans la mesure où le présent livre constitue le cadre minimal applicable à toute forme de relation juridique ou administrative concernant au minimum une Autorité publique et des données publiques valorisées ou partagées.

Ce cadre minimal et primordial sera le cas échéant le seul applicable en matière de gouvernance de données dans l'hypothèse où les liens juridiques ou administratifs visés ne correspondent pas à des cas de partages administratifs, de réutilisations ou encore de Communications, qui sont les seules opérations de valorisation et de partage de données très spécifiques régies par le présent Code et juridiquement encadrées sur le plan de la gestion des données (au niveau bruxellois et européen).

Mais ces cas de figure particuliers ne sont pas les seuls cas de figure possible en matière de partage et de valorisation de données, ce qui explique l'intérêt

de poser un cadre minimal pour tous les autres cas possibles.

Ainsi, lorsqu'un partenariat entre deux Autorités publiques est identifié dans le but d'un partage administratif de données, il doit faire l'objet d'un protocole conformément au livre C.IV. Toutefois, la notion de partenariat ne se confond pas avec celle de protocole d'accord. La notion de partenariat numérique de données est beaucoup plus large et a pour unique fonction de définir à partir de quelle hypothèse les Autorités publiques vont devoir s'accorder à qualifier communément les parties au partenariat et les données qu'il vise.

Le cadre minimal décrit dans le présent titre vise à créer les conditions de base nécessaires à la mise en place d'un contrôle des données publiques entre partenaires qui soit respectueux des droits de tous.

Partant, la notion de partenariat numérique ne se confond pas non plus avec la notion de contrat ou, *a fortiori*, avec la notion de marché public : il s'agit là de régimes juridiques précis, ce qui, comme exposé, n'est pas l'objectif du concept de partenariat numérique de données.

Cela signifie donc que la qualification de partenariat numérique peut coexister avec un grand nombre de formes juridiques différentes.

Par ailleurs, nous soulignons qu'est visée tant la notion de lien juridique, qui pourrait coexister avec la présence d'un contrat ou encore d'une obligation légale, que la notion de lien administratif qui est présente lorsque deux services d'une même Autorité publique, organisent conjointement un partage ou une valorisation de données.

La conclusion d'un partenariat numérique n'appelle pas de formalisme juridique spécifique dans la mesure où il s'agit uniquement de qualifier une relation juridique ou administrative pour déterminer quelles qualités doivent être apposées à quelle partie au partenariat et quelles catégories de données est concernée par le partenariat.

Ces obligations de qualification doivent être perçues dans une optique de gouvernance globale dans la mesure où elles permettront in fine aux Autorités publiques de classifier leurs données et répertorier leur actif numérique, et d'organiser la remontée des informations jusqu'au Catalogue des données.

Les partenariats numériques peuvent être conclus entre Autorités publiques et tout autre type de partie qui n'est pas une Autorité publique : les cas de partenariats numériques mixtes de données :

Dans l'hypothèse d'un partenariat numérique mixte de données, l'Autorité publique ne peut au travers d'un partenariat numérique avec une autre partie qui n'est pas une Autorité publique se dédouaner des obligations que lui impose le Code mais au contraire devra s'assurer que l'autre partie respecte bien, également, dans le cadre du partenariat les obligations qui sont imposées à l'Autorité publique par le présent Code. Par exemple, que l'Autorité publique assure elle-même la sécurité de ses données ou non, le niveau de sécurité visé par le code pour les données publiques doit être garanti de la même manière. Pour cette raison, ces partenariats doivent être encadrés d'une manière encore plus précise conformément à l'article C.III.3.

L'objectif poursuivi par la mise en place des partenariats numériques est de permettre aux Autorités publiques de garder le contrôle sur toutes les données publiques nécessaires à leurs missions de services public et obligations d'intérêt général, que ces Autorités publiques fassent appel à une personne extérieure ou non.

Les cas de partenariats numériques dans lesquels les Autorités publiques ont recours à une personne extérieure qui n'est pas une Autorité publique en vue d'effectuer des traitements concernant des données publiques sont potentiellement extrêmement larges. Cette collaboration peut d'ailleurs aller jusqu'à la mutualisation des données dans le cadre de projets communs.

Les partenariats numériques peuvent être conclus entre Autorités publiques uniquement : les cas de partenariats numériques publics de données :

La collaboration sous forme de partenariat numérique peut concerner des Autorités publiques entre elles, ou des entités (services, directions, comité, …) au sein d'une même Autorité publique. Des Autorités publiques peuvent par exemple décider de mutualiser certains outils, voire certaines compétences ou certains postes.

Il s'agit, par exemple, d'un projet de mutualisation des données relatives à un territoire intelligent qui peut concerner des infrastructures numériques comme les réseaux de télécommunication, les centres d'hébergement ou des plateformes de traitement des données dédiées à un domaine spécifique (mobilité, agriculture, occupation territoire, …).

Article C.III.3.
Les partenariats mixtes de données

Le présent article traite des partenariats mixtes de données et de la nécessité pour les Autorités

publiques d'organiser leurs relations avec la ou les autre(s) partie(s) avec lesquelles elles traitent dans le cadre de la gestion de leurs données publiques.

Indépendamment de la forme de la relation entre l'Autorité publique et l'autre entité – et notamment qu'il s'agisse d'un marché public ou non, pour autant qu'il y ait un lien de droit ou un lien administratif –, l'Autorité publique doit endosser un rôle actif afin que les tiers soient conscients de leurs obligations en matière de gestion des données et responsables du respect de ces obligations.

L'ajout d'une clause exigeant la transparence dans le traitement, l'analyse et l'utilisation des données à caractère personnel améliore la protection des données personnelles.

En imposant une obligation de transparence, les entités qui traitent des données personnelles doivent dévoiler clairement leurs méthodes et objectifs. Cela les oblige à être plus conscients et responsables de leurs actions, réduisant ainsi les abus ou les utilisations négligentes des données personnelles.

En rendant obligatoire l'évaluation et la prise en compte des impacts de l'utilisation des données, les entités sont encouragées à anticiper et à éviter les utilisations abusives ou préjudiciables des données à caractère personnel.

Enfin, l'article impose de qualifier les parties au regard du RGPD (sous-traitant/responsable de traitement) afin de s'assurer des obligations et des droits des parties au partenariat.

Par ailleurs, dans un souci d'harmonisation et de cohérence, toutes les parties doivent être qualifiées conformément au chapitre 2 du présent livre.

L'alinéa 2 rappelle qu'il ne pourrait être exigé de toute autre partie qui ne serait pas une Autorité publique qu'elle mette en œuvre exactement les mêmes obligations que les Autorités publiques visées par le Code et avec la même intensité, lorsque le respect du présent livre ne l'exige pas directement. Le niveau d'exigence des Autorités publiques à l'égard de l'autre partie doit toujours être adapté au regard de la nature des données concernées et de la mission confiée à l'autre entité qui n'est pas une Autorité publique : cette évaluation doit être menée *in concreto*.

Enfin, l'Autorité publique doit être en mesure de vérifier que l'autre partie avec laquelle elle noue un partenariat numérique met effectivement en œuvre, préalablement et durant l'entièreté de l'exécution de sa mission, les obligations de gouvernance convenue.

Le paragraphe 2 présente un éventail non exhaustif des possibles parties avec lesquelles les Autorités publiques pourraient être amenées à conclure des partenariats mixtes de données.

Les prestataires de service d'intermédiation de données sont les prestataires visés par le Règlement sur la gouvernance des données.

En ce qui concerne les prestataires de services informatiques de stockage, il est précisé que cela concerne tant les prestataires de services de stockage physiques que dits « en nuage » ou « cloud ».

Néanmoins, nous rappelons que les services de stockage « cloud » sont généralement exécutés sur des serveurs distants et accessibles via internet. Ces prestataires en particulier peuvent offrir des coûts d'installation et d'entretien plus faibles, et les données peuvent être plus facilement partagées et analysées. Cependant, les données sont stockées sur des serveurs distants et peuvent être plus vulnérables aux risques de fuites et de violations de données. Les Autorités publiques exigent que les prestataires de services en nuage choisis aient, *in concreto*, des protocoles de sécurité et de gestion de données robustes pour protéger les données publiques et qu'ils soient compatibles avec les données concernées.

Par ailleurs, les opérateurs de services de plateformes numériques ne doivent pas se confondre avec le gestionnaire de la Plateforme bruxelloise de la donnée.

L'on notera encore que les exigences détaillées s'apprécient à l'aune du présent Code et des instruments réglementaires européens. Dans le cas où des données sont transférées vers un système juridique sans équivalence – hors de l'Espace Économique Européen, par exemple –, des mesures supplémentaires pourraient alors être nécessaires. On citera, entre autres, les clauses contractuelles standards, ou d'autres mesures de protection.

CHAPITRE 2
Qualification des parties à un partenariat numérique de données

Article C.III.4.
La qualification des parties

Les parties d'un partenariat numérique doivent être qualifiées conformément au présent titre afin de préciser les responsabilités qui sont les leurs.

Une même partie peut recevoir différentes qualifications (producteur, diffuseur, …) selon la fonction qui lui est attribuée dans le cadre du partenariat examiné.

Ainsi, une partie qualifiée de producteur de données peut également être un utilisateur. Cela peut se produire lorsque les données sont utilisées par la personne qui les a collectées.

Par exemple, dans un partenariat numérique, les parties peuvent être, selon le cas, des services d'intermédiation, des prestataires informatiques ou des opérateurs économiques.

À titre d'exemple, la qualification de chaque partie est une condition indispensable à la valorisation des données visée par le chapitre 3 du présent livre et à la réutilisation visée par le livre C.IV. Les responsabilités des parties sont différentes en fonction de leurs qualifications. L'ouverture des données publiques et leur mise en open data ne peut être organisée que dans l'hypothèse où c'est bien une Autorité publique qui se voit qualifiée de producteur des dites données. Il s'agit donc d'identifier de manière prioritaire qui est le producteur de ces données, qui seul pourra décider, par exemple, de leur réutilisation.

Un paragraphe 2 a été ajouté à la suite de l'avis de l'APD de manière à ce que les parties à un partenariat soient également qualifiées au regard du RGPD, soit en tant que responsable de traitement ou en tant que sous-traitants.

Article C.III.5.

Les détenteurs de données

Le Règlement sur la gouvernance des données *définit* le détenteur de données comme suit :

« une personne morale, y compris des organismes du secteur public et des organisations internationales, ou une personne physique qui n'est pas une personne concernée pour ce qui est des données spécifiques considérées, qui, conformément au droit de l'Union ou au droit national applicable, a le droit d'octroyer l'accès à certaines données à caractère personnel ou non personnel ».

Dans un souci d'harmonisation des termes, la même définition a été reprise par le Code dans le livre A.III relatives aux définitions de la partie C.

Nous attirons l'attention sur le fait que les deux rôles peuvent se cumuler, dès lors qu'un producteur peut également diffuser les données.

Article C.III.6.
Les producteurs de données

Le présent article définit qui peut être qualifié de producteur de données et quelles seront les responsabilités qui en découlent.

Le paragraphe 3 liste les responsabilités du producteur de données.

Les qualités de producteur des données et de propriétaire des données ne se confondent pas, bien qu'elles se rejoignent dans de nombreux cas. Le propriétaire de la donnée est celui qui possède l'ensemble des droits sur la donnée. Le producteur des données peut, selon les cas, être une Autorité publique ou un opérateur économique.

Un producteur de données est une entité, qu'elle soit une personne ou une organisation, qui crée, collecte ou génère des données. Les données peuvent être de différentes natures, comme des données à caractère personnel, des statistiques sur le marché, des données météorologiques, etc.

D'un autre côté, un propriétaire de données est une entité qui possède légalement ou détient des droits sur les données. Le propriétaire peut être le producteur de données lui-même ou une autre entité qui a acquis les droits de propriété sur les données.

Premièrement, le producteur de données est chargé de la mise à jour des données qu'il a lui-même produit.

Deuxièmement, le producteur de données est chargé de l'identification de l'ensemble des données qu'il produit. Cette identification est également détaillée dans le cadre de la déclaration de principes selon les conditions visées à l'article C.III.12, mais l'obligation visée à cet article s'impose à l'Autorité publique indépendamment de sa qualité de producteur des données soumises à identification.

Troisièmement, il est généralement admis que c'est le producteur de données qui détermine comment les données peuvent être utilisées ou partagées. Les producteurs de données sont en effet chargés de garantir la qualité et l'intégrité des données, ainsi que de protéger les intérêts de toutes les parties impliquées dans la gestion des données.

Les producteurs de données n'ont pas un pouvoir absolu sur les données et leurs décisions ne doivent pas être considérées comme irrévocables. Ainsi, la possibilité pour le producteur de données de définir les conditions de l'utilisation ou de la mise à disposition, par exemple, doit être lue dans le respect de la réglementation applicable.

Le paragraphe 4 précise que le producteur de données est chargé de la désignation du ou des diffuseurs visés à l'article C.III.7 du présent livre.

Il convient de noter que :

a) le cas échéant, cette désignation est déjà induite par la réglementation applicable, qu'il s'agisse du présent Code ou d'un autre cadre légal;

b) le producteur peut « s'auto-désigner », de telle sorte qu'il cumule les qualités de producteur et de diffuseur;

c) le producteur peut désigner plusieurs diffuseurs de données.

Le paragraphe 5 prévoit que les producteurs sont, en principe, responsables du suivi des demandes formulées par les utilisateurs finaux des données. Cela peut concerner le cas où une personne concernée par des données à caractère personnel veut faire valoir ses droits dans le cadre de procédures déjà prévues par d'autres instruments comme le RGPD, mais cela concerne également tout autre intérêt légitime (droit intellectuel, non-respect d'un droit à la réutilisation, accès, suppression, etc. …) qu'un utilisateur final ferait valoir sur une donnée produite.

Article C.III.7.
Les diffuseurs de données

Il est important de distinguer les deux qualités de producteur et de diffuseur, car cela permet de définir clairement les responsabilités et les obligations de chacun, et d'éviter les malentendus ou les conflits potentiels.

Par exemple, si les données sont incorrectes ou ne respectent pas les normes de confidentialité, le producteur de données sera considéré comme responsable, tandis que le diffuseur de données ne sera considéré que comme responsable de la diffusion de ces données (par exemple pour une question d'accès aux données concernées).

Un diffuseur de données est responsable de la publication et de la mise à disposition des données pour les utilisateurs. Il peut, par exemple et dans le cadre du champ d'application du présent Code, s'agir d'une plateforme de données ouvertes comme celle visée au livre C.V ou d'un portail communal confié à un prestataire informatique.

Le paragraphe 3 traite de la question du format des données, laquelle est capitale. L'obligation formulée à l'égard des diffuseurs est de privilégier des formats qui répondent aux conditions énoncées. Le format à privilégier doit être :

1° ouvert : en effet, plus le format des données est ouvert, plus ces données sont susceptibles d'être facilement réutilisées et exploitées;

2° lisible par une machine. Cela signifie que les données doivent être organisées et formatées de manière à ce qu'une machine puisse les comprendre et les utiliser. Un jeu de données n'est pas lisible pour une machine si les données ne sont pas structurées de manière logique ou si elles ne sont pas dans un format compatible avec les programmes informatiques qui les utilisent. Par exemple, un jeu de données en format PDF ou image ou en papier ne serait pas lisible pour une machine car les données ne sont pas structurées et il n'y a pas de moyen de les extraire;

3° accessible, traçable et réutilisable;

4° avec les métadonnées.

Si le diffuseur fait appel à des services algorithmiques, il y a lieu de renvoyer, le cas échéant, à l'article C.III.20 concernant la gestion des modèles analytiques, des algorithmes et des systèmes exploitant l'intelligence artificielle;

Néanmoins, le paragraphe 4 précise qu'il n'existe aucune obligation de format nommément identifiée, au-delà des conditions précitées. Cela laisse la possibilité aux diffuseurs d'opter pour le format le plus adapté au regard des évolutions technologiques en vigueur au moment du choix d'un format pour la diffusion d'un jeu de données en particulier.

Le paragraphe 4 précise que, dans le cas où les données sont diffusées, la conversion vers un format ouvert doit être réalisée en amont de la diffusion.

Le paragraphe 5 renvoie à l'article C.III.6.

Article C.III.8.
Les gestionnaires de données

Outre les producteurs et les diffuseurs de données, certains rôles clefs d'un partenariat doivent également être identifiés : il s'agit des rôles d'administration.

Les administrateurs de base de données, de sécurité, système et les administrateurs réseau ont tous des rôles différents dans la gestion d'un système informatique : bien que ces rôles peuvent être remplis par les mêmes personnes en fonction du partenariat numérique, il est important de les distinguer lorsque l'on parle d'un partenariat numérique de données

publiques afin d'établir les responsabilités qui en découlent.

Un administrateur de base de données (ou DBA, pour Database Administrator) est une personne responsable de la gestion et de l'entretien d'une ou plusieurs bases de données. Les tâches d'un DBA peuvent inclure la planification, l'installation, la configuration, la mise à niveau, la sauvegarde, la restauration, la sécurité, la performance et la surveillance des bases de données. Il peut également être responsable de la mise en place de politiques et de procédures pour garantir la qualité des données et la disponibilité des bases de données pour les utilisateurs.

Par ailleurs, voici quelques exemples de cas d'application de mise en cause de la responsabilité des administrateurs de sécurité, d'administrateur système et d'administrateur réseau :

1° Administrateur de sécurité :

a) une violation de données a eu lieu en raison de la mauvaise configuration des pare-feu;

b) des données sensibles ont été volées car les politiques d'accès n'étaient pas suffisamment strictes;

c) des données ont été modifiées ou détruites par un utilisateur non autorisé car il n'y avait pas de surveillance efficace des activités de l'utilisateur;

2° Administrateur système :

a) un système a été infecté par un virus car il n'a pas été mis à jour;

b) des données ont été perdues car une sauvegarde n'a pas été effectuée correctement;

c) les utilisateurs ont rencontré des problèmes techniques qui n'ont pas été résolus de manière efficace;

3° Administrateur réseau :

a) une interruption de service a été causée par un problème de configuration de l'équipement réseau;

b) les données ont été interceptées par un tiers car les politiques de sécurité du réseau n'étaient pas suffisamment strictes;

c) la bande passante a été surchargée car il n'y avait pas de planification adéquate pour gérer les besoins en bande passante croissants.

Il pourrait arriver qu'une Autorité publique valorise ou partage des données en dehors de tout partenariat numérique de données. Dans ce cas, l'Autorité publique revêt elle-même les différentes qualités d'administrateur listées.

Le dernier paragraphe vise à inciter les Autorités publiques à se mettre en règle mais également à vérifier les responsabilités de chaque partie avec lesquels elle travaille en matière de données numériques. À défaut, l'ensemble des responsabilités leur sont attribuées, que le partenariat ne concerne qu'une Autorité publique (dans le cadre d'un partenariat mixte de données) ou plusieurs (dans le cadre d'un partenariat public de données).

CHAPITRE 3
La catégorisation des données

Article C.III.9.
La catégorisation des données

Dans la cadre de la mise en place d'une gouvernance de données publiques applicable à l'ensemble des Autorités publiques visées par le présent Code, il convient de fixer un cadre harmonisé de catégories applicables aux données publiques afin de les identifier et de leur garantir des traitements uniformisés au travers d'une nomenclature qui sera partagée par toutes les Autorités publiques concernées. Cette nomenclature/catégorisation commune est un préalable nécessaire à la mise en place optimale du Catalogue des données visé au livre C.V.

Implémenter une nomenclature de données claire et commune est crucial pour établir une gouvernance des données effective pour plusieurs raisons :

1. **Interprétabilité** : une nomenclature commune permet à toutes les parties prenantes de comprendre les données de la même manière, facilitant ainsi la communication et la collaboration.

2. **Intégrité des données** : une nomenclature standardisée aide à maintenir la qualité et la cohérence des données en s'assurant que tous utilisent les mêmes définitions et formats. Cela réduit les erreurs et les incohérences dans la collecte, le traitement et l'analyse des données.

3. **Efficacité** : la standardisation des données permet une gestion plus efficace des ressources, car elle réduit le temps et les efforts nécessaires pour convertir, comparer ou intégrer des données provenant de sources différentes.

4. **Conformité légale** : dans le contexte du RGPD ou de l'OpenData et d'autres législations sur les données, une nomenclature claire aide les Autorités publiques à s'assurer de la conformité au cadre légal en facilitant la traçabilité, l'audit et la gestion des consentements, ainsi que la protection des données personnelles.

5. **Interopérabilité** : une nomenclature commune améliore l'interopérabilité entre différents systèmes d'information, ce qui est essentiel pour le partage de données et la collaboration entre différentes Autorités publiques.

La création d'un cadre harmonisé permet ainsi de garantir, d'une part, la confidentialité et la sécurité des données pertinente, et d'autre part, la transparence et la responsabilité des acteurs grâce à la publication des données en open data.

Le paragraphe 1er exprime l'obligation pour les Autorités publiques d'identifier et de classifier les données conformément au présent chapitre. Il est important de préciser que la catégorisation proposée est un cadre minimal sur lequel peuvent venir se greffer d'autres catégories identifiées selon le cas par les Autorités publiques ou tout autre partie. il est envisageable que de nouvelles classifications, ou de nouveaux types de données apparaissent au fil des usages.

Chaque donnée est identifiée au regard de chacune des classifications proposées en vue de générer les métadonnées telles que prévues par le titre 4. Cela permet de générer des métadonnées (données qui fournissent des informations sur d'autres données) utiles et compréhensibles pour tous puisque les catégories de données sont normalisées au travers de la nomenclature commune. Chaque utilisateur peut donc récupérer les données pertinentes pour ses besoins.

Ces métadonnées sont nécessaires à la mise en place du Catalogue, institué par le présent Code, qui reprendra uniquement les métadonnées des jeux de données qu'il renseigne. Il faut donc que toutes les Autorités publiques soumises à la partie C du Code puisse identifier les jeux de données visés par le Catalogue selon les catégories de données définie par les Code et annoncées par l'article C.III.9.

Cette catégorisation commune vise à s'assurer que les métadonnées générées sont compréhensibles et pertinentes peu importe le point de vue de l'utilisateur. Cela signifie que, que l'on soit un analyste, un gestionnaire de données, un décideur, ou un auditeur externe, les métadonnées fournissent une information claire et immédiatement utile sur les données concernées.

Chaque catégorie de donnée est encadrée par un ensemble de dispositions juridiques et administratives (par exemple le RGPD pour les données à caractère personnel, les respect des droits d'auteurs pour les données protégées par des droits intellectuels, …).

Le paragraphe 2 rappelle qu'une même donnée peut revêtir plusieurs caractéristiques à la fois et dès lors appartenir à plusieurs catégories.

Ainsi, une donnée à caractère personnel peut-être ouverte ou fermée, et peut donc parfois figurer dans une base « open data ». Le nom d'auteur d'un livre est une donnée ouverte qui peut figurer dans un catalogue tandis que le même nom, associé à l'attribution d'une adresse de domicile est une donnée personnelle fermée qui n'a pas vocation à se retrouver dans le Catalogue des données. De la même manière, une donnée privée peut-être donc être ouverte.

Enfin, le paragraphe 3 rappelle qu'un jeu de données peut comprendre plusieurs catégories de données proposées par le présent titre. L'Autorité publique devra veiller à s'assurer pour chacune des donnée le respect du ou des cadres légaux et du ou des cadres techniques qui s'y appliquent.

Par exemple, lorsqu'un jeu de données contient des données à caractère personnel qui sont fournies librement, il faut tenir compte du RGPD pour l'aspect légal (base légale, licéité du traitement et finalité etc.) mais aussi du fait que ces données doivent être sécurisées techniquement bien plus qu'une donnée publique observée qui peut/le cas échéant doit être publiée en open data. En effet, il y a toujours un cadre légal et un cadre technique propre à chaque catégorie dont il faut tenir compte.

Article C.III.10.
Typologie des catégories de données

Fournir une classification précise permettra d''identifier de manière harmonisée les données concernées afin que tant l'Autorité publique détentrice que toutes les autres Autorités publiques, ou toute autre partie, puisse connaître rapidement le régime juridique à appliquer aux données. L'objectif de la typologie présentée ici est d'être utilisée de manière transversale chaque fois que des données sont traitées par des Autorités publiques. L'objectif est notamment que cette typologie des données permette de faire remonter vers le Catalogue des données mis en place au niveau de la Plateforme bruxelloise de la donnée du livre C.V les informations concernant les données répertoriées conformément à cette classification des données.

Le paragraphe 1er prévoit une catégorisation basée sur le régime de propriété des données. Ce régime est pertinent en ce que qu'il permet aux autorités d'en déduire qui est responsable de la collecte, du traitement, des protections et de réglementer en conséquence les réutilisations éventuelles qui peuvent en découler et la matière dont elle doit être encadrée.

Le paragraphe 2 prévoit une catégorisation basée sur la manière dont les données ont été produites.

Les données déduites sont des informations qui sont obtenues par raisonnement logique ou inférence à partir de données existantes. Elles ne sont pas mesurées ou observées directement, mais sont déduites à partir de données brutes ou d'autres informations connexes. Par exemple, si vous avez un ensemble de données qui indiquent le chiffre d'affaires d'une entreprise au cours des cinq dernières années, vous pouvez déduire que la croissance annuelle moyenne est de X %. Cette donnée déduite est obtenue en effectuant un calcul mathématique à partir des données brutes disponibles.

Les données dérivées, en revanche, sont des informations qui sont obtenues à partir de mesures ou d'observations directes de phénomènes physiques. Elles sont généralement obtenues par l'application de formules mathématiques ou de calculs à des données brutes.

Il est envisageable, en effet, que des données soient fournies directement pas les personnes ou entités concernées, soient observées par les Autorités publiques – par exemple au travers d'outils de mesure (en matière de mobilité ou de qualité de l'air), soient dérivées de données déjà détenues par les Autorités publiques (l'on pense à des statistiques établies sur la base de données initiales) ou déduites de ces mêmes données, ou soient acquises à titre gratuit ou à titre onéreux auprès de tiers.

Le paragraphe 3 prévoit une catégorisation basée sur le degré d'ouverture des données. Les différents degrés d'ouverture d'un jeu de données sont « fermés », « partagé » et « ouvert » et permettront de distinguer les données qui alimentent le Catalogue des données de celles qu'il convient de ne pas partager.

Ces différentes notions font l'objet des définitions dans le livre A.III.

À cet égard, un rappel s'impose quant à la distinction à opérer entre les données « ouvertes » et les données « partageables » :

1° les données ouvertes sont des données qui sont librement accessibles;

2° les données partageables, quant à elles, sont les données ouvertes des Autorités publiques dont la réutilisation peut-être plus ou moins conditionnée (redevance, licence, accord d'exclusivité).

Dans le cas où un jeu de données implique différents types d'accès eu égard aux données le composant, les Autorités publiques adoptent pour le jeu de données le niveau d'accès le plus restrictif.

Le paragraphe 4 a été modifié afin d'introduire à la suite de l'avis de l'APD une distinction entre les données à caractère personnel confidentielles et non confidentielles. L'ajout d'une clause exigeant la transparence dans le traitement, l'analyse et l'utilisation des données à caractère personnel améliore la protection des données personnelles.

En imposant une obligation de transparence, les entités qui traitent des données personnelles doivent dévoiler clairement leurs méthodes et objectifs. Cela les oblige à être plus conscients et responsables de leurs actions, réduisant ainsi les abus ou les utilisations négligentes des données personnelles.

En rendant obligatoire l'évaluation et la prise en compte des impacts de l'utilisation des données, les entités sont encouragées à anticiper et à éviter les utilisations abusives ou préjudiciables des données personnelles.

Enfin, l'article impose de qualifier les parties au regard du RGPD (sous-traitant/responsable de traitement) afin de s'assurer des obligations et des droits des parties au partenariat.

Le paragraphe 5 prévoit une catégorisation fondée sur les dommages potentiels liés au traitement des données. L'évaluation menée par l'Autorité publique en vue de la qualification des données sous cet angle doit comprendre l'ensemble des mesures visant à réduire les risques à un niveau acceptable, c'est-à-dire la gravité potentielle et la probabilité de divulgation de l'information. De plus, pour déterminer le niveau de sensibilité et la valeur de l'information, il faut tenir compte à la fois du degré de dommage potentiel dans le cas de divulgation (divulgation non autorisée, modification ou perte) ainsi que de la valeur potentielle des données. La détermination du risque permettra de qualifier la donnée en tant que donnée sensible ou donnée classifiée.

La liste de catégories de données dressée n'est bien entendu par exhaustive.

TITRE 3
La valorisation des données détenues par les Autorités publiques

Article C.III.11.
La valorisation des données

La valorisation de données est au centre de tout projet lié aux données. Cette valorisation se doit d'être responsable et éthique.

À titre préliminaire, il faut comprendre que la valorisation vise l'enrichissement, le renforcement ou l'amélioration des connaissances relatives aux données existantes de manière à leur conférer une certaine valeur. Cet avantage pourrait, entre autres, être un avantage économique, en l'espèce numérique. Les objectifs liés à un projet de valorisation de données sont très variés et dépendent du champ d'application concerné.

Par la valorisation des données, les Autorités publiques vont faire des données de véritables biens publics concourant à l'amélioration de l'efficacité de leurs services et de la mise en œuvre de leurs missions. À ce jour, beaucoup d'Autorités génèrent des données, sans avoir conscience de la valeur qu'elles possèdent. Cette méconnaissance du patrimoine numérique bruxellois peut aboutir à des opportunités manquées et engendrer des pertes financières (par ignorance des traitements qui peuvent être mutualisés par exemple) ou par la mise en cause de responsabilités à la suite de fuites de données insuffisamment sécurisées, faute de prise en considération de leur importance ou de leur sensibilité.

Le titre 3 a pour objectif de permettre aux Autorités publiques d'augmenter leur capacité à adapter et mettre en place des solutions en partant des données dont elles disposent ou pourraient disposer. Dans ce cadre, les Autorités publiques doivent adopter une démarche de résolution de problèmes à l'aide de données.

Les Autorités publiques sont invitées à investir dans la création de processus, de compétences et de ressources leur permettant de mieux valoriser leurs données.

Les données identifiées, classées et gérées conformément aux principes du chapitre 3 du titre 2 vont être valorisées de manière à améliorer concrètement la relation des Autorités publiques avec les citoyens, améliorer la connectivité de tout un chacun mais également permettre à des acteurs économiques de tout type de fournir de nouveaux services fondés sur les données détenues à ce jour par les Autorités publiques (services d'optimisation de la mobilité, création d'interface numérique multiservices mixte Autorité public/employeur, système de collecte et recyclage de déchets avec incitants, objets connectés sur la voie publique, etc.)

Cette classification devra également permettre la mise en place d'une architecture dite DATA CENTRIC.

De manière théorique, on peut noter que la valorisation des données peut revêtir différentes formes. La doctrine distingue par exemple (voir à cet égard L.-D., Benyayerd, S., Chignard, Datanomics, FYP Editions, Paris, p. 49) :

1° *« quand elles sont revendues par ceux qui les collectent ou les agrègent, les données prennent une forme de matière première.*

2° *quand elles sont utilisées sans marchandisation, par exemple pour réduire des coûts ou développer les revenus, elles prennent une forme de levier.*

3° *quand elles constituent une arme stratégique pour défendre ou conquérir une position concurrentielle, elles prennent une valeur d'actif. ».*

Dans le cas des Autorités publiques, la majorité des cas de valorisation se rapportent à la mise en place de leviers. Les données détenues par les Autorités publiques seront notamment et principalement utilisées et partagées pour :

1° prendre de meilleures décisions et réduire les coûts de fonctionnement des Autorités publiques;

2° offrir de meilleurs ou de nouveaux services aux citoyens.

Il ne faut pas pour autant oublier que les données produites par les Autorités publiques peuvent être utilisées par des opérateurs privés pour d'autres types de valorisation.

L'objectif est donc au minimum double :

1° permettre une meilleure gestion interne des services publics et des obligations d'intérêt général des Autorités publiques, par une meilleure valorisation des données; identifier les données qu'une Autorité publique possède lui permettra d'optimiser ses process internes et sa relation avec ses administrés, de sécuriser davantage les données et d'augmenter la confiance qui en découle,

2° permettre de véritables partages de données dans le cadre de réutilisations ou entre Autorités publiques (*open data*/réutilisation de données protégées ou application du *once only*) grâce à une meilleure gestion interne des données prêtes à l'usage pour d'autres Autorités publiques ou tout opérateur économique intéressé. La déclaration de principe permettra de mettre en place les bases (métadonnées et données de références) de ce qui constitue le Catalogue des données de la Plateforme bruxelloise de la donnée (voir le livre B.V).

L'opérationnalisation de la valorisation passe par des actions concrètes et l'attention portée à des points essentiels qui garantissent, s'ils sont mis en place, une valorisation responsable et éthique des données.

Une gestion efficace et cohérente des données, telle que décrite au titre 4 du présent livre, représente une condition *sine qua non* à la valorisation des données. Il ne semble pas possible de valoriser de manière éthique et responsable des données sans en assurer une gestion efficace et cohérente. La valorisation n'est cependant pas l'unique finalité de la gestion des données. Certaines données doivent faire l'objet de mesures de gestion importantes à d'autres fins que la valorisation en vue d'un éventuel partage.

CHAPITRE 1
La déclaration de principes

Article C.III.12.
La déclaration de principes

La déclaration de principes est un document informatif dont l'objectif est de fournir des informations quant à la gestion des données au sein de chaque Autorité publique. Par la déclaration de principes, les informations utiles seront fournies au Bureau de la donnée et au gestionnaire de la Plateforme bruxelloise de la donnée.

Les Autorités publiques ont l'obligation de mettre en place une déclaration de principes qui a pour objectif :

1° de décrire globalement l'action actuelle de l'Autorité publique dans le cadre de sa politique en matière de données;

2° d'illustrer de manière concrète la manière dont les principes directeurs, objectifs stratégiques et objectifs opérationnels décrits au livre C.II sont respectés et mis en œuvre;

3° de synthétiser sa situation actuelle concernant les données que l'Autorité publique détient et les actions à mettre en place afin de permettre ou d'améliorer la valorisation et, lorsque cela est pertinent, le partage de ces dernières.

La déclaration de principe permet notamment une remontée d'information de l'Autorité publique vers le Bureau de la donnée et le Comité de concertation. Elle informe également tout tiers sur la gestion numérique de chaque Autorité publique.

La déclaration de principe peut être mise à jour sur une base annuelle. En aucun cas, la déclaration de principes ne doit être un outil de gestion opérationnelle des données. Les aspects opérationnels sont traités dans des outils spécifiques comme le Catalogue des données.

Le Bureau de la donnée peut proposer des modèles en vue d'établir des standards en matière de déclaration de principe.

La déclaration de principes doit exposer :

1° Le modèle opérationnel mis en place pour gérer les données

Le modèle opérationnel reprend les rôles et responsabilité de l'Autorité concernant les différentes bases de données qu'elle détient.

L'Autorité publique indique notamment l'identité de l'administrateur local des données, du ou des responsables en matière de sécurité, l'identité du DPO, ainsi que tout autre organe de gouvernance mis en place.

2° La manière dont les données qu'elle détiennent sont gérées, documentées, décrites, organisées et formatées sous forme de jeux de données, de données de contenu, de données de référence et de métadonnées

Dans ce cadre, l'Autorité publique est amenée à définir ses priorités en vue d'établir sa stratégie au regard des données à valoriser en priorité, comme exposé à l'article C.II.14.

3° Accessibilité

La question de l'accessibilité des sites des Autorités est également reprise dans la déclaration de principes. Il s'agit d'une application du principe directeur de transparence. Les autorités doivent distinguer les données (ou le contenu) considérées comme accessibles et celles qui ne le sont pas, ainsi que les justifications qui en découlent. Cela peut concerner, par exemple, les données de contact de l'administration ou celles des différentes informations de contact qui pourraient être impli-

quées dans la gestion de la donnée (données protégées, actualisation).

Pour rappel, la manière dont on peut accéder au site d'une Autorité publique est en soi une donnée qui décrit l'accessibilité générale à l'Autorité, à ses services et aux données qu'elle utilise.

Actuellement, la matière est réglée par l'ordonnance du 4 octobre 2018 relative à l'accessibilité des sites internet et des applications mobiles des organismes publics régionaux et des communes, qui transpose la Directive (UE) 2016/2102 du Parlement européen et du Conseil du 26 octobre 2016 relative à l'accessibilité des sites internet et des applications mobiles des organismes du secteur public. Cette directive n'a pas été transposée par le COCOF et la COCOM, de sorte que seules les Autorités publiques qui dépendent de la Région bruxelloise y sont soumises.

4° La manière dont l'Autorité publique compte atteindre l'objectif stratégique d'exploitation efficiente et responsable

Il est essentiel de démontrer l'application du principe d'exploitation efficiente et durable notamment en matière de conservation des données qui est l'un des postes les plus énergétiques.

Une donnée qui est traitée de manière plus respectueuse de l'environnement à une valeur plus importante et s'inscrit dans une gestion circulaire.

Cet objectif stratégique est repris dans la déclaration de principes dans la mesure où il est difficile pour les tiers d'avoir une vision, en dehors de la déclaration de principes, sur la manière dont cet objectif est implémenté au sein de chaque Autorité publique. En effet, la prise en compte de cet objectif est moins visible de prime abord que les autres principes et objectifs visés dans le livre C.II qui transparaissent au niveau de la gestion générale des données.

5° En cas de recours à des traitements algorithmiques, la manière dont sont gérés et documentés les principaux traitements algorithmiques utilisés dans l'accomplissement des missions de service public ou les obligations d'intérêt général. L'utilisation de mécanismes automatisés de traitement ne dispense pas l'Autorité publique de la transparence à l'égard de la manière dont ces traitements sont organisés.

Ces informations sont récupérées automatiquement du Catalogue des données.

6° Les modalités d'application de redevances en cas de réutilisation des données

Le calcul du coût d'une réutilisation permet d'influencer la valeur d'une donnée pour le réutilisateur qui doit répercuter ce coût dans la gestion de son utilisation des données réutilisées.

Le calcul du coût d'une réutilisation permet par ailleurs à l'administration d'anticiper, le cas échéant, tout dispositif technique nécessaire afin d'optimiser l'usage des données concernées.

Par exemple, si une Autorité publique permet une réutilisation statistique de données à caractère personnel, il lui appartiendra de financer une interface de mise à disposition et d'anonymisation pour un service d'intermédiation et de partage. Le coût de mise en place de cette interface pourrait être répercuté dans une redevance.

Ces informations sont récupérées automatiquement du Catalogue des données.

7° L'organisation d'accord d'exclusivité

Le Règlement sur la gouvernance des données et la directive ISP limitent les conditions dans lesquelles de tels accords peuvent être conclus.

Des jeux de données qui sont réservés pour certains opérateurs privés présentent une valeur économique importante sur le marché concerné dès lors que ces opérateurs pourront valoriser le fait d'être les seuls à disposer des jeux de données concernés. Partant, Il convient de le renseigner par application du principe de transparence.

Ces informations sont récupérées automatiquement du Catalogue des données.

8° Tout autre élément pertinent présentant une importance particulière au regard de la stratégie numérique mise en place par l'Autorité publique dans le cadre de son activité spécifique

Un dernier cas de figure est ajouté afin de permettre à chaque Autorité publique de personnaliser sa déclaration de principes et y reprendre les autres principes et objectifs du livre B.II qui prendraient le cas échéant dans le cadre de leur politique numérique une importance particulière, pour laquelle une communication s'impose.

CHAPITRE 2
La valorisation des données d'usage

Article C.III.13.
Valorisation des données d'usage

Les données d'usage peuvent servir aux Autorités publiques qui les collectent essentiellement pour améliorer la qualité de leurs services numériques et la manière dont ils sont proposés.

La valorisation des données d'usage permet aux Autorités publiques de personnaliser et de rendre plus ergonomiques ou « *user friendly* » leurs services numériques, dans une optique d'amélioration continue du service public ou des obligations d'intérêt général qu'elles assurent.

Le point 3 de l'article permettrait par exemple à une autorité qui a récolté des données d'usage sur les collectes de déchet ou le tri d'informer d'autres citoyens d'une même zone géographique des possibilités de tris ou de collecte existant dans la même zone.

La représentation d'un usager fait référence à la création d'une image en fonction de son comportement et de ses interactions avec un service public. Cela implique l'analyse des données collectées lors de l'utilisation d'un service pour comprendre les habitudes, les préférences et ses besoins afin d'améliorer les interactions avec l'Autorité publique.

Conformément à la demande de l'APD, les paragraphes 2 et 3 ont été ajoutés afin de préciser les finalités de traitements des données d'usage qui seraient également des données à caractère personnel. Les éléments essentiels de ce traitement sont également mentionnés.

CHAPITRE 3
Le respect des droits sur les données protégées

Article C.III.14.
Le respect des droits des tiers
sur les données protégées

La valorisation des données ne peut faire obstacle au respect des droits détenus par des tiers sur les données protégées. L'étendue de ces droits, en outre, ne peut être modifiée par la valorisation des données.

C'est ce principe que contient le paragraphe 1er.

Le paragraphe 2, alinéa 1er, rappelle que tout traitement doit reposer sur une base légale valide. En l'occurrence, en ce qui concerne les données à caractère personnel, l'article 6 du RGPD impose l'obligation de disposer d'une base légale pour organiser un traitement de données personnelles dans le cadre légal prévu.

Or, le traitement des autres types de données doit également disposer d'une base légale pour pouvoir être effectué. Il convient donc de prévoir une base légale pour les autres données protégées que les Autorités publiques viendraient à traiter dans le cadre de leurs missions (secrets d'affaires et commerciaux, droits d'auteur, secrets statistiques), à savoir l'autorisation des titulaires des droits sur ces données.

En effet, il semble qu'à ce jour, certaines données protégées qui ne sont pas des données à caractère personnel soient traitées sur la base d'une autorisation implicite et, d'une certaine manière, absolu, vu qu'aucun cadre légal ne la détermine ou la limite. Dans ces cas, il semble que la finalité complète du traitement ne soit à aucun moment complètement explicite, de sorte qu'un risque important en résulte tant pour les titulaires de droits sur ces données que dans le chef de celui qui traite, dès lors qu'il ne connaît pas l'étendue exacte des droits visés.

Ainsi, par exemple, si des secrets d'affaires sont transmis à des Autorités publiques par des opérateurs économiques afin d'obtenir des aides financières ou des subsides, le fait de transmettre des informations suppose l'autorisation de l'intéressé pour le traitement de ses données protégées afin d'obtenir les aides financières et les subsides visés. Toutefois, cette autorisation implicite ne porte pas sur l'éventuelle valorisation (ex. analyse statistique) et sur le partage de ces données, lesquels supposent une véritable autorisation explicite afin de garantir la sécurité juridique de ces autres traitements et les droits des opérateurs économiques.

Ainsi, moyennant autorisation et occultation des données protégées à caractère non personnel, ces dernières pourront être partagées aux conditions fixées par l'article 11 du Règlement sur la gouvernance des données.

Le consentement ou l'autorisation apparaît comme un point crucial de la valorisation en ce qui concerne les données protégées. En effet, en l'absence de consentement ou d'autorisation, leur réutilisation sera possible (ou non), et des processus pourront ou non être mis en place en vue du partage, ce qui impactera également le coût de leur réutilisation éventuelle.

L'alinéa 2 envisage la mise en place d'une méthode de consentement ou d'autorisation dite « dynamique ».

Cette méthode, également utilisée dans d'autres parties du monde –- voir notamment l'exemple canadien repris i.a. dans S., Gagnon-Turcotte, M.,

Schulthorps, S. Coutts, *Les partenariats de données numériques : mettre les bases d'une gouvernance de données collaborative dans l'intérêt public*, Nord Ouvert, Montréal, 2021, pp. 60 et suivants — garantit une réutilisation correcte des données dans le temps. Ce mécanisme d'obtention du consentement ou de l'autorisation au cours de multiples phases de la collecte et du traitement des données offre généralement des options granulaires à différents moments du cycle de vie des données. Au fur et à mesure de l'évolution de la vie de la donnée, il convient de demander le consentement ou l'autorisation d'utilisation (ou la réutilisation) d'un même ensemble de données à caractère personnel ou d'autres données protégées (par exemple des secrets d'affaires ou des informations commerciales) chaque fois que les finalités de la collecte, du traitement, du partage de ces données changent.

Lorsque les Autorités publiques proposent cette fonctionnalité, ils veillent à ce que cette méthode « dynamique » du consentement ou de l'autorisation respecte les exigences du RGPD ou du Règlement sur la gouvernance des données lorsque le partage concerne des données protégées. Lorsqu'un organisme public a l'intention de partager les données protégées pour une finalité différente de celle pour laquelle les données ont été collectées, il en informe préalablement les titulaires de droits sur ces données, en décrivant tout nouveau risque résultant de ce partage secondaire. Les personnes doivent avoir la possibilité de retirer leur consentement ou leur autorisation si elles ne sont pas ou plus favorables au partage secondaire de leurs données.

Le paragraphe 3 rappelle aux Autorités publiques l'ensemble des mécanismes procéduraux visant à protéger la confidentialité des données qu'elles doivent mettre en place lors du traitement de données protégées.

En ce qui concerne particulièrement les données à caractère personnel, l'anonymisation et la pseudonymisation sont des processus visant à rendre négligeable le risque qu'une personne physique soit identifiée au moyen de certaines données.

Le RGPD définit ces deux notions mais ne dit pas dans quel cas il faut y recourir.

Pour l'application du présent Code et dans le cadre de la valorisation des données, ces méthodes doivent être appliquées en fonction des risques liés à l'utilisation ou la réutilisation des données visées. Ainsi, un partage administratif entre Autorités publiques n'implique pas les mêmes risques qu'une réutilisation.

Les techniques d'anonymisation peuvent viser différents degrés d'identifiabilité des données. La norme ISO/IEC 19441 (développée pour assurer l'interopérabilité et la portabilité des données dans le cadre de services infonuagique) distingue cinq catégories à cet effet :

1° Données identifiables : données qui peuvent être associées sans ambiguïté à une personne particulière parce que des renseignements permettant d'identifier cette personne y sont observables.

2° Données pseudonymisées : données dans lesquelles tous les identificateurs sont remplacés par des pseudonymes, la fonction d'attribution étant telle que les remplacements ne peuvent pas être inversés au moyen d'efforts raisonnables par une personne différente de celle qui les fait.

3° Données pseudonymisées non liées : données dans lesquelles tous les identificateurs sont effacés ou remplacés par des pseudonymes, la fonction d'attribution étant effacée ou irréversible, de sorte que les liens ne puissent pas être rétablis par des efforts raisonnables, y compris de la part de l'entité qui a effectué l'opération.

4° Données anonymisées : données non liées dont les attributs sont modifiés (par exemple, par randomisation ou généralisation de leurs valeurs) de façon à ce que ces données seules ou combinées à d'autres données ne permettent pas d'identifier directement ou indirectement une personne avec un niveau de confiance raisonnable.

5° Données agrégées : données statistiques qui ne contiennent pas d'entrées de niveau individuel et qui sont classées au moyen de renseignements sur tellement de personnes différentes que les attributs de niveau individuel ne sont pas identifiables.

Dans le cadre de l'application du présent Code, il est demandé que les Autorités publiques adaptent les techniques d'anonymisation en fonction de l'identifiabilité des données telle qu'elle est envisagée ci-dessus.

L'alinéa 3 envisage la nécessité d'occulter certaines données préalablement à leur partage.

Il existe deux hypothèses dans lesquelles le partage de données protégées peut avoir lieu sans occultation :

1) si une disposition législative ou réglementaire autorise un tel partage sans occultation;

2) si les personnes disposant des droits sur les données protégées ont donné leur consentement à un traitement non occulté.

En dehors de ces hypothèses, les données protégées doivent être occultées.

Enfin, le paragraphe 4 prévoit que les Autorités publiques sont tenues d'organiser les recours *ad hoc* afin de permettre aux personnes détenant des droits sur les données de s'assurer de leur respect. En effet, bien que le RGPD organise déjà ce type de recours en ce qui concerne les données à caractère personnel, les développements qui précèdent démontrent la nécessité de prévoir de tels recours dans les autres cas de figure envisageables, notamment en cas de réutilisation par les services d'intermédiation (Règlement sur la gouvernance des données).

L'article C.III.14, § 4, est établi sans préjudice de la compétence de l'autorité de protection des données compétente pour les recours en matière de données à caractère personnel.

Les Autorités publiques fournissent des canaux par lesquels les personnes physiques et morales du secteur privé peuvent soumettre des plaintes ou des problèmes concernant les données protégées à l'égard desquelles ils détiennent des droits.

Ces plaintes et problèmes doivent permettre aux Autorités publiques de contribuer à améliorer, à maintenir la qualité de la donnée ou à se conformer aux dispositions légales applicables notamment en matière de données protégées y compris en matière de données personnelles.

L'article C.III.14, § 5, envisage un processus de plaintes qui doit se distinguer d'un processus de réclamation plus élaboré.

CHAPITRE 4
L'évaluation des risques

Article C.III.15.
Évaluation des risques

Dans le cadre de la valorisation de leurs données, les Autorités publiques doivent mener une évaluation des risques relatifs aux données, notamment les données à caractère personnel, les secrets d'affaires et les données classifiées. Bien que cette évaluation soit déjà prévue par le RGPD pour ce qui concerne les données à caractère personnel, il semble opportun d'en étendre la portée à l'ensemble des types de données à valoriser.

Les Autorités publiques choisissent des outils et des méthodologies qui ont pour objectif de calibrer et d'opérationnaliser leurs obligations légales, par exemple en matière de protection de la vie privée ou de secret d'affaires, contenus dans les lois et Règlements, en fonction des risques et avantages réels posés par l'utilisation des données proposées.

De manière concrète, une Autorité publique doit être en mesure d''effectuer un choix éclairé quant à la localisation – hors de l'Union Européenne ou dans l'Union Européenne, par exemple – de la solution d'hébergement qu'elle choisit selon que les données soient protégées ou non, cryptées ou non, ou en fonction de la nature de ces données. Elle peut bien entendu être appuyées dans ces choix par le Bureau de la donnée.

L'évaluation des risques vise à identifier en amont les menaces pesant sur les données ou les préjudices pouvant découler du traitement des données et de retracer leurs causes.

Les Autorités publiques doivent réaliser une évaluation des risques liés à la protection des données en tenant compte des informations à leur disposition quant :

1° à la nature des données à traiter, selon qu'elles soient, entre autres, à caractère personnel, de nature commerciale ou grevées de droits de propriété intellectuelle. Ces types de données sont, par nature, particulièrement sensibles au regard de secrets commerciaux, des libertés et des droits fondamentaux et méritent une protection spécifique;

2° au type d'opérations à réaliser. Par exemple, le « profilage » est un type d'opération comportant des risques élevés possibles pour les titulaires de droits. Nous attirons l'attention sur le fait que cela peut également concerner d'autres types de données que les données à caractère personnel, comme par exemple les données issues de secrets d'affaires;

3° à la portée des opérations de traitement et leur contexte (en ce compris la portée environnementale de l'opération). Ainsi, la réalisation d'opérations sur les données concernant un grand nombre de personnes est un facteur qui peut accroître les risques. Le contexte des opérations de traitement renvoie également aux catégories de titulaires de droits sur les données concernées (les risques ne seront pas similaires concernant les secrets d'un ensemble de startup, l'identification du personnel des Autorités publiques et leur lieu de travail, rôle et tâches des personnes, des données concernant des enfants, par exemple), l'incidence éventuelle

de l'environnement (le préjudice éventuel causé à des personnes en raison de leur culture spécifique, par exemple), etc.;

4° aux finalités des traitements et à leur durée (par exemple gérer des communications par courrier électronique sur une durée particulière, évaluer la performance des membres du personnel sur une année, stocker et traiter des illustrations et des vidéos des séquences de vidéosurveillance pour une durée plus ou moins longue).

TITRE 4
La gestion des données

Article C.III.16.
La gestion des données

La notion de gestion des données couvre l'ensemble des besoins relatifs aux données d'une organisation, en l'occurrence les Autorités publiques visées par le Code. La gestion des données tend à les valoriser en tant que biens publics de nature numérique de la manière décrite au Titre 3 du présent livre, et permet d'envisager le développement d'architectures, de pratiques et de procédures qui gèrent correctement les besoins des autorités au travers de l'ensemble du cycle de vie des données.

La gestion des données des Autorités publiques visées par le présent Code doit être efficace et cohérente.

Une gestion efficace et cohérente des données implique que les Autorités publiques soient en mesure de vérifier, à tout moment du cycle de vie de la donnée, que des mesures techniques et organisationnelles sont mises en œuvre en vue de respecter les principes, les objectifs stratégiques et les objectifs opérationnels pertinents pour la gestion des données et décrits au livre C.II. Il s'agit de l'objet de l'alinéa 2.

Les alinéas 3 et 4 traitent de l'actualisation des données, ou leur mise à jour. Il s'agit d'un élément déterminant permettant de garantir la plus haute qualité des données possible et, *in fine*, leur valorisation. En gestion des données, la manière dont les données sont traitées et stockées est fonction de la durée pendant laquelle les données sont traitées : il s'agit de leur « échelle de temps ». L'alinéa 4 a été adapté à la suite de l'avis de l'APD sur la question spécifique des données à caractère personnel.

Les Autorités publiques ont la responsabilité de définir la fréquence à laquelle les données qu'elles détiennent sont actualisées. Cette obligation s'entend d'une obligation de moyen. Cette fréquence est proportionnelle aux modifications qu'elles subissent de par leur nature et en fonction de leur utilité dans le cadre d'un partage entre Autorités publiques. Ainsi, une Autorité publique ne doit, *a priori*, pas mettre à jour des données d'identification de personnes physiques, comme par exemple les noms et prénoms ou encore le numéro de registre national – par nature stable, de la même manière qu'elle doit mettre à jour des données dont la nature est mouvante et qui ne sont valorisables que si elles sont régulièrement mises à jour, comme des données de mobilité ou de trafic.

Les Autorités publiques doivent mettre à jour ces données avec la plus haute fréquence possible ou nécessaire au regard du contexte du traitement, en vue de garantir leur qualité, et informer systématiquement les utilisateurs de mises à jour réalisées si elles en sont les producteurs. De la même manière, les Autorités publiques doivent permettre aux titulaires de droits sur les données protégées détenues de solliciter leur mise à jour si celles-ci sont incomplètes, incorrectes ou périmées. Néanmoins, en ce qui concerne les données à caractère personnel en particulier, l'attention est attirée sur le fait que des dispositions existent déjà dans le RGPD. Les processus mis en place par les Autorités publiques ne doivent pas faire double emploi avec les procédures déjà garanties dans ce cadre.

L'alinéa 5 traite du cycle de vie de la donnée. Il s'agit d'un cadre de gestion utile qui permet de visualiser facilement les différentes étapes que traversent les données dans le cadre d'un projet, de leur collecte à leur destruction.

Le cycle de vie de la donnée se décompose en six étapes de traitement essentielles que sont :

1° la collecte;

2° le stockage;

3° l'utilisation;

4° l'analyse;

5° l'archivage, ou la conservation;

6° la destruction.

Ce dernier point doit être considéré sous réserve de toute conservation au titre d'archivage historique vu l'intérêt patrimonial, culturel, historique de la donnée, ou de tout autre type d'archivage éventuel, par exemple à des fins statistiques.

La maîtrise du cycle de vie implique également l'identification et l'organisation des rôles et responsabilités de chaque partie, des process à mettre en

œuvre ainsi que des mesures techniques et organisationnelles mises en œuvre.

Les Autorités publiques ne doivent pas négliger que certaines étapes peuvent leur être spécifiques ou présenter des particularités. Ainsi en va-t-il de la publication en *open data*, qui peut intervenir dès la collecte (par exemple en cas de diffusion en temps réel de ces données) ou l'archivage dont les dispositions obligent à la conservation de nombreuses données publiques et selon des durées qui varient en fonction de l'utilité administrative.

L'alinéa 5 précise que les Autorités publiques doivent tenir compte du contexte d'utilisation et du cas d'usage.

Le contexte d'utilisation des données décrit les circonstances dans lesquelles les données sont collectées, utilisées et traitées. Il inclut des éléments tels que les objectifs de la collecte de données, les parties impliquées, les méthodes utilisées pour collecter les données et les règles et les lois en vigueur qui régissent l'utilisation des données. De nombreux opérateurs, publics ou privés, interviennent dans un contexte d'utilisation de données particuliers : c'est la raison pour laquelle les intervenants aux partenariats sont énoncés dans le chapitre 2 du titre 2.

Le cas d'utilisation, quant à lui, décrit comment les données sont utilisées pour résoudre un problème ou pour atteindre un objectif spécifique. Il inclut des informations sur les étapes nécessaires pour utiliser les données, les résultats attendus et les avantages attendus pour les parties impliquées. Les Autorités publiques qui partagent des données doivent mettre en place des normes claires et adaptées à leur contexte et à leur cas d'usage pour assurer la qualité de leurs données.

Il est préférable que le choix et la mise en œuvre des mécanismes permettant la gestion de la qualité des données soient faits de manière collective afin d'assurer l'adhésion de tous les intervenants impliqués par la valorisation ou le partage de données aux règles en place et afin de faciliter la responsabilité de chaque partie en cas de problèmes.

Une gestion efficace et cohérente des données implique également l'intégration dans la gouvernance des données de certaines problématiques particulières et notamment :

1° la gestion des données de référence et des métadonnées;

2° la gestion des modèles analytiques et des algorithmes;

3° la gestion des données générées par l'intelligence artificielle;

4° la gestion des bases de données.

Eu égard aux précisions à apporter concernant chacune des problématiques un article par problématique particulière est formulé dans la suite de ce Titre.

En outre, une gestion efficace et cohérente nécessite la mise en œuvre d'un ensemble de méthodes de sécurité informatique dont les principes sont exposés ci-dessous, concernant notamment la gestion des accès et des privilèges, ainsi que la gestion de la sécurité informatique. Le fonctionnement détaillé de ces principes est exposé dans un texte à valeur réglementaire distinct du présent texte.

Une gestion efficace des données implique donc qu'une Autorité publique mette en place des procédures ou utilisent des outils qui lui permettent de réaliser les points évoqués dans cet article en fonction de la nature des données concernées.

CHAPITRE 1
La gestion de la qualité des données

SECTION 1
La gestion des données de référence et des métadonnées

Article C.III.17.
La gestion des données de référence et des métadonnées

L'un des objectifs opérationnels identifiés dans le livre C.II du présent Code concerne la gestion des données de références et des métadonnées. Le présent article a pour objectif de fournir les outils nécessaires aux Autorités publiques en vue de remplir cet objectif opérationnel.

Les données de référence sont des données utilisées pour caractériser d'autres données.

Les données dites « maîtres » ont une vocation structurante et transversale. Elles soutiennent l'activité courante de tout organisme dans la prise de décision et dans le transfert et la structuration d'informations.

L'organisation de données de référence implique que cette organisation soit indépendante des canaux

de communications, du secteur d'activité ou de subdivisions métier ou géographiques en vue d'éviter :

1° les biais ou les lacunes dans les données de référence qui pourraient résulter d'une focalisation excessive sur un secteur ou une région spécifique,

2° les doublons et les incohérences dans les données de référence, qui pourraient entraîner des erreurs ou des incohérences dans les analyses et les décisions.

Les données de référence sont variables en fonction des Autorités publiques concernées mais contiennent notamment des données d'organisation – le nombre de services et d'agents –, des actifs digitaux – données graphiques, patrimoine numérique, logos et pictogrammes de référence –, des données de localisation – adresses des sites, etc. Ces données sont importantes au même titre que les métadonnées.

Un exemple de telles données peut être trouvé en France ([3]), où ces données de références sont pour l'*open data* de l'administration. Dans ce cadre, les autorités françaises ont défini neuf bases de données différentes de données de référence, dont la base de données des adresses nationales qui recense un très grand nombre de noms de rue et de numéros.

Cette base de données peut ensuite être réutilisée – pour des services de géolocalisation (vente immobilière, livraison, mobilité, …). Les données de référence sont dans ce cas des données de référence (de contenu) dont les métadonnées associées (descriptives) sont par exemple « #localisation », « #adresses » ou les métadonnées de classification proposées au livre B.III du présent Code.

Outre les données de classification établies au titre 2 du présent livre, les Autorités publiques établissent des métadonnées fiables permettant d'identifier les paramètres clefs des données décrites.

Les métadonnées permettent le classement et l'identification des données et fournissent de l'information sur la donnée. Il s'agit, comme pour les livres d'une bibliothèque, d'en identifier l'origine, le format, le type ou encore la date de création, sans pour autant consulter la donnée elle-même.

Les Autorités publiques doivent apporter un soin particulier à la gouvernance des métadonnées, dès lors que sans gestion cohérente et efficace, ces métadonnées n'ont pas de sens ni de valeur.

Cet article a été adapté à la demande de l'APD afin de mentionner les éléments essentiels de traitements de données de références ou de métadonnées à caractère personnel.

(3) https://www.data.gouv.fr/fr/datasets/base-adresse-nationale

SECTION 2
La gestion des modèles analytiques et la transparence des algorithmes

Article C.III.18.
Respect des missions de services publics et des obligations légales applicables

L'objectif de cet article est de garantir que les autorités publiques utilisent des procédures de décision automatisées de manière responsable, en ligne avec leurs missions de service public et en conformité avec le RGPD.

Les technologies de prise de décision automatisée offrent une efficacité accrue dans la gestion des services publics.

L'article assure un équilibre entre l'utilisation de ces technologies et le respect des droits des individus, conformément à l'article 22 du RGPD.

Il met en lumière l'importance de la transparence et de la responsabilité dans l'utilisation de l'automatisation.

Article C.III.19.
Droits de la personne concernées en cas de décision d'une Autorité publique fondée exclusivement sur un traitement automatisée

L'objectif de cet article est de protéger les droits des individus face aux décisions automatisées, en assurant transparence, explications claires, et possibilités de recours.

L'article reconnaît l'importance du droit individuel à comprendre et contester les décisions qui les affectent et met l'accent sur la nécessité d'une intervention humaine pour prévenir les erreurs et les biais dans les décisions automatisées.

Article C.III.20.
La gestion des modèles analytiques, des algorithmes et des systèmes exploitant l'intelligence artificielle

Les Autorités publiques font déjà régulièrement appel à des systèmes d'intelligence artificielle, de manière directe ou indirecte, dans le périmètre de l'action publique (gestion des territoires (*Smart City*), transport et mobilité, entretien des infrastructures, gestion de la qualité de l'air, gestion des déchets

(poubelles connectées), gestion de l'anonymisation, etc. …). Ces systèmes sont appelés à se multiplier.

La distinction entre les notions de modèles analytiques ou algorithmes et d'intelligence artificielle n'est pas l'objet du présent Code. Dès lors que la distinction entre les obligations imposées aux Autorités publiques pour l'un ou l'autre de ces types de systèmes est ténue ou serait en tous les cas artificielle, il est fait le choix de leur appliquer le même corps de règles.

La manière dont ces modèles sont étudiés, développés et implémentés ont une incidence plus que conséquente sur la qualité des données qu'ils génèrent notamment compte tenu de la masse des informations qu'elles peuvent traiter.

Le présent article a pour vocation à guider l'action des Autorités publiques lorsqu'elles décident de recourir à de tels modèles, en imposant un contrôle *a priori* et tout au long de l'utilisation de ces modèles.

L'alinéa 1er définit une série de points, non exhaustifs, auxquels les Autorités publiques doivent porter attention dans le cadre de l'utilisation de systèmes reposant sur des modèles algorithmiques ou d'intelligence artificielle.

Ces points constituent des règles de base qui permettent d'offrir un minimum de garanties et de transparence à l'égard de deux types d'utilisation de tels systèmes, soit lorsqu'ils sont utilisés pour collecter des données et en déduire un résultat, comme par exemple, l'octroi ou non d'une aide publique, soit lorsque de tels systèmes sont mis à disposition d'une Autorité par une autre Autorité, par exemple pour améliorer ou optimiser la mobilité sur un territoire donné.

Eu égard aux considérations précitées, les Autorités publiques doivent déterminer quelles pratiques sont les plus appropriées selon les capacités et les risques de ces systèmes.

Cela commence par l'élaboration d'une approche dédiée – point 1) – et une connaissance inventoriale des systèmes utilisés – point 2). Les Autorités publiques doivent également mener une évaluation ex ante en profondeur du système au niveau de ses effets disparates potentiels – point 3) –, de sa transparence – point 4) – de sa sécurité – point 5) – ou des responsabilités qu'il prévoit – point 6). Cela continue également en mettant en place des contrôles – point 7) – et une information complète – point 8) – qui permettent que l'information soit comprise par toute personne physique amenée à utiliser le système. Enfin, les Autorités publiques doivent garantir que ces systèmes soient accessibles à tous – point 9).

Les Autorités publiques doivent évaluer régulièrement à quel point ces systèmes peuvent être compris par une personne physique, soit grâce à une information et une responsabilisation adéquate, soit grâce à la transparence du système lui-même.

À cet égard, il est précisé qu'un « effet disparate », visé au point 3), est une différence de traitement accidentelle qui résulte de l'utilisation d'un modèle algorithmique alors qu'une telle différence de traitement n'était pas souhaitée par l'Autorité publique au travers de l'utilisation du ou des modèles.

Le deuxième alinéa repose sur la philosophie de l'article 14, § 2, g), du RGPD, lequel impose une pareille obligation dans le cadre du traitement de données à caractère personnel.

L'article a été revu afin d'intégrer des dispositions visant à prévenir les discriminations, conformément à l'avis remis par l'Institut pour l'égalité des chances.

L'objectif de cet article est d'assurer une utilisation éthique et responsable des technologies avancées telles que l'intelligence artificielle par les autorités publiques.

L'article souligne l'importance d'une gouvernance et d'une supervision adéquates des technologies émergentes pour prévenir les abus et les discriminations et met en évidence la nécessité d'évaluer continuellement et d'ajuster les systèmes pour garantir leur conformité éthique et légale.

Ainsi faisant, le code encourage la transparence et la responsabilisation, essentielles dans la gestion des technologies pouvant avoir un impact significatif et positif sur les individus et la société.

Ces motivations s'alignent avec les principes de bonne gouvernance, de respect des droits individuels et de responsabilité dans l'usage des technologies. Elles visent à établir un cadre légal solide pour guider les autorités publiques dans l'ère numérique, tout en protégeant les droits fondamentaux des citoyens.

SECTION 3
La gestion des bases de données

Article C.III.21.
La gestion des bases de données

Dans le cadre de l'exercice de leurs missions, les Autorités publiques gèrent un grand nombre de bases de données.

Les Autorités publiques adoptent une politique de gestion qui désigne clairement la ou les personnes

responsables de chacune des bases de données. Il s'agit de l'objet du premier tiret.

Le cadre de gestion précise que les personnes responsables de la base agissent, comme le ferait un fiduciaire à l'égard des données qui y sont conservées. Les infrastructures nécessaires au fonctionnement de la base, pour leur part, peuvent appartenir à une personne physique ou morale du secteur privé.

Le but de cet article est d'assurer la bonne gestion et la transparence du fonctionnement des bases de données. Qui y a accès, qui peut en changer le contenu, qui est responsable des opérations qui font appel à la base de données en question. Il s'agit d'une disposition afférente à la gestion de la base et non relative à son contenu.

Nous précisons au deuxième tiret que si la destination de la base devait changer alors qu'elle concerne des données protégées, l'autorisation des titulaires des droits les concernant doit être demandée puisqu'il s'agit d'un nouveau traitement.

CHAPITRE 2

La sécurité et la protection des données

SECTION 1

La gestion des accès et des privilèges associés

Article C.III.22.

Gestion de la sécurité et de la protection des données

Les Autorités publiques veillent à ce que tout accès à un système d'information et à ses ressources soit contrôlé et que seulement les accès autorisés puissent avoir lieu.

Le système d'autorisations doit contenir diverses règles qui déterminent et limitent la manière dont les données peuvent être consultées ou manipulées (copiées, transférées, effacées, éditées …). Les Autorités publiques adoptent un système d'accès qui permet de moduler les privilèges associés aux autorisations d'accès en fonction de divers critères selon le contexte et les besoins des intervenants impliqués par la valorisation ou le partage de données. Un utilisateur, un processus ou un programme ne devrait être autorisé à accéder aux informations autorisées qu'en raison d'un objectif légitime (maintenance, édition, transfert, etc.).

Article C.III.23.

Gestion des accès et des privilèges associés

Les Autorités publiques établissent des accès en tenant compte notamment :

1) de la fonction de l'utilisateur. En appliquant la technique du contrôle d'accès basée sur les rôles, les Autorités publiques pourront permettre à certains utilisateurs de consulter la base de données, alors que d'autres pourront, le cas échéant, en extraire des données ou la modifier;

2) des catégories d'accès par type d'utilisateur. Les Autorités publiques et personnes physiques et morales du secteur privé n'ont généralement pas accès aux mêmes données;

3) du degré de sensibilité des données elles-mêmes. Les données ouvertes sont librement accessibles à tous et librement réutilisables par tous. Les données protégées sont des informations accessibles dans les limites imposées par une licence, une mission de service publique ou la loi. Les données sensibles sont des données contrôlées et à ce titre doivent être conservées dans les conditions les plus sécuritaires possibles, avec des privilèges d'accès extrêmement restreints.

Les Autorités publiques assurent le contrôle des accès aux données par l'application de diverses solutions techniques et de sécurité. De nombreuses options et protocoles peuvent être envisagés, allant de processus relativement simple, tel qu'un formulaire d'inscription exigeant le nom de l'utilisateur, à des systèmes d'accès complexes, tel qu'un processus d'authentification de l'identité de l'utilisateur accompagné d'un contrôle de ses accès basé sur son rôle ou encore d'un mécanisme de double authentification.

SECTION 2

La gestion de la sécurité informatique

Article C.III.24.

Gestion de la sécurité informatique

Les Autorités publiques respectent le principe de sécurisation des données tel que décrit dans le livre C. II du présent Code. Les Autorités publiques vont plus loin et mettent au point une véritable gestion de la sécurité informatique.

Cette gestion se décline notamment, de manière non exhaustive, sous six aspects, listés dans le présent article. Au regard du caractère évolutif des obligations, les dispositions seront décrites dans un texte

réglementaire à adopter par le Gouvernement, le Collège réuni et le Collège.

L'article a été revu afin de répondre aux préoccupations de l'Autorité de protection des données.

La gestion proactive de la sécurité informatique par les Autorités publiques renforce en effet la protection des données à caractère personnel en assurant une gestion sécurisée et conforme.

La surveillance continue de l'évolution technologique et des normes garantit que les pratiques de sécurité respectent les standards actuels, améliorant ainsi la sécurité des données à caractère personnel et la qualité de l'open data de manière continue.

L'établissement de procédures de contrôle par les Autorités publiques assure que la gestion des données respecte les normes établies, renforçant ainsi la sécurité des données à caractère personnel et l'intégrité de l'open data.

La mise en place de procédures pour vérifier et archiver les accès et modifications aux données améliore la transparence et la traçabilité, essentielles tant pour la protection des données à caractère personnel que pour l'efficacité de l'open data.

L'obligation d'authentification multi-facteurs pour accéder aux systèmes de données protégées augmente la sécurité des données à caractère personnel ainsi que la fiabilité de l'open data.

Le chiffrement des données en transit conforme à l'état de l'art protège les données personnelles lors de transmissions sur des réseaux non sécurisés, essentiel pour la sécurité et constitue une amorce pour NISII (directive européenne à venir qui pose le cadre de la sécurité informatique)

L'exigence de gestion spécifique des clés de chiffrement, séparément des données chiffrées, renforce la sécurité des données à caractère personnel notamment en cas de fuite de données.

TITRE 5
Le contrôle de la conformité, la traçabilité et la responsabilité des autorités publiques

Article C.III.25.
Contrôle de la conformité et de la traçabilité

Les Autorités publiques doivent assurer le contrôle de la conformité.

La conformité doit être comprise au sens large, c'est-à-dire qu'elle se réfère notamment aux données utilisées en fonction des objectifs des parties, à leurs principes éthiques, à leurs obligations légales et contractuelles ainsi qu'à leur devoir envers le public. Le contrôle de la conformité peut être accompli par un individu ou encore par une instance précise (comité d'éthique ou d'audit) et doit être documenté. Ce contrôle peut également comporter la mise en place d'audits ou de tests de sécurité périodiques pour vérifier que les autorisations d'accès sont respectées notamment.

La conformité passe également, entre autres, par l'adoption de pratiques, de codes d'éthique ou de politiques d'utilisation, puis à leur communication au sein des Autorités publiques ainsi que le contrôle de la traçabilité des données

Le contrôle de la traçabilité des modifications à des données est essentiel pour garantir la conformité des données, la responsabilité, la gestion des risques et la transparence. Cela permet notamment de maintenir la confiance dans celles-ci et de s'assurer que les données sont utilisées de manière appropriée et conforme au Code et aux réglementations en vigueur.

L'établissement de procédures de contrôle par les Autorités publiques assure que la gestion des données respecte les normes établies, renforçant ainsi la sécurité des données à caractère personnel et l'intégrité de l'open data.

La mise en place de procédures pour vérifier et archiver les accès et modifications aux données améliore la transparence et la traçabilité, essentielles tant pour la protection des données à caractère personnel que pour l'efficacité de l'open data.

La traçabilité est la capacité à relier chaque modification à une source ou à un utilisateur spécifique. Elle doit être implémentée de manière proportionnée en fonction de la nature des données concernées ainsi que des risques afférents à une fuite ou à une altération non souhaitée.

D'une part, comme décrit au paragraphe 1er, les Autorités publiques vérifient si la manière dont est assurée la gestion des données qu'elles détiennent correspond aux obligations du présent Code, mais également à toutes les autres dispositions de nature européenne, fédérale ou régionale qui leur seraient applicables.

D'autre part, comme décrit au paragraphe 2, les Autorités publiques vérifient la traçabilité des données et la conformité technique des outils et systèmes auxquels ils recourent.

Nous attirons l'attention sur le rôle prépondérant de l'exercice d'une veille sur les développements juridiques et les normes en vigueur pour que les pratiques des Autorités publiques soient maintenues à jour. Cette veille concerne également les mises à jour du matériel utilisé.

L'obligation d'authentification multi-facteurs pour accéder aux systèmes de données protégées augmente la sécurité des données à caractère personnel ainsi que la fiabilité de l'open data.

Le chiffrement des données en transit conforme à l'état de l'art protège les données personnelles lors de transmissions sur des réseaux non sécurisés, essentiel pour la sécurité et constitue une amorce pour NISII (directive européenne à venir qui pose le cadre de la sécurité informatique).

L'exigence de gestion spécifique des clés de chiffrement, séparément des données chiffrées, renforce la sécurité des données à caractère personnel notamment en cas de fuite de données.

Le contrôle de conformité doit avoir lieu de manière périodique en fonction de la nature des données contrôlées.

Les mesures de contrôle doivent être mises en place à différents moments du cycle de vie des données (création, stockage) et ce afin d'évaluer les pratiques quotidiennes ou les activités proposées au regard des règles et des solutions informatiques qui sont généralement propres à chaque étape.

La mise en œuvre de cette obligation est capitale en raison des évolutions constantes au niveau juridique, ce qui a déjà pu être constaté avec l'entrée en vigueur du RGPD, et au niveau technique, par exemple au travers de la mise à jour d'un programme ou d'une solution hardware, ou par l'apparition de nouvelles solutions techniques.

C'est précisément pour cette raison que la mobilisation, la sensibilisation, l'information et la formation du personnel en charge de ces questions doivent être mises en place, comme le prévoit le paragraphe 9.

À cet égard, une bonne pratique en matière de contrôle de la conformité consiste en l'établissement une séparation entre cette fonction de contrôle et les instances décisionnelles stratégiques.

LIVRE C.IV.
Partage administratif, réutilisation et communication

Le livre C.IV. du Code concerne l'ensemble des flux de données possibles impliquant au moins une Autorité publique au niveau de la Région, de la COCOM et de la COCOF sous forme de :

1° partage administratif des données entre les Autorités publiques (G2G). Il peut grandement contribuer à l'amélioration des politiques et des services publics, et aussi à la réduction de la charge administrative qui pèse sur les citoyens et les opérateurs privés (par exemple grâce au principe de collecte unique des données issues de sources authentiques – principe « *Once only* »);

2° réutilisation des données des Autorités publiques par les opérateurs privés (flux de données du public vers le privé – G2B); la réutilisation porte sur des informations et données issues du secteur public considérées comme « bien commun » et mises à disposition du grand public (enseignement, presse, recherche, etc.). La mise en œuvre du régime légal lié à la réutilisation améliore aussi la transparence des données contenues au sein des Autorités publiques.

3° communication de données provenant des opérateurs privés par les Autorités publiques (flux de données du privé vers le public – B2G); permettre aux citoyens de bénéficier de l'infrastructure de gestion des données afin de devenir eux-mêmes producteurs de données, et de les communiquer vers le secteur public (C2G, C2B).

Il convient de rappeler d'emblée l'importance d'un partage rendu plus facile et efficace entre les Autorités publiques. En effet, un certain nombre d'études commandées par l'Agence fédérale pour la simplification administrative montrent très clairement que le partage de données disponibles peut entraîner une diminution significative des charges administratives ([4]). En outre, l'application du principe de la collecte unique de données a également un effet positif sur le fonctionnement et l'efficience des Autorités publiques ([5]) dans le cadre de l'exécution de leurs missions.

La réutilisation des données du secteur public par des opérateurs privés est aussi constitutive d'un enjeu essentiel pour le développement de l'économie

(4) Note au gouvernement de la Région de Bruxelles-Capitale sur une stratégie bruxelloise sur les données.

(5) Projet d'ordonnance du 11 mai 2020 garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité, et portant simplification et harmonisation des formulaires électroniques et papier, p. 2.

numérique. Les données générées par le secteur public devraient être disponibles pour le bien commun et être réutilisées par des chercheurs, citoyens, des associations ou tout autre opérateur. Ces données offrent des perspectives en termes de développement de produits et de services ainsi qu'aux acteurs économiques proposant des solutions permettant d'atteindre les objectifs de transition du Gouvernement.

Une première étape avait été franchie par la publication de l'ordonnance open data ([6]).

Le présent livre a pour objet de développer les règles et les modes opératoires spécifiques aux différents flux de données. Malgré la volonté de simplifier, le législateur est tenus de respecter le cadre européen, notamment la Directive ISP ou « open data » ou encore a souhaité anticiper l'application du règlement sur la gouvernance des données.

Par ailleurs, les données provenant du secteur privé peuvent également apporter une contribution significative au bien public en permettant d'améliorer le fonctionnement et la gestion des Autorités publiques et, finalement, le service aux citoyens. Nombreuses sont les possibilités offertes par l'utilisation à des fins d'intérêt général de données mises à disposition volontairement par des opérateurs privés (citoyens, entreprises, etc.). Ces finalités sont notamment les soins de santé, la lutte contre le changement climatique, l'amélioration de la mobilité, l'établissement plus aisé de statistiques officielles ou l'amélioration de la prestation de services publics. Le soutien à la recherche scientifique, et notamment au développement technologique et à la démonstration, à la recherche fondamentale, à la recherche appliquée et à la recherche financée par des fonds privés, devraient également être considérés comme ayant une finalité d'intérêt public ([7]).

Ces flux doivent être organisés dans le strict respect des réglementations applicables imposant, notamment, des garanties spécifiques quant à la protection des données à caractère personnel lors de leurs traitements et mises à disposition.

Parmi celles-ci, les règles de l'Union relatives à la protection des données sont essentielles pour les citoyens (ex : RGPD ([8]), ePrivacy ([9]), etc.). Ces règles européennes sont aussi complétées par des règles nationales (fédérales et/ou des entités fédérées) dont il convient de tenir compte dans la mise en œuvre des objectifs précités ([10]). Elles s'appliquent dès l'instant où les informations en cause permettent d'identifier directement ou indirectement les citoyens et s'imposent tant aux opérateurs privés qu'aux Autorités publiques qui utilisent et mettent à disposition ces données. Ces législations comportent toute une série de garanties dont il doit être tenu compte tant dans la stratégie de gouvernance que dans le traitement et l'exploitation des données. Il convient de les envisager dès la conception des outils de gestion de partage, de réutilisation et de communication (« *Data by design* »).

Au titre de ces garanties, on peut citer les obligations d'information concernant notamment les diverses finalités d'utilisation des données, la limitation de la conservation des données, la mise-à-jour et l'exactitude des données, la reconnaissance de droits d'accès, de rectification ou à l'effacement, la pseudonymisation ou l'anonymisation des données, etc.

Le présent livre se structure comme suit :

1° le titre I prévoit des garanties générales propres à certains flux qui peuvent apparaître dans le cadre des opérations de partage administratif, réutilisation, communication;

2° le titre II traite du partage administratif de données entre Autorités publiques. Ce titre reprend notamment des dispositions des ordonnances

(6) Ordonnance du 27 octobre 2016 visant à l'établissement d'une politique de données ouvertes (open data) et portant transposition de la directive 2019/1024/UE du Parlement européen et du Conseil du 20 juin 2019 (refonte) concernant les données ouvertes et la réutilisation des informations du secteur public; Ordonnance du 10 décembre 2021 modifiant l'ordonnance du 27 octobre 2016 visant à l'établissement d'une politique de données ouvertes (open data) et portant transposition de la directive 2019/1024/UE du Parlement européen et du Conseil du 20 juin 2019 (refonte) concernant les données ouvertes et la réutilisation des informations du secteur public.

(7) Considérant 35 de la proposition de Règlement du Parlement européen et du conseil du 25 novembre 2020 sur la gouvernance européenne des données (acte sur la gouvernance des données).

(8) Règlement (UE) 2016/679 du Parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données).

(9) Proposition de Règlement du Parlement européen et du conseil du 10 janvier 2017 concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (Règlement « vie privée et communications électroniques »).

(10) Par exemple, la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel; la loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du RGPD ou des législations plus spécifiques comme la loi du 19 mai 2010 portant création de la base-carrefour des véhicules ou la loi du 8 août 1983 organisant un registre national des personnes physiques.

Once only (11) et relative à l'intégrateur de services bruxellois (12). Pour le reste, les dispositions ont été créées pour les besoins du Code afin de compléter le cadre légal existant.

3° le titre III traite de la réutilisation des données des Autorités publiques vers les opérateurs privés. Ce titre a, entre autres, pour objet, de reprendre l'ordonnance *open data* (13) qui elle-même transposait la Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la Directive 2003/98/CE concernant la réutilisation des informations du secteur public (Directive ISP) (14) ainsi que d'exécuter les dispositions pertinentes du Règlement 2022/868/CE du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le Règlement (UE) 2018/1724/CE (« Règlement sur la gouvernance des données »);

4° enfin, le titre IV traite de la communication des données, à savoir le flux de données de tout opérateur privé intéressé vers une Autorité publique.

TITRE 1
Garanties communes aux partages administratifs, réutilisations, communications

Article C.IV.1.
Secret professionnel et confidentialité

Les agents de la fonction publique qui ne sont pas soumis au secret professionnel doivent en toute hypothèse respecter un devoir spécifique de confidentialité. Par « confidentialité » », le présent Code englobe également le « devoir de réserve » auquel sont soumis les fonctionnaires.

Article C.IV.2.
Respects de droit des tiers

Les droits des tiers font référence à des droits que des personnes tierces au partage possèdent et qui sont susceptibles d'être violés au vu de la nature et du contenu des données partagées. Il peut s'agir de droits de propriété intellectuelle, de droits relatifs à la protection des lanceurs d'alerte, de droits relatifs à la protection des données à caractère personnel ou encore au secret d'affaire.

Le terme « tiers » doit se comprendre dans le présent Code comme toute personne autre que les participants au partage administratif, à la réutilisation ou à la communication. On attire l'attention sur le fait que le terme « tiers » repris dans le présent Code ne doit pas se confondre avec la notion du tiers déjà définie par le RGPD car il possède une signification différente.

La propriété intellectuelle fait partie intégrante du droit des tiers et nécessite une attention particulière lors du partage administratif, de la réutilisation, ou de la communication de données. En effet, une ou plusieurs données pourraient être reliées à un droit intellectuel, tel que par exemple le droit d'auteur, le droit des marques, le droit des brevets, le droit des dessins et modèles ou encore le droit des bases de données. Dans ces cas-là, les Autorités publiques et les opérateurs privés doivent respecter les règles de propriété intellectuelle et ne pas affecter l'existence, la titularité ou l'exercice de ces droits. Bien entendu, si les tiers titulaires des droits de propriété intellectuelle sur la ou les données autorisent l'utilisation de l'élément protégé faisant l'objet du partage, de la réutilisation ou de la communication, les Autorités publiques ou les opérateurs privés sont libres d'y procéder.

Cet article énonce encore le principe du respect des secrets d'affaires et des informations confidentielles tels que visés au Titre 8/1 du livre XI du Code de droit économique en cas de partage de données qui pourraient y porter atteinte.

Il est rappelé que toute opération visée par le présent livre comprenant des données à caractère personnel est soumise au respect de leur protection garantie notamment par le RGPD et la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Par ailleurs, il s'agit d'insister particulièrement, vu son importance, sur le respect du principe de licéité des traitements ainsi que des principes visés au Chapitre 2 du RGPD.

La protection des lanceurs d'alerte doit également être garantie lorsque des infractions sont découvertes dans le cadre des opérations de partage administratif, réutilisation et communication.

(11) Ordonnance du 17 juillet 2020 garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité, et portant simplification et harmonisation des formulaires électroniques et papier.

(12) Ordonnance du 8 mai 2014 portant création et organisation d'un Centre d'intégration de services régional.

(13) Ordonnance du 10 décembre 2021 modifiant l'ordonnance du 27 octobre 2016 visant à l'établissement d'une politique de données ouvertes (open data) et portant transposition de la directive 2019/1024/UE du Parlement européen et du Conseil du 20 juin 2019 (refonte) concernant les données ouvertes et la réutilisation des informations du secteur public.

(14) Directive 2019/1024/UE du Parlement européen et du Conseil du 20 juin 2019 (refonte) concernant les données ouvertes et la réutilisation des informations du secteur public.

Il est évident, que particulièrement pour ce qui concerne les hypothèses de réutilisation, il s'agit d'être attentif à ne pas créer des distorsions de concurrence par l'octroi d'avantages comparatif, le cas échéant sous la forme d'aides d'État.

Article C.IV.3.

Absence de droit de propriété intellectuelle ou sui generis sur les bases de données publiques

En Belgique, les bases de données sont susceptibles de recevoir une double protection :

Un droit particulier, appelé droit « *sui generis* » protège le contenu de la base de données, c'est-à-dire l'ensemble des données qu'elle contient. Le droit *sui generis* peut protéger les bases de données, même à défaut d'originalité de celles-ci. L'objectif de la protection par le droit *sui generis* est de protéger les investissements réalisés dans le secteur des bases de données et d'empêcher la reprise des bases de données par des concurrents.

Les dispositions relatives à la protection des bases de données par le droit *sui generis* se trouvent dans titre 7 du livre XI du Code de droit économique.

Le droit d'auteur protège la structure de la base de données, si elle est originale. La protection par le droit d'auteur ne suffit pas pour protéger les bases de données dans la mesure où l'originalité fait souvent défaut pour des bases de données dont la présentation se veut méthodique et exhaustive.

La protection des bases de données par le droit d'auteur est réglée par le titre 5 du livre XI du Code de droit économique.

Il est possible de cumuler les deux protections (par le droit *sui generis* et le droit d'auteur) pour une même base de données, si elle satisfait aux conditions des deux régimes.

Partant, il convient de ne pas appliquer ces protections aux bases de données qui sont ouvertes à réutilisation ou au partage sinon, cela risque simplement de l'empêcher

TITRE 2
Partage administratif

CHAPITRE 1
Principe du partage administratif

Article C.IV.4.
Partage administratif et demande de partage administratif

Les Autorités publiques sont appelées à organiser des partages administratifs entres elles conformément aux dispositions du présent titre, pour les raisons reprises dans l'exposé des motifs, à savoir alléger la charge administrative des citoyens, créer des synergies, améliorer la qualité des services publics et d'intérêt général, mutualiser certains frais de fonctionnement etc.

Le partage administratif ne concerne que les Autorités publiques entre elles et non des services administratifs entre eux au sein d'une Autorité publique (ce qui est en revanche visé par la notion de partenariat numérique de donnée, visée au livre C.III, qui est beaucoup plus large que celle de partage administratif). Cela étant, lorsqu'un partage administratif est réalisé entre deux Autorités, il conviendra d'indiquer quels sont les services bénéficiaires au sein d'une autorité au travers du protocole d'accord.

Le principe est donc le partage administratif gratuit entre les Autorités publiques, à savoir sans redevance pour l'usage des données.

Si le partage des données en soi est gratuit, le passage par le Centre d'intégration, à savoir le coût de la diffusion technique, peut en revanche être soumis à une redevance comme exposé dans le livre C.V relatif à la Plateforme bruxelloise de la donnée.

Toutefois, certains partages administratifs ne peuvent avoir lieu dès lors qu'une disposition juridique particulière l'interdit ou encore que les droits des tiers sur les données visées ne l'autorisent pas (non-respect du cadre légal en matière de données à caractère personnel, non-respect des droits intellectuels ou encore du secret des affaires comme rappelé à l'article C.II.2).

Chaque flux de données sollicité dans le cadre d'un partage administratif est donc minutieusement analysé par les Autorités publiques producteurs des données afin de vérifier sa légalité.

Le caractère gratuit du partage se justifie par la volonté de faciliter et d'encourager le partage de données entre Autorités publiques.

L'article a été modifié afin de rencontrer les préoccupations de l'APD qui se fondait sur une interprétation erronée de la mention que les partages administratifs devaient trouver à se réaliser pour autant qu'aucune règle de droit ne l'empêchait. Il va de soi que le respect des limites des missions de services publics ou du principe de spécialité des personnes morales s'imposait et constituait des règles de droit à respecter. L'article a donc été modifié afin de formuler positivement les conditions indispensables à la réalisation d'un partage administratif.

Les partages administratifs ne porteront vraisemblablement que dans une infime proportion sur des données à caractère personnel vu que les exigences restrictives que comporte le RGPD en la matière (principe de légalité et principe du respect des finalités). Toutefois, la logique reste la même, l'ensemble des conditions s'appliquant devant toutes être respectées pour que le partage administratif puisse avoir lieu.

Il est renvoyé aux points 48 à 49 de l'avis de l'APD et principalement à l'extrait de la recommandation n° 02/2020 du 31 janvier relative à la portée de l'obligation de conclure un protocole afin de formaliser les communication de données à caractère personnel en provenance du secteur public fédéral :

« Aux termes de l'article 20 de la LTD, l'obligation de conclure un protocole n'existe que lorsque la communication de données à caractère personnel en provenance d'une autorité publique fédérale est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, ou lorsqu'elle est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement étant entendu que l'obligation légale ou la mission d'intérêt public qui légitime la communication de données à caractère personnel peut exister tant dans le chef du responsable du traitement qui communique les données à caractère personnel que dans le chef du responsable du traitement qui réceptionne ces données.

Cette exigence doit se comprendre à la lumière du principe de l'attribution des compétences administratives, du principe de spécialité des personnes morales ainsi que du principe de légalité qui préside à la définition des conditions auxquelles l'administration peut interférer avec le droit à la protection de la vie privée, lequel inclut le droit à la protection des données à caractère personnel […] Aux termes du principe de l'attribution des compétences administratives, qui est consacré par l'article 105 de la Constitution et 78 de la loi spéciale du 8 août 1980 de réformes institutionnelles, les autorités administratives n'ont d'autres pouvoirs que ceux que leur attribuent formellement la Constitution et les lois et décrets portés en vertu de celle-ci. En outre, le principe de spécialité des personnes morales dispose que toute institution dotée de la personnalité juridique ne peut agir que pour atteindre le(s) but(s) pour le(s)quel(s) elle a été créée, étant entendu que seule une norme législative peut confier une mission de service public à une personne morale. En outre, comme le Conseil d'État l'a rappelé dans son avis sur l'avant- projet de loi « relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », « un transfert de données d'une autorité publique à une autre constitue une ingérence dans le droit à la protection de la vie privée des personnes concernées. En vertu de l'article 8 de la Convention européenne des droits de l'homme et de l'article 22 de la Constitution, tel qu'interprété par une jurisprudence constante de la Cour constitutionnelle, pareille ingérence doit notamment reposer sur une base légale, être proportionnée par rapport à l'objectif poursuivi et être organisée de manière suffisamment précise pour être prévisible pour le citoyen. ».

[…]. Ainsi, une autorité publique ne peut traiter – et donc communiquer – des données à caractère personnel que si cette communication est nécessaire au respect d'une obligation imposée par ou en vertu d'une norme législative à l'un des responsables du traitement ou si elle est nécessaire à l'exécution d'une mission d'intérêt public qui a été dévolues à l'un des responsables du traitement par ou en vertu d'une norme législative. Comme l'a souligné la CPVP dans son avis concernant l'avant-projet de loi « relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », les communications de données à caractère personnel en provenance du secteur public doivent reposer sur une base légale, étant entendu qu'« un protocole d'échange ne pourra jamais constituer la base légale d'un traitement de données […] ».

Article C.IV.5.
Passage par le Centre d'intégration bruxellois par défaut

L'objectif est de réaliser par principe les partages administratifs au travers du Centre d'intégration bruxellois, en tant qu'outil technique, décrit dans le livre C.V de manière à assurer la gestion opérationnelle et la sécurité des données partagées administrativement.

Le Centre d'intégration bruxellois a pour mission d'intérêt général principale de coordonner des projets de traitement de données, de donner accès à et rendre disponibles ces données et dans une moindre mesure d'agréger des données. Le passage obligatoire par le Centre d'intégration pour le partage administratif des données entre Autorités publiques assure une sécurité technique et organisationnelle. Les mis-

sions ainsi que les modalités de fonctionnement du Centre d'intégration de services bruxellois sont précisées dans les livres C.VI du présent Code.

Outre la mise en place des conditions techniques adéquates, l'Intégrateur de services bruxellois vérifie les éventuelles autorisations des Autorités parties prenantes au partage selon le cadre légal s'imposant à elles et imposant donc la vérification des autorisations nécessaires (exemple : autorisation pour l'accès au registre national). Il appartient en outre en effet à l'intégrateur de services bruxellois de s'assurer que les Autorités publiques qui sollicitent le partage offrent les garanties techniques notamment suffisantes à la sécurité technique de l'opération mais également que les Autorités disposent bien des habilitations légales nécessaires à la réalisation du partage.

Toutefois, d'autres plateformes d'échanges, qui ont pour missions d'assurer le support technique de certains partages administratifs existent déjà actuellement et sont organisées dans le cadre de dispositions légales ou réglementaires particulières, tels que par exemple :

1° la plateforme de vidéosurveillance visée à la section II de l'ordonnance du 28 mai 2015 créant un organisme d'intérêt public centralisant la gestion de la politique de prévention et de sécurité en Région de Bruxelles-Capitale et créant l'École régionale des métiers de la sécurité, de la prévention et du secours – Brusafe;

2° la plateforme mise en place dans le cadre de l'ordonnance du 4 avril 2019 portant sur la plate-forme d'échange électronique des données de santé.

Dans ces hypothèses, le passage par le Centre d'intégration n'est pas imposé, celui-ci intervenant par défaut qu'en l'absence de cadre légal spécifique.

Article C.IV.6.
Partage entre Autorités publiques et Autorités publiques tierces

Le passage par le Centre d'intégration bruxellois peut le cas échéant être possible dans les hypothèses de partage entre des Autorités publiques soumises au présent Code et d'autre entités publiques dépendantes d'autres niveaux de pouvoirs, nationaux ou internationaux, dites Autorités publiques tierces. Dans ces hypothèses de partages administratifs entre des Autorités publiques et des Autorités publiques tierces, le Centre d'intégration peut également intervenir ou assurer le relais entre l'Autorité publique, d'une part, et l' Autorité publique tierce ou, le cas échéant, l'institution assurant la fonction d'intégrateur au service de cette Autorité publique tierce, d'autre part, sauf si un cadre légal particulier règle ces cas de partage avec cette Autorité publique tierce et l'intervention d'une institution désignée pour assurer la fonction d'intégration, ou encore, interdit l'intervention du Centre d'intégration. Ainsi par exemple, les partages de données entre les Autorités publiques soumises au Code et le registre national ou la banque carrefour resteront soumis aux lois fédérales qui les organisent. Cela vise à assurer la compatibilité avec les autres entités belges dans le cadre d'un partage harmonieux des données.

Article C.IV.7.
La qualité de la donnée partagée

Cet article confère à l'Autorité publique producteur des données la responsabilité de la qualité de la donnée partagée administrativement.

La notion de *« en l'état de l'art et de l'évolution des technologies »* doit se comprendre comme ce qui correspond à l'état des connaissances et de la technique au moment du partage. Ce terme permet au Code d'être technologiquement neutre et d'assurer une pérennité au texte quelle que soit l'évolution technologique.

Dans le livre C.III, la question de la qualité de la donnée est également abordée sous l'angle de la gestion des données afin d'expliquer comment elle doit assurer la qualité dans le cadre d'une bonne gestion/valorisation. Ici, la qualité est envisagée sous l'angle de la responsabilité dans le chef du producteur, avant et pendant une mise en partage administratif des données.

Tout d'abord, c'est bien le producteur qui s'assure de la légalité de la collecte et de l'utilisation des données dont il est à l'origine. Le producteur s'assure que les données sont fiables et conformes aux normes légales et techniques établies.

C'est également le producteur qui peut mettre en place des pratiques de contrôle de qualité appropriées pour garantir que les données sont cohérentes, complètes et exemptes d'erreurs.

Article C.IV.8.
Responsabilité de l'Autorité publique destinataire

Cette responsabilité de l'Autorité publique destinataire ne vise que les cas de mise à disposition des données visées par le partage administratif.

En effet, il appartient à l'Autorité publique destinataire de contrôler les accès aux données mises à la disposition des utilisateurs finaux.

Le passage par le Centre d'intégration permet l'accès d'une Autorité aux données mises à sa disposition. Cela étant, seule cette Autorité peut concrètement contrôler les accès individuels des membres de son personnel.

CHAPITRE 2
Conditions du partage administratif

SECTION 1
Conditions générales

Article C.IV.9.
Conclusion d'un protocole d'accord

Cet article prévoit qu'un protocole d'accord doit être rédigé pour formaliser les modalités de chaque partage administratif de données.

Ce système s'inspire de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel qui prévoit la conclusion d'un protocole d'accord comme condition du partage de données à caractère personnel entre Autorités publiques. Dès lors que le présent Code vise tous les flux de données, le principe de la conclusion d'un protocole d'accord est étendu à tous les flux de données échangés entre Autorités publiques.

Le protocole d'accord visé sera très certainement conclu électroniquement.

Le protocole d'accord est la mise en application concrète des partenariats numériques énoncés au livre C.III entre Autorités publiques.

L'objectif du protocole d'accord est d'abord de garantir que le partage respectera toutes les conditions et limites légales et réglementaires qui s'imposent à chaque flux. Il permet de modaliser certaines de ces conditions en tenant compte des particularités de chaque flux (par exemple les mesures de sécurité spécifiques ou certaines garanties au respect des droits des tiers). Il permet aussi aux parties au partage de fixer les droits et obligations de chacune en définissant les modalités techniques et organisationnelles du partage. Des dispositions supplémentaires s'appliquent lorsque des données à caractère personnel sont concernées par le partage.

La paragraphe 2 détaille le contenu minimal du protocole d'accord conclu entre les Autorités publiques qui partagent administrativement des données, sans préjudices des mentions supplémentaires qui s'imposent en cas de partage de données à caractère personnel examinées au paragraphe 3.

Les protocoles d'accord reprennent d'ailleurs une partie des informations qui accompagnent les données elles-mêmes afin d'assurer une bonne gouvernance.

L'obligation légale ou la mission de services publics qui fonde la demande de partage des données doit être indiquée dans le protocole d'accord. L'objectif est d'identifier qu'il s'agit bien d'un partage administratif.

Les mesures de sécurité comprises dans le protocole d'accord ne doivent pas comprendre un degré de détails exagérément précis étant donné que ce protocole d'accord sera publié. Les mesures de sécurité plus précises que celles indiquées par le protocole d'accord, peuvent être insérées dans un accord de niveau de service (*service-level agreement* ou SLA). Cet accord ne fait pas partie du contenu du protocole d'accord.

Le paragraphe 3 prévoit les différentes informations supplémentaires que le protocole d'accord doit contenir lors d'un partage administratif de données à caractère personnel. En effet, en vue de faciliter le partage administratif de telles données, tout en garantissant un équilibre entre les besoins des Autorités publiques, l'intérêt général et la protection des personnes concernées par les données, le Code, sans préjudice de l'application des règles du RGPD et de autres règles protectrices, impose l'ajout de mentions supplémentaires dans le protocole d'accord afin que ces mentions garantissent un meilleur contrôle du respect des législations précitées et de la vie privée des citoyens

Des dispositions supplémentaires sont également à ajouter dans le protocole d'accord en cas d'anonymisation ou pseudonymisation. Il est nécessaire de clarifier et de détailler les mesures organisationnelles et techniques prises dans le cadre du respect des principes de minimisation des données, de protection de la vie privée par défaut et dès la conception, édictés par le RGPD.

Article C.IV.10.
Procédure de conclusion du protocole d'accord

Le paragraphe 1er énonce que le protocole d'accord doit être conclu dans un délai maximal de quarante jours ouvrables à compter de la réception de la demande, et avant tout partage.

Ce délai de quarante jours ouvrables est raisonnable afin de permettre aux Autorités publiques de

négocier et de conclure un protocole d'accord et d'éviter tout blocage concernant le partage.

Les parties peuvent de commun accord prolonger le délai prévu à l'alinéa 1er notamment dans des situations de demandes importantes ou complexes telles que des demandes impliquant des droits de tiers.

Afin d'aider les Autorités publiques dans la mise en place et la conclusion de protocoles d'accord, des modèles de protocoles d'accord sont rédigés et mis à disposition sur la Plateforme. Cependant, les Autorités publiques ne sont pas obligées d'utiliser ces modèles. Les accords d'adhésion qui détailleront les conditions de services de la Plateforme Bruxelloise détailleront également les règles et conditions techniques minimales requises pour l'utilisation des services du Centre d'intégration.

Le paragraphe 4 détaille les différents avis à récolter préalablement à la conclusion d'un protocole d'accord. Il est nécessaire de demander l'avis du conseiller en sécurité de l'information et de l'administrateur local de la donnée, de même que l'avis du DPO en cas de partage de données à caractère personnel.

Lorsque l'un des avis n'est pas suivi par les parties au partage, le protocole d'accord mentionne, en ses dispositions introductives, les raisons pour lesquelles cet avis n'a pas été suivi. Cela permet aux citoyens ou tout autre personne ou Autorité publique intéressée par ce partage de données de connaître tant les motivations du CSI, de l'administrateur local de la donnée et DPO que des raisons qui justifient leur non-respect.

Le conseiller en sécurité de l'information et l'administrateur local de la donnée ont un délai de vingt jours ouvrables afin de se prononcer à partir du jour où le projet de protocole d'accord leur est envoyé. La demande d'avis leur est adressée simultanément afin que le délai de vingt jours commence à courir à la même date pour tous. Ce délai suspend le délai de quarante jours ouvrables prévu au premier paragraphe en vue de conclure le protocole d'accord.

En cas de partage administratif de données à caractère personnel, le DPO donne également son avis sur le partage administratif des données à caractère personnel et sur le projet de protocole d'accord entre les Autorités publiques parties au partage. Cet avis est nécessaire étant donné la compétence et l'expertise du DPO sur le sujet.

Afin de garantir le respect du principe de protection des données par défaut tel que visé à l'article 25.2 du RGPD, l'absence d'avis du DPO dans les délais impartis sera considéré comme négatif. Conformément aux articles 37 et suivants du RGPD, cet avis n'est pas contraignant. Cela implique que le responsable du traitement n'est pas obligé de se conformer à cet avis réputé négatif mais doit motiver sa décision de ne pas le suivre.

Une suspension de trente jours ouvrables du délai de quarante jours prévu initialement permet aussi de laisser le temps nécessaire à la réalisation de l'analyse d'impact.

Pour rappel, une analyse d'impact est nécessaire *« lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques »*. L'article 35 du RGPD décrit le contenu et les modalités de cette analyse d'impact.

Article C.IV.11.

Publicité du protocole d'accord

L'objectif du protocole est également de garantir la transparence des flux de données dans la sphère publique.

Le protocole est publié dans l'outil de publication du Catalogue des données.

L'envoi du protocole à l'intégrateur de services bruxellois permet que ce dernier puisse mettre en place les conditions techniques et organisationnelles nécessaires au partage administratif. Afin de ne pas retarder ledit partage, cet envoi doit avoir lieu dans le mois de la signature du protocole d'accord.

Article C.IV.12.

Recours auprès de la CADADo

La Commission d'accès aux documents administratifs et aux données (CADADo) est l'autorité compétente pour recevoir tout recours concernant un refus par une Autorité publique de donner suite à une demande partage ou concernant les conditions imposées au partage administratif sollicité.

Les compétences et l'organisation de la CADADo, en tant qu'instance de recours des décisions de partage administratif (mais aussi de réutilisation) est insérée dans le livre B.II.

SECTION 2
Conditions particulières relatives à la mise à disposition de données issues de sources authentiques aux fins de collecte unique

SOUS-SECTION 1
Principe de la mise à disposition de données issues de sources authentiques aux fins de collecte unique

Article C.IV.13.
Partage administratif de données authentiques aux fins de collecte unique

D'un point de vue opérationnel, le partage administratif de données authentiques est une mise à disposition de donnée, telle que définie dans le livre A. III. en tant que *« Procédé qui, dans le cadre d'un partage administratif, permet de rendre les données d'une Autorité publique producteur des données accessibles et utilisables par une Autorité publique destinataire de ces données au moyen d'un accès approprié »*.

L'organisation d'un cadre légal permettant la qualification de certaines données en tant que données issues de sources authentiques a pour objectif d'obliger le partage administratif de ces données afin que les Autorités publiques puissent directement utiliser ces données, dont la qualité se veut garantie (voir ci-après), sans avoir à les collecter à nouveau auprès des usagers (à savoir toute personne physique ou morale qui utilise les services de l'Autorité publique concernée). De la sorte, les Autorités publiques n'ont plus à demander aux usagers ces données et tendent à diminuer leur charge administrative et à accélérer la gestion des services publics.

L'avis n° 93/2023 du 17 mai 2023 de l'Autorité de protection des données, relatif à l'avant-projet de décret et ordonnance conjoints de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française relatifs à la transition numérique des institutions, résume parfaitement ce principe :

« 27. Le principe de collecte unique implique, d'une part, qu'une information concernant un citoyen, qualifiée d'authentique, n'est collectée qu'une seule fois auprès de ce dernier et est ensuite réutilisée par d'autres administrations publiques qui en ont besoin dans l'exercice de leurs missions. Ce principe implique, d'autre part, que les services publics, qui ont besoin d'une donnée authentique dans le cadre de l'exercice de leurs missions légales et qui ne sont pas les gestionnaires de la source authentique, ne peuvent plus collecter cette donnée auprès de la personne concernée à partir du moment où ils sont légalement habilités à consulter la source authentique pour l'exercice de leurs missions. Ils doivent alors la recueillir auprès de l'instance en charge de la source authentique. ».

Pour ce qui concerne la collecte de données à caractère personnel contenues dans une source authentique, l'article commenté du Code constitue la base légale de ce traitement ultérieur, en tant qu'obligation légale dans le chef des Autorités publiques producteurs et destinataires des données issues de source authentique.

Il va de soi, et cela découle directement de la notion de partage administratif, que les Autorité publiques destinataires des données ne peuvent collecter les données issues de sources authentiques que dans le cadre de leurs missions d'intérêt public ou obligations légales.

Conformément aux définitions reprises dans le livre A et aux commentaires l'expliquant, le Code distingue les sources authentiques, désignant les sources organisées par n'importe quel niveau de pouvoir fédéré ou fédéral, parmi lesquelles comptent les sources authentiques bruxelloises.

Les partages administratifs portant sur des données issues de sources authentiques bruxelloises s'effectuent par le Centre d'intégration de la Plateforme bruxelloise de la donnée conformément à l'article C.IV.5. Le principe de la collecte unique implique que les Autorités publiques, qui ne sont pas l'Autorité publique producteur de la source authentique, ne peuvent plus obtenir les données issues de la source authentique autrement que par le Centre d'intégration.

Une dérogation temporaire à ce principe, en faveur de certaines ou de toutes les Autorités publiques, pourrait cependant être prévue à l'égard de certaines sources authentiques bruxelloises, nouvellement désignées comme telles par arrêté, pour des raisons organisationnelles et techniques. En effet, toutes les Autorités publiques ne seront pas en mesure dès l'entrée en vigueur d'un arrêté, décret ou l'ordonnance désignant une nouvelle source authentique bruxelloise d'obtenir l'accès à ces sources directement via le Centre d'intégration. Un temps sera parfois nécessaire pour mettre en place les accès techniques et l'organisation y relative. Pendant ce temps, la possibilité est donc prévue qu'un arrêté dispense les Autorités publiques non prêtes, techniquement et opérationnellement, à appliquer le principe de la collecte unique pour ce qui concerne les données issues de la source authentique nouvellement désignée.

Article C.IV.14.
Partage administratif de données à caractère personnel issues de sources authentiques bruxelloises aux fins de collecte unique

Cet article a été ajouté à la suite de l'avis de l'APD, plus précisément les points 51 à 55.

En effet, l'APD rappelle que :

« La consécration dans une norme du rang de loi (en l'occurrence, une ordonnance) du principe de collecte unique des données (principe « only once ») ne dispense pas le législateur et les autorités publiques de veiller à l'application de l'article 6, 4., du RGPD : la collecte indirecte d'une donnée demeure un traitement ultérieur de données soumis à l'article 6, 4., du RGPD. ».

Afin de permettre que le partage de données issues de sources authentiques bruxelloises puisse se réaliser de manière obligatoire dans le chef des Autorités publiques, la note 107 de l'avis expose, selon le contrôleur européen, que :

« Le RGPD introduit une nouveauté : l'article 6, paragraphe 4, codifie également une exception au principe de limitation de la finalité lorsque le traitement ultérieur repose sur le consentement ou sur le droit de l'Union ou d'un État membre […]

Il ne s'agit toutefois pas d'une autorisation illimitée d'adopter tout texte législatif général et large permettant de réutiliser sans fin des données à caractère personnel entre différents ministères. Conformément à la Charte des droits fondamentaux, la loi doit respecter certaines exigences pour qu'il puisse être dérogé au principe de limitation de la finalité.

En particulier, elle doit constituer « une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, paragraphe 1er ». Ces objectifs couvrent la sécurité nationale, la défense, la lutte contre la criminalité et d'autres objectifs spécifiquement mentionnés d'intérêt public.

Certains de ces objectifs d'intérêt public peuvent être pertinents pour certaines applications spécifiques et ciblées du principe « une fois pour toutes » (par exemple, certaines mesures nécessaires et proportionnées pour lutter contre la criminalité au titre de l'article 23, paragraphe 1er, point d) ou en lien avec la perception des impôts en vertu du point e) de la même disposition). L'allégement de la charge administrative sur les personnes physiques ou les organisations, l'efficacité accrue des procédures administratives et l'économie de temps et de ressources, qui sont souvent les objectifs premiers des applications du principe « une fois pour toutes » constituent sans nul doute des objectifs d'intérêt public valables. Néanmoins, ils ne sont pas spécifiquement mentionnés dans la liste visée à l'article 23, paragraphe 1er, et ne constituent pas en soi un motif licite permettant de restreindre la portée du principe de limitation de la finalité pour atteindre ces objectifs. Cela étant, comme indiqué plus haut, on ne peut exclure que dans certains cas spécifiques, l'un ou l'autre des fondements juridiques des limitations visées à l'article 23, paragraphe 1er, point d), puisse être approprié.

En conclusion, conformément aux observations qui précèdent et à moins qu'un motif approprié de limitation visé à l'article 23, paragraphe 1er, soit disponible ou que les personnes concernées aient donné leur consentement, le principe de limitation de la finalité doit être respecté, même lorsqu'une législation de l'Union ou d'un État membre prévoit l'application du principe « une fois pour toutes » (souligné et référence omise par l'Autorité), CEPD, Avis n° 8/2017 sur la proposition de règlement établissant un portail numérique unique et sur le principe « une fois pour toutes », pp. 11-12. »

En dehors des objectifs visés à l'article 23, § 1er, du RGPD, le consentement de la personne concernée s'avère indispensable à la réalisation du partage administratif de données issues de sources authentiques bruxelloises. L'article inséré vise à organiser le régime dudit consentement.

Article C.IV.15.
Clefs d'identification

Cet article reprend l'article 4 de l'ordonnance du 17 juillet 2020 garantissant le principe de la collecte unique des données et l'article 10 de l'ordonnance du 8 mai 2014 portant création et organisation d'un intégrateur de services régional.

Cet article vise à imposer aux Autorités publiques bruxelloises l'utilisation du numéro de registre national ou du numéro d'entreprise pour l'identification respectivement des personnes physiques et morales. L'utilisation de ces numéros est essentielle dans le cadre des partages administratifs des données issues de sources authentiques bruxelloises pour s'assurer de la correcte identification des citoyens, des entreprises et personnes morales.

Cette obligation vient en réalité palier le fait qu'aujourd'hui certaines Autorités publiques bruxelloises n'ont pas encore demandé les autorisations nécessaires pour disposer de ces numéros. L'absence d'autorisation ne pourra donc plus servir d'excuses pour l'absence de partages administratifs des don-

nées disponibles dans la source authentique bruxelloise concernée.

Cet article n'empêche pour autant pas les Autorités publiques de continuer à utiliser un numéro spécifique dans leur propre back office, mais elles sont obligées d'utiliser les clés uniques susmentionnées dans leurs contacts avec l'intéressé et les autres Autorités publiques. L'accès à leurs données à caractère personnel dans les sources authentiques bruxelloises permet ainsi aux personnes concernées de vérifier également qu'aucune information déjà disponible n'a été demandée.

Cet article n'empêche par ailleurs pas les Autorités publiques de demander d'autres informations aux personnes physiques et morales. Afin d'éviter les erreurs liées à la communication d'un mauvais numéro d'identification, les Autorités publiques peuvent par exemple demander également le nom de la personne ou toute autre donnée permettant de s'assurer de l'identité de la personne.

Cette obligation de faire usage du numéro de registre national est en outre uniquement d'application dans le cadre de la collecte unique des données issues des sources authentiques bruxelloises et dans le cadre des obligations d'informations légales à charges des personnes concernées. Cet article n'empêche donc pas que les citoyens puissent toujours s'adresser par lettre ou courriel à une Autorité publique sans l'utilisation de ce numéro.

Un dernier paragraphe est ajouté concernant les clefs d'identification qui ne concernent ni des personnes physiques ou morales.

SOUS-SECTION 2
Gestion des données issues de sources authentiques bruxelloises

Article C.IV.16.
Qualité des données authentiques bruxelloises

La désignation d'une source authentique bruxelloise a pour objectif que la donnée ne soit collectée qu'une seule fois et que l'ensemble des efforts visant la qualité de la donnée, en particulier les mises à jour, soient concentrés entre les mains d'une Autorité publique, désignée producteur de la source authentique bruxelloise.

Cet article a été ajouté afin de répondre au point 64 de l'avis de l'APD :

« 64. Par ailleurs, l'Autorité est d'avis que le Projet devrait déterminer les critères sur la base desquels une banque de données peut être désignée comme une source authentique de données, en réservant une attention particulière quant à la qualité de la donnée (exactitude, caractère à jour, etc.) concernée et sa relation avec la mission d'intérêt public dont est chargé le responsable du traitement de la source authentique. Le Projet comporte à cette fin des concepts utiles au titre du principe de qualité des données consacré dans l'article C.II.5, selon lequel la « qualité de données se définit sous différentes dimensions complémentaires, à savoir notamment : 1° Consistance, 2° exactitude, 3° Exhaustivité, 4° Vérifiabilité, 5° Validité, 6° Unicité, 7° Intégrité, 8° Ponctualité ».

Article C.IV.17.
Désignation de sources authentiques bruxelloises par le Gouvernement

La désignation d'une source authentique bruxelloise pour certains types de données évite la multiplication de bases de données comprenant des données identiques, collectées par différentes Autorités publiques.

Ceci s'inscrit notamment dans la volonté d'éliminer le plus possible les données non authentiques du réseau. Concrètement, si l'on constate que les bases de données des services publics présentent des chevauchements de données (donc des données non authentiques), la Région, la COCOM et la COCOF examineront comment ces données peuvent être réparties sur plusieurs sources authentiques.

Un mécanisme de désignation des sources authentiques bruxelloises est donc prévu :

– par acte réglementaire pour ce qui concerne les sources authentiques bruxelloises ne comprenant pas de données à caractère personnel. L'arrêté sera adopté par l'exécutif dont dépend l'Autorité publique qui est désigné comme producteur de la source authentique bruxelloise visée;

– par acte législatif pour ce qui concerne les sources authentiques bruxelloises comprenant des données à caractère personnel dès lors que cela constitue une atteinte à la vie privée des personnes concernées comme le souligne l'avis précité n° 93/2023 du 17 mai 2023 de l'Autorité de protection des données :

« 29. Tout d'abord, l'Autorité rappelle que le choix de consacrer une base de données à caractère personnel comme source authentique (ce qui implique, par nature, la réutilisation des données y reprises par diverses administrations pour des finalités autres que celles pour lesquelles elles sont été collectées) ne peut être posé que par le législateur

au sens formel du terme, et ce conformément au principe de légalité consacré par l'article 22 de la Constitution (…) »

Il s'agit bien d'une désignation et non d'une création.

Quand une Autorité publique crée et/ou gère une base de données, elle le fait conformément à une base légale qui lui assigne cette mission et dans le respect des principes applicables, notamment en matière de vie privée. Le mécanisme ici mis en place intervient dans un second temps : lorsqu'une base de données existe au sein d'une Autorité publique, elle peut être désignée pour servir de base de données de référence, en tant que source authentique bruxelloise, pour tout ou partie des données qui y sont incluses, pour d'autres Autorités publiques.

L'initiative de la désignation d'une source authentique bruxelloise peut être prise à la demande de l'intégrateur de services bruxellois, de l'Autorité publique concernée ou encore des exécutifs directement. Des avis préalables doivent être joints à toute demande de désignation de source authentique bruxelloise, particulièrement pour ce qui concerne la désignation de sources authentiques bruxelloises comprenant des données à caractère personnel. En effet, cette exigence fait directement suite à l'avis précité n° 93/2023 du 17 mai 2023 de l'Autorité de protection des données selon lequel :

« 30. Ensuite, avant d'ériger une source de données à caractère personnel au rang de source authentique, il convient de veiller d'une part, à que cette norme réponde aux critères de nécessité et de proportionnalité qui s'imposent à toute ingérence dans le droit à la protection des données et, d'autre part, prévoie des dispositions de procédure permettant de garantir la qualité des données y reprises afin de veiller à la préservation dans le temps de la qualité de ces données. ».

L'acte (décret ou ordonnance) de désignation comprend les informations permettant de caractériser la source authentique bruxelloise et les données qu'elle contient.

Ainsi l'identité de l'Autorité publique désignée producteur de la source authentique est bien entendue précisée afin de savoir quelle entité est responsable du respect des obligations assignées au producteur de la source authentique bruxelloise également responsable de traitement.

Les finalités poursuivies par l'Autorité publique producteur de la source authentique bruxelloise doivent être compatibles avec sa mission de service public.

Doivent également être listées, les données qui y sont contenues.

Pour ce qui concerne les conditions obligatoires à la désignation de sources authentique bruxelloise comprenant des données à caractère personnel, l'avis précité n° 93/2023 du 17 mai 2023 de l'Autorité de protection des données a été suivi à la lettre :

« Ce cadre légal devra déterminer les éléments essentiels des traitements visés (détermination des finalités précises et concrètes pour lesquelles les données sont centralisées et utilisables, des catégories de personnes concernées dont les données seront centralisées et des catégories de données centralisées, des catégories de destinataires pouvant y accéder et des circonstances dans lesquelles un tel accès peu être réalisé, du ou des responsables du traitement de cette source authentique et du délai de conservation des données dans cette source Authentique). Ce cadre légal devra, en outre, prévoir, non seulement, des mesures spécifiques pour préserver les droits et libertés des personnes concernées (tels que, par exemple, l'imposition d'obligation de journalisation précise), mais également, des obligations de transparence spécifiques au profit des personnes dont les données seront centralisées et réutilisées (telles que, par exemple, un droit d'accès spécifique électronique en vertu duquel le gestionnaire de la source authentique met activement à disposition des personnes concernées la liste des institutions qui ont accédés à leur données dans les 6 derniers mois). ».

TITRE 3

Réutilisations des documents et des données publiques

Article C.IV.18.

Deux régimes de réutilisation

Deux régimes en matière de réutilisation doivent être distinguées :

1° selon que le régime de la réutilisation est organisé par la Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte), transposée dans le chapitre I du présent titre;

2° selon que le régime de la réutilisation est organisé par le Règlement sur la gouvernance des données, directement applicable.

Le premier régime concerne aussi bien les documents papier que les données numériques; le second régime se concentre sur les données numériques.

Le premier régime exclut pratiquement les données protégées à l'exception des données à caractère personnel qui ne pourraient être réutilisées que dans le respect des conditions strictes du RGPD en matière de traitement ultérieur des données à caractère personnel visées, ce qui rend l'hypothèse très limitée. Le second régime se concentre uniquement sur les données protégées.

CHAPITRE 1
La réutilisation des documents librement accessibles et partageables

SECTION 1
Champ d'application

Article C.IV.19.
Transposition de la directive 2019/1024

Cette disposition ne nécessite pas de commentaire particulier.

Article C.IV.20.
Champ d'application et exceptions

Cet article transpose l'article 1er de la Directive réutilisation et l'article 2 de l'ordonnance du 27 octobre 2016.

Il importe de noter que l'objet de la directive est la réutilisation des documents, ce qui la distingue du Règlement sur la gouvernance des données visant la réutilisation des données numériques.

Ces distinctions existant au sein du cadre européen visant la réutilisation, il est indispensable de distinguer les différentes hypothèses. En effet, tous les documents ne sont pas nécessairement des données.

Concernant l'interprétation du premier point du deuxième paragraphe, il doit en toute hypothèse être établi que les données détenues dans le cadre des missions de services publics d'une Autorité publique doivent pouvoir faire l'objet d'une réutilisation. En effet, la Directive et les dispositions du présent titre qui la transposent organisent l'obligation de principe dans le chef de toutes les Autorités publiques, de permettre la réutilisation de leurs données collectées dans le cadre de leurs missions de service public. En d'autres termes, il suffit que les données aient été collectées dans le cadre des missions de services publics de chaque Autorité publique pour que ces données puissent faire l'objet d'une réutilisation, aux conditions définitions par le présent titre. L'exception visée doit se comprendre uniquement sur le fait de savoir si l'activité à l'origine des documents visés constitue une mission de services publics ou non.

L'exception visée au point 2° du deuxième paragraphe vise en particulier les cas des services d'intérêt économique général (SIEG) confiés à des Autorités publiques, qui peuvent par ailleurs également exercer des activités qui ne relèvent pas de leurs missions de services publics chaque activité devant être clairement distinguée pour des questions liées à la réglementation des aides d'État notamment. Comme précisé, seules les données détenues dans le cadre des missions SIEG de l'Autorité publique sont visées par le présent titre et peuvent faire l'objet de réutilisation, les autres données collectées en dehors des missions SIEG de l'Autorité publique ne sont pas visées par les hypothèses de réutilisations organisées dans le présent titre, et de manière générale par la directive.

Les considérants de la Directive sont très clairs à ce sujet :

« (13) L'un des principaux objectifs de l'établissement d'un marché intérieur est de créer les conditions propices au développement des services et produits à l'échelle de l'Union et dans les États membres. ***Les informations du secteur public ou celles collectées, produites, reproduites et diffusées dans l'exercice d'une mission de service public ou d'un service d'intérêt général constituent une matière première importante*** *pour les produits et les services de contenu numérique et deviendront une ressource de plus en plus importante sur le plan du contenu à mesure que les technologies numériques de pointe, telles que l'intelligence artificielle, les registres distribués et l'internet des objets, se développeront. Il sera aussi essentiel, à cet égard, d'assurer une vaste couverture géographique transfrontalière. (…)*

(20) Un cadre général fixant les conditions de réutilisation des documents du secteur public est nécessaire afin de garantir des conditions équitables, proportionnées et non discriminatoires pour la réutilisation de telles informations. ***Les organismes du secteur public collectent, produisent, reproduisent et diffusent des documents en vue d'accomplir leurs missions de service public. Les entreprises publiques collectent, produisent, reproduisent et diffusent des documents destinés à fournir des services d'intérêt général. L'utilisation de ces documents pour d'autres motifs constitue une réutilisation.*** *(…) ».*

Une modification a été introduite au niveau du point 8 car l'ordonnance actuelle interdit la réutilisation des données à caractère personnel, ce qui ne fait plus sens vu l'adoption du Règlement sur la gouvernance des données qui a pour objectif de faciliter la réutilisation de ces données. En effet, l'ordonnance actuelle n'autorise la réutilisation des données à caractère personnel qu'une fois anonymisées, à savoir dès lors qu'elles ne sont plus des données à caractère personnel. L'anonymisation des données personnelles limitait donc les possibilités de réutilisation garanties par la directive.

Dans les faits toutefois, la réutilisation des données personnelles, en dehors des garanties offertes par le Règlement sur la gouvernance des données reste limitée comme l'expose le considérant 52 de la directive :

« (52) La présente directive n'affecte pas la protection des personnes physiques à l'égard du traitement des données à caractère personnel garanti par le droit de l'Union et le droit des États membres, en particulier le règlement (UE) 2016/679 et la directive 2002/58/CE du Parlement européen et du Conseil mais aussi et y compris de toute disposition de droit national complémentaire. Cela signifie, entre autres, que la réutilisation de données à caractère personnel n'est licite que si le principe de limitation des finalités énoncés à l'article 5, paragraphe 1er, point b), et à l'article 6 du règlement (UE) 2016/679 est respecté. ».

SECTION 2
Principe de réutilisation

Article C.IV.21.
Réutilisation des données des Autorités publiques, des entreprises publiques, des bibliothèques, des musées et des archives

Cet article transpose l'article 3 de la Directive ISP et l'article 4 de l'ordonnance du 27 octobre 2016.

SECTION 3
Demande de réutilisation

Article C.IV.22.
Demande de réutilisation

Cet article transpose l'article 4 de la Directive ISP et l'article 6 de l'ordonnance du 27 octobre 2016.

La compétence de la CADADo et du Bureau de la donnée a été mentionnée.

Une clarification est apportée afin que la directive ISP soit correctement transposée. En effet, la directive énonce que :

*« 3. En cas de décision négative, les organismes du secteur public communiquent au demandeur les raisons du refus fondé **sur les dispositions applicables du système d'accès en vigueur dans ledit État membre** ou sur les dispositions transposant la présente directive, notamment l'article 1er, paragraphe 2, points a) à h), ou l'article 3. En cas de décision négative fondée sur l'article 1er, paragraphe 2, point c), l'organisme du secteur public fait mention de la personne physique ou morale titulaire des droits, si elle est connue, ou, à défaut, du donneur de licence auprès duquel il a obtenu le document en question. Les bibliothèques, y compris les bibliothèques universitaires, les musées et les archives, ne sont pas tenus d'indiquer cette mention ». (article 4.3)*

Les considérants de la directive exposent que :

*« (23) La présente directive ne limite pas et n'entrave pas l'exercice, par les autorités publiques et les autres organismes du secteur public, des missions qui leur incombent en vertu de la loi. La présente directive fait obligation aux États membres de rendre tous les documents existants réutilisables, **à moins que des règles nationales relatives à l'accès aux documents ne limitent ou n'excluent cet accès ou sous réserve des autres exceptions prévues par la présente directive.** La présente directive s'appuie sur les règles d'accès en vigueur dans les États membres et ne modifie pas les règles nationales en matière d'accès aux documents. Elle ne s'applique pas aux cas dans lesquels, conformément aux règles d'accès pertinentes, les citoyens ou les personnes morales ne peuvent obtenir les documents que s'ils peuvent démontrer un intérêt particulier. Au niveau de l'Union, l'article 41 relatif au droit à une bonne administration et l'article 42 relatif au droit d'accès aux documents de la Charte reconnaissent le droit pour tout citoyen de l'Union et pour toute personne physique ou morale résidant ou ayant son siège statutaire dans un État membre d'avoir accès aux documents détenus par le Parlement européen, le Conseil et la Commission. Les organismes du secteur public devraient être encouragés à mettre à disposition en vue de leur réutilisation tous les documents qu'ils détiennent. Les organismes de service public devraient promouvoir et encourager la réutilisation des documents, y compris des textes officiels à caractère législatif et administratif, dans les cas où l'organisme de service public concerné a le droit d'autoriser leur réutilisation. ».*

Par conséquent, les exceptions formulées par les législations en matière de publicité administrative peuvent être reprises afin de justifier un refus de réutilisation.

Le considérant 18 de la directive ISP fait explicitement référence à la directive en matière d'information environnementale en tant que motif de refus de réutilisation :

« (18) Les États membres ont mis en place des politiques en matière de réutilisation au titre de la directive 2003/98/CE et certains d'entre eux ont adopté des approches ambitieuses en ce qui concerne les données ouvertes pour permettre aux citoyens et aux personnes morales de réutiliser les données publiques accessibles au-delà du niveau minimal fixé par ladite directive. Il existe un risque que la disparité des règles entre les États membres fasse obstacle à l'offre transfrontalière de produits et services et empêche que des ensembles de données publiques comparables soient réutilisés pour des applications paneuropéennes fondées sur ces données. Par conséquent, un degré minimal d'harmonisation est nécessaire pour déterminer quelles données publiques sont disponibles à des fins de réutilisation sur le marché intérieur de l'information, ***en conformité avec les régimes d'accès applicables, tant généraux que sectoriels, tels que celui défini dans la directive 2003/4/CE, et sans les affecter****. ».*

Il est en effet logique que si l'accès n'est pas autorisé, la réutilisation ne le soit pas non plus, qu'il s'agisse de documents administratifs ou d'informations environnementales.

SECTION 4

Conditions de réutilisation

Article C.IV.23.

Publicité des conditions

Cet alinéa est repris de l'article 13, § 4, de l'ordonnance du 27 octobre 2016.

Article C.IV.24.

Formats disponibles

Cet article transpose l'article 5 de la Directive ISP et reprend l'article 13 de l'ordonnance du 27 octobre 2016.

Pour rappel, les normes formelles ouvertes sont définies dans la partie A comme : *« norme établie par écrit, précisant en détail les exigences relatives à la manière d'assurer l'interopérabilité des logiciels ».*

Article C.IV.25.

Principe de tarification

Cet article transpose l'article 6 et 7 de la Directive ISP et reprend l'article 14 de l'ordonnance du 27 octobre 2016.

Article C.IV.26.

Licences

Cet article transpose l'article 8 de la Directive ISP et reprend l'article 15 de l'ordonnance du 27 octobre 2016.

Article C.IV.27.

Données de la recherche

Cette disposition ne nécessite pas de commentaire particulier.

SECTION 5

Non-discrimination et commerce équitable

Article C.IV.28.

Non-discrimination

Cet article transpose l'article 11 de la Directive ISP et reprend l'article 16 de l'ordonnance du 27 octobre 2016.

Article C.IV.29.

Accord d'exclusivité

Cet article transpose l'article 12 de la Directive ISP et reprend l'article 17 de l'ordonnance du 27 octobre 2016.

SECTION 6

Ensembles de données de forte valeur

Article C.IV.30.

Catégories thématiques d'ensembles de données de forte valeur

Cet article transpose l'article 13 de la Directive ISP et reprend l'article 18 de l'ordonnance du 27 octobre 2016.

SECTION 7
Recours auprès de la CADADo

Article C.IV.31.
Recours auprès de la CADADo

La Commission d'accès aux documents administratifs et aux données (CADADo) est l'autorité compétente pour recevoir tout recours concernant la décision d'une Autorité publique en matière de réutilisation. La demande peut émaner du réutilisateur, comme de toute personne affectée par la décision de l'Autorité publique concernée.

Les compétences et l'organisation de la CADADo, en tant qu'instance de recours des décisions de réutilisation est insérée dans le livre B.II.

CHAPITRE 2
La réutilisation des données protégées conformément au Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 (DGA)

Article C.IV.32.
Dispositions générales

Cette disposition ne nécessite pas de commentaire particulier.

Le présent chapitre est volontairement incomplet dans la mesure où il a été introduit afin d'organiser que le cadre légal qui devra être mis en place par la Région, la COCOF et la COCOM afin de décider ou non des conditions d'autorisation des données protégées conformément au Règlement sur la gouvernance de la donnée, devra prendre place à cet endroit du Code.

Il va de soi que habilitation confiée au Gouvernement, Collège réuni et Collège se devra de respecter le cadre légal qui sera mis en place dans le respect du principe de légalité (notamment quant aux conditions d'accès des données protégées dont la réutilisation, s'il est autorisées, ne pourra se faire que conformément au Règlement sur la gouvernance des données).

Les commentaires de l'APD aux points 73 à 85 ont mis en évidence que le cadre légal nécessaire aux autorisations de réutilisation des données protégées devait être mûrement réfléchi notamment au regard des questions de répartitions de compétences entre l'État fédéral et les entités fédérées sur certains motifs qui pourraient être l'origine d'un refus de réutilisation des donnée protégées visées. Ce régime sera inséré à cet endroit du Code, une fois finalisé.

L'avis rendu par le Conseil d'État a pris soin de préciser en termes de compétence que :

« Zoals de Raad van State recent heeft uiteengezet over een federaal voorontwerp van uitvoeringstekst van verordening (EU) 2022/868 van het Europees Parlement en de Raad van 30 mei 2022 « betreffende Europese datagovernance en tot wijziging van Verordening (EU) 2018/1724 » is de uitvoering van die verordening niet uitsluitend zaak van de federale overheid, maar tevens van de gemeenschappen en gewesten, onder meer wat betreft het hergebruik van de gegevens die verband houden met hun materiele bevoegdheden. Het Brusselse Hoofdstedelijke Gewest, de Gemeenschappelijke Gemeenschapscommissie en de Franse Gemeenschapscommissie kunnen dan ook in het aan te nemen gezamenlijk decreet en ordonnantie uitvoeringsmaatregelen van deze verordening opnemen, binnen hun materiële bevoegdheden ter zake. ».

Il ne fait en effet aucun doute que la Région la COCOF et la COCOM sont compétentes pour l'implémentation du Règlement sur la gouvernance des données pour ce qui concerner la réutilisation de leurs données protégées.

L'avis de l'APD a toutefois souligné qu'il s'agissait d'organiser le régime d'accès à ces données, pour autant que le principe de la réutilisation des données protégées soit organisé ou décidé par les Autorités publiques. Au point 80 de l'avis de l'APD, celle-ci rappelle en effet que le Règlement sur la gouvernance des données n'emporte « *toutefois aucune obligation de permettre la réutilisation de ces données protégées : c'est au droit national qu'il incombe d'organiser la réutilisation de ces dernières* ». C'est donc bien à la Région, à la COCOF et à la COCOM qu'il appartiendra d'organiser cette réutilisation, non seulement quant à la possibilité de le faire, mais également au niveau du régime d'accès à ces données.

Ce régime d'accès pourrait selon l'avis remis de l'APD pourrait être décidé sur la base de deux options : soit l'organisation d'une nouvelle voie d'accès aux documents, soit le renvoi à l'exercice d'une voie préexistante d'accès aux données.

Bien que la question ne soit pas tranchée par le Code, en toute hypothèse, comme le rappelle la section de législation du Conseil d'État dans son avis n° 65.516/2 concernant le décret et ordonnances conjoints relatif à la publicité administrative :

« II. La compétence des entités concernées par l'avant-projet.

Il résulte de la légisprudence de la section de législation, résumée dans l'avis n° 39,823/3 donné le 28 février 2006 sur l'avant-projet devenu la loi du 5 août 2006 « relative à la publicité de l'information en matière d'environnement », que chaque autorité dispose d'une double compétence : d'une part, déterminer les modalités générales de la publicité de l'administration en ce qui concerne ses propres services et organismes ainsi que les personnes morales dont elle peut régler l'organisation (le critère dit organique) et, d'autre part, fixer, dans le cadre de sa compétence matérielle, les motifs d'exception valant pour toutes les autorités administratives, et donc également pour des autorités administratives autres que celles qui relèvent de la compétence du législateur concerné (le critère dit matériel). Autrement dit, les autorités bruxelloises peuvent prévoir les exceptions à la publicité que devront respecter toutes les autorités administratives, même celles relevant d'un autre niveau de pouvoir, la limite à cette compétence étant que ces exceptions doivent relever de la compétence matérielle des autorités bruxelloises. Plus particulièrement, le seul lien requis entre le document administratif sur lequel porte le motif d'exception et l'autorité qui a fixé celui-ci est le préjudice que la publicité du document peut porter aux intérêts de cette autorité.

(…)

Le corolaire de ce qui précède est que chaque autorité ne peut prévoir d'exceptions que relevant de ses compétences et ne peut se soucier des intérêts des autres niveaux de pouvoir. Ainsi, l'avis n° 24.931/8 précité a-t-il critiqué la mention de la sécurité de la population, des relations internationales, de l'ordre public, du caractère par nature confidentiel des informations d'entreprise ou de fabrication communiquées à l'autorité parmi les motifs d'exception à la publicité en raison du fait que ces matières relevaient de la compétence de l'autorité fédérale. ».

« Par conséquent, comme l'indique le commentaire de l'article C.IV.32 examiné par le Conseil d'État, la question du partage des compétences se situe au niveau des conditions d'accès aux données protégées et de l'articulation des conditions d'accès qui seront fixées par la Région, la COCOM et la COCOF avec les conditions d'accès fixées par les autres niveaux de pouvoir dans le cadre de leurs compétences matérielles. À ce jour, seul un projet de loi fédéral a été soumis pour avis au Conseil d'État mais n'a pas été déposé à la Chambre des représentants. La Région, la COCOM et la COCOF, n'ont par conséquent pas de vue sur la manière dont l'État fédéral a fait usage de ses compétences matérielles quant aux conditions d'accès des données protégées visées par le Règlement sur la gouvernance des données en vue de leur réutilisation.

Article C.IV.33.
Recours après de la CADADo

La Commission d'accès aux documents administratifs et aux données (CADADo) est l'autorité compétente pour recevoir tout recours concernant la décision d'une Autorité publique suite à une demande de réutilisation conformément au Règlement sur la gouvernance des données.

Les compétences et l'organisation de la CADADo, en tant qu'instance de recours des décisions de réutilisation est insérée dans le livre B.II.

TITRE 4
Communication

Article C.IV.34.
Dispositions générales

L'altruisme des données désigne la Communication de données à des fins d'intérêt général, par exemple au profit de projets de la recherche médicale, la lutte contre le réchauffement climatique, l'optimisation de la mobilité, la simplification de l'établissement de statistiques officielles, l'amélioration de l'offre de services publics, la constitution de politiques publiques, …

L'altruisme des données implique les individus et les entreprises qui donnent leur consentement ou la permission de mettre à disposition des données qu'elles génèrent volontairement et sans contrepartie pour être utilisées dans l'intérêt public. Ces données sont le vecteur principal de progression au profit de la recherche et du développement de meilleurs produits et services.

LIVRE C.V.
La plateforme bruxelloise de la donnée

Le présent livre est consacré aux dispositifs techniques mis en place en vue de permettre le partage administratif, la réutilisation de données ou la communication décrits dans le livre C.IV.

Paradigm est désigné en qualité de gestionnaire de la plateforme et est également « intégrateur de service » conformément à la définition reprises au livre A.III.

L'ensemble de l'infrastructure technique est reprise sous le vocable de « Plateforme » mais cette appellation reprend en réalité plusieurs dispositifs techniques, décrits ci-dessous de manière systématique :

1° un Centre d'intégration;

2° un Catalogue des données;

3° un Portail ouvert des données publiques;

4° un Centre d'exploitation et d'analyse des données;

5° un « Point de contact »;

6° le « service d'appui » décrit par le Règlement sur la gouvernance des données.

L'objectif global poursuivi au travers de la mise en place de la Plateforme bruxelloise de la donnée est d'offrir un environnement technique unique et sécurisé qui permette à toutes les Autorités publiques d'avoir recours à des outils communs, ce qui permettra, in fine, d'atteindre les objectifs stratégiques et opérationnels du présent Code.

La Plateforme fournira également de nombreuses informations juridiques et techniques au travers des accords d'adhésion, du cadre documentaire aux bénéficiaires des services.

TITRE 1
Principes de la Plateforme bruxelloise de la donnée

Article C.V.1.
Création et objectif de la Plateforme bruxelloise de la donnée

La Plateforme Bruxelloise de la donnée regroupe un ensemble de services concourant à la mise en place d'une gouvernance des données conforme aux principes du Code.

La mise en place et l'adhésion de toutes les Autorités publiques à la Plateforme bruxelloise de la donnée permettra de rencontrer les objectifs du Code dans plusieurs domaines.

Premièrement, en matière **d'accessibilité**, la création d'une plateforme centralisée permet que les données publiques soient facilement accessibles pour les utilisateurs, en ce compris les Autorités publiques elles-mêmes, ce qui peut encourager son utilisation par une audience sans cesse croissante.

Deuxièmement, l'utilisation d'une Plateforme centralisée facilitera la **cohérence** et l'homogénéité des données en circulation. Les (ré)utilisateurs pourront ainsi être assurés de la qualité des données. En effet, la possibilité de trouver l'ensemble des données partageables en un lieu unique réduira le risque d'erreurs ou de contradictions inhérents à la multiplication de sources ou de canaux.

Troisièmement, l'utilisation d'une Plateforme centralisée participe à un processus **de structuration et de normalisation des données**, et facilite leur comparaison et leur analyse, ce qui peut contribuer à une meilleure compréhension de l'information et à des prises de décision plus éclairées.

Quatrièmement, la centralisation des données publiques permet de réaliser des **économies d'échelle** en réduisant les coûts de collecte, de stockage et de maintenance des données. Cela concerne notamment les services du Centre d'exploitation et d'analyse des données et du Portail ouvert des données publiques.

Cinquièmement, enfin, la mise en place d'une Plateforme centralisée stimule l'innovation en fournissant un accès facile aux données publiques à des développeurs tiers qui peuvent créer des applications et des services innovants basés sur ces données qui leurs sont proposées.

Article C.V.2.
Missions du gestionnaire de la Plateforme bruxelloise de la donnée

L'on note cependant que la mise en œuvre des différentes missions ne peut s'envisager que de manière globale et que le gestionnaire doit adopter une stratégie cohérente et progressive à cet égard.

Le point 1 n'appelle pas de commentaires.

En ce qui concerne le point 2, il serait déraisonnable de prévoir que le gestionnaire doive s'assurer du contrôle de la qualité de l'intégralité des données publiques; il est préférable de prévoir que le gestionnaire ait pour mission de promouvoir des outils dont les utilisateurs pourront bénéficier afin de veiller par eux-mêmes à la qualité de leurs données.

Le point 3 concerne l'établissement des documents juridiques relatifs à l'utilisation de la Plateforme (conditions d'utilisation, modalités d'adhésion aux différents services). Les accords d'adhésion définissent les différentes conditions techniques, juridiques et éventuellement financières de souscription aux services de la Plateforme. Il appartient au gestionnaire de mettre en place le socle commun que l'ensemble des Autorités publiques devra rejoindre. En ce qui concerne plus spécifiquement l'Intégrateur, il s'agit des anciennes banques de règles qui énonçaient les modalités techniques et juridiques moyennant lesquelles l'Intégrateur accordait le droit d'utilisation de ses services.

Le point 4 concerne la vérification de conditions fixées par le Règlement eIDAS pour les schémas

d''identification et l'authentification des services de confiance. Ces questions d'identification ou de certification et qui pourraient intervenir dans certaines interactions avec la plateforme (réutilisation, communication). Ce point est prévu « le cas échéant », dès lors que toute utilisation de la plateforme n'implique pas nécessairement l'usage de moyens d'identification ou de certification au sens de l'EIDAS.

Les tiers de confiance jouent un rôle crucial en matière de protection des données et de garantie de la conformité au RGPD. Ils peuvent offrir divers services, tels que la gestion des clés de chiffrement, la pseudonymisation, ou l'anonymisation de données. Leur objectif est d'apporter une sécurité et une confiance supplémentaires aux individus et aux organisations qui traitent des données personnelles.

Ce dernier doit être soumis à des obligations de secret professionnel et être indépendant par rapport au responsable de traitement initial.

Accorder la possibilité au gestionnaire d'une plateforme de données de désigner un tiers de confiance est une mesure de bonne gouvernance pour plusieurs raisons :

– les tiers de confiance possèdent une expertise spécifique dans la protection des données et la conformité au RGPD. Ils sont formés pour évaluer les risques liés aux données à caractère personnel, mettre en œuvre des mesures de sécurité appropriées et assurer la conformité aux exigences légales en ce qui concerne l'anonymisation ou la pseudonymisation;

– le RGPD place la responsabilité de la protection des données à caractère personnel sur les épaules des organisations qui les collectent et les traitent selon les finalités et les moyens qu'ils ont fixés (les responsables du traitement des données). Cependant, travailler avec un tiers de confiance peut aider à répartir certaines responsabilités et à renforcer la sécurité globale des données. En désignant un tiers de confiance, le gestionnaire de la plateforme démontre son engagement envers une gestion responsable des données personnelles. Toutes les autorités ne disposent pas nécessairement des compétences et/ou des moyens nécessaires à l'anonymisation de données.

– le recours à un tiers de confiance peut renforcer la transparence et la confiance entre les parties prenantes. Les tiers de confiance peuvent fournir des certifications, des rapports d'audit ou des attestations qui témoignent de la conformité de certains partages de données ce qui permet aux utilisateurs de la plateforme d'avoir une plus grande confiance dans la gestion et la protection de leurs données protégées.

Le point 6 est relatif à la fourniture des informations techniques relatives à l'utilisation de la Plateforme et des informations relatives à son usage.

Les statistiques d'usages peuvent faire l'objet de la publication d'un rapport annuel. Ce dernier permettra de connaître le fonctionnement de la Plateforme et de ses services afin de mieux identifier les besoins de ses utilisateurs et le cas échéant de réallouer les ressources en conséquence.

Le point 7 concerne le conseil et l'assistance que doit apporter le gestionnaire aux Autorités publiques qui recourent à ses services. Cette mission de conseil et d'assistance est une mission générale, mais elle peut être illustrée par une série d'exemples. Ainsi, le gestionnaire doit être en mesure de former les utilisateurs, mais également de les épauler au cas où ils décident de lancer un projet particulier relatif aux données publiques et faisant intervenir la Plateforme ou ses services. Dans ce cadre, le conseil du gestionnaire doit intervenir en amont, afin de satisfaire les obligations de conception « data by design ». Parallèlement, le gestionnaire doit également remplir une mission de suivi continu et évolutif des fonctionnalités et de l'architecture de la Plateforme : sa mission est d'assurer le suivi au regard de la stratégie commune relative aux données.

Il faut enfin noter que ce qui est inscrit dans le Code ne pourrait être exhaustif. Les modalités d'organisation des missions dévolues à la Plateforme par l'alinéa 1er sont du ressort du Gouvernement, du Collège réuni, du Collège, qui peut en fixer les limites et les précisions par arrêté.

TITRE 2
Les services de la Plateforme bruxelloise de la donnée

CHAPITRE 1
Dispositions générales

Article C.V.3.
Accord d'adhésion

Conformément aux missions énoncées à l'article C.V.2, le gestionnaire met en place l'accord d'adhésion nécessaire à l'encadrement de l'utilisation des services proposés par la Plateforme à une Autorité publique.

De manière schématique, l'on peut rapprocher la figure de l'accord d'adhésion de l'établissement de conditions générales d'utilisation de la Plateforme.

Cet accord peut prendre des formes très diverses.

En effet, il serait déraisonnable que l'utilisateur personne physique souhaitant uniquement recourir aux services publics de la Plateforme doive effectivement signer, même de manière électronique, un corpus de règles. Dans ce cas, l'utilisateur est informé, de manière active, des conditions générales d'utilisation, dont il peut prendre connaissance à tout moment et de manière aisée.

En revanche, pour les Autorités publiques recourant, par exemple, à des services facultatifs de la Plateforme, cet accord prend une forme bien plus détaillée. Dans ce cas, l'accord mentionne le ou les services ainsi que leurs conditions particulières d'utilisation, notamment en matière financière le cas échéant.

Il est également prévu que le gestionnaire établisse des différents cadres spécifiques en fonction des services sollicités, au regard du nombre d'Autorités publiques potentiellement concernées notamment. En effet, l'adoption d'un tel accord ayant vocation à se répéter avec chacune des Autorités publiques, au minimum pour le partage administratif, celui-ci peut être standardisé afin d'être proposé la signature. Il en va de même pour différents services dont les conditions ont vocation à se répéter.

Par ailleurs, il est nécessaire que l'utilisateur physique signataire, au nom et pour le compte de l'Autorité publique dont il fait partie, ou de toute autre personne morale, ait effectivement reçu un mandat ad hoc pour engager cette entité. Conformément au paragraphe 2, le gestionnaire de la Plateforme garantira en tous les cas que ce mandat lui soit fourni lors de la signature.

Article C.V.4.

Finalités des traitements

Conformément à la jurisprudence constante de l'APD, concernant le principe de légalité et de prévisibilité consacré à l'article 8 de la Convention européenne des droits de l'Homme et à l'article 22 de la Constitution, les éléments essentiels des traitements des données à caractère personnel que comporte la Plateforme doivent être énoncés dans le livre CV. Bien entendu les énoncés de ces éléments essentiels de traitement doivent être lus en combinaison avec la législation organique des Autorités publiques.

Les finalités sont abordées service par service.

Article C.V.5.

Qualification conformément au RGPD

Des données à caractère personnel seront traitées dans le cadre des services de la Plateforme. Il est nécessaire, au regard des dispositions applicables en la matière et notamment du RGPD, de prévoir le rôle que le gestionnaire endosse.

Ce rôle n'est pas similaire en fonction des services envisagés et est éminemment casuistique : bien qu'un listing de chacun des traitements doive être, en pratique, effectué dans le cadre de la Plateforme ainsi que l'identification du rôle correspondant, il serait disproportionné de le prévoir dans le cadre du texte présent Code.

En revanche, en ce qui concerne particulièrement le Centre d'intégration, le gestionnaire définit aussi les moyens pour le recours aux services. Partant, il est, pour cette partie de la Plateforme uniquement, au moins coresponsable ou responsable du traitement.

Il en va également de même du rôle du gestionnaire en ce qui concerne les données à caractère personnel collectées nécessairement pour la gestion technique de la plateforme (ex : login d'accès).

De manière générale, les services offerts par la Plateforme et le détail du fonctionnement de celle-ci n'est pas de nature à fonder ou permettre le traitement de données à caractère personnel en tant que tel. Ces derniers ne sont permis qu'en exécution d'une mission de service public et conformément à la loi organique relative à l'autorité concernée.

PARADIGM offre des services à des Autorités publiques. Lorsque ces services concernent des données à caractère personnel, il est entendu que l'Autorité qui a recours à ceux-ci doit s'assurer du fondement des traitements pour lesquels elle sollicite l'intervention de PARADIGM dès lors que les articles de la présente section n'ont pas pour vocation d'offrir une base de justification pour les traitements des données à caractère personnel.

Les services facultatifs de PARADIGM sont offerts à des Autorités publiques dans le cadre de l'exécution de leurs missions de services publiques et sans préjudice de lois et règlements applicables, notamment à la protection de la vie privée.

Paradigm ne stocke et archive les données personnelles techniques d'utilisateurs de ses services que dans le but d'assurer une traçabilité des opérations de traitements ou plus précisément des transferts de données pour lesquels Paradigm prête son concours. Agissant de la sorte, il sera permis de vérifier la légalité et la traçabilité des accès aux données.

Il n'y a pas à proprement parler de stockage de données personnelles au sein de PARADIGM lorsqu'il assure techniquement un partage administratif via un canal qu'il fixe à la demande d'une autre autorité publique. Le partage organise permet l'accès à une donnée stockée auprès d'une autorité publique autre (régionale ou fédérale) au profit de l'autorité publique qui sollicite PARADIGM pour le partage. Le cas échéant, il n'y ni de stockage ni de conservation, PARADIGM n'offrant que le « chemin » qui sera emprunté par les données entre deux autorités.

Dans le cadre du centre d'intégration, le responsable de la plateforme est responsable d'un unique traitement ayant pour finalité le transfert de tous les types de données à caractère personnel requises par une Autorité dans le cadre de sa mission de service public.

Le gestionnaire de la plateforme traite également des données de contact (nom, prénom, courriel) à caractère personnel des utilisateurs de la plateforme afin d'en assurer la gestion technique et la traçabilité des opérations qui y sont réalisées. La gestion technique recoupe le point de contact et le service d'appui.

Article C.V.6.
Catégories de données à caractère personnel et personnes concernées

Conformément au principe de légalité prévalant en matière de respect de la vie privée, les éléments essentiels des traitements des données à caractère personnel réalisés par la Plateforme bruxelloise de la donnée doivent être mentionnés dans un texte de portée législative.

Pour rappel, la Plateforme bruxelloise de la donnée est un outil technique et numérique mis à la dispositions des Autorités publiques soumises à la partie C du Code. La mission de la Plateforme est d'organiser et sécuriser les échanges de données des Autorités publiques dans le cadre de leurs missions de service public et leurs obligations d'intérêt général. Par conséquent, les données à caractère personnel qui seront traitées par la Plateforme sont les données publiques à caractère personnel des Autorités publiques. Il est impossible de définir autrement ces données car ces données sont directement définies par les missions de services publics et les obligations d'intérêt général des Autorités publiques, en ce qu'elles sont nécessaires à l'exercice de ces activités.

Pour ce qui concerne les Autorités publiques disposant d'un cadre légal organique, soit sous la forme d'un texte à portée législative, éventuellement réglementaire, les données publiques visées, seront conformément au principe de légalité, précisées dans ce cadre légal organique. Pour les Autorités publiques ne disposant pas de pareil cadre légal organique législatif (le cas échéant également réglementaire), les données susceptibles de faire l'objet de traitements par la Plateforme seront les données nécessaires à leurs missions de services public ou leurs obligations d'intérêt général, à savoir les données publiques, selon la définition du Code, de ces Autorités publiques.

Compte tenu de ce qui précède concernant caractère de support numérique de la Plateforme qui se limite à organiser les outils techniques nécessaires aux flux de données des Autorités publiques dans le cadre de leurs missions de services publics et obligation d'intérêt général, les personnes concernées ne peuvent être autrement définies que par références aux personnes concernées des données publiques des Autorités publiques.

Article C.V.7.
La durée de conservation des données

En ce qui concerne les données à caractère personnel nécessaires à la gestion technique des services de la Plateforme bruxelloise de la donnée, les données sont conservées jusqu'à 10 ans après la fin du traitement, ce qui correspond au délai de droit commun en matière de prescription d'obligations personnelles. Le délai de 10 ans se justifie pour des raisons de sécurité et de traçabilité des accès aux données à caractère personnel. Le but est ainsi de s'assurer de pouvoir vérifier les accès et les éventuelles modifications apportées aux données les plus importantes des usagers bruxellois.

En ce qui concerne l'ensemble des traitements des données à caractère personnel réalisés par le Centre d'intégration les données sont conservées jusqu'à la fin du traitement. Le traitement se limitant au transfert, les données ne sont pas conservées, il n'y a pas de délai de conservation les concernant.

L'avis de la section de législation du Conseil d'État a souligné concernant la durée de conservation des données à caractère personnel ayant fait l'objet d'un traitement par le Centre d'exploitation et d'analyse que la fixation de la durée par le responsable de traitement ne répondait pas aux exigences du principe de légalité mentionné à l'article 22 de la Constitution. Ceci témoigne d'une certaine incompréhension quant

aux services offerts par le Centre d'exploitation et d'analyse lequel est défini à l'article C.V.14 comme suit :

« Il est créé un Centre d'exploitation et d'analyse des données.

L'objectif du Centre d'exploitation et d'analyse des données est de proposer, notamment aux Autorités publiques, en vue de la réalisation de leurs missions de service public, des services facultatifs fixés par le Gouvernement, le Collège réuni et le Collège. ».

À ce jour, les services facultatifs du Centre d'exploitation ne sont pas définis et ne le seront que dans le cadre d'un arrêté conjoint. Toutefois, il est évident que, à l'instar des autres services de la Plateforme, le Centre d'exploitation et d'analyse aura pour mission d'offrir des services numériques aux Autorités publiques ou à d'autres entités. La durée de conservation des données traitées par le Centre d'exploitation et d'analyse dans le cadre des services qui seront définis par arrêtés conjoints, notamment afin de cadrer au mieux avec les besoins multiples et ponctuels des Autorités publiques, ne pourra être déterminée que par le responsable de traitement de ces données, à l'égard duquel le Centre d'exploitation et d'analyse ne sera qu'un sous-traitant comme le mentionne l'article C.V.5.

C'est donc l'entité bénéficiaire des services facultatifs du Centre d'exploitation et d'analyse qui, détermine les durées de conservation des données sous-traitées par Paradigm.

En effet, en ce qui concerne les traitements des données à caractère personnel réalisés par le Centre d'exploitation et d'analyse, le Catalogue des données, les durées de conservation sont fixées par le responsable de traitement qui en confie la sous-traitance au gestionnaire de la plateforme.

En ce qui concerne les traitements des données à caractère personnel réalisés par le Portail ouvert des données, les données sont conservées jusqu'à un an après la fin du traitement.

En ce qui concerne les traitements des données à caractère personnel réalisés par le Point de contact et d'information, les données sont conservées jusqu'à un an après la fin du traitement.

En ce qui concerne les traitements des données à caractère personnel réalisés par le Service d'appui, les données sont conservées jusqu'à un an après la fin du traitement.

Les données sont détruites à l'échéance des délais précités ou conservées conformément à la législation et la réglementation en matière d'archivage à des fins historiques ou culturelles.

Article C.V.8.
Destinataires auxquels les données seront communiquées et les circonstances dans lesquelles elles leur seront communiquées

Les données à caractère personnel concernées par les traitements visés à l'article C.V.4. peuvent être communiquées :

– aux Autorités publiques destinataires des partages administratifs,

– aux réutilisateurs conformément au titre 3 du livre C.IV.,

– aux Autorités publiques destinataires d'une Communication.

Article C.V.9.
Traçabilité

Compte tenu du fonctionnement du Centre d'intégration, ce dernier ne réalise, pour l'essentiel, qu'une mise à disposition des données détenues par une Autorité publique au profit d'une autre.

Si le Centre peut vérifier la légalité de l'opération et l'ouverture d'une base de données au profit d'une Autorité publique, il n'a pas pour autant de vision (pour des raisons techniques liées à l'infrastructure de l'Autorité publique destinataire du partage) sur le fonctionnaire/agent qui sera l'utilisateur final de la donnée. Il appartient donc à l'Autorité publique destinataire d'organiser la traçabilité des accès en son sein afin de garantir l'intégrité et la confidentialité des données lorsqu'elles sont utilisées par ses membres.

Idéalement, ceux-ci doivent être identifiés personnellement ainsi que les services dont ils relèvent afin de garantir un usage conforme au protocole prévu.

Article C.V.10.
Financement

Il est prévu que la Plateforme soit financée par deux voies complémentaires. Il s'agit :

1° d'une part du budget octroyé par la Région de Bruxelles-Capitale, la COCOM et la COCOF;

2° d'autre part, des redevances éventuellement perçues de la part des Autorités publiques utilisatrices de la Plateforme.

Le paragraphe 2 prévoit qu'une redevance puisse être fixée par le gestionnaire de la Plateforme pour la rémunération des services techniques prestés dans le cadre de la Plateforme à l'égard de l'Autorité publique utilisatrice de la Plateforme. Ces frais de diffusion doivent être repris dans le cadre du calcul de la redevance visée à l'article C.IV.25 dans le cadre des redevances perçues en matière de réutilisation.

Enfin, dans une idée de transparence, le gestionnaire publie les modalités financières de l'utilisation de la Plateforme afin de permettre aux Autorités publiques d'effectuer un suivi des coûts des services de la Plateforme. Cette publication concerne le mode de calcul de la redevance.

CHAPITRE 2
Le Centre d'intégration bruxellois

Article C.V.11.
Création et objectif

Le Centre d'intégration Bruxellois de la donnée est un service dédié à assurer le partage administratif entre Autorités publiques.

Le passage par le Centre d'intégration est obligatoire pour tous les partages administratifs.

La nature des données visées par le partage administratif, rend nécessaire la mise en place technique de plusieurs canaux au sein de Centre d'intégration. Plus particulièrement, il apparaît nécessaire que les données issues de sources authentiques et les données à caractère personnel soient traitées dans un canal distinct du reste des données, de manière à leur assurer un environnement sécurisé optimal.

Le rôle du Centre d'intégration est double :

1° il dispose d'un rôle technique car il vérifie ou met en place les mesures opérationnelles nécessaires à garantir le partage administratif des données;

2° son rôle est également juridique puisqu'il ne permet l'accès des données qu'aux Autorités publiques qui peuvent effectivement réaliser un partage administratif au regard des missions de service public qui leur sont dévolues et qui sont mobilisées dans le cadre du protocole d'accord y relatif.

Vu la complexité de la gestion technique et, le cas échéant, le caractère évolutif des dispositions techniques mises en place au sein de le Centre d'intégration, il est renvoyé au cadre réglementaire plus souple qui devra être mis en place et implémenté de manière conjointe par les trois exécutifs.

Article C. V. 12.
L'intégrateur de services bruxellois

Paradigm est également désigné comme intégrateur de service au sens défini par le Code et reçoit la qualité d'Intégrateur de service bruxellois, à savoir : l'entité qui recense des données provenant de différentes sources pour les rendre accessibles aux utilisateurs finaux.

Son rôle principal est de faciliter l'accès et l'utilisation des données publiques en les regroupant de manière centralisée et en fournissant des interfaces standardisées pour leur consultation.

Le Centre d'intégration est l'outil technique qui identifie les données pertinentes auprès de diverses Autorités publiques et Autorité publiques tierces.

La gestion de la Plateforme dépasse le cadre de l'intégration de services, car la Plateforme comprend d'autres services étrangers de cette fonction d'intégrateur de services (Catalogue, Portail etc.). La gestion de la Plateforme requiert également la mise en place d'une infrastructure plus importante que celle nécessaire à l'intégration de services au sens strict.

Le gestionnaire de Plateforme a un rôle plus large et peut fournir des services supplémentaires au-delà de l'intégration des données. La plateforme inclut également des fonctionnalités telles que la visualisation des données, des outils d'analyse, des fonctionnalités de collaboration, des services de publication, des mécanismes de contrôle d'accès, etc. Le gestionnaire de Plateforme peut également être responsable de la maintenance technique de la plateforme, de la gestion des utilisateurs, de la sécurité des données, de la gestion des incidents soit autant de missions qui dépassent celles de l'intégrateur de services.

En ce qui concerne l'intégrateur lui-même, les missions qui lui sont confiées sont les suivantes :

1° recevoir et donner, s'il y a lieu, suite aux demandes de consultation et de demande de partage des données enregistrées dans une ou plusieurs base(s) de données.

C'est l'intégrateur qui reçoit les demandes relatives aux accès à des données (authentiques ou personnelles);

2° promouvoir et veiller à l'homogénéité des droits d'accès aux bases de données;

3° élaborer les modalités techniques visant à développer les canaux d'accès de la manière la plus efficace et là plus sûre possible;

4° promouvoir une politique de sécurité coordonnée pour le réseau.

Afin de rendre homogène la gestion des accès, à l'échelle de l'ensemble des autorités publiques Bruxelloises, l'intégrateur propose les modalités d'accès les plus pertinentes en termes de sécurité et traçabilité;

5° procéder au partage administratif de données intégrées à la demande de l'Autorité publique destinataire.

À la demande d'une Autorité publique qui va lui en confier la gestion, l'intégrateur peut réaliser l'intégration de données dans une base dont il sera le diffuseur pour l'autorité producteur;

6° développer pour les services publics participants des applications utiles à l'échange et/ou l'intégration de données conservées dans les banques de données;

7° organiser la collaboration avec d'autres intégrateurs de services.

Les points 6 et 7 n'appellent pas de remarques.

CHAPITRE 3
Le Catalogue des données

Article C.V.13.
Création et objectifs

Le Catalogue des données, qui fait partie de la Plateforme, se présente, du point de vue de l'utilisateur, en deux parties, décrites au paragraphe 1er, alinéa 2, 1° et 2°.

La première est mise en place à l'usage exclusif des Autorités publiques, au travers de laquelle elles pourront prendre connaissance de l'inventaire des données détenues par les autres Autorités publiques; la seconde est mise en place à destination du public sans distinction, et ne contient que la liste des métadonnées relatives aux données détenues par les Autorités publiques.

La mise en place du Catalogue des données permet de rencontrer différents objectifs.

Premièrement, il s'agit d'une démarche visant la **transparence**, puisque le Catalogue des données permet de présenter une vision claire et – destinée à être – complète des données détenues par les Autorités publiques, permettant ainsi aux citoyens de mieux comprendre l'étendue des données détenues par les Autorités publiques grâce à l'outil de publication.

Deuxièmement, il s'agit de renforcer le **contrôle** des Autorités publiques sur leurs données et sur les données des autres Autorités publiques. En identifiant les détenteurs de données, le Catalogue des données aide à assurer une meilleure utilisation et protection des données à l'échelle régionale par l'Autorité publique elle-même qui peut maintenir à jour l'inventaire de ses données grâce à l'outil technique.

Troisièmement, l'objectif est d'assurer une **coordination** et une **harmonisation** entre les différentes Autorités publiques. Une telle coordination améliore la qualité des données et réduit les coûts de collecte et de gestion des données.

L'on précise encore que le Catalogue des données ne permet le stockage d'aucune donnée de contenu : seuls sont rendues disponibles des métadonnées.

En vue des réutilisations, la partie publique du Catalogue des données est en lien direct avec le Portail ouvert des données publiques et permet un accès aux données qui y sont inventoriées.

CHAPITRE 4
Le Portail ouvert des données publiques

Article C.V.14.
Création et objectifs

Le Portail ouvert des données publiques est l'ensemble des jeux de données accessibles en open data via la Plateforme Bruxelloise de la donnée qui les héberge ou permet leur accès (auprès du producteur qui les héberge).

Au jour de l'adoption du présent Code, le portail ouvert des données publiques permet notamment l'accès aux informations visées par l'initiative « *Open budget* », telle que décrite dans la Circulaire du 16 décembre 2021 précisant les modalités de publication en open data des inventaires des marchés publics et des subventions par les autorités bruxelloises visés par les décret et ordonnance conjoints du 16 mai 2019.

Le gestionnaire de la Plateforme bruxelloise obtient les jeux de données open data auprès de l'Autorité publique considérée comme le producteur des données. La qualité et les éventuelles mises à jour des

données sont effectuées par le producteur qui les transmets ensuite à la Plateforme afin d'alimenter le portail ouvert des données publiques.

Les données dont la réutilisation est proposée peuvent être hébergées au sein du portail ouvert des données publiques ou faire l'objet par ce dernier d'un renvoi vers la solution d'hébergement de l'Autorité publique concernée.

Ces données peuvent être réutilisées, dans le cadre des licences renseignées avec les bases de données afin d'offrir des services technologiques pour lesquels ces données sont utiles.

Enfin, le portail ouvert des données publiques doit idéalement renseigner qui sont les réutilisateurs en application du principe de transparence.

CHAPITRE 5
Le Centre d'exploitation et d'analyse des données

Article C.V.15.
Création et objectifs

Le Centre d'exploitation et d'analyse des données regroupe l'ensemble des services et solutions facultatives offertes par Paradigm aux autorités publiques. Ces solutions doivent être adaptées par arrêté conjoint et pourront viser plusieurs outils pour stocker, traiter et analyser les données.

Il s'agirait, à ce stade, de solution d'hébergement, de services d'analyse d'usage (analytics) et des services basés sur l'intelligence artificielle. Toutefois, le gestionnaire de la Plateforme n'offre que des services, les questions relatives à la nature des données, à la sécurité et aux accès sont de la responsabilité exclusive de l'autorité qui fait appel aux services facultatifs offerts.

Paradigm, compte tenu de son expertise technologique, assiste néanmoins l'Autorité publique dans les choix à prendre en fonction de la nature de l'opération à réaliser.

Néanmoins, le Centre d'exploitation et d'analyse des données a vocation, dans le futur, à proposer de nouveaux services facultatifs. Dans le cas où des services seraient rendus obligatoires, une modification du présent Code paraît nécessaire.

CHAPITRE 6
Point de Contact et d'information

Article C.V.16.
Point de contact et d'information visé à l'article 8 du Règlement sur la gouvernance des données

La présente disposition vise à permettre à toute personne intéressée d'obtenir les informations relatives aux données notamment celles dont la réutilisation est permise via la Plateforme.

Le point de contact permet également de remplir un objectif fixé par le règlement « Règlement sur la gouvernance des données » concernant l'information pour la demande de réutilisation.

Le cas échéant, le gestionnaire de la Plateforme redirigera les demandes auprès des autorités compétentes en fonction des questions à traiter.

CHAPITRE 7
Service d'appui

Article C.V.17.
Service d'appui visé à l'article 7 du Règlement sur la gouvernance des données

Cette disposition ne nécessite pas de commentaire particulier.

Vu sa position centrale dans l'architecture générale de la gouvernance de la donnée, il est apparu opportun d'inclure le service d'appui visé dans le Règlement sur la gouvernance des données dans la plateforme gérée par Paradigm.

De par cette position privilégiée, le gestionnaire dispose des compétences techniques et juridiques afin d'assurer ce rôle d'appui auprès des autres institutions bruxelloises.

Certaines problématiques ayant vocation à se répéter, Paradigm pourrait proposer des solutions mutualisables et utiles à plusieurs Autorités (au travers du Centre d'exploitation) afin d'en réduire les coûts individuels.

LIVRE C.VI.
Les structures administratives de la gouvernance

Le présent Livre a pour objectif de décrire la structure administrative, commune à la Région, COCOM et COCOF, en matière de gouvernance numérique et de gouvernance de la donnée.

Le Livre est organisé afin de définir les concepts de gouvernance numérique et de gouvernance de la donnée :

1° le titre 1 concerne la gouvernance numérique et établit les liens entre les 4 organes de la gouvernance numérique appelés à interagir, à savoir : le Secrétariat numérique, le Comité de validation de l'architecture numérique, le Comité de coordination numérique, le Bureau d'achats numériques;

2° le titre 2 concerne la gouvernance de la donnée et les deux organes qui la composent à savoir : le Comite de gouvernance de la donnée et le Bureau de la donnée;

3° le titre 3 concerne les ressources de la gouvernance au sein des Autorités publiques.

TITRE 1
La gouvernance numérique

CHAPITRE 1
Champ d'application

Article C.VI.1.
Les Autorités publiques visées par le titre 1

La Gouvernance numérique a été conçue de manière à ne pas englober le niveau local visé au point c) de la définition d'Autorité publique comprise dans le livre A.I.

En effet, dans un souci de respect de l'autonomie locale, les communes n'entrent pas dans le champ d'application de la gouvernance numérique que la Région, la COCOF et la COCOM entendent mettre en place au travers du présent titre.

CHAPITRE 2
Objectifs

Article C.VI.2.
La gouvernance numérique

L'objectif est de créer un système de gouvernance de l'écosystème numérique bruxellois clair et transparent, commun à la Région, COCOM et COCOF.

La Gouvernance numérique vise principalement à assurer la cohérence numérique au sein de la Région, COCOM et COCOF. Il apparaît que ces matières, souvent hautement techniques, échappent, du fait de cette complexité, à une certaine gestion stratégique, qui pourrait être source de nombreuses économies et d'une meilleure coordination.

Le système de gouvernance numérique mis en place a pour objectif d'assurer que les projets les plus susceptibles d'impacter numériquement les trois collectivités publiques (vu les montants en jeu, vu les options techniques posées, …) soient :

1° non seulement, appréhendés collectivement afin d'en vérifier la cohérence avec l'environnement numériques de la Région, COCOM, et COCOF (visé en tant qu'écosystème numérique bruxellois);

2° mais également, analysés techniquement, dès leurs prémices, pour que la question de savoir si une concertation stratégique doit avoir lieu ou non soit directement guidée par les explications techniques nécessaires à la bonne compréhension des enjeux. L'objectif est qu'au final les synergies numériques et les mutualisations des projets numériques apparaissent clairement.

CHAPITRE 3
Test d'autoévaluation numérique

Article C.VI.3.
Test d'autoévaluation numérique

Cet article décrit le point d'entrée de la gouvernance numérique bruxelloise.

En effet, pour tout projet correspondant aux deux critères visés au paragraphe 2, un test d'autoévaluation numérique doit être organisé par la ou les Autorité(s) publique(s) à l'origine du projet.

Ainsi tout projet (i) qui appelle une intervention de l'un des trois exécutifs ou encore relève de la compétence de l'organe de gestion de l'Autorité publique concernée et (ii) pour autant que ce projet concerne l'écosystème numérique bruxellois dans son ensemble, un test d'autoévaluation numérique est organisé. Dès lors que le projet doit concerner l'écosystème numérique bruxellois, il s'agit de projets et achats ayant une importance ou une application dépassant le cadre de l'Autorité publique visée à l'article C.VI.1 qui le porte.

Les projets relatifs à la commande publique numérique sont également soumis au test d'autoévaluation numérique pour autant que le seuil visé à l'arrêté du 18 juillet 2000 soit rencontré, à savoir le seuil financier au-delà duquel l'intervention du Gouvernement est nécessaire. Actuellement, ce seuil est de 1.250.000 EUR pour les marchés à passer par procédure restreinte ou par procédure concurrentielle avec négociation ou par procédure négociée avec mise en concurrence préalable ou par procédure négociée directe avec publicité préalable lors du lancement de la procédure au sens des articles 38 et 41 ou 120 et

123 de la loi du 17 juin 2016 relative aux marchés publics. Il est fait référence à ce seuil afin que le lien avec les montants retenus en matière de marchés publics, tels que régulièrement indexés, soit directement organisé.

La réalisation du test d'autoévaluation numérique vise à garantir une réflexion raisonnée et la plus cohérente possible sur le maintien, la préservation et l'amélioration de l'écosystème numérique bruxellois dans son ensemble.

Le test, tel que complété, est envoyé au Secrétariat numérique décrit ci-après.

CHAPITRE 4
Les organes de la gouvernance numérique

SECTION 1
Le secrétariat numérique

Article C.VI.4.
Création et missions du Secrétariat numérique

Le secrétariat numérique joue un rôle central, au sein de cette nouvelle organisation de la Gouvernance numérique. Le Secrétariat numérique :

1° assume le secrétariat des deux comités de la gouvernance numérique (Comité de validation de l'architecture numérique et d'échanges des données et le Comité de coordination);

2° assure également l'interface entre ces comités d'une part et les Autorités publiques rentrant dans le périmètre de la gouvernance numérique;

3° analyse les résultats des tests d'autoévaluation numérique et en fonction, sollicitent les avis de

a) du Bureau d'achat numérique,

b) du Comité de l'architecture numérique,

c) du Bureau de la donnée.

Le Bureau de la donnée est un organe visé dans le cadre du titre 2 relatif à la gouvernance de la donnée. Toutefois, la gouvernance de la donnée est comprise pour partie dans la gouvernance numérique plus large. Le Bureau de la donnée est chargé d'établir et de gérer les liens entre les deux gouvernances mises en place pour organiser une véritable gouvernance globale.

Le Secrétariat numérique sollicite les avis et s'assure de leur réception par la suite, avant de les transmettre au Comité de coordination numérique. Ce dernier, sur la base des avis techniques reçus, sera en mesure d'analyser l'aspect stratégique des projets.

Article C.VI.5.
Financement et contrôle

L'activité du Secrétariat, service du Paradigm, est contrôlé au travers d'un rapport d'activités bisannuel, qui sera remis aux ministres compétents de la Région, COCOM et COCOF, de même qu'au Comité de coordination numérique.

SECTION 2
Le Comité de validation de l'architecture numérique

Article C.VI.6.
Compétence et composition du Comité de validation de l'architecture numérique

Le Comité de validation de l'architecture numérique poursuit des objectifs de cohérence et de mutualisation numérique, en tant qu'élément essentiels d'une architecture numérique crédible.

Le Comité de validation de l'architecture numérique est un organe consultatif dont la mission se limite à des avis techniques émanant directement des Autorités publiques du périmètre de la gouvernance numérique.

La composition du Comité de validation de l'architecture numérique est duale, avec d'une part, les membres permanents, qui représentent « les poids lourds » de l'activité numérique au niveau de la Région, de la COCOM et de la COCOF, à savoir les dix Autorités publiques disposant des plus grands budgets généraux. La participation de ces membres est obligatoire dans la mesure où elle est attendue et les absences doivent être justifiées.

La composition du Comité de validation de l'architecture numérique est issue d'une décision du gouvernement sur la nouvelle gouvernance régionale du 18 mars 2021.

Font partie des membres permanents : Directeurs Généraux et les responsables informatiques de dix institutions régionales ayant le budget IT le plus important : Actiris, Bruxelles Environnement, Bruxelles Fiscalité, Bruxelles Formation, Bruxelles Propreté, Paradigm, parking.brussels, SPRB, COCOF et STIB.

Les autres membres sont des membres non permanents dans la mesure où leur participation n'est pas systématique et dépendra de leur intérêt au débat, prévu lors de chaque réunion.

Les Autorités publiques inclues dans le périmètre de la gouvernance numérique, membres du Comité de validation de l'architecture numérique, sont représentées, par des personnes désignées par les Autorités publiques elles-mêmes.

Article C.VI.7.
Rapport d'activités

Le Comité de validation de l'architecture numérique est soumis à une obligation de rapport bisannuel afin d'alimenter la connaissance de l'activité numérique bruxelloise et de vérifier son activité.

SECTION 3
Le Bureau d'achats numérique

Article C.VI.8.
Le Bureau d'achats numériques

Le Bureau d'achats numériques est mis sur pied en vue d'harmoniser la politique de commande publique numérique des Autorités publiques visés par l'ensemble du présent Code. Il est important de souligner que l'activité du Bureau d'achats numériques ne s'adresse pas exclusivement aux Autorités relevant du périmètre de la gouvernance numérique mais également aux autres Autorités publiques soumises à la partie C du Code, même si les modalités de son intervention diffèrent dans la mesure où le régime est contraignant pour les Autorités publiques relevant du périmètre de la gouvernance numérique et ne l'est pas pour les autres Autorités publiques soumises à la partie C du Code.

Le Bureau d'achats numériques, ou BAN, est un service de Paradigm qui a vocation à être un outil mutualisé d'assistance et de prospection pour tout projet de commande publique lancé par une Autorité publique. Il s'agit d'un outil de support légal, administratif et procédural à disposition des Autorités publiques ressortant de la Région de Bruxelles-Capitale, de la COCOM ou de la COCOF.

Le BAN n'est ni un outil mutualisé de passation ou d'attribution de marché, ni une centrale d'achats ou de marchés. Il ne dispose pas de personnalité juridique propre, et à n'a pas vocation à être pouvoir adjudicateur des commandes publiques mutualisables qui lui seraient soumises.

Article C.VI.9.
Les missions du Bureau d'achats numériques

De manière concrète, le BAN offre son appui et son expérience en vue de générer un véritable flux de commandes mutualisées au plus grand nombre d'Autorités publiques.

Les Autorités publiques comprises dans le périmètre de la Gouvernance numérique doivent pour une commande publique numérique consulter le BAN, préalablement à toute décision de lancement de la commande.

Nous précisons également que le terme générique de « commande publique » est ici privilégié afin de couvrir toute marché public, d'achat ou de location de matériel ou de service, peu importe la forme juridique adoptée, la durée ou l'objet visé.

Ces projets de commande publique numérique sont dès lors examinés par le BAN conformément à des critères de mutualisation fixés conjointement par arrêt du Gouvernement, Collège réuni et Collège. Ces critères fonctionnels et opérationnels sont de nature à évoluer de manière très rapide en fonction, notamment, des technologies utilisées; ils devront être revus aussi souvent que cela s'avère nécessaire, la voie d'un arrêté est donc plus indiquée.

Une fois les critères de mutualisation rencontrés, certaines modalités fixées par le même arrêté conjoint s'appliquent, telles que des normes et standards à respecter dans le cadre de l'architecture numérique, des recommandations en matière d'interopérabilité des systèmes d'information, de numérique responsable, de sécurité des données, …

Le BAN se charge de l'analyse du projet afin d'en confirmer le caractère mutualisable en application de l'arrêté fixant les critères de mutualisation, et se charge de même du suivi du projet sur un mode d'avis et d'information, en rappelant les modalités destinées à s'appliquer telles que fixées par voie d'arrêté ou encore du fait du Code et de son implémentation.

En tant qu'organe de la gouvernance numérique, le BAN remet et sollicite des avis à l'instar des autres organes de la gouvernance numérique.

Les paragraphes 2 et 3 concernent la manière dont les Autorités publiques doivent ou peuvent (selon leur appartenance au périmètre de la gouvernance numérique ou pas) faire remonter de l'information vers le BAN alors qu'un projet de commande publique numérique n'est pas encore lancé.

Les obligations et les possibilités des Autorités publiques visées par le Code envers le BAN ne sont en effet pas similaires en fonction de leur appartenance ou non au périmètre de la gouvernance numérique visé à l'article C.VI.1.

Dans le cadre de son analyse, le BAN s'appuie sur les déclarations de besoins numériques pluriannuelles que les Autorités publiques sont tenues (pour les Autorités publiques comprises dans le périmètre de la gouvernance numérique) – ou peuvent (pour les autres Autorités publiques visées par le Code) – lui transmettre, ainsi que sur les critères de mutualisation qu'elle proposera au Gouvernement d'adopter.

La « déclaration de besoins numériques pluriannuelles », une fois transmise au BAN, pourra être croisée avec d'autres déclarations similaires. Cela permettra au BAN d'identifier les projets mutualisables en amont de leur conception et de remplir un rôle d'interface entre les différentes Autorités publiques.

Les déclarations ont vocation à évoluer de manière itérative, de telle sorte qu'elles peuvent être revues à tout moment, et doivent l'être au minimum une fois par an. Cela permet que le BAN dispose toujours d'une information à jour et adapte sa propre stratégie en fonction.

Néanmoins, il arrive que des besoins se manifestent de manière ponctuelle et hors du cadre de la déclaration de besoins numériques pluriannuelles. Dans ce cas, l'Autorité publique complète un formulaire de besoins numériques et le renvoie au BAN. Dans ce formulaire de besoins numériques, elle décrit le besoin auquel elle souhaite répondre via une procédure de commande publique numérique; le BAN peut alors identifier le caractère mutualisable ou non du besoin, et d'éventuels besoins numériques ou projets similaires identifiés par d'autres Autorités publiques, ou formuler toute recommandation à l'égard des Autorités publiques concernées.

Si un projet de commande numérique soumis au BAN voit son caractère mutualisable confirmé, le BAN recommande l'application du test d'autoévaluation numérique s'il apparaît que les critères sont rencontrés. Dans ce cas, le processus décrit au départ de ce test dans le cadre du présent titre est enclenché, à des fins de vérifications in fine de l'enjeu stratégique.

Article C.VI.10.
Financement et contrôle

Le Bureau d'achats numériques a pour vocation d'être au service des Autorités publiques de la Région, de la COCOM, et de la COCOF sur un mode obligatoire ou facultatif selon leur appartenance au périmètre de la gouvernance numérique. Le financement du BAN doit refléter cette mise à disposition.

Le rapport d'activité du BAN se veut annuel dans la mesure où il servira de base au calcul de la participation financière de la Région, de la COCOM et de la COCOF et des Autorités publiques qui en dépendent.

SECTION 4
Le Comité de coordination numérique

Article C.VI.11.
Compétences et composition
du comité de coordination numérique

Le Comité de la coordination numérique est l'organe de gouvernance numérique stratégique, dernier échelon avant la saisine du Gouvernement, du Collège réuni, du Collège.

Le Comité de la coordination numérique forge son avis sur la base des avis des autres organes de la gouvernance numérique qui l'ont précédé dans son analyse afin de l'éclairer techniquement.

La composition du Comité de la coordination numérique est la même que celle du Comité de validation de l'architecture numérique à la différence que les représentants des Autorités publiques membres doivent être en mesure d'engager stratégiquement l'Autorité qu'ils représentent. Ce choix est opéré par chaque Autorité publique individuellement.

Comme l'a souligné le Conseil d'État :

« 10.2. Het verlenen van verordenende bevoegdheid aan een openbare instelling, is in beginsel niet in overeenstemming met de algemene publiekrechtelijke beginselen omdat erdoor geraakt wordt aan het beginsel van de eenheid van de verordenende macht en een rechtstreekse parlementaire controle ontbreekt. Bovendien ontbreken de waarborgen waarmee de klassieke regelgeving gepaard gaat, zoals die inzake de bekendmaking, de preventieve controle van de Raad van State, afdeling Wetgeving, en de duidelijke plaats in de hiërarchie der normen. Dergelijke delegaties kunnen dan ook enkel worden gebillijkt voor zover zij zeer beperkt zijn en een niet beleidsmatig karakter hebben, door hun detailmatige of hoofdzakelijk technische draagwijdte. De instellingen die de betrokken reglementering dienen toe te passen moeten hierbij zowel aan rechterlijke controle als aan politieke controle onderworpen zijn.

De voormelde ontworpen bepalingen kunnen zo worden begrepen dat ermee enkel handelingen van louter beleidsvoorbereidende aard worden beoogd en dat ze geen beslissingsmacht behelzen, laat staan handelingen van verordenende bevoegdheid. Indien dat anders zou zijn, moet zijn voldaan aan de zo-even aangehaalde voorwaarden. ».

Il va bien entendu de soi que le Comité de coordination numérique ne dispose d'aucune compétence réglementaire et aucune compétence décisionnelle, comme le souligne le Conseil d'État. Ce point est confirmé par le paragraphe 1er, alinéa 2 : le Comité de coordination numérique ne formule que des avis à teneur stratégique.

Article C.VI.12.
Rapport d'activités

De la même manière que le Comité de validation de l'architecture numérique et que le Secrétariat numérique, le Comité de la coordination numérique rapporte son activité tous les deux ans aux trois exécutifs.

TITRE 2
La gouvernance de la donnée

CHAPITRE 1
Objectifs

Article C.VI.13.
Objectifs

La Gouvernance de la donnée concerne logiquement, vu le champ d'application général, du Code l'ensemble des Autorités publiques.

CHAPITRE 2
Les organes de la gouvernance de la donnée

SECTION 1
Le Comité de gouvernance de la donnée

Article C.VI.14.
Composition du Comité de gouvernance de la donnée

Le Comité de gouvernance de la donnée est un organe de concertation entre toutes les Autorités publiques afin d'organiser le dialogue et le retour d'information sur toutes les questions que peut susciter l'application du Code dans la pratique et dans sa mise en œuvre opérationnelle et technique.

Le Comité de gouvernance de la donnée travaille par voie de consensus et sur le mode de la collégialité, sans pouvoir de décision mais avec une volonté d'harmonisation des pratiques et des réponses apportées aux questions soulevées par l'application du Code.

Le Comité de gouvernance de la donnée est censé représenter la communauté des Autorités publiques soumises à la partie C du Code et regroupe l'ensemble des agents dont la mission première est de veiller à l'implémentation du Code et à la cohérence de la gouvernance globale de la donnée au niveau bruxellois. Toutefois, pour des raisons évidentes de bonne gestion, la participation au Comité de la gouvernance de la donnée est limitée aux Autorités publiques reprises dans le palier 1 et 2 de l'arrêté fixant les seuils numériques. Les autres Autorités ne sont bien entendu pas exclues du Comité mais participeront en tant qu'invités pour des questions précises les concernant directement.

De manière générale, la préparation de la gouvernance en commun permettra d'emblée une adhésion d'un grand nombre d'Autorités ce qui facilitera une application verticale de la gouvernance.

Article C.VI.15.
Missions

Les missions du Comité de gouvernance de la donnée sont définies de manière large dans la mesure où les possibilités d'intervention sont multiples et seront définies en fonction des questions que soulève l'application du Code. Néanmoins, il est évident que le Comité de gouvernance de la donnée devra remplir ces missions-là de manière régulière pour que le fonctionnement de la communauté numérique des Autorités publiques soit garanti sur un mode concerté de gestion.

Le Comité de gouvernance de la donnée a, du fait de sa représentativité des Autorités publiques qui le compose, la mission d'élaborer la stratégie commune des Autorités publiques en matière de donnée, laquelle est appelée à se décliner en plans d'action annuels en tant que feuilles de route du développement numérique global. Le Bureau de la donnée participe activement à cette rédaction.

Cette stratégique sera *in fine* coulée en arrêtés d'approbation émanant des trois exécutifs.

Article C.VI.16.
Fonctionnement

Pas de commentaire.

SECTION 2
Le Bureau de la donnée

Article C.VI.17.
Création du Bureau de la donnée

Au sein de Paradigm, OIP A de la Région bruxelloise, est créé un Bureau de la donnée dont l'objec-

tif est de prendre en charge un rôle de gouvernance opérationnelle : le Bureau est destiné à être le point de référence des Autorités publiques soumises au Code et l'appui administratif nécessaire au Comité de gouvernance de la donnée.

Il occupe un rôle-clé dans la gouvernance administrative tant numérique que de la donnée du fait du regard à 360 degrés dont il dispose sur l'ensemble des discussions en cours.

Article C.VI.18.
Missions du Bureau de la donnée

Les missions du Bureau de la donnée sont nombreuses et regroupées sous différentes catégories avec une citation non exhaustive des tâches que cela peut viser concrètement.

La mission d'appui est claire et complète le descriptif des missions confiées au Comité de gouvernance de la donnée.

Comme exposé plus haut, le Bureau de la donnée est actif aussi bien en matière de gouvernance de la donnée, que de gouvernance numérique décrite dans le titre 1 du présent livre.

Au-delà de sa mission d'appui administratif, le Bureau de la donnée a aussi la fonction de veiller à l'implémentation du Code en proposant au Comité de gouvernance de la donnée, les initiatives nécessaires à l'application du Code, les questions à trancher collégialement, …

La mission d'accompagnement du Bureau de la donnée s'entend d'une mission de facilitation visant à promouvoir l'application du Code. Le Bureau de la donnée ne dispose d'aucune compétence réglementaire, comme le souligne le Conseil d'État au point 10.1 de son avis. Seul le Comité de gouvernance de la donnée a une compétence décisionnelle dans la mesure où il adopte des décisions sur un mode collégial. Le Bureau de la donnée ne fait que proposer, préparer et faciliter, les décisions collégiales du Comité de gouvernance de la donnée.

La fonction d'initiateur de changement cadre avec la volonté d'organiser la transition numérique et de communiquer à ce sujet.

Le Bureau est aussi appelé à apporter des ressources aux Autorités publiques en proposant des experts sur les questions qui les concernent, ou encore en informant sur les modifications du cadre réglementaire en cours, au niveau européen ou bruxellois.

Article C.VI.19.
Fonctionnement, contrôle et financement

Le Bureau de la donnée, organe de Paradigm OIP A régional, est au service des Autorités publiques de la Région, de la COCOM et de la COCOF, sur le principe qui a été conçu dans le cadre de l'accord de coopération du 12 décembre 2019 entre la Région de Bruxelles-Capitale et la Commission communautaire commune portant sur la désignation d'un intégrateur de services commun pour l'échange électronique de données.

L'avis du Conseil d'État concernant cet accord de coopération précise à ce sujet que :

« 2.2. En principe, toutes les parties à un accord de coopération doivent contribuer au projet commun. L'existence d'un lien de proportionnalité raisonnable est dès lors nécessaire entre le coût des obligations liées aux compétences apportées par chacune des parties et leur financement par celles-ci. L'accord de coopération à l'examen ne contient pas de disposition explicite concernant le financement. Néanmoins, le régime à l'examen peut se réaliser si l'élargissement au Collège réuni du champ d'application de l'article 20 de l'ordonnance intégrateur de services par l'article 3, § 11, de l'accord de coopération s'interprète en ce sens que l'intégrateur de services n'interviendra pour la Commission communautaire commune que dans la mesure où le Collège réuni assure la mise à disposition des moyens nécessaires à cette fin. » (Doc. Parl. Assemblée réunie de la Commission communautaire commune, Sess. ord. 2018-2013, B-168/1, p. 3).

Un financement de même qu'un contrôle politique tripartite est organisé à l'égard du Bureau de la donnée en application du fait qu'il agit en faveur des trois collectivités publiques.

Le rapport d'activité a pour objectif d'assurer un certain contrôle du Bureau de la donnée par les trois collectivités publiques qui le financent.

TITRE 3
Les ressources de la gouvernance de la donnée au sein des Autorités publiques

Article C.VI.20.
Création des fonctions de gouvernance des données

La création de ces fonctions permet aux Autorités publiques de désigner en leur sein des agents chargés plus spécifiquement par le Code de la mise en place des obligations découlant du Code.

La rédaction des alinéas 2 et 3 est inspirée des dispositions du RGPD concernant le Délégué à la protection des données afin de permettre la mutualisation de ces fonctions entre plusieurs Autorités publiques et permettre également l'externalisation de ces fonctions.

Une possibilité de cumul des fonctions d'administrateur local de la donnée et de conseiller de sécurité de l'information est introduite en faveur des Autorités publiques du palier 3.

Article C.VI.21.
L'administrateur local de la donnée

Il est important d'avoir un administrateur local de la donnée (ou data steward) au sein de chaque administration pour différentes raisons.

L'administrateur local de la donnée est responsable de la gestion des données au sein de son Autorité publique. Cette responsabilité claire vise à assurer que les données soient gérées de manière responsable, efficace et conforme aux principes voulus par le présent Code.

Concrètement, il assure le respect des obligations issues du Code et joue un rôle d'intermédiaire entre les décisions des organes de la gouvernance des données et leur mise en pratiques dans son administration.

Les missions de l'administrateur local sont divisées en quatre catégories distinctes.

La première catégorie est une mission à l'égard de l'Autorité publique qui l'a désigné comprenant l'identification des besoins et la définition d'une stratégie interne à l'Autorité publique pour gérer les données conformément à la stratégie commune décidée. En définissant la stratégie interne de l'Autorité publique dont il relève l'administrateur local de la donnée a pour mission d'appliquer au sein de l'Autorité publique la stratégie pluriannuelle de la donnée et les plans d'actions annuels visés à l'article C.VI.15, § 2. Ce faisant, il n'exerce aucune compétence réglementaire comme le souligne le Conseil d'État au point 10.1 de son avis. La stratégie interne est un document interne, de portée politique, qui ne lie en aucun cas les tiers.

L'administrateur local de la donnée définit également le modèle opération définit dans la partie A du Code comme :

« représentation abstraite de la façon dont une organisation opère à travers des domaines de processus, d'organisation et de technologie afin d'accomplir sa fonction ».

À nouveau, il s'agit d'un document interne qui ne possède aucune valeur réglementaire.

L'administrateur est également responsable de la détermination des domaines de données gérés au sein de l'Autorité publique, de la mise en œuvre des objectifs stratégiques et des obligations relatives à la gestion de la donnée, ainsi que de la proposition de mesures techniques ou organisationnelles appropriées à ces domaines.

La deuxième catégorie est une mission exercée vis-à-vis des tiers comprenant l'organisation d'un point de contact unique en matière de gouvernance de la donnée (pour le suivi des demandes éventuelles issues de la Plateforme bruxelloise de la donnée)

La troisième catégorie est une mission à l'égard du Bureau de la donnée à qui l'administrateur est chargé de fournir des informations régulières sur l'exercice de ses missions ou des informations pertinentes.

La quatrième et dernière catégorie est une mission à l'égard des autres Autorités publiques. Si nécessaire, l'administrateur doit assurer une harmonisation horizontale des domaines de données qui concernent plusieurs Autorités publiques, communiquer la documentation établie par lui et faciliter la collaboration et le dialogue entre les administrateurs locaux de la donnée.

Le cas échéant, l'Autorité publique peut confier à l'administrateur ou au conseiller local de la donnée toute autre mission complémentaire aux missions énoncées précédemment et relatives à la gouvernance des données.

Article C.VI.22.
Le Responsable de la donnée

Le Responsable de la donnée (ou *Chief Data Officer* – CDO) est un rôle de plus en plus courant dans les organisations publiques et privées.

Un Responsable de la donnée au sein de chaque Autorité publique pour assurer la mise en pratique d'une bonne gouvernance des données.

1° Sa mission d'implémentation favorisera la stratégie de données : le responsable de la donnée peut travailler avec les parties prenantes de l'écosystème bruxellois pour élaborer une stratégie de données claire, alignée sur les objectifs de son administration et cohérente avec les priorités régionales;

2° L'évaluation continue améliorera la gouvernance des données : le responsable de la donnée met en place des politiques, des procédures et des normes pour assurer une gouvernance efficace des données sur base des instructions du conseiller en sécurité de l'information. Cela inclut des aspects tels que les formats, la qualité des données, la sécurité des données, la confidentialité des données et la conformité aux réglementations en matière de données;

3° Sa mission de contrôle du respect des mesures permet de vérifier que les mesures décidées (notamment en termes de sécurité et de qualité des données) sont bien appliquées par les agents utilisateurs des données concernées.

4° Sa mission de promotion et de supervision permettra une meilleure implémentation de la gouvernance des données au sein de chaque service de son administration utilisant les données issues des domaines dont il a la charge.

5° Une mission de maintenance et de supervision des ressources permettra une meilleure gestion des infrastructures nécessaires à l'implémentation de la gouvernance ainsi que et de leurs coûts.

6° L'élaboration de la documentation adéquate favorisera l'interopérabilité mais également le suivi, les mises à jour et la poursuite des éléments mis en place dans le cadre de la gouvernance en cas de changement de personnel.

Article C.VI.23.

Le conseiller en sécurité de l'information

Le rôle de conseiller est repris de l'ordonnance bruxelloise « intégrateur ».

Le CSI est un acteur central dans l'analyse des risques. Il reçoit l'aide de la hiérarchie et de toute personne adéquate dont les techniciens ICT. Le conseiller ne sera pas forcément le responsable de l'exécution de cette analyse des risques. Il doit certainement être associé de près ou de loin en fournissant, par exemple, une méthodologie et en effectuant le suivi des mesures à prendre.

Les missions 5 et 6 ont été rajoutées aux missions déterminées dans cette ordonnance afin d'assurer la mise en place et le suivi des mesures de sécurité plus spécifiques à la gouvernance des données.

TITRE III

Dispositions finales

Article 3

Vu les modifications introduites au niveau de l'actuelle CADA et de sa composition, l'entrée en vigueur des livres B.I et B.II du Code de la gouvernance et de la donnée est retardée à six mois après la publication afin de permettre la création des nouvelles chambres et la désignation des nouveaux membres pour ces nouvelles chambres, du secrétariat et des experts.

Article 4

Vu la nécessité de retarder l'entrée en vigueur de la réforme relative à l'actuelle CADA appelée à trancher les litiges également en matière de partages administratifs et de réutilisations, l'entrée en vigueur du livre C.IV décrivant les flux de données correspondant à des partages administratifs ou à des réutilisations et le livre C.V. décrivant la Plateforme bruxelloise de la donnée, est également retardée afin de s'aligner sur l'entrée en vigueur du contrôle qui sera à présent organisé par la CADADo.

Par ailleurs, une entrée en vigueur six mois après la publication permettra également aux Autorités publiques concernées de se familiariser avec les nouveaux concepts de partage administratif et de Communication. De même, la Plateforme sera parfaitement opérationnelle après un délai de six mois et l'arrêté d'exécution nécessaire au fonctionnement du Centre d'intégration sera adopté.

Le titre sur les partenariats numériques et le chapitre consacré à la sécurité et la protection des données du titre consacré à la gestion des données dans le cadre du livre C.III entrent en vigueur de manière différée de manière à permettre aux Autorités publiques concernées d'appréhender correctement les concepts développés et les dispositions en matière de sécurité qui seront pour partie reprises dans un arrêté à venir.

De la même manière, le chapitre consacré à la déclaration de principes entre en vigueur deux ans plus tard de manière à laisser le temps aux Autorités publiques de réaliser ce document important pour la première fois.

Article 5

Pour les Autorités publiques regroupées dans le palier n° 3 défini par l'arrêté fixant les seuils numériques, l'ensemble du Code de la gouvernance et de la donnée entre en vigueur deux ans après la publication du décret et de l'ordonnance conjoints. L'objec-

tif est de donner aux plus petites Autorités publiques visées par le Code le temps d'appréhender l'ensemble du Code afin de préparer son implémentation. Ces Autorités ne disposent pas d'une activité numérique intense, de sorte qu'une entrée en vigueur différée à leur égard ne portera pas préjudice de manière démesurée à la bonne gestion de leurs données et à leur participation à la Plateforme bruxelloise de la donnée, de même qu'aux organes de gouvernance.

L'entrée en vigueur du titre III du livre C.IV relatif à la réutilisation des données se distingue, pour ce qui concerne les Autorités publiques du palier n° 3, de l'entrée en vigueur des autres dispositions du Code à l'égard de ces Autorités vu que ce titre correspond à la transposition de la Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public. Seul ce titre qui transpose la directive européenne portant sur la réutilisation des informations du secteur public entre en vigueur six mois après la publication du décret et ordonnance conjoints dès lors qu'il est déjà en vigueur à l'égard des Autorités publiques du palier n° 3 et qu'il s'agit d'une obligation européenne de transposition. L'ensemble des autres dispositions du Code entrent en vigueur deux ans après la publication du décret et de l'ordonnance conjoints pour ce qui concerne les Autorités publiques du palier n° 3.

Article 6

Cet article organise la transmission des compétences actuelles de la CADA vers la nouvelles CADADo, qui voit par ailleurs ses compétences élargies aux questions de partages administratifs.

La poursuite du mandat des actuels 9 membres de la CADA, en ce compris le Président, au sein de la Chambre relative à l'accès aux documents administratifs est organisée. Les 4 nouveaux membres appelés à former les nouvelles chambres de la CADADo doivent être désignés avant l'entrée en vigueur du livre B.I et B.II du Code de la gouvernance et de la donnée. Ces nouveaux membres disposeront d'un mandat dont la durée sera équivalente à la durée du mandat restant des actuels membres de la CADA, afin que l'ensemble des membres composant la CADADo puissent voir leurs mandats renouvelés en même temps.

Le secrétariat de la CADADo et les experts doivent également être opérationnels au moment de l'entrée en vigueur du livre B.I et B.II du Code.

Le dernier alinéa prévoit que l'ensemble des dossiers actuellement pendants devant la CADA, à savoir les recours en matière d'accès aux documents administratifs, les recours en matière de publicité active, les demandes de rectification et les recours en matière de réutilisations de données, sont poursuivis par les membres actuels de la CADA au sein de la chambre relative à l'accès aux documents administratifs. De manière transitoire, cette chambre est donc appelée à poursuivre ses dossiers en matière de réutilisations de données, dans un souci d'efficacité administrative, afin que les dossiers ne doivent pas être réexaminés par les nouveaux membres de la chambre relative à la réutilisation des données au sein de la CADADo. Les dossiers en matière de réutilisation de données introduits après l'entrée en vigueur des livres B.I, B.II, C.IV et C.V. seront exclusivement traitées par la chambre relative à la réutilisation des données.

Article 7

Vu la modification du système de rémunération des membres de la CADADo, cette disposition prévoit qu'à la date de l'entrée en vigueur des livres B.I et B.II, le système des jetons s'applique immédiatement également à l'égard des dossiers introduits avant l'entrée en vigueur des livres B.I et B.II du Code, soit lorsque les membres de la CADA étaient encore rémunérés mensuellement.

Article 8

Cet article est une reprise de l'article 35 des Décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française relatifs à la publicité de l'administration dans les institutions bruxelloises.

Article 9

Cet article est une reprise de l'article 36 des Décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française relatifs à la publicité de l'administration dans les institutions bruxelloises.

Article 10

L'ordonnance dite *once only* est abrogée en même temps que le livre C.IV exposant l'obligation de partage administration en cas de sources authentiques.

L'abrogation des actuels décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française relatifs à la publicité de l'administration dans les institutions bruxelloises correspond à l'entrée en vigueur des livres B.I et B.II du Code de la gouvernance et de la donnée. L'abrogation de la CADA ne pourra se faire qu'après que la CADADo soit parfaitement mise en place et opérationnelle.

L'abrogation de l'ordonnance du 27 octobre 2016 visant à l'établissement d'une politique de données ouvertes (Open Data) et portant transposition de la Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public correspond à l'entrée en vigueur des livres C.IV et C.V. du Code de la gouvernance et de la donnée. Il en va de même pour l'ordonnance relative à l'intégrateur de services régional.

Article 11

Cet article n'appelle pas de commentaire.

PROJET DE DÉCRET ET ORDONNANCE CONJOINTS

de la Région de Bruxelles-Capitale, de la Commission communautaire commune et de la Commission communautaire française portant le Code de la gouvernance et de la donnée

TITRE I
Disposition générale

Article 1er

Le présent décret et ordonnance conjoints règle une matière visée à l'article 39, 135 et 135bis de la Constitution, ainsi qu'aux articles 127 et 128 de la Constitution en vertu de l'article 138 de celle-ci.

TITRE II
Code

Article 2

Les dispositions suivantes forment le Code de la gouvernance et de la donnée :

PARTIE A
DISPOSITIONS COMMUNES ET DÉFINITIONS COMMUNES

LIVRE A.I
Dispositions communes et définitions communes au Code

Article A.I.1.
Respect intégral du RGPD

L'intégralité du présent Code s'applique sans préjudice des dispositions applicables du règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE et sans préjudice de toute disposition de droit international directement applicable.

Article A.I.2.
Application sauf exception des définitions du RGPD

Les définitions formulées à l'article 4 du règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE, s'appliquent au présent Code à l'exception des termes qui reçoivent une définition spécifique dans le cadre des articles A.I.3, A.II. 1 et A.II.2 et A.III.1.

Article A.I.3.
Définitions communes au Code

Au sens du présent Code, on entend par :

1) « Autorité publique » :

a) la Région de Bruxelles-Capitale, la Commission communautaire commune ou la Commission communautaire française;

b) les personnes morales de droit public qui dépendent, directement ou indirectement, de la Région de Bruxelles-Capitale, de la Commission communautaire commune ou de la Commission communautaire française;

c) les communes, les centres publics d'action sociale; les associations visées au Chapitre XII et XII*bis* de la loi du 8 juillet 1976, organique des centres publics d'action sociale;

d) les autorités administratives dépendant de la Région de Bruxelles-Capitale ou de l'Agglomération bruxelloise, dénommées ci-après « autorités administratives régionales ». Pour l'application du présent livre, les organes consultatifs régionaux en matière d'environnement ou d'aménagement du territoire sont assimilés à des autorités administratives régionales;

e) les autorités administratives dépendant de la COCOM et de la COCOF;

f) les autorités administratives communales, en ce compris les organes consultatifs communaux en matière d'environnement ou d'aménagement du territoire;

g) les intercommunales régionales et interrégionales soumises à la tutelle administrative de la Région de Bruxelles-Capitale ainsi qu'à leurs

filiales, aux ASBL communales et pluricommunales et aux régies communales autonomes, visées par l'ordonnance du 5 juillet 2018 relative aux modes spécifiques de gestion communale et à la coopération intercommunale. Pour l'application du présent livre, les intercommunales et leurs filiales, les ASBL communales et pluricommunales, et les régies communales autonomes sont assimilées aux « autorités administratives communales »;

h) les personnes, quelles que soient leur forme et leur nature, qui :

– ont été créées pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial;

– sont dotées de la personnalité juridique;

– et dont soit l'activité est financée majoritairement par les Autorité publiques visées au point a),b),c), soit la gestion est soumise à un contrôle de ces Autorités publiques ou soit plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance sont désignés par ces Autorités publiques;

i) les associations formées par une ou plusieurs Autorités publiques visées au point a), b), c) ou h);

j) toute personne physique ou morale :

a) qui exerce des fonctions administratives publiques, y compris des tâches, activités ou services spécifiques en rapport avec l'environnement ou l'aménagement du territoire;

b) ayant des responsabilités ou des fonctions publiques, ou fournissant des services publics, en rapport avec l'environnement ou l'aménagement du territoire sous le contrôle d'un organe ou d'une personne visée au point d) ou j), a). Pour l'application du présent livre, ces personnes physiques ou morales sont assimilées à des « autorités administratives régionales »;

2) « COCOF » : Commission communautaire française;

3) « COCOM » : Commission communautaire commune;

4) « Gouvernement » : le Gouvernement de la Région de Bruxelles-Capitale;

5) « Collège réuni » : le Collège réuni de la Commission communautaire commune;

6) « Collège » : le Collège de la Commission communautaire française;

7) « Paradigm » : l'organisme l'organisme d'intérêt public encadré par l'ordonnance du 22 février 2024 relative à Paradigm;

8) « Bruxelles Environnement » : l'organisme d'intérêt public créé par l'arrêté royal du 8 mars 1989 créant Bruxelles Environnement;

9) « RGPD » :

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogeant la Directive 95/46/CE (règlement général sur la protection des données).

LIVRE A.II
Définitions de la partie B

Titre I
Définitions du livre B.I.

Article A.II.1
Définitions du livre B.I.

Pour l'application du livre B.I., il faut entendre par :

1) « aménagement du territoire » : toutes les matières reprises à l'article 6, § 1er, I, de la loi spéciale de réformes institutionnelles du 8 août 1980;

2) « environnement » : toutes les matières reprises à l'article 6, § 1er, II, III et V de la loi spéciale de réformes institutionnelles du 8 août 1980;

3) « document administratif » : toute information, sous quelque forme que ce soit, dont une Autorité publique dispose;

4) « information environnementale » : toute information disponible sous forme écrite, visuelle, sonore, électronique ou toute autre forme matérielle, concernant :

a) l'état des éléments de l'environnement, tels que l'air et l'atmosphère, l'eau, le sol, les terres, les paysages et les sites naturels, y compris les biotopes humides, la diversité biologique et ses composantes, y compris les organismes génétiquement modifiés, ainsi que l'interaction entre ces éléments;

b) des facteurs, tels que les substances, l'énergie, le bruit, les rayonnements ou les déchets, les émissions, les déversements et autres rejets dans l'environnement, qui ont ou sont susceptibles d'avoir des incidences sur les éléments de l'environnement visés au point a);

c) les mesures, y compris les mesures administratives, telles que les politiques, les dispositions législatives, les plans, les programmes, l'évaluation des incidences environnementales des plans et programmes, les accords environnementaux et les activités ayant ou étant susceptibles d'avoir des incidences sur les éléments et les facteurs visés aux points a) et b), ainsi que les mesures ou activités destinées à protéger ces éléments;

d) les rapports sur l'application de la législation environnementale;

e) les analyses coût-avantages et autres analyses et hypothèses économiques utilisées dans le cadre des mesures et activités visées au point c);

f) l'état de la santé de l'homme, sa sécurité et les conditions de vie des personnes, les sites culturels et les constructions, pour autant qu'ils soient ou puissent être altérés par l'état des éléments de l'environnement visés au point a), ou, par l'intermédiaire de ces éléments, par l'un des facteurs, mesures ou activités visés aux points b) et c); et

g) l'aménagement du territoire;

5) « informations détenues par une Autorité publique » : le document administratif ou l'information environnementale qui est en la possession de cette Autorité et qui a été reçu ou établi par elle. Sauf si elle ne se rapporte manifestement pas à l'exercice des fonctions de l'intéressé, une donnée détenue par un membre du personnel attaché à une Autorité publique ou par un membre d'une instance collégiale constitutive d'une Autorité publique, est une donnée détenue par l'Autorité publique;

6) « demandeur » : toute personne physique ou morale qui demande un document administratif ou une information environnementale;

7) « public » : une ou plusieurs personnes physiques ou morales ainsi que les associations, organisations ou groupes constitués de ces personnes;

8) « jour ouvrable » : celui qui n'est ni un samedi, ni un dimanche, ni un jour férié;

9) « étude » : travaux de recherche, de mise au point d'une question, d'un projet, réalisés de façon détaillée par des experts au sujet d'une thématique intéressant une ou plusieurs autorités bruxelloises; il peut notamment s'agir d'investiguer une question technique, scientifique, ou juridique, pour autant que l'analyse soit menée de façon approfondie;

10) « subvention » : toute forme de soutien financier, quelles que soient sa forme ou sa dénomination, accordée dans une finalité directe ou indirecte d'intérêt général, à une activité organisée par un tiers, quelle que soit la dénomination de cette activité.

TITRE II
Définitions du livre B.II.

Article A.II.2.
Définitions du livre B.II.

Pour l'application du livre B.II, il faut entendre par :

1) « aménagement du territoire » : toutes les matières reprises à l'article 6, § 1er, I, de la loi spéciale de réformes institutionnelles du 8 août 1980;

2) « environnement » : toutes les matières reprises à l'article 6, § 1er, II, III et V, de la loi spéciale de réformes institutionnelles du 8 août 1980;

3) « document administratif » : toute information, sous quelque forme que ce soit, dont une autorité administrative dispose;

4) « information environnementale » : toute information disponible sous forme écrite, visuelle, sonore, électronique ou toute autre forme matérielle, concernant :

a) l'état des éléments de l'environnement, tels que l'air et l'atmosphère, l'eau, le sol, les terres, les paysages et les sites naturels, y compris les biotopes humides, la diversité biologique et ses composantes, y compris les organismes génétiquement modifiés, ainsi que l'interaction entre ces éléments;

b) des facteurs, tels que les substances, l'énergie, le bruit, les rayonnements ou les déchets, les émissions, les déversements et autres rejets dans l'environnement, qui ont ou sont susceptibles d'avoir des incidences sur les éléments de l'environnement visés au point a);

c) les mesures, y compris les mesures administratives, telles que les politiques, les dispositions

législatives, les plans, les programmes, l'évaluation des incidences environnementales des plans et programmes, les accords environnementaux et les activités ayant ou étant susceptibles d'avoir des incidences sur les éléments et les facteurs visés aux points a) et b), ainsi que les mesures ou activités destinées à protéger ces éléments;

d) les rapports sur l'application de la législation environnementale;

e) les analyses coût-avantages et autres analyses et hypothèses économiques utilisées dans le cadre des mesures et activités visées au point c);

f) l'état de la santé de l'Homme, sa sécurité et les conditions de vie des personnes, les sites culturels et les constructions, pour autant qu'ils soient ou puissent être altérés par l'état des éléments de l'environnement visés au point a), ou, par l'intermédiaire de ces éléments, par l'un des facteurs, mesures ou activités visés aux points b) et c) et

g) l'aménagement du territoire;

5) « informations détenues par une Autorité publique » : le document administratif ou l'information environnementale qui est en la possession de cette Autorité et qui a été reçu ou établi par elle. Sauf si elle ne se rapporte manifestement pas à l'exercice des fonctions de l'intéressé, une donnée détenue par un membre du personnel attaché à une Autorité publique ou par un membre d'une instance collégiale constitutive d'une Autorité publique, est une donnée détenue par l'Autorité publique;

6) « jour ouvrable » : celui qui n'est ni un samedi, ni un dimanche, ni un jour férié;

7) « Commission » : la Commission d'accès aux documents administratifs et aux données;

8) « partage administratif » : partage visé à l'article A. III.1. 68 °;

9) « réutilisation » : réutilisation visée à l'article A. III.1. 69°.

LIVRE A.III
Définitions de la partie C

Article A.III.1.
Définitions de la partie C

Au sens de la partie C du présent Code, on entend par :

1) « arrêté fixant les seuils numériques » :

arrêté conjoint du Gouvernement, du Collège et du Collège réuni fixant les seuils numériques, adopté sur la base de l'article C.III.1;

2) « Règlement sur la gouvernance des données » :

Règlement 2022/868/UE du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724;

3) « Règlement eIDAS » :

Règlement (UE) 910/2014 du Parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, abrogeant la Directive 1999/93/CE;

4) « Directive SRI 2 (NIS 2) » :

Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la Directive (UE) 2018/1972 et abrogeant la Directive (UE) 2016/1148 (Directive SRI 2);

5) « Autorité publique tierce » :

pouvoir public relevant d'un autre niveau de pouvoir, national ou international;

6) « donnée » :

donnée au sens de l'article 2, 1), du Règlement sur la gouvernance des données;

7) « document » :

tout contenu, quel que soit son support (papier ou forme électronique, enregistrement sonore, visuel ou audiovisuel) ou toute partie de ce contenu;

8) « donnée protégée » :

toute donnée qui est protégée pour l'un des motifs suivants :

(a) confidentialité commerciale, y compris le secret d'affaires, le secret professionnel et le secret d'entreprise;

(b) secret statistique;

(c) protection des droits de propriété intellectuelle de tiers;

(d) protection des données à caractère personnel;

9) « donnée sensible » :

toute donnée considérée comme confidentielle compte tenu du risque que son accès ou sa diffusion représenterait pour l'Autorité publique et pour les droits et libertés des personnes, ainsi que toute donnée classifiée;

10) « donnée classifiée » :

donnée nécessitant un degré de protection en matière de sécurité en vertu d'une norme législative ou réglementaire ou des traités internationaux;

11) « jeu de données » :

ensemble cohérent de de données, en tant que ressources ou d'informations (fichiers de données, fichiers d'explications, API, lien …) et de métadonnées (description, producteur, date de publication, mots-clefs, couverture géographique temporelle …) sur un thème donné;

12) « donnée ouverte » :

toute donnée librement accessible;

13) « donnée acquise » :

toute donnée obtenue auprès de tiers au moyen de contrats de licence commerciale ou par des moyens non commerciaux;

14) « (ensemble de) donnée à forte valeur » :

toute donnée qui présente des avantages importants pour la société, l'environnement ou l'économie, en particulier parce qu'elle se prête à la création de services possédant une valeur ajoutée, d'applications et de nouveaux emplois convenables tels que définis par l'arrêté ministériel du 26 novembre 1991 portant les modalités d'application de la réglementation du chômage, ainsi qu'en raison du nombre de bénéficiaires potentiels des services et applications à valeur ajoutée fondés sur ces ensembles de données;

15) « donnée déduite » et « donnée dérivée » :

toute donnée générée par analyse ou mise en relation avec d'autres données;

16) « donnée d'origine privée » :

toute donnée produite par des entités privées;

17) « donnée exclusive » :

toute donnée protégée par des droits de propriété intellectuelle ou commerciaux, dont les droits d'auteur et les secrets commerciaux, ou par des privilèges d'accès et de contrôle;

18) « donnée fermée » :

toute donnée qui n'est en principe pas accessible sauf si la réglementation en vigueur en dispose autrement;

19) « donnée fournie librement » :

toute donnée partagée activement et délibérément par une entité;

20) « donnée observée » :

toute donnée saisie et enregistrée relative à des activités concernant un utilisateur ou tout phénomène observable;

21) « donnée partageable » :

toute donnée qui peut être partagée de façon contrôlée ou restreinte, notamment au travers d'un cadre réglementaire ou légal;

22) « donnée publique » :

toute donnée détenue et gérée par les Autorités publiques dans le cadre de leurs missions de services publics ou mission d'intérêt général;

23) « donnée de contenu » :

toute donnée qui transmet l'essence, la substance, le sens ou le but d'une donnée ou d'une communication informatique stockée ou transmise;

24) « donnée de référence » :

toute donnée considérée comme structurante, par l'Autorité publique ou par l'usage, notamment pour nommer ou identifier des produits, des entités économiques, des territoires ou des personnes physiques et morales;

25) « donnée dynamique » :

toute donnée faisant l'objet d'actualisations fréquentes ou en temps réel, notamment à cause de leur volatilité ou de leur obsolescence rapide; les données émanant de capteurs sont typiquement considérées comme étant des données dynamiques;

26) « données de la recherche » :

toutes données, autres que des publications scientifiques, qui sont recueillis ou produits au cours d'activités de recherche scientifique et utilisés comme éléments probants dans le processus de recherche, ou dont la communauté scientifique admet communément qu'ils sont nécessaires pour valider des conclusions et résultats de la recherche;

27) « métadonnée » :

toute donnée relative à des données ou à des éléments de données, et décrivant un contenu, en mentionnant par exemple la date de création d'un document, l'auteur, le volume ou le format;

28) « donnée issue de source authentique » :

donnée composant une source authentique;

29) « source authentique » :

toute base de données comprenant des données qui font foi comme données uniques et originales concernant la personne ou le fait concerné(e) dont la gestion est assurée exclusivement par une Autorité publique ou une Autorité publique tierce agissant comme producteur de ladite base de donnée;

30) « source authentique bruxelloise » :

source authentique dont l'Autorité publique désignée producteur de la source authentique relève de la compétence de la Région, de la COCOM ou de la COCOF;

31) « domaine de données » :

champ spécifique ou relatif à un sujet d'intérêt dans lequel des données sont gérées;

32) « utilisateur (des données) » :

utilisateur défini au sens de l'article 2, 9), du Règlement sur la gouvernance des données;

33) « administrateur de base de données » :

fonction visant la prise en charge des opérations de surveillance, de maintenance et de gestion des interactions des données avec les applications et processus métiers, disposant de droits privilégiés leur permettant de réaliser leurs tâches d'administration;

34) « administrateur de sécurité informatique » :

fonction visant la prise en charge de la protection des données et des systèmes d'information contre les menaces sur la sécurité;

35) « administrateur réseau » :

fonction portant sur la mise en place, de la maintenance et de la surveillance des réseaux informatiques, également chargé de la configuration des équipements réseau, de l'optimisation des performances, de la sécurité des communications et de la résolution des problèmes relatifs au réseau de communication;

36) « administrateur système » :

fonction visant la prise en charge des systèmes informatiques et de leur bon fonctionnement, dont les tâches visent l'installation, la maintenance et la mise à jour des logiciels et des matériels, la sauvegarde et la restauration des données, ainsi que la résolution des problèmes techniques;

37) « organisation altruiste » :

organisation qui a pour mission d'encourager l'altruisme en matière de données;

38) « altruisme en matière de données » :

activité et finalité définie par l'article 2, 16), du Règlement sur la gouvernance des données;

39) « prestataire de services de confiance » :

prestataire tel que défini à l'article 3, 19), du Règlement eIDAS;

40) « service de confiance » :

service défini à l'article 3, 16), du Règlement eIDAS;

41) « prestataire de services en nuage » :

tout prestataire de service numérique qui permet l'administration à la demande et l'accès large à distance à un ensemble modulable et variable de ressources informatiques pouvant être partagées, y compris lorsque ces ressources sont réparties à différents endroits;

42) « prestataire de services informatiques de stockage » :

prestataire qui fournit des services de stockage de données informatiques pour les entreprises et les organisations;

43) « service d'intermédiation de données » :

service défini à l'article 2, 11), du Règlement sur la gouvernance des données;

44) « écosystème numérique bruxellois » :

le réseau de parties prenantes, partenaires, infrastructures informatiques, systèmes d'informations qui sont interconnectés dans un espace numérique, ainsi que des réseaux de communication électroniques, filaires et radios, au sein du territoire de la Région de Bruxelles-Capitale;

45) « Plateforme bruxelloise de la donnée » :

plateforme visée à l'article C.V.1;

46) « Centre d'intégration bruxellois » :

Centre d'intégration visé à l'article visé à l'article C.V.11;

47) « Catalogue des données » :

catalogue des données visé à l'article C.V.13;

48) « Portail ouvert des données publiques » :

portail ouvert des données publiques visé à l'article C.V.14;

49) « Centre d'exploitation et d'analyse des données » :

centre d'exploitation et d'analyse des données visé à l'article C.V.15;

50) « Point de contact et d'information » :

service visé à l'article C.V.16;

51) « Service d'appui » :

service visé à l'article C.V.17;

52) « Secrétariat numérique » :

service visé à l'article C.VI.4;

53) « Comité de coordination numérique » :

l'organe visé à l'article C.VI.11;

54) « Bureau de la donnée » :

l'organe visé à l'article C.VI.17;

55) « Comité de validation de l'architecture numérique » :

l'organe visé à l'article C.VI.6;

56) « Comité de gouvernance de la donnée » :

l'organe visé à l'article C.VI.14;

57) « Bureau d'achats numériques » :

l'organe visé à l'article C.VI.8;

58) « administrateur local de la donnée » :

la fonction visée à l'article C.VI.21;

59) « responsable de la donnée » :

la fonction visée à l'article C.VI.22;

60) « conseiller en sécurité de l'information » :

la fonction visée à l'article C.VII.23;

61) « entreprise publique » :

toute entreprise :

i) exerçant des activités dans les domaines définis dans la Directive 2014/25/UE;

ii) agissant en qualité d'opérateurs de services publics conformément à l'article 2 du règlement (CE) n° 1370/2007;

iii) agissant en qualité de transporteurs aériens remplissant des obligations de service public

conformément à l'article 16 du règlement (CE) n° 1008/2008;

iv) agissant en qualité d'armateurs communautaires remplissant des obligations de service public conformément à l'article 4 du règlement (CEE) n° 3577/92;

et sur laquelle les autorités publiques peuvent exercer directement ou indirectement une influence dominante du fait de la propriété de l'entreprise, de la participation financière qu'ils y détiennent ou des règles qui la régissent; l'influence dominante des autorités publiques sur l'entreprise est présumée dans tous les cas suivants lorsque ces organismes, directement ou indirectement :

a) détiennent la majorité du capital souscrit de l'entreprise;

b) disposent de la majorité des voix attachées aux parts émises par l'entreprise;

c) peuvent désigner plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance de l'entreprise;

62) « université » :

un organisme du secteur public dispensant un enseignement supérieur post-secondaire sanctionné par des diplômes universitaires;

63) « opérateur privé » :

toute personne physique ou morale ou organisation, ayant une personnalité juridique ou non, et qui n'est pas une Autorité publique;

64) « Autorité publique producteur (de données) » :

Autorité publique qui produit les données qui sont appelées à faire l'objet d'un partage administratif ou d'une réutilisation;

65) « Autorité publique destinataire » :

Autorité publique qui est destinée à recevoir les données dans le cadre d'un partage administratif ou d'une Communication;

66) « valorisation » :

démarche axée sur l'exploitation, le partage, ou l'amélioration des données publiques dans le but de renforcer l'efficacité des politiques publiques;

67) « partage de données » :

partage de données visé à l'article 2, 10), du Règlement sur la gouvernance des données;

68) « partage administratif » :

mise à disposition ou transmission de données publiques entre Autorités publiques, aux seules fins de l'exercice de leurs missions de services publics ou de leurs obligations d'intérêt général, à l'exclusion des partages avec Paradigm dans sa fonction de gestionnaire de la Plateforme bruxelloise de la donnée par rapport au Catalogue des données et à l'exclusion des partages visant les données ouvertes, sans conditions de réutilisation, disponibles dans le Portail ouvert des données publiques de la Plateforme bruxelloise de la donnée;

69) « réutilisation » :

utilisation par des personnes physiques ou morales de documents détenus par :

a) des Autorités publiques, à des fins commerciales ou non commerciales autres que l'objectif initial de la mission de service public pour lequel les documents ont été produits, à l'exception de l'échange de documents entre des Autorités publiques aux seules fins de l'exercice de leur mission de service public, ou;

b) des entreprises publiques, à des fins commerciales ou non commerciales autres que l'objectif initial de fournir les services d'intérêt général pour lequel les documents ont été produits, à l'exception de l'échange de documents entre des entreprises publiques et des Autorités publiques aux seules fins de l'exercice de leur mission de service public;

70) « Communication » :

la fourniture de données d'un opérateur privé vers une ou plusieurs Autorité(s) publique(s) destinataire(s) à des fins exclusives d'utilisation dans le cadre de l'exécution de ses missions de service public ou d'intérêt général;

71) « traitement » :

traitement défini à l'article 2, 12), du Règlement sur la gouvernance des données;

72) « accès » :

accès défini à l'article 2. 13), du Règlement sur la gouvernance des données;

73) « transmission » (dans le cadre d'un partage administratif) :

procédé qui, dans le cadre d'un partage administratif, implique l'envoi ou le déplacement actif d'une donnée depuis l'Autorité publique producteur de la donnée vers l'Autorité publique destinataire de la donnée, généralement via un réseau de communication;

74) « mise à disposition » (dans le cadre d'un partage administratif) :

procédé qui, dans le cadre d'un partage administratif, permet de rendre accessibles et utilisables les données d'une Autorité publique producteur desdites données par une autre Autorité publique destinataire de ces données au moyen d'un accès approprié;

75) « anonymisation » :

processus de transformation des documents en documents anonymes ne permettant pas de remonter à une personne physique identifiée ou identifiable ou processus consistant à rendre anonymes des données à caractère personnel de telle sorte que la personne concernée ne soit pas ou plus identifiable;

76) « occultation » :

processus de transformation des documents ou données confidentielles en documents ou données ne permettant pas d'accéder aux données confidentielles; ou consistant à masquer les données commerciales sensibles ou confidentielles de sorte qu'elles ne soient plus identifiables;

77) « intégration des données » :

processus de combinaison de différents jeux de données pour en créer un seul plus complet et plus cohérent;

78) « archivage » :

conservation des documents et des données compte tenu d'un délai de conservation légal ou de l'utilité administrative caractérisant encore les documents et les données visés;

79) « base de données » :

recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessibles par des moyens électroniques ou d'une autre manière;

80) « autorisation » :

l'autorisation visées à l'article 2. 6), du Règlement sur la gouvernance des données;

81) « interopérabilité » :

capacité de différents systèmes, équipements, logiciels ou services à fonctionner ensemble de manière cohérente et à échanger des informations;

82) « réseau et système d'information » :

cette notion peut désigner :

a) un réseau de communications électroniques au sens de l'article 2, point a), de la Directive 2002/21/CE;

b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques; ou

c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance;

83) « cas d'usage ou cas d'utilisation » :

un scénario spécifique dans lequel des données ouvertes sont utilisées pour réaliser un objectif ou une fonction particulière;

84) « format ouvert » :

format de fichier indépendant des plateformes utilisées et mis à la disposition du public sans restriction visant à empêcher la réutilisation des documents;

85) « informatique en nuage (cloud computing) » :

modèle de gestion informatique permettant l'accès via un réseau à des ressources informatiques partagées et configurables;

86) « modèle opérationnel » :

représentation abstraite de la façon dont une organisation opère à travers des domaines de processus, d'organisation et de technologie afin d'accomplir sa fonction;

87) « interface de programmation d'application » :

tout ensemble de fonctions, de procédures, de définitions et de protocoles qui permet le transfert de machine à machine et l'échange automatisé de données;

88) « intelligence artificielle » :

un système d'intelligence artificielle défini à l'article 3(1) du Règlement du Parlement européen et du Conseil du 13 mars 2024 fixant des règles harmonisées en matière d'intelligence artificielle (loi sur l'intelligence artificielle);

89) « licence type » :

une série de conditions de réutilisation prédéfinies dans un format numérique, de préférence compatible avec des licences publiques normalisées disponibles en ligne;

90) « format lisible par machine » :

un format de fichier structuré de telle manière que des applications logicielles puissent facilement identifier, reconnaître et extraire des données spécifiques, notamment chaque énoncé d'un fait et sa structure interne;

91) « norme formelle ouverte » :

norme établie par écrit, précisant en détail les exigences relatives à la manière d'assurer l'interopérabilité des logiciels;

92) « retour sur investissement raisonnable » :

un pourcentage de la redevance globale, en sus du montant nécessaire au recouvrement des coûts éligibles, ne dépassant pas de plus de cinq points de pourcentage le taux d'intérêt fixe de la BCE;

93) « tiers de confiance » :

le tiers de confiance est une entité indépendante qui dispose des moyens techniques nécessaires à l'anonymisation ou la pseudonymisation des données à caractère personnel dans le cadre des traitements énoncés par l'article 89 du RGPD;

94) « sécurité de l'information » :

stratégie, règles, procédures et moyens de protection de tout type d'information tant dans les systèmes de transmission que dans les systèmes de traitement en vue de garantir la confidentialité, la disponibilité, l'intégrité, la fiabilité, l'authenticité et l'irréfutabilité de l'information;

95) « Intégrateur de services » :

une institution qui, par ou en vertu d'un traité, d'un règlement, d'une directive, d'une loi, d'un décret ou d'une ordonnance, est chargée de l'intégration de services à un niveau de pouvoir ou dans un secteur déterminé;

96) « intégration de services » :

l'organisation d'échanges mutuels de données électroniques entre Autorités publiques entre elles et entre les Autorités publiques et les intégrateurs de services, ainsi que la mise à disposition intégrée de ces données;

97) « Intégrateur de services bruxellois » :

l'institution désignée à l'article C.V.12;

98) « commande publique numérique mutualisable » :

achat en matière numérique considéré comme mutualisable portant sur des travaux, services ou fournitures ayant un impact sur l'écosystème numérique, qui reprend les besoins similaires des différentes autorités publiques;

99) « sécurité informatique » :

ensemble des technologies, processus et pratiques conçus pour protéger les réseaux, les dispositifs, les applications et les données contre les menaces, attaques ou accès non autorisés;

100) « état de l'art » :

les techniques, méthodes, standards et pratiques reconnues comme les plus avancées et les plus efficaces en matière de sécurité informatique;

101) « donnée d'usage » :

donnée qui se réfère aux informations collectées concernant l'interaction des utilisateurs ou des citoyens avec les services publics, les plateformes, les applications et d'autres offres numériques éventuellement proposées par les

Autorités publiques. Ces données peuvent inclure, sans s'y limiter, les durées de connexion, les pages visitées, les fonctionnalités utilisées, les erreurs rencontrées ou encore les retours et commentaires des utilisateurs;

102) « donnée à caractère personnel non confidentielle » :

donnée qui, bien que à caractère personnel, peut être rendue publique pour des objectifs d'intérêt général ou dans le cadre de missions de service public en vertu de normes législatives;

103) « donnée à caractère personnel confidentielle » :

donnée à caractère personnel qui n'est pas une donnée à caractère personnel non confidentielle;

104) « l'individualisation » :

possibilité d'isoler/d'identifier une personne physique;

105) « la corrélation » :

possibilité de relier plusieurs ensembles de données à une personne physique;

106) « l'inférence » :

possibilité de déduire des informations sur une personne physique;

107) « la traçabilité » :

le traitement permettant de suivre une donnée durant son cycle de vie;

108) « réversibilité » :

le traitement permettant de récupérer les états antérieurs d'une donnée durant son cycle de vie;

109) « randomisation » :

méthode d'anonymisation qui implique la modification des données d'une manière aléatoire pour masquer les attributs individuels à caractère personnel;

110) « généralisation » :

technique d'anonymisation qui réduit la précision des attributs de données pour les rendre moins identifiables;

111) « attributs de données » :

propriétés spécifiques qui décrivent les éléments d'un ensemble de données dans un contexte de base de données ou d'analyse de données;

112) « Urbis » :

la base de données de cartographie numérique de référence à grande échelle du territoire de la Région de Bruxelles-Capitale.

PARTIE B
GOUVERNANCE ADMINISTRATIVE

LIVRE B.I.
Publicité administrative

TITRE 1
Dispositions générales

Article B.I.1.
Dispositions générales

Le présent livre a pour objet de renforcer la transparence de l'administration en facilitant l'accès aux documents administratifs et aux informations environnementales.

Il vise également à transposer partiellement la Directive 2003/4/CE du Parlement européen et du Conseil du 28 janvier 2003 concernant l'accès du public à l'information en matière d'environnement et abrogeant la Directive 90/313/CEE du Conseil. À cette fin, il vise à garantir le droit d'accès aux informations environnementales détenues par les Autorités publiques ou pour leur compte, à fixer les conditions de base et les modalités pratiques de ce droit et à veiller à ce que les informations environnementales soient d'office rendues progressivement disponibles et diffusées auprès du public afin de parvenir à une mise à disposition et une diffusion systématique aussi large que possible des informations environnementales auprès du public. Dans ce but, il convient de promouvoir l'utilisation, entre autres, des technologies de télécommunication informatique ou des technologies électroniques, lorsqu'elles sont disponibles.

Le présent livre s'applique sans préjudice des dispositions applicables du règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE et sans préjudice de l'existence d'obligations d'omettre des informations qui doivent être tenues confidentielles en vertu d'une disposition de droit international en vigueur ou d'une norme interne à caractère législatif.

Il s'applique également sans préjudice de l'ordonnance du 4 octobre 2018 relative à l'accessibilité des sites internet et des applications mobiles des organismes publics régionaux et des communes.

Article B.I.2.
Champ d'application ratione personae

Le présent livre s'applique aux Autorités publiques visées à l'article A.I.3, 1), a) à g) et j).

Le présent livre s'applique également aux autorités administratives autres que celles visées à l'alinéa 1er, mais seulement dans la mesure où elles prohibent ou restreignent la publicité de documents administratifs pour des motifs relevant de la compétence de la Commission communautaire commune, de la Région de Bruxelles-Capitale et de la Commission communautaire française.

Article B.I.3.
Calcul des délais

Les délais prévus dans le présent livre commencent à courir le jour qui suit celui qui constitue le point de départ du délai. Le jour de l'échéance est compris dans le délai. Si ce jour n'est pas un jour ouvrable, le jour de l'échéance est reporté au jour ouvrable qui suit.

TITRE 2
Publicité active

CHAPITRE 1
Dispositions générales

Article B.I.4.
Publications sur les sites internet de chaque Autorité publique

§ 1er. – Les Autorités publiques disposent de sites internet qui comprennent, parmi les éléments de la page d'accueil, une rubrique « transparence » aisément identifiable.

Cette rubrique contient au minimum :

1° un document décrivant les compétences, l'organisation et le fonctionnement de l'Autorité publique;

2° un inventaire des subventions accordées dans le courant de l'année précédente, mentionnant le bénéficiaire, l'objet de la subvention et son montant;

3° un inventaire des études réalisées pour le compte de l'Autorité publique dans le courant de l'année précédente, pour autant qu'elles aient été réalisées par un partenaire externe. L'inventaire mentionne, pour chaque étude, l'identité de son auteur, c'est-à-dire le nom de la personne morale ou physique à qui l'étude a été confiée, ainsi que son coût et le titre de l'étude;

4° un inventaire des marchés publics conclus dans le courant de l'année précédente, comprenant la mention de l'adjudicataire et le montant engagé;

5° les appels à candidats et les conditions de recrutement, de promotion ou de remplacement de tous les emplois que l'Autorité publique entend pourvoir, publiés dans les sept jours ouvrables de la décision de procéder à un recrutement, une promotion ou un remplacement, ainsi que la liste des recrutements réalisés, des promotions accordées ou des remplacements organisés des emplois des agents de niveau A que l'Autorité publique pourvoit, le nom et la fonction des agents concernés étant publiés dans les sept jours ouvrables de la décision les concernant et pour une durée de soixante jours.

Les inventaires visés à l'alinéa 2, 2° à 4°, sont également intégrés au Catalogue visé à l'article C.V.13, du Code via l'outil de gestion, par les Autorités publiques visées à l'article C.I.1 également soumises au présent livre conformément à l'article B.I.2, en vue d'une publication dans le cadre du Portail ouvert des données publiques visé à l'article C.V.14. Ces informations sont également reprises, selon des modalités déterminées par le Gouvernement, le Collège réuni et le Collège, sous forme de cadastre des subsides et des marchés publics afin d'exploiter visuellement et graphiquement ces informations de manière à les rendre compréhensibles et aisément accessibles à tous.

Le contenu des études visées à l'alinéa 2, 3° est publié pour autant qu'il présente un intérêt économique, social, sanitaire ou environnemental. Les Autorités publiques vérifient préalablement à toute publication si des exceptions visées à l'article B.I.17 s'opposent à la publication de tout ou partie de de ces études. Les Autorités publiques ne publient pas le contenu de l'étude, de même que, par dérogation au paragraphe 1er, alinéa 2, 3°, son titre, si l'intérêt du public de la publicité ne l'emporte pas sur la protection de l'un des intérêts visés par les exceptions.

Le document visé à l'alinéa 2, 1°, est mis à jour sans délai dès qu'un changement affecte les compétences, l'organisation ou le fonctionnement de l'Autorité publique. Les inventaires visés à l'alinéa 2, 2° à 4°, sont publiés chaque année au plus tard le 1er avril.

Le Gouvernement, le Collège réuni et le Collège peuvent, conjointement, déterminer les autres docu-

ments qui doivent figurer sous la rubrique visée à l'alinéa 1er.

§ 2. – Le Gouvernement, le Collège réuni et le Collège publient, le temps de chaque législature, au sein de la rubrique transparence de leur site internet la liste actualisée de tous les membres des cabinets ministériels, en mentionnant leur nom et leur fonction.

Le Collège communal publie, le temps de chaque législature, au sein de la rubrique transparence du site internet de la commune la liste actualisée de tous les membres des cabinets employés au service du bourgmestre et des échevins, en mentionnant leur nom et leur fonction.

Le président du CPAS publie, le temps de son mandat, au sein de la rubrique transparence du site internet du CPAS la liste actualisée de tous les membres de son cabinet, en mentionnant leur nom et leur fonction.

§ 3. – Le Gouvernement, le Collège réuni et le Collège diffusent au sein de la rubrique transparence de leur site internet :

1° au plus tard la veille de leurs réunions, l'ordre du jour définitif de celles-ci;

2° au plus tard le jour ouvrable qui suit leur réunion, les décisions qu'ils ont adoptées ainsi que les notes du Gouvernement, du Collège réuni, et du Collège, ainsi que leurs annexes, sur lesquelles les décisions se fondent, sauf lorsqu'il s'agit de décisions de portée individuelle. Concernant les notes et leurs annexes, le Gouvernement, le Collège réuni et le Collège vérifient, préalablement à leur publication, si des exceptions visées à l'article B.I.17 sont d'application. Ils ne publient pas ces documents ou ne publient qu'une partie de ceux-ci si l'intérêt du public ne l'emporte pas sur la protection de l'un des intérêts visés par les exceptions.

Les publications au sein de la rubrique « transparence » des sites internet des Autorités publiques ne constituent pas des publications officielles.

§ 4. – Les finalités poursuivies par la publication des données à caractère personnel en application des paragraphes 2 à 3 sont :

1° de permettre à chacun un contrôle externe effectif de l'action de l'administration et de veiller au respect de l'État de droit par les Autorités publiques;

2° de rééquilibrer la relation de pouvoir entre l'administré et les Autorités publiques et de renforcer la confiance du premier en la seconde ainsi que les bonnes relations entre ceux-ci;

3° de fournir les informations nécessaires aux administrés dans le cadre de l'exercice de leurs droits;

4° de mettre à disposition de tous le savoir financé par les deniers publics.

La personne concernée a le droit de s'opposer conformément à l'article 21 du RGPD à la publication de ses données. La personne concernée expose les raisons tenant à sa situation particulière à l'Autorité publique qui peut décider de ne pas publier les données à caractère personnel de la personne concernée au sein de sa rubrique transparence.

Article B.I.5.
Désignation de la personne en charge de la publicité active

Les Autorités publiques désignent en leur sein au minimum une personne chargée de recueillir les documents administratifs ainsi que les informations à caractère environnemental devant être publiées sous la rubrique « transparence » de leurs sites internet et de procéder à la publication requise par le présent livre.

Les Autorités publiques transmettent à la Commission d'accès aux documents administratifs et aux données le nom et les coordonnées de cette personne.

Article B.I.6.
Indication de la personne disposant de l'information et des modes de saisine du médiateur bruxellois

§ 1er. – Toute correspondance émanant d'une Autorité publique indique le nom, le prénom, la qualité, l'adresse administrative, le numéro de téléphone et l'adresse courriel de la personne en mesure de fournir de plus amples informations sur le dossier.

Par dérogation à l'alinéa 1er, les correspondances de même nature envoyées à plus de cent destinataires peuvent se limiter à mentionner l'adresse administrative, le numéro de téléphone et, si elle existe, l'adresse courriel spécifique de l'unité administrative compétente.

§ 2. – Tout acte administratif unilatéral à portée individuelle notifié à un administré indique la possibilité de saisir le médiateur bruxellois, ainsi que les modalités de cette saisine et les voies éventuelles de recours administratifs, les instances compétentes pour en connaître, ainsi que les formes et délais à respecter, faute de quoi le délai de prescription pour introduire le recours ne prend pas cours.

Article B.I.7.
La disponibilité des informations publiées

La publication au sein de la rubrique « transparence » des sites internet des Autorités publiques consiste, soit à rendre le document ou l'information directement disponible à la lecture, à l'impression ou à la réutilisation, soit à renseigner un lien vers un autre site Internet permettant la lecture, l'impression ou la réutilisation du document ou de l'information.

Le Gouvernement, le Collège réuni et le Collège arrêtent, s'il échet conjointement, les modalités techniques et pratiques destinées à permettre une récolte et un traitement aisé des données à publier.

CHAPITRE 2
Dispositions spécifiques aux informations relatives à l'environnement et l'aménagement du territoire

Article B.I.8.
Publications actives spécifiques à Bruxelles Environnement

Bruxelles Environnement publie sur son site internet les textes des traités, conventions et accords internationaux, ainsi que de la législation européenne, fédérale, régionale et locale concernant l'environnement ou s'y rapportant. Il veille à ce que ces textes soient tenus à jour.

Article B.I.9.
Publication active d'informations environnementales

Les Autorités publiques compétentes publient, sous la rubrique « transparence » de leurs sites internet, dans les 30 jours ouvrables de leur adoption, les plans et programmes environnementaux, les plans et schémas d'aménagement du territoire, les règlements d'urbanisme, les lignes de conduite en matière d'environnement ou d'aménagement du territoire qu'elles adoptent, ainsi que le rapport sur les incidences environnementales qui accompagne les informations environnementales précitées.

Article B.I.10.
Publication active des permis d'urbanisme et de lotir ainsi que des rapports et études jointes

Dans les 10 jours ouvrables de leur délivrance, les autorités publiques compétentes publient, sous la rubrique transparence de leur site internet, les permis d'urbanisme, les permis de lotir et leurs modifications qui ont fait l'objet d'un rapport ou d'une étude d'incidences. Ce rapport ou cette étude est joint à la publication. Lorsque la demande de permis d'urbanisme était soumise aux mesures particulières de publicité, les plans de synthèse sont joints à la publication.

Indépendamment de la réalisation d'un rapport ou d'une étude d'incidences, les Autorités publiques compétentes publient, dans le même délai, les permis d'urbanisme, les permis de lotir et leurs modifications lorsque ceux-ci sont susceptibles d'avoir un impact significatif sur l'environnement ou sur l'aménagement du territoire.

Lorsque les documents visés aux alinéas 1er et 2 comportent des éléments relatifs à la vie privée, des éléments faisant l'objet d'un droit de propriété intellectuelle ou des éléments dont la divulgation serait susceptible de porter gravement atteinte à la sécurité publique, l'Autorité publique s'assure, préalablement à la publication, que ces éléments soient omis du document publié.

Article B.I.11.
Publication active des mesures de protection du patrimoine immobilier

Le Gouvernement publie sur son site Internet les mesures de protection du patrimoine immobilier qu'il adopte, dans les 10 jours ouvrables de leur adoption.

Article B.I.12.
Publication active des permis d'environnement

§ 1er. – Dans les 10 jours ouvrables de leur délivrance ou de la décision, les Autorités publiques compétentes publient, sous la rubrique « transparence » de leurs sites internet, les permis d'environnement, les modifications d'autorisation, les scissions de permis d'environnement, les prolongations de permis d'environnement, les modifications de condition d'exploiter des installations classées ainsi que les suspensions et les retraits de permis d'environnement qui ont fait l'objet d'un rapport ou d'une étude d'incidences. Ce rapport ou cette étude est joint à la publication.

Indépendamment de la réalisation d'un rapport ou d'une étude d'incidences, les autorités publiques compétentes publient, dans le même délai, les documents visés à l'alinéa 1er, lorsque ceux-ci sont susceptibles d'avoir un impact significatif sur l'environnement ou sur l'aménagement du territoire.

Lorsque les documents visés aux alinéas 1er et 2 comportent des éléments relatifs à la vie privée, des éléments faisant l'objet d'un droit de propriété intellectuelle ou des éléments dont la divulgation serait susceptible de porter gravement atteinte à la sécurité publique, l'Autorité publique s'assure, préalablement

à la publication, que ces éléments soient omis du document publié.

§ 2. – Bruxelles Environnement publie sur son site Internet :

1° la liste des agréments visés à l'article 78 de l'ordonnance du 5 juin 1997 relative aux permis d'environnement;

2° les rapports d'inspection requis par l'article 19, § 6, de l'arrêté du Gouvernement de la Région de Bruxelles-Capitale du 21 novembre 2013 relatif à la prévention et la réduction intégrées de la pollution due aux émissions industrielles dans les 30 jours ouvrables de leur notification à l'exploitant;

3° les informations qui doivent être tenues à la disposition du public ou publiées en vertu des articles 9 et 10 de l'ordonnance du 5 mars 2009 relative à la gestion et à l'assainissement des sols pollués.

Lorsque les documents visés à l'alinéa 1er comportent des éléments relatifs à la vie privée, des éléments faisant l'objet d'un droit de propriété intellectuelle ou des éléments dont la divulgation serait susceptible de porter gravement atteinte à la sécurité publique, l'Autorité publique s'assure, préalablement à la publication, que ces éléments soient omis du document publié.

Article B.I.13.
Publication active en cas de menace imminente

Les Autorités publiques compétentes publient immédiatement au sein de la rubrique « transparence » de leur site internet, en cas de menace imminente pour la santé humaine ou pour l'environnement résultant d'activités humaines ou de causes naturelles, toutes les informations qui pourraient permettre à la population susceptible d'être affectée de prendre des mesures pour prévenir ou atténuer le dommage lié à la menace en question.

Article B.I.14.
Rapport sur l'état de l'environnement bruxellois

Sans préjudice des obligations de faire rapport découlant d'autres législations, le Gouvernement publie sur son site internet, tous les quatre ans, un rapport détaillé sur l'état de l'environnement bruxellois, qu'il transmet également au Parlement de la Région de Bruxelles-Capitale, et il publie sur son site internet tous les deux ans une note de synthèse comportant les principaux indicateurs environnementaux.

Ce rapport et cette note de synthèse sont établis par Bruxelles Environnement et décrivent la situation des différentes composantes du milieu environnemental, visées à l'article A.II.1, 4°, les pressions qui y sont exercées, le contexte socio-économique, les entreprises, les transports, les changements socio-démographiques et les perspectives d'évolution.

Ils se basent sur des données régionales ou éventuellement locales, dont certaines doivent permettre une comparaison cohérente avec les données rassemblées par diverses institutions internationales dans le cadre de rapports au niveau des pays ou au niveau des régions urbaines et d'autres doivent détailler des spécificités bruxelloises. Ils sont ensuite soumis à l'avis du Conseil de l'Environnement, qui sera également publié sur le site internet du Gouvernement.

Le rapport comprend en outre les indicateurs socio-économiques suivants :

1° structures des entreprises (primaire-secondaire-tertiaire);

2° accidents industriels;

3° évolution des modes de transport.

TITRE 3
Publicité passive

Article B.I.15.
Principes

§ 1er. – Chacun, selon les conditions prévues par le présent livre, peut prendre connaissance sur place de tout document administratif et de toute information environnementale émanant d'une Autorité publique, obtenir des explications à son sujet et en recevoir communication sous forme de copie.

§ 2. – L'obtention de copies de documents administratifs ou d'informations environnementales peut être soumise à une rétribution, qui ne peut en excéder le prix coûtant. Ces rétributions sont payables au comptant si la copie est reçue par le demandeur auprès de l'Autorité publique. Celle-ci délivre un récépissé à titre de preuve de paiement. Si la copie est transmise au demandeur par la poste ou un autre moyen de transmission, les rétributions sont payées préalablement à cette transmission, par virement ou versement au compte des recettes de l'autorité concernée.

§ 3. – Pour les documents administratifs contenant de l'information se rapportant à une personne physique identifiée ou identifiable, lorsque cette information constitue une appréciation ou un jugement de

valeur relatif à cette personne ou lorsqu'elle se rapporte à un comportement de cette personne dont la divulgation peut manifestement lui causer préjudice, le demandeur doit justifier d'un intérêt.

L'alinéa 1er n'est pas applicable aux informations environnementales.

Article B.I.16.
Demande d'accès au document administratif ou à une information environnementale

§ 1er. – La consultation d'un document administratif ou d'une information environnementale, les explications y relatives ou sa communication sous forme de copie ont lieu sur demande. La demande indique clairement la matière concernée et si possible, les documents administratifs ou les informations environnementales concernés et est adressée par envoi postal, électronique ou par porteur à l'Autorité publique compétente.

§ 2. – La demande est irrecevable :

1° si elle n'est pas signée par le demandeur.

Les personnes morales, outre la signature de leur fondé de pouvoir, mentionnent dans leur demande leur numéro d'inscription à la banque-carrefour des entreprises visée à l'article III.15 du code de droit économique ou fournissent une copie de leurs statuts lorsqu'il s'agit d'une personne morale de droit étranger.

En cas d'envoi de la demande par courriel, celui-ci est considéré comme valablement signé lorsque le demandeur, ou le fondé de pouvoir de la demanderesse personne morale, joint à son courriel une photocopie, une photographie ou un scan d'un document d'identité.

Lorsque la demande est signée par un avocat ou qu'elle est transmise par courriel par un avocat, le demandeur ne doit pas y joindre les documents visés par les alinéas précédents;

2° si elle ne précise pas le nom et l'adresse du demandeur;

3° si elle n'est pas adressée à l'Autorité publique de façon à lui assurer une date certaine.

Quand une demande n'est pas recevable, l'Autorité publique compétente doit le faire savoir au demandeur dans les plus brefs délais, pour autant que ce dernier soit identifié dans la demande.

§ 3. – Lorsque la demande de consultation, d'explication ou de communication sous forme de copie est adressée à l'Autorité publique qui n'est pas compétente ou si celle-ci n'est pas en possession du document administratif ou de l'information environnementale, elle en informe sans délai le demandeur et lui communique la dénomination et l'adresse de l'autorité qui, selon les informations dont elle dispose, est compétente ou est détentrice du document administratif. Si l'Autorité publique considère que le document est inexistant, elle le communique également sans délai au demandeur.

§ 4. – Le demandeur veille à indiquer la façon dont il souhaite pouvoir prendre connaissance du document ou de l'information environnementale. À défaut de précisions, la communication d'une copie par courriel est privilégiée.

§ 5. – L'Autorité publique consigne les demandes écrites dans un registre, classées par date de réception.

Article B.I.17.
Rejet des demandes

§ 1er. – L'Autorité publique peut rejeter une demande de consultation, d'explication ou de communication sous forme de copie d'un document administratif ou d'une information environnementale dans la mesure où la demande :

1° concerne un document administratif ou une information environnementale dont la divulgation peut être source de méprise, le document étant inachevé ou incomplet. Le cas échéant, l'Autorité publique désigne l'autorité qui élabore les documents ou les informations en question et indique le délai jugé nécessaire pour les finaliser;

2° concerne un avis ou une opinion communiqués librement et à titre confidentiel à l'autorité;

3° est manifestement abusive;

4° demeure formulée de manière trop générale, même après l'application de l'article B.I.18, § 3.

§ 2. – L'Autorité publique rejette la demande de consultation, d'explication ou de communication sous forme de copie d'un document administratif, si elle constate que l'intérêt de la publicité ne l'emporte pas sur la protection de l'un des intérêts suivants :

1° les libertés et les droits fondamentaux des administrés, en ce compris la vie privée;

2° les relations internationales et la sécurité publique;

3° la bonne marche de la justice, la possibilité pour toute personne d'être jugée équitablement ou la capacité d'un pouvoir public de mener une enquête à caractère pénal ou disciplinaire;

4° le secret de l'identité de la personne qui a communiqué le document ou l'information à l'Autorité publique à titre confidentiel pour dénoncer un fait punissable ou supposé tel;

5° un intérêt économique ou financier de la Commission communautaire commune, de la Région de Bruxelles-Capitale, de la Commission communautaire française, des communes et CPAS ainsi que de l'ensemble des autorités visées à l'article B.I.2;

6° la confidentialité des délibérations des pouvoirs publics;

7° la confidentialité des informations commerciales ou industrielles, lorsque cette confidentialité est prévue par le droit régional ou européen afin de protéger un intérêt économique légitime;

8° la protection de l'environnement auquel se rapportent les informations sollicitées, telles que la localisation d'espèces rares;

9° la confidentialité requise en vue de mener des évaluations des membres du personnel de l'Autorité publique concernée et des audits internes.

Le présent paragraphe n'est pas applicable aux informations environnementales.

§ 3. – L'Autorité publique rejette la demande de consultation, d'explication ou de communication sous forme de copie d'une information environnementale si elle constate que l'intérêt du public servi par la publicité ne l'emporte pas sur la protection de l'un des intérêts suivants :

1° la confidentialité des délibérations des pouvoirs publics, lorsque cette confidentialité est prévue par le droit;

2° les relations internationales et la sécurité publique;

3° la bonne marche de la justice, à la possibilité pour toute personne d'être jugée équitablement ou à la capacité pour un pouvoir public de mener une enquête à caractère pénal ou disciplinaire;

4° la confidentialité des informations commerciales ou industrielles, lorsque cette confidentialité est prévue par le droit régional ou européen afin de protéger un intérêt économique légitime;

5° la confidentialité des données à caractère personnel et des dossiers concernant une personne physique si cette personne n'a pas consenti à la divulgation de ces informations au public, lorsque la confidentialité de ce type d'information est prévue par le droit régional ou européen;

6° aux intérêts ou la protection de toute personne qui a fourni les informations demandées sur une base volontaire sans y être contrainte par la loi ou sans que la loi puisse l'y contraindre, à moins que cette personne n'ait consenti à la divulgation de ces données;

7° la protection de l'environnement auquel se rapportent les informations sollicitées, telles que la localisation d'espèces rares.

L'Autorité publique ne peut, en vertu des points 1°, 4°, 5°, 6°, 7°, rejeter une demande lorsqu'elle concerne des informations relatives à des émissions dans l'environnement.

§ 4. – L'article 7 du RGPD est applicable aux consentements visés aux paragraphes 2 et 3.

§ 5. – L'Autorité publique rejette la demande de consultation, d'explication ou de communication sous forme de copie d'un document administratif si la publicité porte atteinte à une obligation de secret instaurée par une ordonnance de la Région de Bruxelles-Capitale, une ordonnance de la Commission communautaire commune ou un décret de la Commission communautaire française.

Le présent paragraphe n'est pas applicable aux informations environnementales.

§ 6. – Les exceptions à l'accès aux documents administratifs et à l'information environnementale, fixées par le présent article s'appliquent sans préjudice d'autres exceptions fixées par l'État fédéral et les Communautés dans le cadre de leur compétences matérielles.

§ 7. – Pour l'application des paragraphes 2 et 3, le rejet de la demande de communication sous forme de copie d'un document administratif ou d'une information environnementale n'implique pas nécessairement le rejet de la demande de consultation de ce document ou de cette information environnementale ou la demande d'explication à son sujet.

Lorsque, en application des paragraphes 2, 3, et 5, un document administratif ou une information environnementale ne doit ou ne peut être soustrait que partiellement à la publicité, la consultation, l'explication ou la communication sous forme de copie est limitée à la partie restante.

Article B.I.18.
Délais

§ 1er. – Sans préjudice du Titre II et de la faculté, pour une Autorité publique, de les laisser consulter immédiatement sur place, l'autorité saisie d'une demande met les documents administratifs et les informations environnementales à la disposition du demandeur dès que possible ou, au plus tard, dans les 20 jours ouvrables qui suivent la réception de la demande par elle, en tenant compte du délai indiqué par le demandeur dans sa demande écrite et, le cas échéant, de l'urgence invoquée par celui-ci.

§ 2. – Ce délai est porté à 40 jours ouvrables lorsque le volume et la complexité des informations sont tels que le délai de 20 jours ouvrables ne peut être respecté. Dans ce cas, le demandeur est informé dès que possible et en tout état de cause, avant la fin du délai de 20 jours ouvrables, de toute prolongation du délai et des motifs de cette prolongation.

§ 3. – Si une demande est formulée de manière trop vague, l'Autorité publique invite le demandeur, dès que possible et avant l'expiration du délai de 20 jours ouvrables, à la préciser et l'aide à cet effet.

§ 4. – Le demandeur a la faculté de solliciter l'examen de sa demande en urgence. Il doit exposer les raisons qui justifient l'urgence dans sa demande. L'urgence dûment motivée par le demandeur est celle qui rend manifestement inapproprié aux faits de la cause le respect des délais de traitement établi aux paragraphes § 1er et § 2, en raison des inconvénients graves susceptibles d'affecter la situation du demandeur si les délais précités devaient être observés.

Lorsque l'Autorité publique reconnaît l'urgence de la demande, elle y répond dès que possible et au plus tard dans les 7 jours ouvrables qui suivent la réception de la demande.

Lorsque l'Autorité publique considère que l'urgence invoquée n'est pas fondée, elle en informe immédiatement le demandeur par une décision motivée et applique les délais déterminés par les paragraphes § 1er et § 2.

§5 . Par dérogation aux paragraphes § 1er à § 4, les demandes sont traitées prioritairement et selon une procédure accélérée lorsque la demande d'accès concerne une décision soumise à une procédure d'enquête publique en cours, en vertu du Code Bruxellois de l'Aménagement du territoire ou des normes prises en exécution de celui-ci, de l'ordonnance du 5 juin 1997 relative aux permis d'environnement ou de l'ordonnance du 18 mars 2004 relative à l'évaluation des incidences de certains plans et programmes sur l'environnement.

Dans ce cas, l'Autorité publique à laquelle la demande est adressée met les documents et informations demandés à disposition du demandeur immédiatement et, si le document ou l'information ne se trouve pas dans les lieux prévus pour la consultation du dossier soumis à l'enquête publique, au plus tard une semaine avant l'expiration du délai de l'enquête publique.

Article B.I.19.
Notification de la décision

Toute décision de refus, total ou partiel, d'accès ou de refus d'accès sous la forme ou dans le format demandé est notifiée au demandeur par écrit, dans les délais visés à l'article B.I.18, § 1er à § 4, selon le cas.

Si l'Autorité publique à laquelle une demande est formulée dans le cadre d'une enquête publique estime que l'accès au document ou à l'information demandée doit être refusé ou limité en vertu d'un des motifs visés à l'article B.I.17, elle le notifie au demandeur dans les sept jours ouvrables de la demande.

La notification indique de manière claire, précise et complète, les motifs qui justifient le refus et indique l'existence du recours prévu au livre B.II ainsi que les formes et délais à respecter, de même que la possibilité de saisir le médiateur bruxellois et les modalités de sa saisine.

Le défaut de notification dans les délais visés à l'article B.I.18, § 1er à § 4 équivaut à un refus.

TITRE 4
Correction d'informations inexactes ou incomplètes

Article B.I.20.
Principe

Lorsqu'une personne démontre qu'un document administratif ou une information environnementale émanant d'une Autorité publique comporte des informations inexactes ou incomplètes la concernant, cette Autorité est tenue d'apporter les corrections requises sans frais pour l'intéressé.

La rectification s'opère à la demande écrite de l'intéressé.

Article B.I.21.
Demande de rectification

L'Autorité publique donne suite à une demande de rectification au plus tard dans un délai d'un mois à

compter de la réception de la demande. En cas de refus, elle communique les motifs de rejet.

Ce délai peut être prolongé de deux mois compte tenu de la complexité de la demande ou du nombre de demandes. Dans ce cas, l'Autorité publique en informe l'intéressé dans un délai d'un mois à compter de la réception de la demande.

En l'absence de réponse à l'Autorité publique dans les délais prescrits, la demande est réputée avoir été rejetée.

Article B.I.22.
Renvoi vers l'Autorité publique compétente

Lorsque la demande est adressée à une Autorité publique qui n'est pas compétente pour apporter les corrections, celle-ci en informe immédiatement le demandeur et lui communique la dénomination et l'adresse de l'Autorité qui, selon ses informations, est compétente pour le faire.

TITRE 5
Dispositions finales

Article B.I.23.
Obligations de publicité plus étendues

Le présent livre ne préjudicie pas aux dispositions législatives qui prévoient une publicité plus étendue de l'administration.

Article B.I.24.
Qualité des informations environnementales

Les Autorités publiques veillent, dans la mesure où cela leur est possible, à ce que toute information environnementale compilée par elles ou pour leur compte soit à jour, précise et comparable.

Sur demande, les Autorités publiques répondent aux demandes d'informations environnementales en indiquant, le cas échéant, l'endroit où les indications concernant les procédés de mesure, y compris les procédés d'analyse, de prélèvement et de préparation des échantillons, utilisés pour la compilation des informations, peuvent être trouvées ou en faisant référence à une procédure standardisée.

LIVRE B.II.
La Commission d'accès aux documents administratifs et aux données (CADADo)

TITRE 1
Dispositions générales

Article B.II.1.
Transposition partielle

Le présent livre transpose partiellement la Directive 2003/4/CE du Parlement européen et du Conseil du 28 janvier 2003 concernant l'accès du public à l'information en matière d'environnement et abrogeant la Directive 90/313/CEE du Conseil.

Article B.II.2.
Calcul des délais

Les délais prévus dans le présent livre commencent à courir le jour qui suit celui qui constitue le point de départ du délai. Le jour de l'échéance est compris dans le délai. Si ce jour n'est pas un jour ouvrable, le jour de l'échéance est reporté au jour ouvrable qui suit.

TITRE 2
Composition et organisation de la Commission

Article B.II.3.
Compétences de la Commission et indépendance

§ 1er. – La Commission connaît des recours dirigés contre :

1° les manquements aux obligations de publicité active prévues au titre 2 du livre B.I, à l'exception de l'obligation, visée à l'article B.I.15, d'établir un rapport détaillé sur l'état de l'environnement et une note de synthèse;

2° les rejets des demandes d'accès aux documents administratifs visées au titre 3 du livre B.I;

3° les refus de rectification visés au titre 4 du livre B.I;

4° les décisions ou les conditions fixées par une Autorité publique visée à l'article C.I.1. relatives au partage administratif ou à la réutilisation visés au livre C.IV.

§ 2. – La Commission peut, d'initiative, émettre des avis sur l'application générale du livre B.I. portant sur la publicité administrative du livre B.II l'instituant et du livre C.IV en matière de partage administratif et de réutilisation, ainsi que sur les arrêtés d'exécution de ces livres. Elle peut soumettre au Parlement ou au Gouvernement de la Région de Bruxelles-Capitale,

à l'Assemblée ou au Collège réuni de la COCOM, à l'Assemblée ou au Collège de la COCOF, des propositions relatives à leur application et leur révision éventuelle.

La Commission peut également remettre des avis à la demande d'une Autorité publique à propos d'une question générale, en dehors de toute demande particulière, relative à l'application du livre B.I. portant sur la publicité administrative, du présent livre et du livre C.IV en matière de partage administratif et de réutilisation, ainsi que sur les arrêtés d'exécution de ces livres.

La Commission est consultée sur tout projet pouvant avoir une influence sur les compétences ou le fonctionnement de la Commission.

§ 3. – La Commission exerce ses missions en toute indépendance et dans le respect de l'impartialité. Elle ne peut recevoir aucune instruction dans l'exercice de ses missions.

Ses membres ne peuvent faire l'objet d'une évaluation ou d'une procédure disciplinaire sur la base des éléments de fait ou de droit motivant une décision de la Commission adoptée conformément aux dispositions du présent livre.

Article B.II.4.
Composition générale

§ 1er. – La Commission est composée d'un secrétariat général et de trois chambres : une chambre relative à l'accès aux documents administratif et à l'information environnementale, une chambre relative au partage administratif de données et une chambre relative à la réutilisation.

§ 2. – Le secrétariat général est composé d'un secrétaire principal et d'un secrétaire adjoint qui s'occupent de la gestion administrative et organisationnelle de la Commission. Les secrétaires de la Commission sont désignés par arrêté conjoint du Gouvernement, du Collège réuni et du Collège parmi les membres du personnel des Autorités publiques. Ils doivent être titulaires d'un diplôme universitaire en droit de deuxième cycle et exercer leur mission à temps plein.

§ 3. – La Commission est composée de treize membres, parmi lesquels est désigné un président qui est membre du Conseil d'État ou de son auditorat, ou membre de la Cour Constitutionnelle ou magistrat de l'ordre judiciaire. Le président dirige les débats et signe au nom de la Commission toute correspondance, toutes les recommandations et tous les avis.

Par dérogation à l'alinéa 1er, la Commission peut être composée de moins de treize membres si certains membres siègent au sein de deux chambres en application de l'article B.II.5, § 4.

Article B.II.5.
Composition des chambres

§ 1er. – La chambre relative à l'accès aux documents administratifs et à l'information environnementale est composée du Président de la Commission, de huit autres membres et d'un membre du secrétariat général.

Quatre des membres de la chambre, en dehors du Président, sont désignés parmi les membres du personnel des Autorités publiques visées à l'article B.I.2. Les membres désignés en cette qualité doivent être titulaires d'un diplôme universitaire de deuxième cycle en droit et justifier d'une expérience suffisante en matière de publicité de l'administration et d'accès à l'information environnementale.

Quatre des membres de la chambre, en dehors du Président, sont désignés en raison de leur connaissance approfondie dans le domaine de la publicité de l'administration et de l'information environnementale. Ils doivent être titulaires d'un diplôme universitaire de deuxième cycle en droit et ne peuvent pas être fonctionnaires au sein d'une Autorité publique visées à l'article B.I.2 ou de toute autre autorité administrative.

§ 2. – La chambre relative au partage administratif des données est composée du Président de la Commission, de deux autres membres, et d'un membre du secrétariat général.

Les deux membres de la chambre, en dehors du Président, sont désignés en raison de leur connaissance approfondie dans le domaine de la gestion des données dans le secteur public. Ils doivent être titulaires d'un diplôme universitaire de deuxième cycle et justifier d'une connaissance et d'une expérience suffisantes en matière de gestion des données dans le secteur public. La chambre doit être composée au minimum d'une personne titulaire d'un diplôme universitaire de deuxième cycle en droit et d'une personne démontrant une compétence technique dans le secteur des nouvelles technologies, les deux compétences pouvant le cas échéant être cumulées sur une même tête.

§ 3. – La chambre relative à la réutilisation est composée du Président de la Commission, de deux autres membres, et d'un membre du secrétariat général.

Les deux membres de la chambre, en dehors du Président, sont désignés en raison de leur connais-

sance approfondie dans le domaine de la gestion des données dans le secteur public et du partage de données et de documents entre le secteur public et le secteur privé. Ils doivent être titulaires d'un diplôme universitaire de deuxième cycle et justifier d'une connaissance et d'une expérience suffisantes en matière de gestion et de partage des données dans le secteur public. La chambre doit être composée au minimum d'une personne titulaire d'un diplôme universitaire de deuxième cycle en droit et d'une personne démontrant une compétence technique dans le secteur des nouvelles technologies, les deux compétences pouvant le cas échéant être cumulées sur une même tête.

§ 4. – À l'exception du président, un membre de la Commission déjà nommé pour siéger dans l'une des chambres de la Commission, conformément à l'article B.II.7, § 1er, peut le cas échéant être désigné dans le cadre d'un second mandat, également conformément à l'article B.II.7, § 1er, afin de siéger dans une autre chambre, pour autant qu'il soit désigné conformément aux conditions fixées aux paragraphes 1, 2 ou 3 du présent article selon la chambre dans laquelle le membre exerce son second mandat.

§ 5. – Le Président et le secrétariat sont communs aux trois chambres. Le secrétaire n'a pas voix délibérative.

§ 6. – Il est désigné pour chacun des membres un suppléant aux mêmes conditions que les membres effectifs.

En cas d'empêchement ou d'absence de longue durée d'un membre, celui-ci est remplacé par son suppléant.

Le suppléant achève le mandat de son prédécesseur au cas où ce dernier démissionne ou cesse pour une raison quelconque de faire partie de la Commission.

§ 7. – Toutes chambres confondues, la Commission ne comporte pas plus des deux tiers des membres du même sexe.

§ 8. – Toutes chambres confondues, la Commission ne comporte pas plus des deux tiers des membres du même rôle linguistique, celle-ci étant vérifiée par la langue dans laquelle les diplômes requis pour leur fonction ont été obtenus.

§ 9. – Le Gouvernement, le Collège réuni et le Collège peuvent déterminer conjointement les règles complémentaires relatives à la composition de la Commission.

Article B.II.6.
Experts

Un minimum de trois experts sur des questions spécialisées en matière de partage administratif et de réutilisation sont désignés auprès de la Commission, sur la base d'une liste proposée par le Président et les autres membres de la Commission, par arrêté conjoint du Gouvernement, du Collège réuni et du Collège. La désignation de chaque expert a une durée de 5 ans et peut être renouvelée une fois.

Les experts justifient d'une expérience de plus de cinq ans dans les questions relatives au partage administratif et à la réutilisation impliquant des Autorités publiques visées à l'article C.I.1. Ils justifient également de plusieurs publications académiques sur ces questions.

Les experts sont désignés par le Président pour des dossiers ou des missions spécifiques et ne siègent que pour les nécessités de ces dossiers ou de ces missions. Ils ne possèdent pas de voix délibérative et ne peuvent émettre que des avis sur les dossiers et missions pour lesquels ils sont désignés.

Les paragraphes 2 et 3 de l'article B.II.7 s'appliquent également aux experts.

Article B.II.7.
Mandats des membres

§ 1er. – Les membres de la Commission sont désignés conjointement par le Gouvernement, le Collège réuni et le Collège pour un mandat de 5 ans renouvelable pour siéger dans l'une des chambres de la Commission.

§ 2. – À la demande du Président ou de tout membre de la Commission, et après l'audition de la personne visée, le Gouvernement, le Collège réuni et le Collège peuvent conjointement mettre fin anticipativement au mandat du Président et de tout autre membre de la Commission dans les cas suivants :

1° S'il ne remplit plus les conditions de désignation au mandat en question ou manque à ses devoirs tels que définis dans le présent livre et dans le règlement d'ordre intérieur visé à l'article B.II.9, § 3;

2° S'il porte atteinte à la dignité de sa fonction;

3° S'il ne respecte pas le caractère confidentiel des délibérations ou diffuse des documents confidentiels auxquels il a accès dans l'exercice de son mandat;

4° S'il participe aux délibérations de la Commission alors qu'il se trouve dans une situation de conflit d'intérêts visées au troisième paragraphe.

§ 3. – Il est interdit aux membres de la Commission et d'être présents à une délibération concernant des dossiers et missions dans lesquelles ils ont un intérêt personnel et direct ou dans lesquelles leurs parents ou alliés jusqu'au quatrième degré ont un intérêt personnel et direct.

Il est en outre interdit aux membres visés à l'article B.II.5, § 1er, alinéa 2, d'être présents à une délibération lorsque l'affaire concerne une autorité administrative dont il relève.

Article B.II.8.
Rémunération

§ 1er. – Les membres de la Commission et les experts sont rémunérés par recours visé à l'article B.II.3, § 1er, ou demande d'avis traité. Chaque dossier traité donne droit à un jeton.

Le rapporteur désigné pour chaque dossier reçoit un jeton d'un montant supérieur.

§ 2. – Le Gouvernement, le Collège réuni et le Collège fixent conjointement les modalités et le montant des jetons en faveur des membres, experts et rapporteurs.

Article B.II.9.
Fonctionnement

§ 1er. – Le Président dirige les débats au sein de chaque chambre. Il désigne pour chaque dossier, un membre rapporteur et le cas échéant, un ou plusieurs experts. Il fixe, en concertation avec le secrétaire, la date des réunions, leurs modalités, dont leur tenue en présentiel ou distanciel, et en établit l'ordre du jour.

§ 2. – La Commission se réunit, toutes les chambres réunies, au moins deux fois par an. Le secrétaire envoie au Président, à chaque membre et, le cas échéant, aux experts, pour chacune des réunions de la Commission, une convocation contenant l'ordre du jour, accompagnée de la documentation nécessaire et les modalités de la tenue de la réunion.

Chaque convocation est envoyée au moins trois jours ouvrables avant la date de la réunion.

§ 3. – La Commission doit établir un Règlement d'ordre intérieur interne dans les trois mois de son entrée en fonction, concernant également le fonctionnement des chambres de la Commission.

§ 4. – Le Gouvernement, le Collège réuni et le Collège déterminent conjointement les règles complémentaires relatives au fonctionnement de la Commission.

TITRE 3
Les demandes d'avis

Article B.II.10.
Modalités des demandes d'avis

Conformément à l'article B.II.3, § 2, les demandes d'avis des Autorités publiques sont soit envoyées via le formulaire en ligne sur le site internet de la Commission, soit adressées au secrétariat de la Commission par courrier électronique. Le secrétariat en accuse réception en toute hypothèse.

Article B.II.11.
Information des membres

Chaque fois qu'une demande d'avis est introduite auprès de la Commission, le Secrétariat de la Commission en informe immédiatement l'ensemble des membres de la Chambre concernée par voie électronique.

Article B.II.12.
Délibération de la Commission

§ 1er. – Le secrétariat désigne un rapporteur qui rédige une proposition d'avis. Cette proposition est ensuite soumise à l'approbation de la Chambre concernée.

§ 2. – Chaque chambre de la Commission ne peut délibérer valablement quant à la formulation de l'avis que si le Président ainsi qu'au minimum deux membres de la Chambre concernée sont présents.

Les avis sont adoptés à la majorité simple des suffrages exprimés. En cas de parité des voix, celle du Président est prépondérante.

Article B.II.13.
Délai dans lequel la Commission statue

La Commission statue sur la demande d'avis dans les 60 jours de la réception de la demande d'avis visée à l'article B.II.10.

Article B.II.14.
Secrétariat

§ 1er. – Le secrétariat est chargé de la conservation des documents et des archives de la Commission.

§ 2. – Le secrétariat s'assure de la communication des avis à l'Autorité publique à l'origine de la demande d'avis, ainsi que la publication de cet avis.

Article B.II.15.
Publication de l'avis

La Commission publie sur son site internet les avis visés à l'article B.II.3, § 2, rendus dans un délai de 20 jours ouvrables à compter de la date à laquelle ils sont adoptés.

Sauf consentement préalable de toute personne concernée par des données à caractère personnel contenues dans un avis de la Commission, la Commission opère une anonymisation des avis qu'elle remet avant leur publication. Elle omet également toute information qu'elle jugera confidentielle.

TITRE 4
Les recours

Article B.II.16.
Délai pour introduire un recours

§ 1er. – Sous peine d'irrecevabilité, la Commission est saisie d'un recours visé à l'article B.II.3, § 1er, dans les 30 jours de la décision de l'Autorité publique ou dans les 30 jours à compter de la prise de connaissance du manquement visé à l'article B.II.3, § 1er, 1°.

§ 2. – Lorsque le requérant sollicite l'examen de son recours en urgence, le délai pour introduire son recours est réduit à 5 jours ouvrables.

§ 3. – Le point de départ des délais est le jour de la prise de connaissance de la décision expresse de l'Autorité publique, ou, à défaut d'une telle décision, le jour de l'expiration du délai durant lequel l'Autorité publique devait se prononcer sur la demande, ou encore la date de la prise de connaissance du manquement visé à l'article B.II.3, § 1er, 1°.

§ 4. – Les délais visés au paragraphe 1er sont interrompus par l'introduction d'une réclamation devant le médiateur bruxellois. Un nouveau délai commence à courir à dater soit de la réception par le requérant de la notification du médiateur l'informant de la fin de son intervention, soit à l'expiration d'un délai de 4 mois à compter de l'introduction de la réclamation devant le médiateur, si la notification n'est pas intervenue plus tôt.

Article B.II.17.
Modalités d'introduction du recours

Les recours sont introduits par une requête adressée au secrétariat de la Commission par lettre recommandée ou par tout autre moyen conférant date certaine à l'envoi.

Article B.II.18.
Formalités des recours

§ 1er. – Sous peine d'irrecevabilité, le recours est introduit par une requête qui :

1° est signée par le requérant.

Les personnes morales, outre la signature de leur fondé de pouvoir, mentionnent dans leur requête et leur numéro d'inscription à la banque-carrefour des entreprises visée à l'article III.15 du Code de droit économique ou fournissent une copie de leurs statuts lorsqu'il s'agit d'une personne morale de droit étranger.

En cas d'envoi de la requête par courriel, celui-ci est considéré comme valablement signé lorsque le requérant, ou le fondé de pouvoir de la personne morale requérante, joint à son courriel une photocopie, une photographie ou un scan d'un document d'identité. Lorsque la requête est signée par un avocat ou qu'elle est transmise par courriel par un avocat, le requérant ne doit pas y joindre les documents visés par les alinéas précédents;

2° précise le nom et l'adresse du requérant;

3° est adressée à la Commission de façon à lui assurer une date d'envoi certaine;

4° comprend le cas échéant une motivation de l'urgence invoquée conformément à l'article B.II.16, § 2.

§ 2. – Dans le cas des recours visés à l'article B. II.3, § 1er, 2° à 4°, le recours contient, sous peine d'irrecevabilité, une copie de la demande d'accès, de rectification, de partage administratif ou de réutilisation, ou le cas échéant des conditions et des protocoles d'accord de partage administratif et de réutilisation et, si le refus est exprès, une copie de la décision de refus.

§ 3. – Quand un recours est irrecevable pour l'un des motifs visés aux articles B.II.16 à B.II.18, la Com-

mission doit le faire savoir au requérant dans les plus brefs délais, pour autant que celui-ci soit identifié dans le recours.

§ 4. – Lorsqu'elle est saisie d'un recours, la Commission le notifie sans délai à l'Autorité publique concernée et adresse une demande d'obtention, si elle l'estime nécessaire, des documents visés à l'article B.II.19., § 1er, alinéa 2.

Article B.II.19.
Délais d'obtention par la Commission des documents, informations environnementales et données, ou note en justifiant le refus d'accès

§ 1er. – La Commission dispose de pouvoirs d'investigation et de contrainte.

À la demande de la Commission, l'Autorité publique est tenue de lui communiquer, dans les sept jours ouvrables à compter de la réception de la notification visée à l'article B.II.18, § 4, selon l'hypothèse :

1° le document ou l'information environnementale dont l'accès ou la rectification est sollicité, ou,

2° les données visées par le partage administratif, ou,

3° les données visées par la réutilisation demandée.

L'Autorité publique peut adresser à la Commission une note justifiant son refus d'accéder à la demande initiale dans les sept jours ouvrables à compter de la réception de la notification visée à l'article B.II.18, § 4. À défaut d'être transmise dans le délai de sept jours ouvrables, la Commission n'est pas tenue de prendre en considération la note justifiant ledit refus.

Pour ce qui concerne les Autorités publiques visées à l'article C.I.1, la communication des documents visés à l'alinéa 2 correspond à un partage administratif.

Par dérogation à l'alinéa 2, lorsque l'Autorité publique considère que la demande était manifestement abusive ou qu'elle était formulée de façon manifestement trop vague, elle n'est pas tenue de transmettre à la Commission les documents visés à l'alinéa 2. Lorsque l'Autorité n'a pas répondu à la demande initiale, si elle considère celle-ci manifestement abusive ou manifestement trop vague, elle en informe la Commission par une décision motivée dans les sept jours ouvrables à compter de la réception de la notification visée à l'article B.II.18, § 4.

Dans l'hypothèse où le Président de la Commission ou le membre qu'il désigne reconnaît l'urgence invoquée par le requérant, le délai de sept jours visé aux alinéas 2, 3 et 4 est réduit à deux jours ouvrables.

Lorsque l'Autorité publique ne transmet pas à la Commission, alors que celle-ci en a fait la demande, les documents visés à l'alinéa 2 dans les délais établis aux alinéas 2, 3, 5 et 6, la Commission en fait mention dans le rapport annuel visé à l'article B.II.25.

§ 2. – En toute hypothèse, le Président de la Commission ou le membre qu'il désigne peut se rendre sur place pour prendre connaissance et copie des documents visés au paragraphe 1er, alinéa 2 concernés par le recours et de tout autre document nécessaire au traitement de ce recours, en ce compris en faisant appel à la force publique.

§ 3. – Si, malgré les pouvoirs de la Commission visés aux paragraphes 1er et 2, après en avoir fait la demande, la Commission n'obtient pas les documents visés à l'alinéa 2, la Commission, moyennant le respect des exceptions prévues à l'article B.I.17 et les conditions fixées par le livre C.IV, peut faire usage de son pouvoir visé à l'article B.II.23.

Article B.II.20.
Délai maximal pour statuer sur le recours

§ 1er. – À partir du moment où elle dispose des documents demandés conformément à l'article B.II.19, § 1er, alinéa 2, la Commission en informe le requérant. Elle statue sur le recours dans les 60 jours de la réception documents visés à l'article B.II.19, § 1er, alinéa 2.

Lorsque l'Autorité publique considère la demande comme étant manifestement abusive ou manifestement trop vague conformément à l'article B.II.19, § 1er, alinéa 5, la Commission statue dans les 60 jours de la réception du recours.

Toutefois, si la Commission considère pour sa part que la demande n'est ni manifestement abusive ni trop vague et estime nécessaire de disposer des documents visés à l'article B.II.19, § 1er, alinéa 2, le délai de 60 jours commence à courir conformément à l'alinéa 1er.

Si les délais prévus aux alinéas 1 à 3 ne sont pas respectés, le recours est censé être rejeté.

§ 2. – Le délai de 60 jours visé au paragraphe 1er, alinéas 1er à 3, est suspendu :

1° lorsque la Commission a sollicité l'avis de l'Autorité de protection des données, jusqu'à la réception de cet avis;

2° à compter du jour où la Commission reçoit du médiateur bruxellois l'information selon laquelle celui-ci est saisi d'une réclamation dont l'objet

est identique à celui du recours introduit devant la Commission. Le médiateur notifie au même moment à la Commission et au requérant la fin de son intervention et les éventuelles recommandations qu'il a formulées. Dans ce cas, il appartient au requérant de notifier à la Commission s'il maintient son recours au terme de l'intervention du médiateur. En l'absence de notification du maintien de son recours par le requérant dans un délai de 15 jours à compter de la réception de la notification du médiateur, le requérant est réputé se désister de son recours.

§ 3. – Lorsque l'urgence invoquée par le requérant dans son recours est reconnue par le Président de la Commission ou par le membre qu'il désigne, la Commission statue sur le recours dans un délai de 10 jours ouvrables à compter de la réception du recours. En cas de rejet de l'urgence par le Président de la Commission ou par le membre désigné par le Président, le recours est examiné par la Commission dans le délai ordinaire déterminé au paragraphe 1er.

L'urgence dûment motivée par le requérant est celle qui rend manifestement inapproprié aux faits de la cause le respect du délai ordinaire établi par le paragraphe 1er, en raison des inconvénients graves susceptibles d'affecter la situation du requérant si le délai précité devait être observé.

§ 4. – Le Gouvernement, le Collège réuni et le Collège peuvent arrêter conjointement des règles de procédure devant la Commission complémentaires à celles figurant dans le présent livre.

Article B.II.21.
Délibération de la Commission

La Commission ne peut délibérer valablement que si son Président ainsi qu'au minimum deux membres de la Chambre concernée sont présents.

Les décisions sont prises à la majorité simple des suffrages exprimés. En cas de parité des voix, celle du Président est prépondérante.

Article B.II.22.
Notification de la décision de la Commission

La Commission notifie dans les plus brefs délais sa décision par écrit aux parties concernées.

Article B.II.23.
Pouvoirs de réformation de la Commission

§ 1er. – La Commission dispose d'un pouvoir de réformation et peut elle-même accorder l'accès aux documents administratifs, aux informations environnementales ainsi que leur rectification; elle peut elle-même accorder ou de refuser l'accès aux données visées par un partage administratif ou une réutilisation aux conditions qu'elle fixe.

Dans ce cas, la Commission donne l'injonction à l'Autorité publique de se conformer à sa décision et de l'exécuter dans le délai qu'elle établit, lequel ne peut excéder 30 jours.

§ 2. – À l'expiration du délai de 30 jours visé au premier paragraphe, si l'Autorité publique n'a pas respecté la décision de la Commission dans le délai imparti, cette dernière communique elle-même, lorsqu'elle en dispose, la copie du document administratif, l'information environnementale ou les données ou les documents visés par le partage administratif ou la réutilisation. Dans cette hypothèse, la Commission avertit l'Autorité publique au minimum 15 jours avant la communication faite au requérant.

§ 3. – Lorsque la Commission constate le défaut pour une Autorité publique visée à l'article B.I.2. de satisfaire à une obligation visée au titre 2 du livre B.I, la Commission lui donne l'injonction de satisfaire sans délai à cette obligation.

Article B.II.24.
Publication des décisions, avis et propositions

La Commission publie sur son site internet visé à l'article B.II.26, dans les 20 jours ouvrables de leur adoption, les décisions, avis et propositions qu'elle adopte.

Sauf consentement préalable du requérant en vue d'une publication nominative, la Commission opère une anonymisation des décisions avant leur publication. Elle omet également toute information qu'elle jugera confidentielle.

TITRE 5
Rapport annuel et site web

Article B.II.25.
Rapport annuel

§ 1er. – La Commission rédige un rapport annuel.

Ce rapport comprend au moins :

1° le nombre de recours introduits et le nombre de décisions adoptées;

2° le nombre de demandes d'avis introduits et le nombre d'avis adoptés;

3° le délai moyen de traitement d'un recours et d'un avis;

4° le nombre de réunions par chambre ou en plénière;

5° une synthèse des principales problématiques auxquelles la Commission a été confrontée, tant sur le fond des affaires que sur le fonctionnement de la Commission elle-même;

6° un budget prévisionnel pour les deux années à venir et une justification de l'utilisation de la dotation reçue pour l'année faisant l'objet du rapport;

7° une liste répertoriant les cas dans lesquels les délais de communication des documents ou des données demandés et faisant l'objet des recours n'ont pas été respectés. Cette liste mentionne l'Autorité publique concernée et le nombre de dépassements des délais.

§ 2. – Le rapport annuel est présenté par le Président de la Commission ou le membre qu'il désigne au Parlement de la Région de Bruxelles-Capitale, au Parlement francophone bruxellois et à l'Assemblée réunie au plus tard le 31 mars de l'année qui suit celle à laquelle il se rapporte.

§ 3. – Le rapport annuel est publié sur le site internet de la Commission.

§ 4. – La Commission adresse au Gouvernement, au Collège réuni et au Collège un bilan sur la pertinence des modifications introduites dans les 2 ans après l'entrée en vigueur du présent Livre.

Article B.II.26.
Site Web

§ 1er. – La Commission doit tenir un site web à destination du public contenant au minimum les informations suivantes :

1° une information sur les missions de la Commission, son fonctionnement et les bases légales qui fondent ses interventions;

2° une information sur les membres et les experts de la Commission;

3° les avis et décisions sur recours qui ont été rendus.

TITRE 6
Dotation

Article B.II.27.
Dotation

§ 1er. – Une dotation est inscrite au budget général de la Région de Bruxelles-Capitale, de la COCOM, de la COCOF pour financer le fonctionnement de la Commission et lui permettre d'exécuter les missions qui lui sont confiées par le présent Code.

§ 2. – Le Gouvernement, le Collège réuni et le Collège déterminent conjointement les modalités relatives à la dotation.

PARTIE C
GOUVERNANCE DE LA DONNÉE

LIVRE C.I
Champ d'application ratione personae et dispositions générales

Article C.I.1.
Champ d'application ratione personae

La partie C du présent Code s'applique aux Autorités publiques visées à l'article A. I.3., 1), a), b), c), h), i).

Article C.I.2.
Dispositions générales

Dans le cadre du présent Code, chaque Autorité publique met en œuvre des traitements de données à caractère personnel, sur la base des missions d'intérêt public dont elle est investie et des obligations légales qui lui incombent, pour les finalités suivantes :

1. exécution de sa mission de service public ou de ses obligations d'intérêt général;

2. amélioration et évaluation des politiques publiques auxquelles elle participe;

3. facilitation de l'accès des usagers à leurs droits;

4. partage de données entre Autorités publiques;

5. gestion de ses relations administratives et contractuelles;

6. recherche, développement de ses activités dans le cadre de ses missions d'intérêt public et formation interne;

7. contrôle interne du respect des dispositions légales ou réglementaires.

LIVRE C.II
Principes généraux

TITRE 1
Les principes directeurs

Article C.II.1.
Les quatre principes directeurs

Dans le cadre de l'exercice de leurs missions de services publics ou d'intérêt général, lorsqu'elles traitent des données, les Autorités publiques doivent respecter les principes directeurs suivants :

1° le principe de protection et de sécurisation;

2° le principe de partage;

3° le principe de transparence;

4° le principe de qualité.

Les Autorités publiques garantissent par toute mesure technique et organisationnelle disponible, dès le début du cycle de vie de la donnée, le plus haut niveau possible de respect des principes applicables. Dans ce cadre, les Autorités publiques tiennent compte de la réglementation particulière applicable aux données, de l'état des connaissances, des coûts de mise en œuvre ainsi que de la nature, de la portée, du contexte, des finalités du traitement des données et des risques qui y sont afférents.

Article C.II.2.
Principe de protection et de sécurisation des données

§ 1er. – Les Autorités publiques protègent les droits des tiers sur les données qu'elles détiennent.

§ 2. – Les Autorités publiques sécurisent les données, et plus spécifiquement les données protégées, en toute circonstance, à des fins de qualité et de respect des droits des tiers.

§ 3. – Le principe de protection et de sécurisation des données appelle une application différenciée en fonction des catégories particulières de données visées à l'article C.III.10.

Article C.II.3.
Principe de partage

§ 1er. – Les Autorités publiques autorisent, conformément aux dispositions du présent Code, le partage de leurs documents et de leurs données publiques.

§ 2. – Les Autorités publiques organisent, le cas échéant, dans le respect des conditions légales et réglementaires applicables, le partage administratif de données entre elles afin, non seulement, d'améliorer l'exercice de leurs missions de services publics et de leurs missions d'intérêt général, mais également, d'alléger si possible le cas échéant la charge administrative des citoyens.

§ 3. – Les Autorités publiques utilisent les sources authentiques afin de collecter les données nécessaires à l'exécution des missions d'intérêt public ou des obligations légales qui leur incombent.

Les Autorités publiques reçoivent les données issues de sources authentiques via le Centre d'intégration de la Plateforme bruxelloise de la donnée conformément à la section 2, du chapitre 2, du titre 2, du livre C.IV.

§ 4. – Les Autorités publiques permettent également la réutilisation de leurs données publiques conformément aux conditions fixées au titre 3 du livre CIV.

Article C.II.4.
Principe de transparence

§ 1er. – Les Autorités publiques gèrent les données qu'elles détiennent dans le cadre de leurs missions de services publics et leurs missions d'intérêt général conformément à un impératif de transparence.

§ 2. – En vue de favoriser les réutilisations, les Autorités publiques mettent à disposition leurs données ouvertes, en assurant le plus haut degré d'ouverture. À défaut, si cela s'avère impossible, les Autorités publiques adoptent des outils afin de permettre d'extraire et d'exploiter librement tout ou partie des bases de données contenant de telles données.

§ 3. – Le principe de documentation participe à l'application du principe de transparence. Conformément au principe de documentation, les Autorités publiques assurent une transparence active par la mise à disposition d'office de la documentation relative aux processus qu'elles mettent en place en vertu des obligations imposées par le Code, sans préjudice des dispositions assurant la protection de certaines données.

Les Autorités publiques assurent une transparence passive en fournissant sur demande toute fonction de support et d'information portant sur la gouvernance des données numériques, nécessaire à leurs propres services et aux tiers, dans les limites de l'article B.I.1.8.

Article C.II.5.
Principe de qualité

Les Autorités publiques doivent garantir le niveau le plus élevé de qualité des données proportionnellement aux usages qui en sont faits.

La qualité des données se définit sous l'angle de différentes dimensions complémentaires, à savoir notamment :

1° Consistance;

2° Exactitude;

3° Exhaustivité;

4° Vérifiabilité;

5° Validité;

6° Unicité;

7° Intégrité;

8° Ponctualité.

Les Autorités publiques sont en mesure d'évaluer, à tout moment, la qualité des données qu'elles détiennent.

TITRE 2
Les objectifs stratégiques

Article C.II.6.
Six objectifs stratégiques

Dans le cadre de leurs missions, les Autorités publiques appliquent une gouvernance des données qui :

1° met les données au centre de leur action;

2° définit les rôles et responsabilités des parties prenantes;

3° se base sur des standards communs;

4° adopte une gouvernance évolutive;

5° favorise l'éducation numérique de toutes les parties prenantes;

6° exploite les données de manière éthique, efficiente et responsable.

Article C.II.7.
Approche centrée sur la donnée

Les Autorités publiques adoptent des processus qui placent les données au centre de la gestion de leurs obligations de services publics et de leurs obligations d'intérêt général, de même que de leur gouvernance. Les données des Autorités publiques sont assimilées à des actifs à part entière.

Article C.II.8.
Définition des rôles et responsabilités

Les Autorités publiques désignent en leur sein les organes, services ou personnes responsables de la gestion des données, conformément aux qualifications décrites notamment au chapitre 2 du titre 2 du livre C.III.

Article C.II.9.
Adoption de standards communs

Les Autorités publiques déploient des solutions qui privilégient les standards communs.

Article C.II.10.
Gouvernance évolutive

Les Autorités publiques adoptent un modèle de gouvernance qui permet de s'adapter de manière continue aux évolutions techniques et réglementaires.

Article C.II.11.
Éducation des parties prenantes

Les Autorités publiques favorisent la culture de la donnée, notamment par la mobilisation, l'information, la sensibilisation et la formation de toutes les parties prenantes.

Article C.II.12.
Exploitation éthique, efficiente et responsable

Les Autorités publiques exploitent les données qu'elles détiennent de manière éthique, efficiente et responsable tout au long du cycle de vie de la donnée, de la collecte au stockage et à l'archivage.

TITRE 3
Les objectifs opérationnels

Article C.II.13.
Huit objectifs opérationnels

Dans le cadre de leurs missions, les Autorités publiques s'engagent à :

1° valoriser leurs données, le cas échéant en fonction de leurs priorités en matière de gouvernance de la donnée;

2° identifier le ou les régime(s) juridique(s) applicable(s) à chaque donnée;

3° respecter la confidentialité des données protégées;

4° assurer l'interopérabilité des systèmes;

5° garantir la traçabilité et la réversibilité des données;

6° procéder à l'intégration des données;

7° générer les métadonnées et les données de références de leurs données;

8° contrôler les conditions relatives à l'hébergement des données.

Article C.II.14.
Valorisation des données

Les Autorités publiques identifient les données qu'elles détiennent et définissent une stratégie de valorisation à leur égard dans le cadre de leurs missions de services publics et de leurs missions d'intérêt général.

Plus particulièrement, les Autorités publiques identifient si les données qu'elles détiennent :

1° sont des données de forte valeur conformément à la liste établie conformément à l'article C.IV.30;

2° sont relatives aux espaces de données européens communs, dont la thématique relève de leurs compétences.

Article C.II.15.
Identification du ou des régime(s) juridique(s) applicable(s)

Les Autorités publiques identifient le ou les régimes juridiques applicables aux données qu'elles détiennent.

Les Autorités publiques tiennent compte de ces régimes juridiques dans les partenariats numériques visés à l'article C.III.2 dans lesquelles elles sont impliquées lorsqu'ils concernent tout ou une partie de la gestion des données.

Article C.II.16.
Respect de la confidentialité des données protégées

§ 1er. – Si nécessaire à l'aide d'un tiers de confiance, les Autorités publiques sont en mesure de procéder le cas échéant et en fonction des données concernées, à l'occultation, l'anonymisation ou la pseudonymisation des données lorsque cela s'avère pertinent et notamment en vue d'en permettre la réutilisation.

§ 2. – Tout processus d'anonymisation devra éliminer tout risque de réidentification. Les Autorités sont tenues d'identifier les informations pertinentes qui doivent être conservées et de supprimer les éléments d'identification directe.

Article C.II.17.
Interopérabilité

Les Autorités publiques prennent toutes les mesures nécessaires (organisationnelles, juridiques et techniques) pour assurer l'interopérabilité des données qu'elles détiennent et ce, dès la conception de leurs processus.

Les Autorités publiques recourent à des systèmes interopérables qui s'appuient, chaque fois que cela est possible, sur des standards reconnus au niveau national ou international.

Article C.II.18.
Traçabilité et réversibilité

Les Autorités publiques recourent, lorsque cela est pertinent et de manière proportionnée au regard de l'objectif poursuivi, à la traçabilité et à la réversibilité des données.

La traçabilité et la réversibilité ne s'appliquent que jusqu'au moment où l'anonymisation éventuelle des données est requise ou que les données ne peuvent plus être traitées ou doivent être détruites conformément à la législation ou la règlementation applicable.

Les Autorités publiques utilisent les outils informatiques permettant la traçabilité et la réversibilité des données tout en garantissant la protection de celles-ci.

Article C.II.19.
Intégration des données

Les Autorités publiques intègrent les données susceptibles de l'être.

Article C.II.20.
Génération et gestion des métadonnées et données de référence

Les Autorités publiques documentent les données qu'elles détiennent au moyen de métadonnées.

Les Autorités publiques identifient les données de référence et en favorisent l'usage.

Les Autorités publiques établissent des politiques de gestion des données de référence et des métadonnées qui permettent d'identifier les données qu'elles détiennent et de garantir, le cas échéant, le partage des données.

Article C.II.21.
Contrôle des conditions d'hébergement et de stockage des données

Les Autorités publiques contrôlent les conditions d'hébergement et de stockage des données qu'elles détiennent.

LIVRE C.III
Obligations de gouvernance des Autorités publiques

TITRE 1
Champ d'application ratione personae

Article C.III.1.
Champ d'application du présent livre par palier

Le Gouvernement, le Collège réuni et le Collège déterminent conjointement certaines catégories d'Autorités publiques en fonction de seuils numériques. À chaque seuil numérique correspond un palier numérique déterminant l'importance de l'activité numérique des Autorités publiques qui y sont regroupées.

Le premier palier est appelé à respecter l'ensemble des obligations du présent livre.

Le deuxième palier est soumis au :

– Titre 1 du présent livre;

– Titre 2 du présent livre;

– Titre 3 du présent livre à l'exception du chapitre 2;

– Titre 4 du présent livre.

Le troisième palier est soumis au :

– Titre 1 du présent livre;

– Titre 2 du présent livre;

– Chapitre 3 du titre 3 du présent livre;

– Article C.III.16, alinéas 1 et 2 du titre 4 du présent livre.

TITRE 2
Les partenariats numériques de données

CHAPITRE 1
Principe

Article C.III.2.
La notion de partenariat numérique de données aux fins de valorisation des données

§ 1er. – Afin d'identifier les ressources numériques dont elles disposent et qu'il leur appartient de valoriser, les Autorités publiques identifient les partenariats numériques de données dont elles sont parties.

Est un partenariat numérique de données toute initiative impliquant la valorisation ou le partage de données publiques et liant juridiquement ou administrativement, soit deux ou plusieurs entités au sein d'une même Autorité publique, soit deux ou plusieurs entités disposant de la personnalité juridique dont au moins une est une Autorité publique.

§ 2. – Lorsque le partenariat numérique de données est conclu entre au minimum une Autorité publique, d'une part, et une personne autre qu'une Autorité publique, d'autre part, il s'agit d'un partenariat numérique mixte de données.

§ 3. – Lorsque le partenariat de données n'est conclu qu'entre des Autorités publiques, ou entre différentes entités au sein d'une même Autorité publique, il s'agit d'un partenariat numérique public de données.

Article C.III.3.
Les partenariats mixtes de données

§ 1er. – Dans le cadre des partenariats numériques mixtes de données, les Autorités publiques s'assurent que :

1° l'autre partie gère les données publiques concernées par le partenariat conformément aux dispositions du présent livre et de ses arrêtés d'exécution;

2° l'autre partie soit transparente dans sa manière de traiter, d'analyser et d'utiliser les données, les impacts découlant d'éventuels traitements de données à caractère personnel devant être légitimes, clairement évalués et pris en compte.

3° chaque partie soit qualifiée conformément au chapitre 2 du présent livre et conformément au RGPD lorsque le partenariat implique un traitement de donnée à caractère personnel afin que chaque partie soit investie des responsabilités qui en découlent.

Les conditions visées à l'alinéa 1er sont organisées entre les parties dans le respect du principe de proportionnalité compte tenu de l'importance et de la nature des traitements et des données visées par le partenariat.

Les Autorités publiques exigent de leurs partenaires qu'ils mettent en place les moyens techniques et organisationnels appropriés afin d'être en mesure de vérifier à tout moment le respect des conditions imposées au premier alinéa à l'autre partie.

§ 2. – Les Autorités publiques mettent en œuvre les obligations décrites au paragraphe 1er notamment dans les partenariats qu'ils entretiennent avec :

1° Les prestataires de services d'intermédiation de données;

2° Les prestataires de services informatiques;

3° Les opérateurs de services de plateformes numériques;

4° Les prestataires de services informatiques de stockage;

5° Les organisations altruistes en matière de données reconnues et inscrites au « Registre d'organisations altruistes en matière de données » conformément à l'article 19.1 du Règlement sur la Gouvernance des données.

CHAPITRE 2
Qualification des parties à un partenariat numérique de données

Article C.III.4.
La qualification des parties

§ 1er. – Chaque partie dans le cadre d'un partenariat numérique de données est qualifiée conformément au présent titre.

Une même partie peut cumuler différentes qualifications.

§ 2. – Sans préjudice du présent chapitre, en toute hypothèse, les Autorités publiques s'assurent également de leur qualification en tant que responsables de traitement ou de sous-traitant et ce conformément à l'article 4, 7) et 8) du RGPD pour tout traitement de données à caractère personnel dans le cadre de l'exécution de leur mission d'intérêt public et des obligations du présent Code.

Article C.III.5.
Les détenteurs de données

Le détenteur de données est soit producteur de données, soit diffuseur de données.

Article C.III.6.
Les producteurs de données

§ 1er. – Est producteur la personne qui assure la création de données généralement à l'aide d'outils et de techniques informatiques.

§ 2. – Conformément à sa mission organique et sans préjudice des dispositions du présent code et du RGPD, une Autorité publique qui procède à l'intégration des données est considérée comme producteur des données intégrées.

§ 3. – Le producteur de données est responsable :

1° de la qualité des données, en ce compris notamment de la mise à jour des données;

2° de l'identification de l'ensemble des données qu'il détient, de la manière dont elles sont gérées, documentées, décrites, organisées et formatées sous forme de jeux de données, de données de contenu, de données de référence et de métadonnées;

3° de la définition des conditions de l'utilisation ou, éventuellement, des conditions de partage des données.

§ 4. – Sauf si le présent Code, une législation ou une réglementation particulière en dispose autrement, le producteur de données désigne le ou les diffuseurs de données pour chacune des données ou jeux de données qui peuvent être partagés.

§ 5. – Sauf si le présent Code, une législation ou une réglementation particulière en dispose autrement, les producteurs de données sont responsables du traitement des demandes formulées par les utilisateurs finaux ou le cas échéant, orientent les utilisateurs finaux vers le service compétent pour traiter leurs demandes.

Article C.III.7.
Les diffuseurs de données

§ 1er. – Est diffuseur la personne qui met des données à disposition des utilisateurs.

§ 2. – Le diffuseur de données est responsable de :

1° la publication des données;

2° la gestion de la qualité des données au sens du chapitre 1er du titre 4 du présent livre;

3° la sécurité et la protection des données au sens du chapitre 2 du titre 5 du présent livre;

4° la conservation et la récupération des données;

5° la mise en forme et la présentation des données;

6° la mise en place des mécanismes d'accès et de téléchargement des données;

7° des garanties de confidentialité et sécurité des données.

Le diffuseur de données garantit un niveau de performance et de disponibilité proportionnel à la nature des données et de l'objectif poursuivi.

§ 3. – Conformément au principe énoncé à l'article C.II.4, les diffuseurs doivent publier les données dans un format :

1° ouvert;

2° lisible par une machine;

3° accessible, traçable et réutilisable;

4° accompagné des métadonnées.

§ 4. – Dans l'hypothèse où la donnée sollicitée est disponible sous un format répondant aux exigences d'un format ouvert, le diffuseur n'est pas tenu de publier les données sous un format différent de celui qu'il utilise déjà pour satisfaire une demande particulière. Dans le cas contraire, le diffuseur devra procéder aux conversions nécessaires.

§ 5. – En application de l'article C.III.6, § 5, le diffuseur de données doit renvoyer les demandes formulées par les utilisateurs finaux vers le producteur de données, sauf si le présent Code, une législation ou une réglementation particulière en dispose autrement.

Article C.III.8.
Les gestionnaires de données

§ 1er. – Dans tout partenariat numérique de données, les parties définissent :

1° l'administrateur de base de données;

2° l'administrateur de sécurité informatique;

3° l'administrateur système;

4° l'administrateur réseau.

§ 2. – Selon le mode de partage des responsabilités entre les parties au partenariat, les administrateurs peuvent se trouver sous la responsabilité de l'une ou l'autre partie.

§ 3. – Les Autorités publiques qui dans le cadre d'un partenariat n'identifient pas les responsabilités visées à l'alinéa premier sont responsables des prestations informatiques relatives aux données qu'elles traitent.

CHAPITRE 3
La catégorisation des données

Article C.III.9.
La catégorisation des données

§ 1er. – Les données publiques d'un partenariat sont catégorisées au minimum conformément au présent titre.

Les catégories de données énoncées au présent titre constituent les identifiants minimums des métadonnées et des données de référence telles que visées à l'article C.III.17 afin d'être intégrées dans le Catalogue des données de la Plateforme bruxelloise de la donnée.

§ 2. – Chaque catégorie de ces données est régie par des politiques, ensembles de normes ou meilleures pratiques, et processus spécifiques.

§ 3. – Les catégories des données ne s'excluent pas mutuellement et les obligations légales et techniques qui leur sont associées peuvent leur être appliquées concomitamment.

Dans le cas où un jeu de données contiendrait des données relevant de catégories différentes, les Autorités publiques tiennent compte du cadre juridique applicable à chacune des catégories de données concernées ainsi que des mécanismes techniques qu'implique chacune des catégories de données.

Article C.III.10.
Typologie des catégories de données

§ 1er. – Les données appartiennent, en fonction de leur régime de propriété, à l'une ou plusieurs des catégories suivantes, qui déterminent les règles concernant leur utilisation :

1° données à caractère personnel;

2° données exclusives;

3° données publiques;

4° données à forte valeur;

5° données d'origine privée.

§ 2. – Les données appartiennent à l'une des catégories suivantes, en fonction du lien entre l'origine des données et le mode de production de la donnée :

1° données fournies librement;

2° données observées;

3° données dérivées et déduites;

4° données acquises.

§ 3. – Les données appartiennent à l'une des catégories suivantes, selon le niveau d'accès à accorder aux données et les possibilités de partages organisées :

1° données ouvertes;

2° données partageables;

3° données fermées.

§ 4. – Les données à caractère personnel appartiennent à l'une des catégories suivantes, selon qu'elles peuvent être rendues publiques ou non :

1° données à caractère personnel confidentielles;

2° données à caractère personnel non confidentielles;

§ 5. – Les données appartiennent à l'une des catégories suivantes, selon le risque de dommages potentiels liés aux traitements des données :

1° données à risques inexistants;

2° données à risques faibles;

3° données à risques importants.

La détermination du risque conformément à l'alinéa 1er permet la catégorisation de certaines données en tant que données sensibles ou en tant que données classifiées.

§ 6. – D'autres catégories de données peuvent être utilisées en complément des catégories visées par le présent article en fonction des usages des Autorités publiques et des autres parties.

TITRE 3
La valorisation des données détenues par les Autorités publiques

CHAPITRE 1
Disposition générale

Article C.III.11.
La valorisation des données

La valorisation des données détenues par les Autorités publiques vise à organiser la gestion des données en tant que sources de valeur et véritables actifs numériques.

La valorisation des données repose sur :

1° la déclaration de principes;

2° la valorisation des données d'usage;

3° le respect des droits des tiers sur les données protégées;

4° l'évaluation des risques.

CHAPITRE 2

La déclaration de principes

Article C.III.12.

La déclaration de principes

Les Autorités publiques adoptent une déclaration de principes qui établit et décrit :

1° le modèle opérationnel mis en place pour gérer les données;

2° les bases de données qu'elles détiennent et la manière dont les données qu'elles détiennent sont gérées, documentées, décrites, organisées et formatées sous la forme de jeux de données, de données de contenu, de données de référence et de métadonnées;

3° le cas échéant, la déclaration d'accessibilité visée à l'article 7 de l'ordonnance du 4 octobre 2018 relative à l'accessibilité des sites internet et des applications mobiles des organismes publics régionaux et des communes;

4° la manière dont l'Autorité publique compte atteindre l'objectif stratégique d'exploitation éthique, efficiente et responsable visé à l'article C.II.12;

5° en cas de recours à des traitements algorithmiques ou d'intelligence artificielle, une description de la manière dont ils sont utilisés dans l'accomplissement des missions de service public ou de missions d'intérêt général;

6° en cas d'application d'une redevance dans le cadre d'une réutilisation de données, conformément à l'article C.IV.25, les modalités de calcul et le montant effectif des redevances;

7° la manière dont sont gérés et documentés les accords d'exclusivité visés aux articles C.IV.29;

8° tout autre élément pertinent présentant une importance particulière au regard de la stratégie numérique mise en place par l'Autorité publique dans le cadre de ses missions.

La déclaration de principes est publiée sur le site de chaque Autorité publique ou disponible à première demande.

CHAPITRE 3

La valorisation des données d'usage

Article C.III.13.

Valorisation des données d'usage

§ 1er. – Les Autorités publiques collectent et valorisent les données d'usage en vue :

1° d'identifier des profils d'usage, repérer des modes d'engagement avec les contenus ou les habitudes d'utilisation;

2° d'améliorer la lisibilité et l'accès à leurs services;

3° d'informer d'autres usagers ou citoyens que les usagers ou citoyens identifiés au départ des données d'usage déjà récoltées;

4° d'améliorer la représentation des usagers de leurs services;

5° de protéger la vie privée des usagers ou citoyens en collectant les refus et les consentements en tant que donnée d'usage.

§ 2. – Les traitements des données d'usage comprenant des données à caractère personnel ont uniquement pour finalités d'améliorer la qualité des services, d'optimiser l'expérience utilisateur, d'adapter les offres de service en fonction des besoins des utilisateurs et de développer de nouvelles fonctionnalités ou politiques basées sur les interactions des utilisateurs. Tout partage de données d'usage vise à promouvoir l'amélioration des services publics ou à répondre à des objectifs de recherche pertinents.

§ 3. – Les usagers ou citoyens sont informés de la collecte des données d'usage à caractère personnel et ont la possibilité de refuser cette collecte, soit en totalité, soit en partie. Les Autorités publiques mettent à disposition la nature des données collectées, la finalité de cette collecte, et les droits des usagers ou citoyens en relation avec ces données dans leur politique de confidentialité.

§ 4. – Les données d'usage sont conservées pour une durée proportionnelle à leurs finalités qui ne peut excéder dix ans et sont protégées par des mesures de sécurité adaptées pour prévenir tout accès non autorisé, perte, altération ou divulgation.

Le Gouvernement, le Collège et le Collège réuni peuvent définir conjointement des durées de conservation inférieures au délai prévu à l'alinéa précédent.

CHAPITRE 4
Le respect des droits sur les données protégées

Article C.III.14.
Le respect des droits des tiers sur les données protégées

§ 1er. – Dans le cadre de la valorisation des données qu'elles détiennent, les Autorités publiques respectent les droits des tiers sur les données protégées.

§ 2. – Sans préjudice de l'article 6 du RGPD pour ce qui concerne les données à caractère personnel, les Autorités publiques recueillent les consentements et les autorisations nécessaires à la valorisation et au partage de données protégées de la part des titulaires de droits sur ces données.

Le cas échéant, et sans préjudice des dispositions d'autres réglementations applicables au traitement des données concernées, les Autorités publiques mettent en place un mécanisme de consentement ou d'autorisation dynamiques.

§ 3. – Dans le cadre de la valorisation des données qu'elles détiennent, les Autorités publiques respectent la confidentialité des données protégées.

Sauf disposition contraire applicable ou consentement des personnes concernées, les Autorités publiques adaptent leurs techniques, d'anonymisation ou de pseudonymisation au regard de la nature des données à caractère personnel traitées et des risques liés à leur valorisation.

Les Autorités publiques utilisent des techniques d'anonymisation telles que la randomisation ou la généralisation.

Sauf disposition contraire applicable ou autorisation des personnes disposant des droits sur ces données, les données protégées pour des raisons de confidentialité commerciale ou de secrets statistiques, par le secret d'affaires ou pour la protection de droits de propriété intellectuelle doivent être occultées avant tout partage.

§ 4. – Pour qu'un jeu de données soit considéré comme anonymisé, toute individualisation, corrélation ou inférence doit être impossible.

Si l'ensemble de ces critères ne sont pas remplis, l'Autorité publique responsable du traitement doit garantir que le risque de réidentification est inexistant.

§ 5. – Sans préjudice des droits des personnes concernées et des recours organisés par le RGPD, les Autorités publiques organisent la possibilité de déposer plainte pour les personnes titulaires de droits sur les données protégées. La procédure de plainte organise un dépôt de la plainte auprès des services ou des personnes compétentes au sein des Autorités publiques. Les personnes titulaires de droits sur les données protégées peuvent déposer plainte dès qu'elles estiment que leurs droits ne sont pas respectés ou sont menacés.

CHAPITRE 5
L'évaluation des risques

Article C.III.15.
Évaluation des risques

Sans préjudice des articles 35 et 36 du RGPD, les Autorités publiques doivent réaliser une évaluation des risques liés à la protection des données protégées en tenant compte des informations à leur disposition concernant :

1° la nature des données protégées à traiter;

2° le type d'opérations à réaliser;

3° la portée des opérations de traitement et leur contexte;

4° la finalité et la durée des traitements.

TITRE 4
La gestion des données

CHAPITRE 1
Dispositions générales

Article C.III.16.
La gestion des données

Les Autorités publiques mettent en place une gestion efficace et cohérente des données qu'elles détiennent.

Dans ce cadre, les Autorités publiques adoptent les mesures techniques et organisationnelles appropriées et tout processus pertinent afin de vérifier, à tout moment, que les données qu'elles détiennent :

1° font l'objet d'une sécurisation adéquate telle qu'énoncée à l'article C.II.2;

2° ont le niveau de qualité requis pour atteindre les objectifs de valorisation identifiés;

3° sont intégrées dans des systèmes d'information interopérables, tels que décrits à l'article C.II.17;

4° sont réversibles, conformément à l'article C.II.18.

Les Autorités publiques définissent la fréquence des mises à jour des données qu'elles détiennent.

En tous les cas, les Autorités publiques :

1° garantissent la plus haute fréquence de mise à jour compte tenu de la nature des données traitées et de l'objectif poursuivi;

2° documentent et publient la fréquence de mise à jour des données qu'elles détiennent;

3° garantissent que les titulaires de droits sur les données protégées puissent mettre à jour ou modifier les données à tout moment;

4° garantissent que la mise à jour des données n'est organisée que dans les limites permises de la mission d'intérêt public ou de l'obligation légale servant de fondement au traitement des données à caractère personnel concernées.

Les Autorités publiques gèrent les données qu'elles détiennent tout au long du cycle de la vie de la donnée, en tenant compte de leur contexte d'utilisation et de leur cas d'usage, ainsi que des éventuelles modifications.

CHAPITRE 2
La gestion de la qualité des données

SECTION 1
La gestion des données de référence et des métadonnées

Article C.III.17.
La gestion des données de référence et des métadonnées

§ 1er. – Le présent article vise à fournir les outils nécessaires aux Autorités publiques pour atteindre l'objectif opérationnel décrit à l'article C.II.20.

§ 2. – Les Autorités publiques utilisent, définissent, stockent, les données de référence et organisent une vue complète, fiable et à jour des données de référence qu'elles détiennent au sein d'un système d'information, indépendamment des canaux de communications, du secteur d'activité ou des subdivisions métiers ou géographiques.

§ 3. – Les Autorités publiques définissent, stockent, et organisent une vue complète, fiable et à jour des métadonnées des données qu'elles détiennent au sein d'un système d'information.

§ 4. – Les traitements de données de références à caractère personnel par les Autorités publiques ont uniquement pour finalités d'assurer la cohérence de leurs systèmes d'informations, d'optimiser la performance administrative et d'assurer le suivi de leurs actions. Lorsque les données de référence contiennent des données à caractère personnel, elles sont traitées sans préjudice du Règlement Général sur la Protection des Données.

§ 5. – Les traitements de métadonnées à caractère personnel ont uniquement pour finalités d'optimiser l'accessibilité, la compréhension et la réutilisation des données auxquelles elles sont associées. Lorsque les métadonnées contiennent des données à caractère personnel, elles sont traitées conformément au Règlement Général sur la Protection des Données.

§ 6. – Les Autorités publiques ont l'obligation d'informer la personne concernée par l'utilisation d'une donnée à caractère personnel la concernant au titre de donnée de référence ou de métadonnée.

§ 7. – Les données de références et métadonnées à caractère personnel sont conservées par les Autorités publiques pendant une période identique avec la durée de vie des données qu'elles décrivent.

§ 8. – Pour gérer les métadonnées et les données de référence, les Autorités publiques utilisent l'outil de gestion du Catalogue des données. Les Autorités publiques établissent des métadonnées fiables permettant notamment d'identifier :

1° les types de données à valoriser ou partager;

2° l'utilité que les données représentent en termes d'information;

3° l'origine des données;

4° la localisation des données;

5° la manière dont les données se déplacent dans les systèmes;

6° l'entité responsable de ces données;

7° les conditions d'accès aux données;

8° les partenariats numériques de données en vigueur;

9° la qualité des données en ce compris leur fréquence de mise à jour et leur exhaustivité (complétude);

10° le ou les responsables de traitements relatifs à une donnée lorsqu'elle revêt un caractère personnel.

§ 9. – Les données de référence, les métadonnées et l'identification des données qu'elles décrivent sont transmises au gestionnaire de la Plateforme bruxelloise de la donnée par chaque Autorité publique au moins une fois par an à l'aide de l'outil de gestion du Catalogue des données.

SECTION 2
La gestion des modèles analytiques et la transparence des algorithmes

Article C.III.18.
Respect des missions de services publics et des obligations légales applicables

Les Autorités publiques peuvent recourir à des procédures de décisions fondées exclusivement sur un traitement automatisé dans le cadre de sa mission de service public ou d'une obligation légale lui incombant conformément à l'article 22 du RGPD.

Article C.III.19.
Droits de la personne concernée en cas de décision d'une Autorité publique fondée exclusivement sur un traitement automatisé

Toute personne concernée, à l'égard de laquelle une décision totalement automatisée a été prise par une Autorité publique :

1. est informée de manière claire, explicite et transparente de la nature automatisée de la décision, de ses droits relatifs à la protection des données personnelles et de la manière dont ces droits peuvent être exercés;

2. reçoit une explication complète des motifs conduisant à cette décision;

3. dispose du droit d'obtenir une intervention humaine de la part de l'Autorité publique responsable de traitement;

4. dispose du droit de contester la décision auprès de l'Autorité publique.

Article C.III.20.
La gestion des modèles analytiques, des algorithmes et des systèmes exploitant l'intelligence artificielle

Les Autorités publiques adoptent des mesures techniques et organisationnelles appropriées en vue de garantir que tout système qu'elles utilisent et qui recourt à des modèles analytiques, des algorithmes ou des solutions d'intelligence artificielle puisse faire l'objet d'un contrôle. À cet effet, les autorités publiques veillent, notamment, concernant les modèles analytiques, algorithmes et systèmes, à :

1° établir une stratégie de gouvernance ciblée intégrant les risques et bénéfices qui en découlent de leur usage, notamment concernant d'éventuels effets discriminatoires;

2° développer un inventaire de ceux qu'elles utilisent et de mécanismes permettant d'évaluer l'impact de l'ajout de nouveaux éléments ou de la modification des éléments existants;

3° les concevoir et les tester pour éviter les effets non désirés éventuels et plus particulièrement des traitements discriminatoires;

4° garantir la transparence de leurs modèles techniques et commerciaux de manière à permettre aux personnes concernées de comprendre comment leurs données à caractère personnel sont utilisées et de contester toute utilisation discriminatoire;

5° évaluer leur résilience, leur sécurité, et s'ils développent des moyens proportionnés aux buts recherchés;

6° mettre en place des mécanismes de contrôle assurant la responsabilité et la transparence de leur fonctionnement et le contrôle de leurs résultats par leurs utilisateurs;

7° instaurer des contrôles opérés par l'administrateur local de la donnée;

8° informer et responsabiliser les agents des Autorités publiques qui les utilisent quant au fonctionnement des systèmes et à leurs conséquences potentielles notamment en matière de discrimination;

9° garantir leur accessibilité à tous.

SECTION 3
La gestion des bases de données

Article C.III.21.
La gestion des bases de données

Les Autorités publiques adoptent des mesures techniques et organisationnelles appropriées en vue de garantir la gestion des bases de données. À cet effet, les Autorités publiques veillent notamment à :

1° placer chaque base de données sous la responsabilité d'une personne physique désignée et adopter, dans ce cadre, une politique de gestion qui désigne le ou les administrateurs de la base de données, décrivant les rôles, les fonctions et les niveaux

d'accès de ces administrateurs. Cette politique peut également imposer différentes exigences aux administrateurs relativement à l'exercice de leurs fonctions;

2° notifier, en cas notamment de modification, de fusion ou de transfert d'une base de données, aux personnes concernées et aux titulaires de droits sur d'éventuelles données protégées, les changements intervenus.

CHAPITRE 3
La sécurité et la protection des données

SECTION 1
La gestion des accès et des privilèges associés

Article C.III.22.
Gestion de la sécurité et de la protection des données

Les Autorités publiques assurent la sécurisation et la protection des données qu'elles détiennent ou des données issues de sources authentiques bruxelloises dont elles sont les producteurs au travers de :

1° la gestion des accès et des privilèges associés;

2° la gestion de la sécurité informatique.

Article C.III.23.
Gestion des accès et des privilèges associés

Les Autorités publiques adoptent des processus de contrôle et de gestion des accès.

Tout accès à un système d'information et à ses ressources est contrôlé et seuls les accès autorisés peuvent avoir lieu.

La gestion des accès assure que les données ne soient accessibles qu'aux agents des Autorités publiques faisant état d'un besoin légitime.

Les accès sont établis en tenant compte notamment de :

1° de la fonction de l'utilisateur;

2° des catégories d'accès par type d'utilisateur;

3° de la catégorisation, telle qu'envisagée au chapitre 3 du titre 2 du présent livre, des données elles-mêmes.

Les données protégées doivent être stockées et protégées séparément des autres données et bénéficier d'un niveau de sécurité renforcé.

Le Gouvernement, le Collège réuni et le Collège définissent conjointement les modalités de la gestion des accès.

SECTION 2
La gestion de la sécurité informatique

Article C.III.24.
Gestion de la sécurité informatique

§ 1er. – Les Autorités publiques garantissent la gestion de la sécurité informatique en lien avec les données qu'elles détiennent.

§ 2. – Les Autorités publiques ont l'obligation de surveiller continuellement l'évolution de la technologie et des normes associées, et de s'assurer que leurs pratiques de sécurité sont régulièrement mises à jour afin de se conformer aux derniers principes et standards de l'état de l'art.

§ 3. – La gestion de la sécurité informatique recouvre notamment :

1° l'appréciation des risques informatiques;

2° la définition de la politique de sécurité de l'information;

3° la gestion de la sécurité de l'information dans la gestion de projet;

4° la définition des rôles et responsabilités dans la sécurité de l'information;

5° la gestion des relations avec les tiers;

6° la gestion des incidents liés à la sécurité de l'information.

§ 4. – Le Gouvernement, le Collège réuni et le Collège, définissent conjointement l'étendue des obligations et les modalités des Autorités publiques en matière de gestion de la sécurité informatique.

TITRE 5
Le contrôle de la conformité, la traçabilité et la responsabilité des Autorités publiques

Article C.III.25.
Contrôle de la conformité et de la traçabilité

§ 1er. – Les Autorités publiques mettent en place des procédures de contrôle afin de s'assurer qu'elles gèrent les données et leurs accès conformément au présent Code, aux dispositions légales et réglementaires applicables en vigueur, de même que conformément aux politiques et normes qu'elles ont établies.

§ 2. – Les Autorités publiques mettent en place des procédures de contrôle permettant de vérifier et d'archiver les accès et les modifications aux données qu'elles détiennent et aux données issues de sources authentiques bruxelloises qu'elles produisent ainsi que la conformité technique des outils et des systèmes utilisés pour gérer les données.

§ 3. – La mise en œuvre d'une authentification multi-facteurs est obligatoire pour accéder aux systèmes contenant des données protégées et plus spécifiquement des données à caractère personnel.

§ 4. – Conformément avec l'état de l'art, le chiffrement des données protégées en transit est obligatoire, notamment lors de la transmission via des réseaux non sécurisés.

§ 5. – Les clés de chiffrement doivent être conservées séparément des données chiffrées et gérées selon des procédures spécifiques.

§ 6. – Les mesures de contrôle ainsi que la vérification de la conformité technique des outils et des systèmes utilisés pour celles-ci sont établies périodiquement à des points précis du cycle de vie des données pour évaluer les pratiques et les activités de l'Autorité publique.

§ 7. – Un audit de la sécurité est réalisé par les Autorités publiques au moins tous les deux ans et à chaque fois qu'un changement majeur est apporté aux systèmes, afin d'évaluer les pratiques au regard de l'état de l'art.

Les autorités corrigent toute lacune ou vulnérabilité identifiée lors de cet audit.

§ 8. – Un contrôle de la sécurité pour chaque jeu de données est effectué par les Autorités publiques au moins une fois par an.

§ 9. – Les Autorités publiques procèdent aux renforcements des capacités et des compétences de leurs agents par la mobilisation, l'information, la sensibilisation et la formation, en vue d'atteindre l'objectif stratégique d'éducation des parties prenantes décrit à l'article C.II.11.

§ 10. – Tout incident de sécurité doit être rapporté aux éventuelles Autorités publiques concernées par l'incident dans les 72 heures suivant sa découverte.

LIVRE C.IV
Partage administratif, reutilisation et communication

TITRE 1
Garanties communes aux partages administratifs, réutilisations, communications

Article C.IV.1.
Secret Professionnel et confidentialité

Toute personne au sein des Autorités publiques qui, en raison de ses fonctions, participe à des opérations de partage administratif, de réutilisation ou de Communication, lesquelles, en vertu de dispositions légales ou réglementaires, seraient couvertes par le secret professionnel, est tenue de respecter ces dispositions légales ou réglementaires en matière de secret professionnel.

Article C.IV.2.
Respects de droit des tiers

Les opérations de partage administratif, de réutilisation ou de Communication respectent les droits des tiers tels que définis à l'article C.II.2, à savoir notamment :

1° les droits de propriété intellectuelle conformément à la législation applicable;

2° le secret des statistiques;

3° la protection des secrets d'affaires de tiers telle que visée par le titre 8/1 du livre XI du Code de droit économique;

4° la protection des personnes physiques à l'égard du traitement des données à caractère personnel garanti, en particulier, par le RGPD;

5° la protection des personnes qui signalent des violations du droit de l'Union et du droit national, au sens de la Directive (UE) 2019/1937 sur la protection des personnes qui signalent des violations du droit de l'Union;

6° les principes de concurrence repris dans le Livre IV du Code de droit économique et la réglementation applicable en matière d'aides d'État.

Article C.IV.3.

Absence de droit de propriété intellectuelle ou sui generis sur les bases de données publiques

Les Autorités publiques ne peuvent pas se prévaloir d'un droit de propriété intellectuelle, ni du droit « *sui generis* » prévu par les articles XI.307 et suivants du Code de droit économique sur les bases de données publiques qu'elles détiennent, produisent ou éditent. Elles ne peuvent, en outre, prendre des mesures restrictives d'accès ou de réutilisation de ces informations, que dans les cas où cela est nécessaire à la sauvegarde des prérogatives des tiers ou à des motifs de sécurité publique.

TITRE 2

Partage administratif

CHAPITRE 1

Principe du partage administratif

Article C.IV.4.

Partage administratif et demande de partage administratif

Les Autorités Publiques organisent, à la demande de l'une d'entre elles, des partages administratifs de données entre elles, gratuitement, dans la mesure où ces partages administratifs sont nécessaires à l'exécution d'une mission d'intérêt public ou d'intérêt général et dans la mesure où ces partages administratifs respectent les conditions imposées par toute norme législative ou réglementaire ou encore internationale ou européenne directement applicable, visant notamment à protéger les droits des tiers.

Les modalités des demandes de partage administratif formulées par les Autorités publiques destinataires sont déterminées par le Bureau de la donnée en concertation avec le Comité de Gouvernance de la donnée.

L'absence de réponse à une demande de partage administratif est assimilée à un refus de partage administratif dans le chef de l'Autorité publique productrice des données.

Article C.IV.5.

Passage par le Centre d'intégration par défaut pour les partages administratifs

Tout partage administratif est réalisé au travers du Centre d'intégration, en l'absence de dispositions législatives ou réglementaires particulières organisant spécifiquement le partage administratif visé.

L'intégrateur de services bruxellois vérifie le cas échéant les autorisations nécessaires en vertu d'une disposition législative ou réglementaire dans le chef des parties impliquées, avant de permettre le partage administratif.

Article C.IV.6.

Partage entre Autorités publiques et Autorités publiques tierces

En l'absence de toute disposition légale ou réglementaire particulière organisant spécifiquement le partage visé, les partages entre Autorités publiques et Autorités publiques tierces peuvent être réalisés au travers du Centre d'intégration. Dans ces hypothèses, le Centre d'intégration constitue le relais entre les Autorités publiques et les intégrateurs de services desservant les Autorités publiques tierces et ce, notamment afin d'assurer une compatibilité technique et juridique avec ces mêmes Autorités publiques tierces.

Article C.IV.7.

La qualité de la donnée partagée

L'Autorité publique identifiée comme le producteur des données visées par le partage administratif est responsable de sa qualité.

L'Autorité publique producteur met en œuvre tous les moyens à sa disposition pour atteindre le plus haut niveau de qualité au regard de l'état de l'art et de l'évolution des technologies, ainsi que conformément aux règles de gouvernance du présent Code et des règles, lignes directrices ou recommandations de qualité adoptées en matière de gouvernance des données par le Comité de gouvernance de la donnée.

Article C.IV.8.

Responsabilité de l'Autorité publique destinataire

L'Autorité publique destinataire assure la confidentialité des données issues du partage administratif transitant par le Centre d'intégration, la gestion des accès à ces données. L'Autorité publique destinataire est responsable des accès sur les données mises à disposition ou transmises.

CHAPITRE 2
Conditions du partage administratif

SECTION 1
Conditions générales

Article C.IV.9.
Conclusion d'un protocole d'accord

§ 1er. – Les Autorités publiques parties au partage administratif concluent un protocole d'accord.

Les Autorités publiques peuvent se faire représenter par leur administrateur local de la donnée.

§ 2. – Chaque protocole d'accord comprend au moins les informations suivantes :

1° l'identité et les coordonnées de l'Autorité publique producteur des données, en ce compris celles de son représentant;

2° l'identité et les coordonnées de l'Autorité publique destinataire, en ce compris celles de son représentant;

3° en application du chapitre 2 du titre 2 du livre C.III, les qualités de chaque partie;

4° les finalités précises pour lesquelles les données font l'objet d'un partage administratif;

5° les catégories de données visées conformément au chapitre 3 du titre 2 du livre C. III et les types de données concernées;

6° le format et le support éventuel de la donnée;

7° l'obligation légale, la mission de services publics qui fonde la demande de partage administratif des données;

8° le niveau de qualité de la donnée et la durée pour laquelle ce niveau est garanti par l'Autorités publique producteur;

9° les modalités techniques de l'opération visée et plus spécifiquement les conditions d'interopérabilité;

10° les normes de sécurité implémentées et les normes techniques et organisationnelles de la base de données concernée;

11° les procédures en cas de fuite de données et non disponibilité des données;

12° les modalités de fin du partage administratif et du Protocole d'accord.

§ 3. – Dans l'hypothèse où le partage administratif vise des données à caractère personnel, le protocole d'accord comprend également au moins les informations suivantes :

1° l'identification du responsable de traitement au sein de chaque Autorité publique, partie au partage administratif;

2° les coordonnées des Délégués à la protection des données et Conseillers en sécurité de l'information au sein de chacune des Autorités publiques parties au partage administratif;

3° les catégories de données à caractère personnel concernées, dans le respect du principe de minimisation, au sens du RGPD;

4° toute mesure spécifique prise conformément au principe de proportionnalité et aux exigences de protection des données dès la conception et par défaut;

5° les restrictions légales applicables aux droits de la personne concernée et la justification de leur application en l'espèce;

6° les modalités d'exercice des droits de la personne concernée.

Les partages administratifs de données à caractère personnel ne peuvent être réalisés que dans le respect des dispositions du RGPD, en particulier du principe de limitation des finalités notamment visé à l'article 6.4.

Article C.IV.10.
Procédure de conclusion du protocole d'accord

§ 1er. – Le protocole d'accord est conclu préalablement au partage administratif des données dans un délai maximal de quarante jours ouvrables à compter de la réception, par l'Autorité publique producteur des données, de la demande de partage administratif visée à l'article C.IV.4, alinéa 2.

Les parties peuvent de commun accord prolonger d'un mois au maximum le délai prévu à l'alinéa 1er, notamment pour des demandes importantes ou complexes.

§ 2. – Le Bureau de la donnée en concertation avec le Comité de gouvernance de la donnée propose des modèles de protocoles d'accord disponibles sur la Plateforme bruxelloise de la donnée, permettant d'encadrer les partages administratifs.

§ 3. – Le délai de quarante jours ouvrables est suspendu pendant les demandes d'avis visées au paragraphe 4 pour une durée de vingt jours ouvrables maximum et, en cas d'analyse d'impact visée à l'article 35 du RGPD, pour une durée de trente jours ouvrables maximum.

L'absence de conclusion d'un protocole d'accord dans le délai légal est assimilée à un refus de conclusion du Protocole d'accord dans le chef de l'Autorité producteur des données.

§ 4. – Le protocole d'accord est adopté après les avis respectifs du Conseiller en sécurité de l'information et de l'administrateur local de la donnée, et, en cas de partage administratif de données à caractère personnel, du Délégué à la protection des données. Ces avis sont remis dans un délai de vingt jours ouvrables, à compter du jour où le projet de protocole d'accord leur a été envoyé simultanément. À défaut, l'avis sera considéré comme négatif.

Ces avis sont annexés au protocole d'accord.

Lorsqu'un de ces avis n'est pas suivi par les parties, le protocole d'accord mentionne, en ses dispositions introductives, les raisons pour lesquelles cet avis n'a pas été suivi.

Article C.IV.11.

Publicité du protocole d'accord

Sauf motifs de sécurité publique, les protocoles d'accord sont publiés, dans les meilleurs délais et au plus tard avant tout partage administratif, par les Autorités publiques via le Catalogue des données.

L'Autorité publique producteur des données envoie le protocole d'accord à l'Intégrateur de services bruxellois, au plus tard dans le mois suivant son adoption.

Article C.IV.12.

Recours auprès de la CADADo

Toute personne physique ou morale directement affectée par une décision relative à une demande de partage administratif de données dispose d'un droit de recours devant la CADADo dans les conditions prévues au Livre B.II.

SECTION 2

Conditions particulières relatives aux partages administratifs organisant la mise à disposition de données issues de sources authentiques aux fins de collecte unique

SOUS-SECTION 1

Principe des partages administratifs organisant la mise à disposition de données issues de sources authentiques aux fins de collecte unique

Article C.IV.13.

Partage administratif de données issues de sources authentiques aux fins de collecte unique

§ 1er. – Les partages administratifs de données issues de sources authentiques visent la mise à disposition de ces données au profit des Autorités publiques destinataires afin qu'elles n'en organisent plus elle-même la collecte.

Dans le cadre du présent article le partage administratif peut également s'entendre d'un partage entre Autorités publiques et Autorités publiques tierces.

§ 2. – Les Autorités Publiques ne collectent les données issues de sources authentiques qu'auprès des Autorités publiques ou des Autorités publiques tierces désignées producteur de la source authentique, le cas échéant à travers le Centre d'intégration, selon les modalités techniques prévues par ce dernier concernant le canal relatif aux données issues de sources authentiques.

Les Autorités publiques ne peuvent plus réclamer directement les données visées au premier alinéa à d'autres Autorités publiques, personnes, ou entités.

§ 3. – Le Gouvernement, le Collège réuni et le Collège peuvent suspendre pour des raisons techniques ou organisationnelles, et pour toutes ou certaines Autorités publiques uniquement, l'application du présent paragraphe pour une période transitoire renouvelable qui ne peut excéder cinq ans à dater de la désignation de la source authentique bruxelloise par arrêté, décret ou ordonnance, conformément à l'article C.IV.17 afin de permettre aux Autorités publiques de se connecter de manière effective au Centre d'intégration.

Article C.IV.14.

Partage administratif de données à caractère personnel issues de sources authentiques bruxelloises aux fins de collecte unique

À l'exception des partages administratifs de données à caractère personnel visant à garantir les objectifs visés à l'article 23, paragraphe 1, du RGPD, les partages administratifs de données à caractère per-

sonnel issues d'une source authentique bruxelloise ne peuvent être réalisés qu'avec le consentement de la personne concernée.

L'Autorité publique désignée comme producteur de la source authentique bruxelloise, détenant les données dans le cadre de ses missions de services publics ou d'intérêt général, récolte les consentements des personnes concernées afin que leurs données soient utilisées par d'autres Autorités publiques dans le cadre du principe de la collecte unique.

Ce consentement peut être retiré à chaque instant.

Le producteur de la source authentique bruxelloise s'assure du consentement libre, spécifique, éclairé et univoque de la personne concernée selon les principes suivants :

1. Information sur le traitement ultérieur : lors de la collecte initiale, la personne concernée est informée de tout traitement ultérieur possible de ses données par d'autres Autorités publiques à la suite d'un partage administratif de données issues de sources authentiques bruxelloises ainsi que des autres finalités que celles justifiant la collecte;

2. Consentement pour de nouvelles finalités poursuivies par l'Autorité publique destinataire : le nouveau consentement est obtenu de la part de la personne concernée spécifiquement pour ces nouvelles finalités;

3. Partage vers une autre Autorité publique destinataire identifiée : avant de partager des données à caractère personnel avec une autre Autorité publique dans le cadre d'un partage administratif de données issues de sources authentiques bruxelloises, le producteur s'assure que la personne concernée a été informée et a consenti à ce partage et à la nouvelle finalité du traitement;

4. Droit des personnes concernées de retirer leur consentement : les personnes concernées ont le droit de retirer leur consentement à tout moment.

Article C.IV.15.
Clefs d'identification

§ 1er. – Afin d'utiliser les données nécessaires à l'exécution des missions d'intérêt public ou des obligations légales qui leur incombent, pour l'identification de personnes physiques, les Autorités publiques utilisent, dans le cadre des partages administratifs de données issues de sources authentiques :

1° le numéro du Registre national attribué en exécution de l'article 2, § 3, de la loi du 8 août 1983 organisant un Registre national des personnes physiques;

2° ou le numéro d'identification de la Banque-Carrefour attribué en exécution de l'article 4, § 2, alinéa 3, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, s'il s'agit de données qui concernent une personne physique non reprise dans le Registre national.

§ 2. – Dans le cadre des partages administratifs de données issues de sources authentiques, pour l'identification de personnes morales, les Autorités publiques utilisent, pour l'exécution de leurs missions légales, le numéro d'entreprise attribué en exécution de l'article III.17 du Code de droit économique.

§ 3. – Dans le cadre de l'accomplissement d'une obligation légale d'identification auprès d'une Autorité publique, les personnes physiques et morales utilisent :

1° le numéro du Registre national attribué en exécution de l'article 2, paragraphe 3, de la loi du 8 août 1983 organisant un Registre national des personnes physiques, ou

2° le numéro d'identification de la Banque-Carrefour attribué en exécution de l'article 4, § 2, alinéa 3, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale et le numéro d'entreprise attribué en exécution de l'article III.17 du Code de droit économique.

§ 4. – Dans le cadre des partages administratifs de données issues de sources authentiques, les Autorités publiques peuvent utiliser, pour l'exécution de leurs missions d'intérêt public :

1° le numéro d'identification des parcelles cadastrales;

2° les identifiants repris dans les bases de données UrbiS concernant toutes les données à caractère géographique relatives au territoire bruxellois.

SOUS-SECTION 2
Gestion des données issues de sources authentiques bruxelloises

Article C.IV.16.
Qualité des données issues de sources authentiques

§ 1er. – L'Autorité publique désignée comme producteur de la source authentique bruxelloise met tout en œuvre pour garantir aux Autorités publiques des-

tinataires la qualité de la donnée issue de la source authentique bruxelloise, en assurant notamment son caractère exact et mis à jour au regard des finalités d'utilisation.

L'Autorité publique désignée comme producteur de la source authentique bruxelloise s'assure :

1° de l'authenticité et de l'intégrité des données issues de la source authentique bruxelloise : l'Autorité publique producteur de la source authentique bruxelloise assure la mise en place de mécanismes d'authentification et de vérification d'intégrité afin de prouver l'origine et de garantir la non-altération des données depuis leur création ou leur dernière mise à jour;

2° de la traçabilité et de la réversibilité : la journalisation de toutes les opérations effectuées sur les données issues de sources authentiques bruxelloises doit être effectuée et mise à jour conformément à l'article C.III.25;

3° de la sécurité de la transmission des données issues de sources authentiques bruxelloises : des garanties de sécurité doivent être mises en œuvre pour la transmission des données entre les différentes Autorités publiques et les intégrateurs de services, afin d'empêcher toute interception ou altération non autorisée et ce conformément à l'article C.III.24;

4° du respect des critères de qualité énoncé à l'article C.II.5 et de l'adéquation de la création de données issues de sources authentiques bruxelloises en conformité avec sa mission d'intérêt public;

5° de l'existence de procédures destinées à préserver les données en cas de violation de la sécurité des données : en cas de violation de la sécurité affectant la confidentialité, l'intégrité, la qualité ou la disponibilité des données issues de sources authentiques bruxelloises, des procédures de réponse rapide peuvent être activées pour atténuer les impacts et restaurer la normalité.

§ 2. – Si le destinataire des données issues de sources authentiques constate que ces données sont imprécises, incomplètes ou inexactes, il est tenu d'en informer immédiatement le producteur de la source authentique bruxelloise et l'intégrateur de services bruxellois qui sont tenus d'y donner suite.

§ 3. – Le Gouvernement et le Collège réuni, le Collège peuvent conjointement adopter des normes de qualité ou des lignes conduites en matière de qualité des données issues de sources authentiques bruxelloises.

Article C.IV.17.
Désignation de sources authentiques bruxelloises

§ 1er. – Sans préjudice des sources authentiques reconnues par des Autorités publiques tierces, le Gouvernement, le Collège réuni et le Collège, désignent par arrêté, les sources authentiques bruxelloises, les traitements et les finalités qui y sont liés, dont l'Autorité publique désignée comme producteur de la source authentique relève de leur compétence.

§ 2. – Par dérogation au paragraphe 1er, les sources authentiques bruxelloises comprenant des données à caractère personnel sont désignées par décret ou ordonnance selon la Collectivité publique dont dépend l'Autorité publique désignée producteur de la source authentique bruxelloise.

§ 3. – La désignation des sources authentiques bruxelloises visées au paragraphe 1er s'effectue :

1° soit sur demande de l'Intégrateur de services bruxellois auprès du Gouvernement, Collège réuni ou Collège;

2° soit sur demande de l'Autorité publique qui se propose comme producteur de la source authentique bruxelloise auprès du Gouvernement, Collège réuni ou Collège;

3° soit d'initiative par le Gouvernement, le Collège réuni ou le Collège.

§ 4. – Sous peine d'irrecevabilité, la demande visée au paragraphe 3, 1° et 2°, est soumise préalablement à :

1° l'avis du service compétent de la Région bruxelloise pour la simplification administrative;

2° l'avis du Conseiller en sécurité de l'information de l'Autorité publique proposée comme producteur de la source authentique bruxelloise;

3° l'avis du Délégué à la protection des données de la même Autorité publique;

4° l'avis de l'administrateur local des données de la même Autorité publique.

Dans l'hypothèse visée au paragraphe 3, 3°, le Gouvernement, le Collège réuni et le Collège demandent d'office les avis visés à l'alinéa 1er.

Lorsque la base de données dont la désignation en tant que source authentique bruxelloise est demandée contient des données à caractère personnel, les avis examinent, d'une part, dans quelle mesure la désignation de cette source authentique répond aux

critères de nécessités et de proportionnalité qui s'imposent à toute ingérence dans le droit à la protection des données à caractère personnel et, d'autre part, quelles procédures sont envisagées afin de garantir la qualité des données à caractère personnel de la source authentique bruxelloise au sens de l'article C. IV.16.

§ 5. – L'acte de désignation visé au paragraphe 1er indique, notamment, pour chaque source authentique bruxelloise :

1° l'identité de l'Autorité publique producteur de la source authentique bruxelloise, chargé de la collecte des données, de leur mise à jour, de leur mise à disposition et de tout autre traitement pertinent et nécessaire à son maintien, en fonction de l'état de l'art et de l'évolution des technologies;

2° les modalités selon lesquelles sont tenues à jour et rendues accessibles les données dont l'hébergement est confié à l'Autorité publique producteur de la source authentique bruxelloise;

3° la ou les finalités poursuivies par l'Autorité publique producteur par la constitution de la source authentique bruxelloise lors la collecte des données visées;

4° la liste des données contenues dans la source authentique bruxelloise;

5° les modalités particulières de financement de la collecte des données comprises dans la source authentique bruxelloise, de leur mise à jour, de leur mise à disposition et de tout autre traitement pertinent et nécessaire à son maintien.

Pour ce qui concerne la désignation de sources authentiques bruxelloises comprenant des données à caractère personnel, le décret ou l'ordonnance indique également :

– les éléments essentiels du traitement;

– les mesures prévues protégeant les droits des personnes concernées;

– les obligations de transparence prévues à l'intention des personnes concernées.

TITRE 3
Réutilisations des documents et des données publiques

CHAPITRE 1
Dispositions générales

Article C.IV.18.
Deux régimes de réutilisation

Deux régimes de réutilisation doivent être distingués :

1° la réutilisation des documents et des données publiques des Autorités publiques ouverts et des documents partageables accessibles aux conditions décrites dans le présent titre conformément à la transposition de la Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte);

2° la réutilisation des données publiques protégées des Autorités publiques telles que visées par l'article 3.1. du Règlement sur la gouvernance des données.

CHAPITRE 2
La réutilisation des documents librement accessibles et partageables

SECTION 1
Champ d'application

Article C.IV.19.
Transposition de la Directive 2019/1024

Le présent titre transpose la Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte).

Les ordonnances, les arrêtés ministériels et toute autre réglementation existante qui font référence à la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public sont présumés faire référence à la Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte).

Article C.IV.20.
Champ d'application et exceptions

§ 1er. – Le présent chapitre s'applique aux :

1° documents existants détenus par les Autorités publiques;

2° documents existants détenus par les entreprises publiques;

3° données de la recherche, sous réserve des limitations et exceptions prévues par le présent chapitre.

§ 2. – Le présent chapitre ne s'applique pas :

1° aux documents étrangers à la mission de service public dévolue à l'Autorité publique, sous réserve que l'objet des missions de service public soit transparent et soumis à réexamen;

2° aux documents détenus par des entreprises publiques :

a) dont la production ne relève pas de la fourniture des services d'intérêt général au sens de la loi;

b) relatifs aux activités directement exposées à la concurrence et qui, par conséquent, conformément à l'article 34 de la Directive 2014/25/UE, ne sont pas soumises aux règles relatives à la passation des marchés;

3° aux documents sur lesquels des tiers détiennent les droits de propriété intellectuelle;

4° aux documents, tels que les données sensibles, dont l'accès est exclu ou dont l'accès est limité conformément aux règles législatives et réglementaires d'accès aux documents administratif en matière de publicité administrative, notamment pour les motifs suivants :

a) la protection de la sécurité nationale (c'est-à-dire la sécurité de l'État), la défense ou la sécurité publique;

b) la confidentialité des données statistiques;

c) la confidentialité des informations commerciales (notamment le secret d'affaires, le secret professionnel ou le secret d'entreprise);

5° aux documents dont l'accès est exclu ou limité pour des motifs d'informations sensibles relatives à la protection des infrastructures critiques au sens de l'article 2, point d), de la Directive 2008/114/CE;

6° aux documents dont l'accès est limité légalement notamment dans les cas où un intérêt personnel ou particulier est requis pour avoir accès aux documents;

7° aux logos, armoiries ou insignes;

8° aux documents dont l'accès est exclu ou limité en application de règles d'accès pour des motifs de protection des données à caractère personnel, et aux parties de documents accessibles en vertu desdites règles qui contiennent des données à caractère personnel dont la réutilisation a été définie par une norme législative comme étant incompatible avec la législation concernant la protection des personnes physiques à l'égard du traitement de données à caractère personnel ou comme portant à atteinte à la protection de la vie privée et de l'intégrité de la personne concernée, en particulier au regard des dispositions de droit de l'Union ou de droit national sur la protection des données à caractère personnel;

9° aux documents détenus par les radiodiffuseurs de service public et leurs filiales et par d'autres organismes ou leurs filiales pour une mission de radiodiffusion de service public;

10° aux documents détenus par des établissements culturels autres que des bibliothèques y compris des bibliothèques universitaires, des musées et des archives;

11° aux documents détenus par les établissements d'enseignement de niveau secondaire et au-dessous et, dans le cas de tous les autres établissements d'enseignement, aux documents autres que ceux pouvant être assimilés à des données de recherche visées au paragraphe 1, 3);

12° aux documents autres que les données de recherches visées au paragraphe 1, 3), détenus par des organismes exerçant une activité de recherche et des organisations finançant une activité de recherche y compris des organisations créées pour le transfert des résultats de la recherche.

SECTION 2
Principe de réutilisation

Article C.IV.21.
Réutilisation des documents des Autorités publiques, des entreprises publiques, des bibliothèques, des musées et des archives

Sous réserve des limites fixées à l'article C.IV.20, les Autorités publiques permettent la réutilisation à

des fins commerciales ou non commerciales des documents détenus par les Autorités publiques.

Les Autorités publiques peuvent soumettre la réutilisation des documents à des conditions, conformément aux dispositions du présent chapitre, plus particulièrement les sections IV et V.

Les documents pour lesquels les bibliothèques, y compris les bibliothèques universitaires, les musées et les archives sont titulaires de droits de propriété intellectuelle et les documents détenus par des entreprises publiques peuvent être réutilisés, lorsque la réutilisation de ces documents est autorisée, à des fins commerciales ou non commerciales, conformément aux conditions du présent chapitre, plus particulièrement les sections IV et V.

SECTION 3
Demande de réutilisation

Article C.IV.22.
Demande de réutilisation

Les Autorités publiques traitent les demandes de réutilisation et mettent le document à la disposition du demandeur en vue de la réutilisation, si possible et s'il y a lieu, sous forme électronique.

Si l'obtention du document requiert l'emploi d'une licence, l'Autorité publique sollicitée par la demande de réutilisation envoie au demandeur une offre de licence.

L'Autorité publique traite la demande et fournit le document au demandeur en vue de la réutilisation ou, si une licence est nécessaire, présente au demandeur l'offre de licence définitive dans un délai maximal de vingt jours ouvrables à compter de la réception de la demande. Ce délai peut être prolongé de vingt jours ouvrables supplémentaires pour des demandes importantes ou complexes. En pareils cas, dans les trois semaines qui suivent la demande initiale, le demandeur est informé qu'un délai supplémentaire est nécessaire pour traiter la demande ainsi que des raisons qui justifient ce délai.

En cas de décision négative, l'Autorité publique communique au demandeur les raisons du refus, notamment lié à l'article C.IV.20, § 2, 1) à 12), ou C.IV.21 ou en application de la législation applicable en matière d'accès aux documents administratifs et à l'information environnementale. En cas de décision négative fondée sur l'article C.IV.20, § 2, 3), l'Autorité publique fait mention de la personne physique ou morale titulaire des droits, si elle est connue, ou, à défaut, du donneur de licence auprès duquel elle a obtenu le document en question. Les bibliothèques, y compris les bibliothèques universitaires, les musées et les archives ne sont pas tenus d'indiquer cette mention

Toute décision relative à la réutilisation des documents notifiée au demandeur indique les voies de recours contre cette décision auprès de la CADADo, conformément à l'article C.IV.33 et au livre B.II.

Le Bureau de la donnée fournit les informations appropriées en vue de faciliter la réutilisation efficace des documents.

À défaut des indications visées à l'alinéa 5, le délai de prescription pour introduire le recours ne prend pas cours.

Les entités suivantes ne sont pas tenues de se conformer au présent article :

1° les entreprises publiques;

2° les établissements d'enseignement, les organismes exerçant une activité de recherche et les organisations finançant une activité de recherche.

SECTION 4
Conditions de réutilisation

Article C.IV.23.
Publicité des conditions

Les conditions applicables à la réutilisation des documents doivent être rendues publiques préalablement, et de préférence par voie électronique.

Article C.IV.24.
Formats disponibles

§ 1er. – L'Autorité publique et les entreprises publiques mettent à disposition leurs documents sous une forme et une langue préexistante, et, si possible, sous forme électronique, sans que cela entraîne d'obligation de créer, d'adapter ou de fournir des extraits de documents qui engendrerait des efforts disproportionnés dépassant la simple manipulation.

§ 2. – Dans toute la mesure du possible, l'Autorité met à disposition les documents dans des formats ouverts et lisibles par machine, accessibles, traçables, réutilisables et accompagnés de leurs métadonnées conformément à l'article C.III.7, § 3. Ces formats et métadonnées doivent répondre à des normes formelles ouvertes au sens du présent Code.

§ 3. – Les Autorités publiques ne sont pas tenues de poursuivre la production de documents en vue

de leur réutilisation. Toutefois, elles sont tenues de rendre leurs décisions publiques dans les meilleurs délais.

§ 4. – Les Autorités publiques mettent les données dynamiques à disposition aux fins de réutilisation aussitôt qu'elles ont été recueillies, en recourant à des API appropriées et, le cas échéant, sous la forme d'un téléchargement de masse.

Lorsque la mise à disposition des données dynamiques aux fins de réutilisation ayant eu lieu immédiatement après la collecte, comme prévu à l'alinéa 1er, excéderait les capacités financières et techniques de l'Autorité publique, en imposant de ce fait un effort disproportionné, ces données dynamiques sont mises à disposition aux fins de réutilisation dans un délai ou avec des restrictions techniques temporaires qui ne portent pas indûment atteinte à l'exploitation de leur potentiel économique et social.

§ 5. – Les paragraphes 1er à 4 s'appliquent aux documents existants détenus par des entreprises publiques qui sont disponibles aux fins de réutilisation.

§ 6. – Les ensembles de données de forte valeur dont la liste est établie conformément à l'article C. IV.30, sont mises à disposition à des fins de réutilisation dans des formats lisibles par machine, en recourant à des API appropriées et, le cas échéant, sous la forme d'un téléchargement de masse.

Article C.IV.25.
Principe de tarification

§ 1er. – Une redevance peut être demandée pour la mise à disposition d'un document.

§ 2. – Lorsqu'une redevance est prélevée, elle ne peut couvrir que les coûts marginaux de reproduction, de mise à disposition et de diffusion d'anonymisation de données à caractère personnel et des mesures prises pour protéger des informations confidentielles à caractère commercial.

§ 3. – Lorsque l'Autorité publique applique un système de redevance type pour la réutilisation des documents, le montant effectif et la base de calcul doivent être préalablement fixés et publiés, de préférence par voie électronique.

En l'absence de redevance type, les facteurs pris en compte dans le calcul desdites redevances sont d'emblée indiqués. Le demandeur peut, sur simple demande, être informé par l'Autorité publique concernée de la manière dont la redevance a été calculée dans le cadre d'une demande particulière de réutilisation.

Si les documents sont disponibles en ligne, la publication du système de redevance doit être assurée également par voie électronique.

§ 4. – La restriction visée au § 2 ne s'applique pas aux :

1° Autorités publiques qui sont tenues de générer des recettes destinées à couvrir une part substantielle des coûts liés à l'accomplissement de leurs missions de service public;

2° bibliothèques, y compris aux bibliothèques universitaires, aux musées et aux archives;

3° entreprises publiques.

Le Gouvernement, le Collège réuni et le Collège publient une liste des Autorités publiques visées au paragraphe 4, 1°.

§ 5. – Dans les cas visés aux points 1e et 3e, le montant total des redevances est calculé selon des critères objectifs, transparents et vérifiables définis par arrêté du Gouvernement, du Collège réuni et du Collège.

Le total des recettes provenant de la fourniture et des autorisations de réutilisation des documents pendant la période à calculer ne dépasse pas le coût de la collecte, de la production, de la reproduction, de la diffusion, et du stockage des données, tout en permettant un retour sur investissement raisonnable, ainsi que, le cas échéant, d'anonymisation de données à caractère personnel et des mesures prises pour protéger des informations confidentielles à caractère commercial.

Dans les cas visés au point 2° du paragraphe 4, le total des recettes provenant de la fourniture et des autorisations de réutilisation pendant la période comptable appropriée ne dépasse pas le coût de collecte, de production, de reproduction, de diffusion, de stockage de données, de conservation et de l'acquisition des droits, ainsi que, le cas échéant, d'anonymisation de données à caractère personnel et des mesures prises pour protéger des informations confidentielles à caractère commercial, tout en permettant un retour sur investissement raisonnable.

§ 6. – Le calcul des redevances s'effectue conformément aux principes comptables applicables aux Autorités publiques concernées.

§ 7. – La réutilisation des éléments suivants est gratuite pour l'utilisateur :

1° sous réserve de l'article C.IV.30, les ensembles de données de forte valeur, dont la liste est établie conformément à l'alinéa 1er dudit article;

2° les données de la recherche visées à l'article C. IV.20, § 1er, 3°.

Article C.IV.26.
Licences

Les Autorités peuvent autoriser une réutilisation inconditionnelle de documents ou imposer des conditions, si nécessaire par le biais d'une licence.

Les conditions contenues dans la licence ne limitent pas indûment les possibilités de réutilisation et ne sont pas utilisées pour restreindre la concurrence. Les conditions fixées par les licences doivent être objectives, proportionnées, non discriminatoires et justifiées sur la base d'un objectif d'intérêt général.

Les différentes licences types seront fixées par le Gouvernement, le Collège réuni et le Collège, par arrêté conjoint ou non dans le cadre de leur compétences respectives. Les licences types peuvent être adaptées à des demandes de licence particulières.

Article C.IV.27.
Données de la recherche

Sans préjudice de l'article C.VI.20, § 2, 3°, les données de la recherche sont réutilisables à des fins commerciales ou non commerciales, conformément au présent titre, dans la mesure où elles sont financées au moyen de fonds publics et où des chercheurs, des organismes exerçant une activité de recherche ou des organisations finançant une activité de recherche les ont déjà rendues publiques par l'intermédiaire d'une archive ouverte institutionnelle ou thématique. À cette fin, il est tenu compte des intérêts commerciaux légitimes, des activités de transmission des connaissances et des droits de propriété intellectuelle préexistants.

SECTION 5
Non-discrimination et commerce équitable

Article C.IV.28.
Non-discrimination

§ 1er. – Toute condition applicable en matière de réutilisation des documents ne peut être discriminatoire pour des catégories comparables de réutilisation ou de demandeurs.

§ 2. – Lorsqu'une Autorité publique réutilise des documents dans le cadre de ses activités commerciales étrangères à sa mission de service public, les conditions tarifaires et autres applicables à la fourniture des documents destinés à ces activités sont les mêmes que pour les autres utilisateurs qui ne sont pas des Autorités publiques.

Article C.IV.29.
Accord d'exclusivité

§ 1er. – Les accords d'exclusivité de réutilisation sont interdits, à moins qu'ils ne s'avèrent nécessaires pour la prestation d'un service d'intérêt général.

Excepté pour ce qui concerne la numérisation des ressources culturelles, lorsqu'un droit d'exclusivité est accordé dans l'intérêt général, le bien-fondé de celui-ci fait l'objet, tous les trois ans au moins, d'un réexamen.

Les accords d'exclusivité en vigueur le 16 juillet 2019 ou après cette date sont rendus publics en ligne au moins deux mois avant leur prise d'effet. Ces accords sont transparents et rendus publics en ligne à l'initiative de l'autorité qui l'accorde.

§ 2. – La période d'exclusivité accordée pour la numérisation des ressources culturelles ne dépasse pas, en général, dix ans. Lorsque ladite durée est supérieure à dix ans, elle fait l'objet d'un réexamen au cours de la onzième année et ensuite, le cas échéant, tous les sept ans.

Les accords d'exclusivité visés au premier alinéa sont transparents et sont rendus publics en ligne deux mois avant leur prise d'effet.

Dans le cas d'un droit d'exclusivité visé au premier alinéa, une copie des ressources culturelles numérisées est adressée gratuitement à l'autorité publique dans le cadre des accords conclus. À l'expiration de la période d'exclusivité, ladite copie est mise à disposition à des fins de réutilisation.

Les dispositifs juridiques ou pratiques qui, sans accorder expressément de droit d'exclusivité, visent à restreindre la disponibilité de documents à des fins de réutilisation par des entités autres que l'opérateur privé partie au dispositif, ou qui peuvent raisonnablement être considérés comme susceptibles de la restreindre, sont rendus publics en ligne au moins deux mois avant leur entrée en vigueur. L'effet de tels dispositifs juridiques ou pratiques sur la disponibilité des

données à des fins de réutilisation fait l'objet, tous les trois ans au moins, d'un réexamen.

§ 3. – Les accords d'exclusivité en vigueur le 17 juillet 2013, hormis ceux bénéficiant de l'exception visée au § 1er et 2, prennent fin à l'échéance du contrat ou, en tout état de cause, au plus tard le 18 juillet 2043.

Les accords d'exclusivité en vigueur le 16 juillet 2019 qui ne relèvent pas des exceptions prévues aux paragraphes 1er et 2 prennent fin à la date d'échéance du contrat ou, en tout état de cause, au plus tard le 17 juillet 2049.

SECTION 6
Ensembles de données de forte valeur

Article C.IV.30.
Catégories thématiques d'ensembles de données de forte valeur

Afin de mettre en place des conditions soutenant la réutilisation d'ensembles de données de forte valeur, une liste des catégories thématiques d'ensembles de données de forte valeur est incluse à l'annexe du Code.

Le Gouvernement, le Collège réuni, le Collège établit les modalités de publication et de réutilisation des ensembles de données de forte valeur relevant des catégories figurant à l'annexe du présent Code basées sur la liste d'ensemble de données de forte valeur dressée par la Commission Européenne conformément à l'article 14 de la Directive (UE) 2019/2024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public.

SECTION 7
Recours auprès de la CADADo

Article C.IV.31.
Recours auprès de la CADADo

Toute personne physique ou morale directement affectée par une décision relative à une demande de réutilisation de données visées par le présent chapitre dispose d'un droit de recours devant la CADADo dans les conditions prévues au Livre B.II.

L'absence de réponse à une demande de réutilisation de données visées par le présent chapitre est assimilée à un refus de réutilisation dans le chef de l'Autorité publique.

CHAPITRE 3

La réutilisation des données protégées conformément au règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 (DGA)

Article C.IV.32.

Disposition générale

Conformément aux compétences matérielles de la Région, de la Commission Communautaire commune, de la Commission Communautaire française, le Gouvernement, le Collège réuni et le Collège exécutent le Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724.

Article C.IV.33.

Recours après de la CADADo

Toute personne physique ou morale directement affectée par une décision relative à une demande de réutilisation de données protégées dispose d'un droit de recours devant la CADADo dans les conditions prévues au Livre B.II.

L'absence de réponse à une demande de réutilisation de données protégées est assimilée à un refus de réutilisation dans le chef de l'Autorités publique.

TITRE 4

Communication

Article C.IV.34.

Dispositions générales

Par l'intermédiaire du Point de contact de la Plateforme bruxelloise de la donnée, le gestionnaire de la Plateforme bruxelloise de la donnée organise l'altruisme en matière de données pour l'ensemble des Autorités publiques par la Communication des données à caractère personnel ainsi que toutes autres données qui seraient volontairement mises à disposition à des fins d'intérêt général.

LIVRE C.V
La plateforme bruxelloise de la donnée

TITRE 1
Principes de la Plateforme bruxelloise de la donnée

Article C.V.1.
Création et objectif de la Plateforme bruxelloise de la donnée

§ 1er. – Il est créé une Plateforme bruxelloise de la donnée, institué au sein de Paradigm.

La Plateforme bruxelloise de la donnée offre notamment des services destinés à permettre le partage administratif de données, la réutilisation de données ou la Communication de données décrites au livre C.IV.

§ 2. – Paradigm est désigné en qualité de gestionnaire de la Plateforme bruxelloise de la donnée.

Article C.V.2.
Missions du gestionnaire de la Plateforme bruxelloise de donnée

Le gestionnaire de la Plateforme bruxelloise de la donnée est chargé des missions suivantes :

1° l'administration technique de la Plateforme, notamment en ce qui concerne l'infrastructure, la sécurité, la gestion ou la disponibilité des informations ou, le cas échéant, des données;

2° la promotion de l'utilisation et de l'usage efficace de la Plateforme, notamment en ce qui concerne la qualité et l'interopérabilité des données proposées;

3° l'établissement du cadre documentaire de base et d'accord d'adhésion permettant son utilisation, notamment en ce qui concerne les formalités ou les modalités d'adhésion à la Plateforme et d'utilisation de ses services, ou la mise à disposition des modèles de Protocoles d'accord;

4° le cas échéant, le contrôle des schémas d'identification électronique ou de la certification au sens du Règlement (UE) No 910/2014 (EIDAS);

5° le cas échéant, la désignation d'un prestataire indépendant en qualité de tiers de confiance;

6° la documentation du fonctionnement de la Plateforme, notamment en ce qui concerne les processus mis en place, et les statistiques d'utilisation notamment au regard des données d'usage spécifiques de la Plateforme;

7° le conseil et l'assistance aux Autorités publiques utilisatrices ainsi que la coordination avec leurs représentants, notamment en ce qui concerne la formation à l'utilisation, la prise en charge de projets particuliers, ou tout autre domaine pertinent en relation avec l'utilisation de la Plateforme;

8° la conception évolutive de l'architecture de la Plateforme conformément à la stratégie pluriannuelle de la donnée ainsi que les plans d'actions annuels, visés à l'article C.VI.15, § 2.

Le Gouvernement, le Collège réuni et le Collège peuvent définir conjointement les modalités d'organisation des missions visées ci-dessus.

TITRE 2
Les services de la Plateforme bruxelloise de la donnée

CHAPITRE 1
Dispositions générales

Article C.V.3.
Accord d'adhésion

§ 1er. – La mise à disposition des services de la Plateforme bruxelloise de la donnée fait l'objet d'un accord d'adhésion entre le gestionnaire de la Plateforme et l'utilisateur de la plateforme.

L'utilisateur de la Plateforme marque son accord de manière électronique, préalablement à l'utilisation de la Plateforme.

Le cas échéant, l'accord d'adhésion mentionne les conditions particulières qui s'appliquent en fonction du ou des services que l'utilisateur souhaite utiliser.

§ 2. – Le cas échéant, l'utilisateur concluant l'accord d'adhésion pour une entité dispose du mandat nécessaire pour ce faire.

Article C.V.4.
Finalités des traitements

Les traitements réalisés dans le cadre des services de la Plateforme bruxelloise de la donnée poursuivent les finalités suivantes :

1° pour l'ensemble de la gestion technique de Plateforme, le traitement des données à caractère personnel a pour finalité de s'assurer du bon fonctionnement de celle-ci et de la traçabilité des accès;

2° au niveau du Centre d'intégration, le traitement des données à caractère personnel a pour finalités la transmission ou la mise à disposition des données vers les Autorités publiques destinataires;

3° au niveau du Catalogue de la donnée, l'éventuel traitement des données à caractère personnel a pour finalité le diagnostic qualitatif des données en vue de leur documentation;

4° au niveau du Centre d'exploitation et d'analyse, le traitement des données à caractère personnel a pour finalité la prestation de services facultatifs visés à l'article C.V.15 ou l'analyse qualitative des données;

5° au niveau du Portail ouvert des données, les éventuels traitements des données à caractère personnel ont pour finalités le stockage, la publication des données ou l'identification de son gestionnaire;

6° au niveau du Point de contact et d'information, le traitement des données à caractère personnel a pour finalité le traitement des demandes des usagers de la Plateforme;

7° au niveau du Service d'appui, le traitement des données à caractère personnel a pour finalité la gestion technique de la Plateforme.

Article C.V.5.
Qualification conformément au RGPD

L'intégrateur de services bruxellois agit en tant que responsable de traitements pour les traitements des données à caractère personnel nécessaires à la gestion technique de la Plateforme ainsi que pour l'ensemble des traitements du Centre d'intégration.

Le gestionnaire de la Plateforme bruxelloise de la donnée agit pour le compte des Autorités publiques en tant que sous-traitant pour les services du Catalogue, du Portail ouvert des données publiques et du Centre d'exploitation et d'analyse des données.

Le gestionnaire de la Plateforme gère ses bases de données conformément à la loi 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ainsi qu'au RGPD.

Article C.V.6.
Catégories de données à caractère personnel et personnes concernées

Les traitements réalisés dans le cadre des services de la Plateforme bruxelloise de la donnée concernent :

1° les données à caractère personnel qui font l'objet d'un partage administratif;

2° les données à caractère personnel nécessaires à l'utilisation de la Plateforme et à sa gestion technique, à savoir l'identité des agents des Autorités publiques ou des autres usagers de la Plateforme;

3° les données à caractère personnel des Autorités publiques sous-traitées par celles-ci au gestionnaire de la plateforme dans le cadre de leurs missions d'intérêt public et par le service du centre d'exploitation et d'analyse.

Les catégories de données à caractère personnel visées par les traitements sont les données publiques à caractère personnel des Autorités publiques.

Les personnes concernées sont les personnes concernées par les données publiques à caractère personnel des Autorités publiques.

Article C.V.7.
La durée de conservation des données

En ce qui concerne les données à caractère personnel nécessaires à la gestion technique des services de la Plateforme bruxelloise de la donnée, les données sont conservées jusqu'à 10 ans après la fin du traitement.

En ce qui concerne les traitements des données à caractère personnel réalisés par le Centre d'exploitation et d'analyse, les données sont conservées pour une durée fixée en fonction des finalités déterminées par le responsable de traitement.

En ce qui concerne les traitements des données à caractère personnel réalisés par le Catalogue des données, la durée de conservation est limitée à la durée du traitement.

En ce qui concerne les traitements des données à caractère personnel réalisés par le Portail ouvert des données, les données sont conservées jusqu'à un an après la fin du traitement.

En ce qui concerne les traitements des données à caractère personnel réalisés par le Point de contact et d'information, les données sont conservées jusqu'à un an après la fin du traitement.

En ce qui concerne les traitements des données à caractère personnel réalisés par le Service d'appui, les données sont conservées jusqu'à un an après la fin du traitement.

Les données à caractère personnel nécessaires à la gestion technique des autres services de la Plateforme bruxelloise de la donnée que ceux visés dans les alinéas 1 à 6, sont conservées jusqu'à 6 mois après la fin du traitement.

Les données sont détruites à l'échéance des délais précités ou conservées conformément à la législation et la réglementation en matière d'archivage à des fins historiques ou culturelles.

Article C.V.8.
Destinataires auxquels les données seront communiquées et les circonstances dans lesquelles elles leur seront communiquées

Les données à caractère personnel concernées par les traitements visés à l'article C.V.4. peuvent être communiquées :

1° aux Autorités publiques destinataires des partages administratifs;

2° aux réutilisateurs conformément au titre 3 du livre C.IV.;

3° aux Autorités publiques destinataires d'une Communication.

Article C.V.9.
Traçabilité des accès aux données

Le gestionnaire de la Plateforme assure la traçabilité des accès aux services du Centre d'intégration pour chaque Autorité publique. Il appartient ensuite à celle-ci d'organiser la traçabilité des accès internes par ses services et ses agents.

La traçabilité des accès aux données du Catalogue et au Portail ouvert des données est assurée par le gestionnaire de la Plateforme.

La traçabilité des accès aux services proposés par le Centre d'exploitation et d'analyse des données est organisée au cas par cas par le gestionnaire de la Plateforme ou par l'Autorité publique utilisatrice.

Article C.V.10.
Financement

§ 1er. – Paradigm, en sa qualité de gestionnaire de la Plateforme bruxelloise de la donnée, exerce ses missions dans les limites des redevances éventuellement perçues et du budget octroyé par le Gouvernement, le Collège réuni et le Collège, proportionnellement à l'activité de la Plateforme consacrée aux Autorités publiques relevant de leurs compétences respectives.

§ 2. – Le Gouvernement, le Collège réuni et le Collège établissent conjointement les modalités de calcul des redevances éventuelles pour l'utilisation des services de la Plateforme bruxelloise de la donnée et arrêtent conjointement leurs modalités de financement

Les redevances appliquées dans le cadre des réutilisations de données, notamment concernant les frais de diffusion des données, sont calculées conformément à l'article C.IV.25.

Le calcul de la redevance est publié par le gestionnaire sur la Plateforme bruxelloise de la donnée.

CHAPITRE 2
Le Centre d'intégration

Article C.V.11.
Création et objectif

§ 1er. – Il est créé un Centre d'intégration au sein de la Plateforme bruxelloise de la donnée.

L'objectif du Centre d'intégration est d'assurer techniquement les partages administratifs.

§ 2. – À chaque partage administratif, le gestionnaire de la Plateforme détermine le canal correspondant au type de données visées :

1° soit le canal correspondant aux partages administratifs visant des données issues de sources authentiques ou des données à caractère personnel;

2° soit le canal correspondant aux partages administratifs visant tous les autres types de données.

Le Gouvernement, le Collège réuni et le Collège peuvent déterminer conjointement les modalités techniques et opérationnelles des canaux du Centre d'intégration visés à l'alinéa 1er.

Article C.V.12.
La fonction d'intégrateur de services bruxellois

Paradigm est désigné en qualité d'intégrateur de services bruxellois dans le cadre de sa gestion du Centre d'intégration.

L'intégrateur de services a pour missions :

1° recevoir et donner, s'il y a lieu, suite aux demandes de consultation et de demande de partage des don-

nées enregistrées dans une ou plusieurs base(s) de données;

2° promouvoir et veiller à l'homogénéité des droits d'accès aux bases de données;

3° élaborer les modalités techniques visant à développer les canaux d'accès de la manière la plus efficace et la plus sûre possible;

4° promouvoir une politique de sécurité coordonnée pour le réseau;

5° procéder au partage administratif de données intégrées à la demande de l'Autorité publique destinataire;

6° développer pour les services publics participants des applications utiles à l'échange et/ou l'intégration de données conservées dans les banques de données;

7° organiser la collaboration avec d'autres intégrateurs de services.

CHAPITRE 3
Le Catalogue des données

Article C.V.13.
réation et objectifs

§ 1er. – Il est créé un Catalogue des données au sein de la Plateforme bruxelloise de la donnée.

Le Catalogue des données est un service composé :

1° d'un outil de gestion des métadonnées et des données de référence générées par les Autorités publiques, qui permet de dresser un inventaire des données détenues par les Autorités publiques, afin d'organiser une partie du Catalogue des données mise à la disposition des Autorités publiques par le gestionnaire de la Plateforme, et;

2° d'un outil de publication de la liste des données publiques et de leur catégorisation au regard de la typologie présentée au chapitre 3, du titre 2 du livre C.III, afin d'organiser une partie publique au Catalogue des données.

§ 2. – L'objectif du Catalogue des données est :

1° d'en réaliser un inventaire de l'ensemble des données détenues par les Autorités publiques permettant notamment d'identifier :

a) les données;

b) l'Autorité publique qui les détient;

c) leur catégorisation au regard de la typologie présentée au chapitre 3 du titre 2 du livre C.III;

d) les déclarations de principe visées à l'article C. III.12;

e) le cas échéant, les protocoles d'accord relatifs à des partages administratifs;

2° de fournir un glossaire;

3° de publier tout ou une partie de l'inventaire des données détenues par chaque Autorité Publique via l'outil de publication visé au paragraphe 1er, alinéa 2.

§ 3. – Les Autorités publiques utilisent l'outil de gestion du Catalogue des données afin de dresser l'inventaire des données qu'elles détiennent sous forme de métadonnées et de données de références qui peuvent être utilisées par le gestionnaire de la Plateforme en vue de leur intégration dans le Catalogue des données et sa partie publique.

CHAPITRE 4
Le Portail ouvert des données publiques

Article C.V.14.
Création et objectifs

§ 1er. – Il est créé un Portail ouvert des données publiques au sein de la Plateforme bruxelloise de la donnée.

Le Portail ouvert des données publiques propose les données disponibles à la réutilisation, notamment le cadastre des subsides, des marchés publics et des études visés à l'article B.I.4.

§ 2. – Les licences ouvertes ou les licences type relatives aux données réutilisables proposées par le Portail ouvert des données publiques sont disponibles dans le Portail ouvert des données publiques.

§ 3. – Pour chaque jeu de données ayant fait l'objet d'une réutilisation, le Portail ouvert des données publiques indique le nombre et l'identité des réutilisateurs.

CHAPITRE 5
Le Centre d'exploitation et d'analyse des données

Article C.V.15.
Création et objectifs

Il est créé un Centre d'exploitation et d'analyse des données.

L'objectif du Centre d'exploitation et d'analyse des données est de proposer, notamment aux Autorités publiques, en vue de la réalisation de leurs missions de service public, des services facultatifs fixés par le Gouvernement, le Collège réuni et le Collège.

CHAPITRE 6
Point de Contact et d'information

Article C.V.16.
Point de contact et d'information visé à l'article 8 du Règlement sur la gouvernance des données

Conformément à l'article 8 du Règlement sur la gouvernance des données, il est créé un Point de contact et d'information au sein de la Plateforme bruxelloise de la donnée.

L'objectif du Point de contact est de fournir des informations complètes et précises sur les données disponibles, les modalités de réutilisation et de fourniture de données ainsi que faciliter la Communication de données par des entités privées relevant notamment de l'altruisme de données.

Le cas échéant, le Point de contact reçoit ou redirige les plaintes conformément à l'article C.III.14 du présent Code.

CHAPITRE 7
Service d'appui

Article C.V.17.
Service d'appui visé à l'article 7 du Règlement sur la gouvernance des données

Un service d'appui et d'assistance est créé au sein de la Plateforme bruxelloise de la donnée; il fournit les services visés à l'article 7 du Règlement sur la gouvernance des données.

LIVRE C.VI
Les structures administratives de la gouvernance

TITRE 1
La gouvernance numérique

CHAPITRE 1
Champ d'application

Article C.VI.1.
Les Autorités publiques visées par le titre 1er

Le présent titre s'applique aux Autorités publiques visées à l'article A.I.3, 1), a), b), et h) et les associations formées par l'une ou plusieurs des Autorités visées au à l'article A.I.3, 1), a), b) et h).

CHAPITRE 2
Objectifs

Article C.VI.2.
La gouvernance numérique

§ 1er. – La gouvernance numérique a pour objectif d'optimiser la cohérence et la mutualisation de l'écosystème numérique bruxellois.

Dans ce cadre, la gouvernance numérique :

1° vérifie la conformité des projets et des achats ayant un impact sur l'écosystème numérique bruxellois par rapport à l'architecture numérique commune à la Région, la COCOM et la COCOF, ainsi que la potentielle mutualisation de ces projets et achats;

2° identifie les projets stratégiques qui comportent des composantes numériques ayant un impact sur l'écosystème numérique bruxellois à des fins de cohérence et de mutualisation pour la Région, la COCOM et la COCOF.

§ 2. – Les organes de gouvernance de l'écosystème numérique bruxelloise sont :

1° le Comité de coordination numérique;

2° le Comité de validation de l'architecture numérique.

Deux organes assurent un rôle support à la gouvernance numérique :

1° le Secrétariat numérique;

2° le Bureau des achats numériques.

CHAPITRE 3
Test d'autoévaluation numérique

Article C.VI.3.
Test d'autoévaluation numérique

§ 1er. – Afin de déceler et de faciliter les projets des Autorités publiques visées à l'article C.VI.1 qui comprennent une composante numérique ayant un impact sur l'écosystème numérique bruxellois et de recueillir l'avis des organes participant à la gouvernance numérique organisés dans le cadre du présent titre, un test est réalisé par lesdites Autorités publiques sous la forme d'un formulaire d'autoévaluation numérique.

Ce test est dénommé « test d'autoévaluation numérique ».

§ 2. – Sont soumis au test d'autoévaluation numérique, les projets des Autorités publiques visées à l'article C.VI.1 :

1° visant l'adoption de décisions relatives à l'écosystème numérique bruxellois soit par le Gouvernement, le Collège réuni et le Collège, en ce compris les avant-projets d'ordonnance, de décret ou d'arrêté, soit par l'organe de gestion des Autorités publiques visées à l'article C.VI.1;

2° ou visant une procédure de commande publique relative à l'écosystème numérique bruxellois et dont le montant estimé global est au minimum visé à l'article 5, 10°, 1), 7e tiret, de l'arrêté du 18 juillet 2000 de la Région de Bruxelles-Capitale portant règlement de son fonctionnement et réglant la signature des actes du Gouvernement.

Le contenu du test d'autoévaluation numérique ainsi que la procédure associée à ce test sont fixés conjointement par le Gouvernement de la Région de Bruxelles Capitale, le Collège réuni et le Collège.

Les résultats des tests sont ensuite transmis au Secrétariat numérique pour examen.

CHAPITRE 4
Les organes de la gouvernance numérique

SECTION 1
Le Secrétariat numérique

Article C.VI.4.
Création et missions du Secrétariat numérique

§ 1er. – Le Secrétariat numérique, créé au sein de Paradigm, assure le secrétariat du Comité de coordination numérique et du Comité de validation de l'architecture numérique.

Il assure l'interface entre ces deux comités, d'une part, et les Autorités publiques visées à l'article C.VI.1, d'autre part.

§ 2. – Le Secrétariat numérique reçoit les tests d'autoévaluation visés à l'article C.VI.3 et en examine les résultats.

En fonction de l'examen qu'il aura réalisé des résultats du test d'autoévaluation, le Secrétariat numérique sollicite l'avis de l'un ou de plusieurs des organes consultatifs suivants :

1° le Bureau d'achat numérique;

2° le Comité de validation de l'architecture numérique;

3° le Bureau de la donnée.

À la demande d'avis du Secrétariat numérique, est joint le test d'autoévaluation complété et le projet ou achat visé à l'article C.VI.3, § 2, qui y a été soumis, de même que, le cas échéant, une brève analyse des résultats de ce test réalisé par le Secrétariat numérique pour justifier sa demande d'avis à l'un ou plusieurs des organes visés à l'alinéa 2.

Le Secrétariat numérique rassemble ensuite les avis de chaque organe visé à l'alinéa 2 consulté et les transmet d'office au Comité de coordination numérique, accompagnés des résultats du test d'autoévaluation et du projet visé à l'article C.VI.3, § 2, qui y a été soumis.

Article C.VI.5.
Financement et contrôle

§ 1er. – Le Secrétariat numérique effectue ses missions en faveur des Autorités publiques visées à l'article C.VI.1.

§ 2. – Le Secrétariat numérique transmet tous les deux ans un rapport d'activités au Ministre compétent à l'égard de Paradigm et aux Ministres compétents en matière de gouvernance numérique du Collège réuni et du Collège.

Ce rapport d'activités est également adressé au Comité de coordination numérique.

SECTION 2
Le Comité de validation de l'architecture numérique

Article C.VI.6.
Compétence et composition
du Comité de validation de l'architecture numérique

§ 1er. – Le Comité de validation de l'architecture numérique est responsable de la gouvernance de l'architecture numérique régionale à des fins de cohérence et de mutualisation.

§ 2. – Afin de réaliser sa mission visée au paragraphe 1er, le Comité de validation de l'architecture numérique :

1° remet des avis sur les projets visé à l'article C.VI.3, § 2, soumis au test d'autoévaluation numérique qui lui ont été transmis par le Secrétariat numérique conformément à l'article C.VI.4, § 2, alinéa 2;

2° remet des avis sur les demandes adressées par le Bureau d'achats numériques conformément à l'article C.VI.9, § 4;

3° remet, d'initiative ou à la demande, des avis au Comité de coordination numérique, au Bureau d'achats numériques et au Bureau de la donnée.

§ 3. – Le Comité de validation de l'architecture numérique est composé par :

1° des membres permanents qui représentent, parmi les Autorités Publiques visées à l'article C.VI.1 :

a) Actiris;

b) Bruxelles Environnement;

c) Bruxelles Fiscalité;

d) Bruxelles Formation;

e) Bruxelles Propreté;

f) Paradigm;

g) Parking.brussels;

h) SPRB;

i) COCOF;

j) STIB;

2° des membres non permanents qui représentent les autres Autorités publiques visées à l'article C.VI.1, en dehors des 10 membres permanents.

Les membres permanents ou non permanents sont représentés, au sein du Comité de validation de l'architecture numérique, par des représentants désignés par chaque membre en fonction du point à l'ordre du jour de la réunion. Les membres désignent les personnes présentant la plus grande compétence technique en la matière.

Les membres permanents sont présents à chaque réunion du Comité de validation de l'architecture numérique. Toute absence doit être justifiée.

Les membres non permanents sont invités aux réunions. Leur participation est facultative. Ils informent préalablement le Secrétariat numérique de leur participation.

Les membres du Comité de validation de l'architecture numérique peuvent inviter toute personne physique, personne morale de droit public ou de droit privé, dont la présence est jugée pertinente en fonction de l'ordre du jour des réunions.

Le Comité de validation de l'architecture numérique adopte son règlement d'ordre intérieur afin de définir son fonctionnement.

Article C.VI.7.
Rapport d'activités

Le Comité de validation de l'architecture numérique transmet tous les deux ans un rapport d'activités au Gouvernement, au Collège réuni et au Collège.

Ce rapport d'activités est également adressé au Comité de coordination numérique.

SECTION 3
Le Bureau d'achats numériques

Article C.VI.8.
Le Bureau d'achats numériques

Le Bureau d'achats numériques, créé au sein de Paradigm, fournit tout appui opérationnel, légal ou technique, aux Autorités publiques visées à l'article C.I.1, concernant les processus de commande publique numérique mutualisable.

Article C.VI.9.
Les missions du Bureau d'achats numériques

§ 1er. – Le Bureau d'achats numériques a pour mission générale :

1° de fournir une assistance nécessaire à toute Autorité publique dans le cadre de tout processus de commande publique numérique mutualisable susceptible d'affecter l'écosystème numérique bruxellois;

2° de proposer au Gouvernement, au Collège Réuni et au Collège qui les arrêtent conjointement, les critères de mutualisation pertinents en matière de commande publique numérique dans le cadre de l'écosystème numérique bruxellois ainsi que les modalités applicables aux commandes publiques numériques jugées mutualisables;

3° d'analyser les déclarations de besoins numériques pluriannuels visés au paragraphe 2 et les formulaires de besoins numériques visés au paragraphe 3 au regard des critères de mutualisation arrêtés conjointement par le Gouvernement, le Collège réuni et le Collège et en déterminer leur caractère mutualisable conformément à ces critères;

4° de recommander aux Autorités publiques les modalités applicables aux commandes publiques numériques mutualisables conformément à l'arrêté conjoint visés au point 2°;

5° de remettre des avis sur les projet soumis au test d'autoévaluation numérique qui lui ont été transmis par le Secrétariat numérique conformément à l'article C.VI.4, § 2, alinéa 2;

6° de remettre, d'initiative ou à la demande, des avis au Comité de validation de l'architecture numérique, au Comité de coordination numérique et au Bureau de la donnée.

§ 2. – Les Autorités publiques visées à l'article C.VI.1 transmettent au Bureau d'achats numériques leurs déclarations de besoins numériques pluriannuelles.

Les Autorités publiques visées à l'article C.I.1, autres que les Autorités publiques visées à l'article C.VI.1, peuvent transmettre d'initiative au Bureau d'achats numériques leurs déclarations de besoins numériques pluriannuelles.

La déclaration de besoins numériques pluriannuelles soumise par une Autorité publique, visée à l'alinéa 1er et 2, au Bureau d'achats numériques peut être mise à jour à tout moment, et doit être mise à jour au minimum une fois par an.

§ 3. – Lorsqu'un projet de commande publique numérique n'est pas repris dans la déclaration de besoins numériques pluriannuelles, les Autorités publiques visées à l'article C.VI.1 doivent transmettre au Bureau d'achats numériques dès que possible, ce projet de commande publique au travers d'un formulaire de besoins numériques, à déterminer par le Bureau d'achats numériques, décrivant de manière circonstanciée le besoin numérique auquel elle est confrontée en dehors de sa déclaration de besoins numériques pluriannuelle.

Lorsqu'un projet de commande publique numérique n'est pas repris dans la déclaration de besoins numériques pluriannuelles, les Autorités publiques visées à l'article C.I.1, autres que celles visées à l'article C.VI.1, peuvent transmettre, à tout moment, d'initiative, un ou plusieurs besoins numériques au travers d'un formulaire de besoins numériques, décrivant de manière circonstanciée le besoin numérique auquel elle est confrontée en dehors de sa déclaration de besoins numériques pluriannuelle.

§ 4. – Dans le cadre de son analyse des déclarations de besoins numériques pluriannuelles et des formulaires de besoins numériques conformément au paragraphe 1er, 3e tiret, le Bureau d'achats peut demander l'avis :

1° du Comité de validation de l'architecture numérique;

2° du Bureau de la donnée;

3° du Comité de coordination.

§ 5. – Dans l'hypothèse où le Bureau d'achats numériques confirme auprès des Autorités publiques concernées le caractère mutualisable de leur projet, il peut recommander l'application d'un test d'autoévaluation numérique conformément à l'article C.VI.3 si les critères visés à l'article C.VI.3, § 2, sont rencontrés.

Article C.VI.10.
Financement et contrôle

§ 1er. – La Région bruxelloise, la COCOM et la COCOF participent au financement du Bureau des achats numériques proportionnellement à l'importance de l'activité du Bureau en faveur des Autorités publiques visées à l'article C.I.1 ou à l'article C.VI.1 relevant de leurs compétences respectives.

Le Gouvernement, le Collège réuni et le Collège arrêtent conjointement les modalités relatives au financement du Bureau d'achats numériques à charge de la Région, de la COCOM et de la COCOF et, le

cas échéant, des Autorités publiques visées à l'article C.I.1 ou à l'article C.VI.1 qui en dépendent.

§ 2. – Le Bureau d'achats numériques transmet annuellement un rapport d'activités au Ministre compétent à l'égard de Paradigm et aux Ministres compétents en matière numérique du Collège réuni et du Collège.

Ce rapport d'activités est également adressé au Comité de coordination.

SECTION 4
Le Comité de coordination numérique

Article C.VI.11.
Compétences et composition
du Comité de coordination numérique

§ 1er. – Le Comité de coordination numérique analyse stratégiquement tous les projets visés à l'article C.VI.3, § 2, soumis au test d'autoévaluation numérique visés qui ont été préalablement analysés par le Bureau d'achats numériques, le Comité de validation de l'architecture numérique, et le Bureau de la donnée, ou seulement par certains de ces organes consultatifs.

Le Comité de coordination numérique remet, selon le cas, au Gouvernement, au Collège réuni, au Collège, ou aux organes de gestions compétents, des avis relatifs aux projets pour lesquels il a été saisi ainsi que les procès-verbaux de ses réunions.

Il peut remettre, d'initiative ou à la demande, des avis aux autres organes de gouvernance numérique, au Gouvernement, au Collège réuni, au Collège, et aux organes de gestion des Autorités publiques visées à l'article C.VI.1.

§ 2. – Le Comité de coordination numérique est composé par :

1° des membres permanents qui représentent, parmi les Autorités Publiques visées à l'article C.VI.1 :

a) Actiris;

b) Bruxelles Environnement;

c) Bruxelles Fiscalité;

d) Bruxelles Formation;

e) Bruxelles Propreté;

f) Paradigm;

g) Parking.brussels;

h) SPRB;

i) COCOF;

j) STIB;

2° des membres non permanents qui représentent les autres Autorités publiques visées à l'article C.VI.1, en dehors des 10 membres permanents.

Les membres permanents sont présents à chaque réunion. Toute absence doit être justifiée.

Les membres non permanents sont invités aux réunions. Leur participation est facultative. Ils informent préalablement le Secrétariat numérique de leur participation.

Les membres permanents et non permanents du Comité de coordination numérique sont représentés par la personne compétente pour engager stratégiquement en matière numérique l'Autorité publique concernée.

Les membres du Comité de coordination numérique peuvent inviter toute personne physique, personne morale de droit public ou de droit privé, dont la présence est jugée pertinente en fonction de l'ordre du jour des réunions.

Le Comité de coordination numérique adopte son règlement d'ordre intérieur.

Article C.VI.12.
Rapport d'activités

Le Comité de la coordination numérique transmet tous les deux ans un rapport d'activités au Gouvernement, au Collège réuni et au Collège.

TITRE 2
La gouvernance de la donnée

CHAPITRE 1
Objectifs

Article C.VI.13.
Objectifs

La gouvernance de la donnée se centre sur la mise en œuvre quotidienne, pratique et opérationnelle du Code.

CHAPITRE 2
Les organes de la gouvernance de la donnée

SECTION 1
Le Comité de gouvernance de la donnée

Article C.VI.14.
Composition du Comité de gouvernance de la donnée

§ 1er. – Le Comité de gouvernance de la donnée est le lieu de concertation entre les Autorités publiques visées à l'article C.I.1 quant à l'implémentation du Code.

§ 2. – Le Comité de gouvernance de la donnée est composé :

1° du coordinateur de la donnée du Bureau de la donnée visé à l'article C.VI.19, § 1er;

2° des Administrateurs locaux de la donnée au sein des Autorités publiques visées à l'article C.I.1 reprises dans les paliers 1 et 2 conformément à l'arrêté fixant les seuils numériques;

3° d'un ou plusieurs représentant(s) du service compétent pour la simplification administrative;

4° des représentants du gestionnaire de la Plateforme bruxelloise de la donnée.

Les membres du Comité de gouvernance de la donnée peuvent inviter toute personne physique, personne morale de droit public ou de droit privé, dont la présence est jugée pertinente en fonction de l'ordre du jour des réunions.

Afin d'organiser la discussion sur des thématiques précises, le Comité de gouvernance de la donnée peut instituer en son sein des groupes de travail ne comprenant que certains de ses membres et le cas échéant des invités *ad hoc*.

Article C.VI.15.
Missions

§ 1er. – Le Comité de gouvernance de la donnée a pour objectifs :

1° de fixer les objectifs opérationnels du Bureau de la donnée;

2° de communiquer au Bureau de la donnée les besoins et les priorités des Autorités publiques visées à l'article C.I.1;

3° de susciter le partage d'expérience et la présentation des projets réalisés au sein des Autorités publiques visées à l'article C.I.1;

4° de revoir et valider les standards, bonnes pratiques et modèles soumis pour proposition par le Bureau de la Donnée, notamment en matière d'interopérabilité;

5° de s'assurer de l'opérationnalité des dispositions du Code en se concertant sur l'ensemble des points nécessitant des responsabilités claires, notamment la désignation de commun accord de l'identité de la ou des Autorités publiques investies de la responsabilité de la gestion d'un domaine spécifique de données.

§ 2. – Le Comité de gouvernance de la donnée élabore la stratégie pluriannuelle de la donnée ainsi que les plans d'action annuels en concertation avec le Bureau de la donnée.

La stratégie pluriannuelle de la donnée ainsi que les plans d'actions annuels sont approuvés conjointement par le Gouvernement, le Collège réuni et le Collège.

§ 3. – Par arrêté conjoint, le Gouvernement, le Collège réuni et le Collège peuvent attribuer d'autres missions complémentaires aux missions visées au paragraphe 1er. Le Gouvernement de la Région bruxelloise, le Collège réuni et le Collège définissent conjointement les conditions selon lesquelles le Comite de gouvernance de la donnée exerce ces missions complémentaires.

Article C.VI.16.
Fonctionnement

§ 1er. – Le Comité de gouvernance de la donnée se réunit au moins huit fois par an et à chaque demande conjointe d'au minimum cinq membres de cinq Autorités publiques différentes.

§ 2. – Le Comité de gouvernance de la donnée adopte un règlement d'ordre intérieur.

SECTION 2
Le Bureau de la donnée

Article C.VI.17.
Création du Bureau de la donnée

Il est créé un Bureau de la donnée au sein de Paradigm.

Le Bureau de la donnée coordonne et supervise la mise en œuvre transversale et opérationnelle de la gouvernance de la donnée décrite par le Code au sein des Autorités publiques et entre elles.

Article C.VI.18.
Missions du Bureau de la donnée

Le Bureau de la donnée est investi des missions suivantes exercées en concertation avec le Comité de Gouvernance de la donnée :

1° une mission d'appui administratif, de secrétariat et d'animation du Comité de gouvernance de la Donnée conformément aux objectifs opérationnels fixé par le Comité de gouvernance de la donnée en vertu de l'article C.VI.15, § 1er, 1°;

2° une mission d'intégration de la gouvernance de la donnée au sein de la gouvernance numérique par la rédaction d'avis :

a) d'initiative ou à la demande du Bureau d'achats numériques, du Comité de validation de l'architecture numérique ou, du Comité de gouvernance de la donnée ou du Comité de coordination numérique;

b) sur les projet soumis au test d'autoévaluation numérique qui lui ont été transmis par le Secrétariat numérique conformément à l'article C. VI.4, § 2, alinéa 2;

3° une mission de coordinateur de la donnée, avant validation par le Comité de gouvernance de la donnée, notamment au travers de :

a) la proposition de modèles standard de documents en matière de déclaration de principes visée à l'article C.III.12, de protocole d'accord visé à l'article C.IV.9;

b) la proposition de de licences types au Gouvernement, Collège réuni et Collège conformément à l'article C.IV.26;

c) l'organisation d'un cadre pour la gestion de l'interopérabilité au sens de l'article C.II.17;

4° une mission d'accompagnement à la mise en œuvre des obligations du Code en matière de gestion de la donnée notamment au travers de :

a) la contribution à la compréhension par tous les acteurs et opérateurs de la Plateforme bruxelloise de la donnée des enjeux de la sécurité et de la protection des données au sens du chapitre 2 du titre 4 du livre C.III;

b) la proposition de directives, de standards, de cadres et de lignes directrices à faire approuver par le Comité de gouvernance de la donnée;

c) la promotion d'instruments de politiques internes aux Autorités publiques concernant la gestion des données au sens du chapitre 1er du titre 4 du livre C.III, en ce compris la gestion des modèles analytiques, des algorithmes et des systèmes exploitant l'intelligence artificielle au sens de l'article C.III.20;

5° une mission d'initiateur du changement au travers de :

a) la mise en place de communautés de pratiques;

b) l'organisation de formations visant à améliorer les compétences régionales en matière de gestion des données;

c) l'organisation d'événements visant à augmenter la culture des données au sein de la Région bruxelloise, de la COCOM et de la COCOF;

6° une mission de support aux Autorités publiques au travers de la mise à disposition d'experts en gouvernance de la donnée lorsque les Autorités publiques ne disposent pas des ressources suffisantes;

7° une mission de veille et d'explication pour l'ensemble des Autorités publiques, notamment en ce qui concerne le suivi de la réglementation et des initiatives, projets et financements européens, et leur transposition ou leur implémentation éventuelle au niveau national ou bruxellois.

Article C.VI.19.
Fonctionnement, contrôle et financement

§ 1er. – Le Bureau de la donnée est placé sous la responsabilité d'un coordinateur de la donnée.

§ 2. – Le Bureau de la donnée effectue ses missions au service des Autorités publiques de la Région bruxelloise, de la COCOM et de la COCOF.

Le Ministre compétent à l'égard de Paradigm et les Ministres compétents en matière numérique du Collège réuni et du Collège définissent conjointement les objectifs stratégiques du Bureau de la donnée et en vérifient annuellement l'application.

§ 3. – La Région bruxelloise, la COCOM et la COCOF participent au financement du Bureau de la donnée proportionnellement à l'importance de l'acti-

vité du Bureau en rapport avec les Autorités publiques relevant de leurs compétences respectives.

Le Gouvernement, le Collège réuni et le Collège arrêtent conjointement les modalités relatives au financement du Bureau de la donnée à charge de la Région, de la COCOM et de la COCOF ou des Autorités publiques qui en dépendent.

§ 4. – Le Bureau de la donnée communique au moins deux fois par an l'état d'avancement de ses travaux au Comité de coordination numérique.

§ 5. – Le Bureau de la donnée transmet et présente annuellement un rapport d'activités au Ministre compétent à l'égard de Paradigm et aux Ministres compétents en matière numérique du Collège réuni et du Collège.

TITRE 3
Les ressources de la gouvernance de la donnée au sein des Autorités publiques

Article C.VI.20.
Création des fonctions de gouvernance de la donnée

Chaque Autorité publique désigne :

1° un administrateur local de la donnée visé à l'article C.VI.21;

2° un ou plusieurs responsables de la donnée visés à l'article C.VI.22;

3° un conseiller de sécurité de l'information visé à l'article C.VI.23.

Un groupe d'Autorités publiques peut désigner conjointement les personnes assurant les fonctions visées au premier alinéa pour autant que cela ne compromette par le respect du Code et l'implémentation du Plan stratégique visé à l'article C.VI.15, § 2, et que cela soit cohérent par rapport à la structure organisationnelle et à la taille des Autorités publiques concernées.

Les personnes en charge des fonctions visées au premier alinéa peuvent être un membre du personnel de l'Autorité publique ou un sous-traitant, ou exercer ses missions sur la base d'un contrat de service.

Pour les Autorités publiques faisant partie du palier 3 défini par l'arrêté fixant les seuils numériques, la fonction d'administrateur local de la donnée et la fonction de conseiller de sécurité de l'information peuvent être cumulées par la même personne.

Article C.VI.21.
L'administrateur local de la donnée

§ 1er. – L'Administrateur local de la donnée est le pivot et principal organisateur de la gouvernance des données au sein de l'Autorité publique qui l'a désigné.

Il identifie les besoins et définit la stratégie interne de l'Autorité publique, en conformité avec la stratégie pluriannuelle de la donnée et les plans d'actions annuels visés à l'article C.VI.15, § 2, et veille à son implémentation.

Il définit et veille à l'implémentation du modèle opérationnel interne à l'Autorité publique définissant la gouvernance interne ainsi que les rôles et responsabilités des différents acteurs de la donnée tel que décrit dans la déclaration de principes visées à l'article C.III.12

§ 2. – L'administrateur local de la donnée est investi des missions suivantes :

1) une mission à l'égard de l'Autorité publique qui l'a désigné, sous réserve, le cas échéant, d'une validation par l'organe légalement compétent en la matière, au regard de :

   a) l'identification des besoins et la définition d'une stratégie interne à l'Autorités publique, en adéquation avec la stratégie pluriannuelle de la donnée ainsi que les plans d'action annuels visés à l'article C.VI.15;

   b) la détermination des domaines de données gérés par l'Autorité publique;

   c) la mise en œuvre des objectifs stratégiques rappelés aux articles C.II.6 et suivants;

   d) la mise en œuvre des obligations relatives à la gestion de la donnée visées aux articles C.III.16 et suivants, en ce compris en organisant la répartition des responsabilités entre les parties et en collaborant avec le responsable de la donnée et le Conseiller en sécurité de l'information;

   e) la proposition de toute mesure technique ou organisationnelle pertinente concernant l'infrastructure ou l'architecture des données;

   f) la documentation de l'ensemble des processus et règles opérationnelles, protocoles d'accord, déclaration de principes propres à l'Autorité publique qui l'a désigné afin d'alimenter le Catalogue des données, le cas échéant en collaboration avec le responsable de la donnée de chacun des domaines de données concernés;

2) une mission à l'égard des tiers à l'Autorité publique qui l'a désigné, en matière d'organisation d'un point de contact unique en matière de gouvernance de la donnée;

3) une mission à l'égard du Bureau de la donnée, au regard de :

   a) la fourniture de toute information pertinente, d'initiative ou sur demande, quant à l'exercice de ses missions;

   b) la collecte de l'information mise à disposition par le Bureau concernant les processus, les normes et les meilleures pratiques que l'administrateur local de la donnée se chargera de transmettre au responsable de la donnée;

4) une mission à l'égard des autres Autorités publiques visées par le présent Code, le cas échéant au travers du Comité de Gouvernance de la donnée quant à :

   a) l'assurance d'une harmonisation horizontale des domaines de données qui concernent plusieurs Autorités publiques;

   b) la communication, si nécessaires, de la documentation établie par lui;

   c) la collaboration et le dialogue entre les administrateurs locaux de la donnée.

§ 3. – L'Autorité publique peut confier à l'administrateur local de la donnée toute autre mission complémentaire aux missions énoncées au premier paragraphe.

Article C.VI.22.
Le responsable de la donnée

§ 1er. – Le responsable de la donnée est chargé d'un ou plusieurs domaines de données.

Le responsable de la donnée travaille sous la supervision de l'administrateur local de la donnée et en collaboration avec le Délégué à la protection des données et le Conseiller en sécurité de l'information.

§ 2. – Le responsable de la donnée est investi des missions suivantes concernant le ou les domaines de données desquels il est chargé :

1° une mission d'implémentation, notamment au regard de la stratégie interne définie par l'Administrateur local de la donnée et approuvée par l'organe légalement compétent, ou de toute autre mesure technique ou organisationnelle pertinente;

2° une mission d'évaluation continue des mesures mises en place au regard des politiques, normes et meilleures pratiques dans chacun du ou des domaines de données, en vue de leur amélioration;

3° une mission de contrôle du respect des mesures mises en place dans chacun du ou des domaines de données, par toute personne;

4° une mission de promotion et de diffusion des politiques, normes et meilleures pratiques mises en place par l'Autorité publique qui l'a désigné;

5° une mission de maintenance et de supervision des ressources nécessaires à la gestion des données relevant du ou des domaines de données concernés;

6° une mission de documentation, notamment à l'égard de toute mesure opérationnelle mise en place.

Article C.VI.23.
Le conseiller en sécurité de l'information

§ 1er. – Chaque Autorité publique désigne un conseiller en sécurité de l'information.

Le conseiller en sécurité de l'information travaille en collaboration avec l'administrateur local de la donnée, le Délégué à la protection des données et le responsable de la donnée.

§ 2. – Le conseiller en sécurité de l'information est investi de missions qui concernent notamment les obligations relatives à la sécurité et à la protection des données telles que définies au chapitre 2 du titre 4 du livre C.III :

1. une mission d'analyse de risque et d'implémentation de toute mesure opérationnelle pertinente, toute norme ou toute obligation en matière de sécurité;

2. une mission de vérification de la mise en œuvre effective de toute mesure opérationnelle pertinente, toute norme ou toute obligation en matière de sécurité;

3. une mission d'alerte concernant tout risque pour la sécurité et leur incidence sur la confidentialité, l'intégrité et la disponibilité des ressources d'information;

4. une mission d'avis, d'initiative ou sur demande, concernant toute question relative à la sécurité des données;

5. une mission de collaboration avec les conseillers en sécurité d'autres Autorités publiques, le cas échéant au travers du Comite de gouvernance de la donnée;

6. une mission de sensibilisation, au sein de son Autorité publique et à l'égard de tout tiers, concernant la sécurité et la protection des données.

TITRE III
Dispositions finales

Article 3

Les livres B.I. et B.II entrent en vigueur six mois après la publication des présents décret et ordonnance conjoints.

Article 4

Les livres C.IV et C.V entrent en vigueur six mois après la publication des présents décret et ordonnance conjoints pour les Autorités publiques regroupées dans les paliers n° 1 et 2 définis par l'arrêté fixant les seuils numériques.

Le titre II du livre C.III et le chapitre 2 du titre IV du même livre du Code de la gouvernance et de la donnée entrent en vigueur un an après la publication des présents décret et ordonnance conjoints pour les Autorités publiques regroupées dans les paliers n° 1 et 2 définis par l'arrêté fixant les seuils numériques.

Le chapitre I du titre III du livre C. III du Code de la Gouvernance et de la donnée entre en vigueur deux ans après la publication des présents décret et ordonnance conjoints pour les Autorités publiques regroupées dans les paliers n° 1 et 2 définis par l'arrêté fixant les seuils numériques.

Article 5

Les livres C.II., C.III, C.IV, à l'exception du titre III, C.V, et C.VI du Code de la gouvernance et de la donnée entrent en vigueur deux ans après la publication des présents décret et ordonnance conjoints pour les Autorités publiques regroupées dans le palier n° 3 défini par l'arrêté fixant les seuils numériques.

Seul le titre III du livre C.IV entre en vigueur six mois après la publication des présents décret et ordonnance conjoints pour les Autorités publiques regroupées dans le palier n° 3 défini par l'arrêté fixant les seuils numériques.

Article 6

Toutes les compétences dévolues à la Commission d'accès aux documents administratifs instituée par les Décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française relatifs à la publicité de l'administration dans les institutions bruxelloises sont exercées dès son entrée en vigueur par la Commission d'accès aux documents administratifs et aux données, dénommée la CADADo et instituée par le livre B.II du Code de la gouvernance et de la donnée.

La CADADo reprend l'ensemble des droits et obligations précédemment détenues par la CADA.

Les membres de la Commission d'accès aux documents administratifs instituée par les décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française relatifs à la publicité de l'administration dans les institutions bruxelloises poursuivent leur mandat au sein de la chambre relative à l'accès aux documents administratifs de la Commission d'accès aux documents administratifs et aux données instituée par le livre B.II du Code de la gouvernance et de la donnée.

Le Gouvernement, le Collège réuni et le Collège désignent conjointement conformément à l'article B.II.8 quatre nouveaux membres pour former la chambre relative au partage administratif de données et la chambre relative à la réutilisation de données, dans les six mois suivants la publication du présent décret et ordonnance conjoints. Les mandats de ces nouveaux membres s'achèvent en même temps que celui des membres visés à l'alinéa 3 qui poursuivent leur mandat.

Le secrétariat de la CADADo visé à l'article B.II.5 est désigné dans les six mois suivants la publication du présent décret et ordonnance conjoints.

Les experts visés à l'article B.II.7 doivent également être désignés dans les six mois suivants la publication du présent décret et ordonnance conjoints.

Les recours et les demandes de consultation introduits avant la date d'entrée en vigueur des livres B.I, B.II, C.IV et C.V. devant la Commission d'accès aux documents administratifs instituée par les décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française relatifs à la publicité de l'administration dans les institutions bruxelloises, visés à l'article 25 desdits décret et ordonnance conjoints du 16 mai 2019, de même que les recours introduits avant la même date et visés à l'article 7 de l'ordonnance du 27 oc-

tobre 2016 visant à l'établissement d'une politique de données ouvertes (Open Data) et portant transposition de la Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, sont poursuivis par la chambre relative à l'accès aux documents administratifs de la CADADo visée dans le livre A.II du Code de la gouvernance et de la donnée.

Article 7

Les membres de la Commission d'accès aux documents administratifs instituée par les Décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française relatifs à la publicité de l'administration dans les institutions bruxelloises, devenus les membres de la Chambre d'accès aux documents administratifs de la CADADo après l'entrée en vigueur des livres B.I et B.II, perçoivent des jetons conformément à l'article B.II.9 pour l'ensemble des dossiers clôturés après l'entrée en vigueur des livres B.I et B.II du Code, mais introduits avant l'entrée en vigueur desdits livres.

Article 8

Dans l'attente de la détermination, par les autorités administratives, de la rétribution qui peut éventuellement être exigée pour la délivrance d'un document administratif ou d'une information environnementale sous forme de copie, les montants maximum suivants sont applicables :

– 0,01 euro, par face, pour un document au format A4 en noir et blanc;

– 0,02 euro, par face, pour un document supérieur au format A4, mais ne dépassant pas le format A3, en noir et blanc;

– 0,04 euro, par face, pour un document au format A2, en noir et blanc;

– 0,08 euro, par face, pour un document au format A1, en noir et blanc.

Les montants précités sont triplés pour les copies en couleur.

Si une rétribution est exigée, le prix de la copie plus celui du coût de sa communication sur place ou par envoi postal ou autre moyen de transmission est fixé à un minimum de 1 euro.

Article 9

Les décisions, les actes et les documents qui doivent faire l'objet d'une publicité active en vertu du livre B.I du Code de la gouvernance et de la donnée sont ceux qui sont adoptés après l'entrée en vigueur dudit livre.

Article 10

L'ordonnance du 17 juillet 2020 de la Région de Bruxelles-Capitale garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité, et portant simplification et harmonisation des formulaires électroniques et papier, est abrogée six mois après l'entrée en vigueur des présents décret et ordonnance conjoints.

Les décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française relatifs à la publicité de l'administration dans les institutions bruxelloises sont abrogés six mois après l'entrée en vigueur des présents décrets et ordonnances conjoints.

L'ordonnance du 27 octobre 2016 de la Région de Bruxelles-Capitale visant à l'établissement d'une politique de données ouvertes (Open Data) et portant transposition de la Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public est abrogée six mois après l'entrée en vigueur des présents décrets et ordonnances conjoints.

L'ordonnance du 8 mai 2014 de la Région de Bruxelles-Capitale portant création et organisation d'un intégrateur de services régional est abrogée six mois après l'entrée en vigueur des présents décrets et ordonnances conjoints.

L'accord de coopération du 28 février 2019 entre la Région de Bruxelles-Capitale et la COCOM portant sur la désignation d'un intégrateur de services commun pour l'échange électronique de données est abrogé six mois après l'entrée en vigueur des présents décrets et ordonnances conjoints.

Article 11

Pour l'application de l'article C.IV.26, les Autorités publiques utilisent les licences prévues au Chapitre II de l'arrêté du Gouvernement de la Région de Bruxelles-Capitale du 1er février 2018 portant exé-

cution de l'ordonnance du 27 octobre 2016 visant à l'établissement d'une politique de données ouvertes (open data) et portant transposition de la Directive 2013/37/UE du Parlement européen et du conseil du 26 juin 2013 modifiant la Directive 2003/98/CE du Parlement européen et du conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, jusqu'à ce que celui-ci soit abrogé.

Bruxelles le 18 avril 2024

Pour a Commission communautaire française,

La Présidente du Collège, membre du Collège en charge de la Fonction Publique,

Barbara TRACHTE

Annexes

Annexe 1

Liste des catégories thématiques d'ensembles de données de forte valeur visée à l'article C.IV.30 du Code :

1. Géospatiales

2. Observation de la terre et environnement

3. Météorologiques

4. Statistiques

5. Entreprise et propriété d'entreprises

6. Mobilité

Annexe 2

Tableau de concordance

Directive 2019/1024	Code de la gouvernance et de la donnée
Art. 1, 1. et 2.	Art. C. IV. 19
Art. 2 1) 2) 3) 4) 5) 6) 7) 8) 9) 10) 11) 12) 13) 14) 15) 16) 17)	 Art. A.I.3. 1), a), b), c), h), i) 62) 63) 90) 7) 76) 26) 27) 14 70) 91) 85) 92) 93) 64)
Art. 3	Art. C. IV. 21
Art. 4	Art. C. IV. 22 Art. C.IV. 13
Art. 5	Art. C. IV. 24
Art. 6	Art. C. IV. 25, § 1er, § 2, §§ 4 à 7
Art. 7.	Art. C. IV.25 § 3
Art. 8	Art. C. IV. 26
Art. 9	Art. C. IV.
Art. 10	Art. C. IV. 27
Art. 11	Art. C. IV. 28
Art. 12	Art. C. IV. 29
Art. 13	Art. C. IV. 30

ANNEXE 1

AVIS N° 75.207/VR DU CONSEIL D'ÉTAT DU 25 MARS 2024

Le Conseil d'État, section de législation, saisi par la Présidente du Collège de la Commission communautaire française, chargée de la promotion de la santé, des Familles, du Budget et de la Fonction publique, le 22 décembre 2023, d'une demande d'avis, dans un délai de trente jours prorogé à quarante cinq jours (*), sur un avant-projet de décret et ordonnance conjoints « portant le Code de la gouvernance et de la donnée », a donné l'avis suivant :

1. En application de l'article 84, § 3, alinéa 1er, des lois sur le Conseil d'État, coordonnées le 12 janvier 1973, la section de législation a fait porter son examen essentiellement sur la compétence de l'auteur de l'acte, le fondement juridique (1) et l'accomplissement des formalités prescrites.

PORTÉE DE L'AVANT-PROJET

2. L'avant-projet de décret et ordonnance conjoints de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française soumis pour avis a pour objet d'introduire, en ce qui concerne la Commission communautaire française, un Code de la gouvernance et de la donnée (article 2 de l'avant-projet). Le Code en projet comporte trois parties.

2.1. La partie A compte deux livres et contient toutes les définitions du Code, ainsi qu'un certain nombre de dispositions communes à l'ensemble du Code.

2.2. La partie B est constituée de deux livres et comporte des dispositions relatives à la gouvernance administrative.

Le livre B.I renferme des définitions en matière de publicité de l'administration. Il a pour objet de renforcer la transparence de l'administration en facilitant l'accès aux documents administratifs et aux informations environnementales et vise également à transposer partiellement la directive 2003/4/CE du Parlement européen et du Conseil du 28 janvier 2003 « concernant l'accès du public à l'information en matière d'environnement et abrogeant la directive 90/313/CEE du Conseil ».

Le livre B.II vise également à transposer partiellement la directive 2003/4/CE et transforme l'actuelle Commission d'accès aux documents administratifs (CADA) de la Région de Bruxelles-Capitale (2) en une Commission d'accès aux documents administratifs et aux données (CADADo). Dorénavant, cette Commission constituera non seulement l'organe de recours pour les demandes d'accès aux documents administratifs, mais également pour les demandes de partage administratif et de réutilisation des données.

2.3. La partie C est composée de six livres et contient des dispositions en matière de gestion des données.

Le livre C.I définit le champ d'application de la partie C et renferme des dispositions communes à l'ensemble de la partie C.

Le livre C.II expose les principes généraux de la gestion des données. Le titre 1er contient les principes directeurs que doivent respecter les autorités publiques. Le titre 2 comporte les objectifs stratégiques en matière de gestion des données. Le titre 3 renferme les objectifs opérationnels en matière de gestion des données.

Le livre C.III concerne les obligations de gouvernance des autorités publiques. Le titre 1er règle le champ d'application de ce livre. Le titre 2 contient des dispositions relatives à l'identification des partenariats numériques de données dont les autorités publiques sont parties, ainsi qu'à la qualification des parties, et l'organisation et la catégorisation des données qui sont traitées dans un partenariat numérique de données. Le titre 3 comporte des dispositions relatives à la valorisation des données tenues à jour par les autorités publiques, entre autres en ce qui concerne ses principes, le respect des droits sur les données protégées, une déclaration de principe et l'évaluation des risques. Le titre 4 renferme des dispositions relatives à la gestion des données, notamment en ce qui concerne la qualité des données et leurs sécurisation et protection. Le titre 5 contient une disposition rela-

(*) Cette prorogation résulte de l'article 84, § 1er, alinéa 1er, 2°, des lois « sur le Conseil d'État », coordonnées le 12 janvier 1973, qui dispose que le délai de trente jours est prorogé à quarante-cinq jours dans le cas où l'avis est donné par les chambres réunies en application de l'article 85*bis*.

(1) S'agissant d'un avant-projet de loi, on entend par « fondement juridique » la conformité avec les normes supérieures.

(2) Instituée par le décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française « relatifs à la publicité de l'administration dans les institutions bruxelloises ».

tive au contrôle de la conformité, de la traçabilité et de la responsabilité des autorités publiques.

Le livre C.IV comporte des dispositions en ce qui concerne les flux de données pour lesquels une autorité publique au moins est concernée au niveau de la Région de Bruxelles-Capitale, de la Commission communautaire commune ou de la Commission communautaire française, notamment le partage administratif, la réutilisation et la communication des données. Le titre 1er porte sur les garanties communes aux partages administratifs, réutilisations et communications des données. Le titre 2 contient des dispositions en ce qui concerne le partage administratif des données. Ce titre expose le principe du partage administratif et renferme les conditions du partage administratif (tant les conditions générales que les conditions particulières pour la mise à disposition de données issues de sources authentiques aux fins d'une collecte unique). Le titre 3 contient des dispositions relatives à la réutilisation de documents publics et de données publiques et vise à transposer la directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 « concernant les données ouvertes et la réutilisation des informations du secteur public ». Le titre 4 comporte une disposition concernant la communication des données.

Le livre C.V renferme des dispositions relatives à la Plateforme bruxelloise de la donnée, qui est créée au sein du Centre d'informatique pour la Région bruxelloise (en abrégé : « CIRB »). Il fixe les missions de la Plateforme bruxelloise de la donnée ainsi que les éléments essentiels du traitement de données à caractère personnel par la Plateforme bruxelloise de la donnée. Par ailleurs, ce livre contient des dispositions en ce qui concerne les différents organes et services qui sont créés : le centre d'intégration, le catalogue des données, le portail ouvert des données publiques, le centre d'exploitation et d'analyse des données, le point de contact et d'information et le service d'appui.

Le livre C.VI comporte des dispositions relatives aux structures administratives de la gouvernance. En ce qui concerne la gouvernance numérique, le titre 1er renferme des dispositions sur les objectifs et sur les tests dits d'autoévaluation numérique et règle les organes de la gouvernance numérique, à savoir le secrétariat numérique, le comité de validation de l'architecture numérique, le bureau d'achats numériques et le comité de coordination numérique. En ce qui concerne la gouvernance de la donnée, le titre 2 contient des dispositions sur les objectifs et sur les organes de la gouvernance de la donnée, à savoir le comité de gouvernance de la donnée et le bureau de la donnée. Le titre 3 comporte des dispositions relatives à la désignation d'un administrateur local de la donnée, d'un ou plusieurs responsables de la donnée et d'un conseiller de sécurité de l'information. Le titre 4 envisage la création du réseau bruxellois de fibre optique.

3. Les articles 13 à 20 (lire : 3 à 10) de l'avant-projet renferment les dispositions finales.

Les articles 13 à 15 (lire : 3 à 5) de l'avant-projet contiennent les dispositions d'entrée en vigueur des différents livres du Code à adopter.

Les articles 16 et 17 (lire : 6 et 7) de l'avant-projet règlent la succession de la Commission d'accès aux documents administratifs par la Commission d'accès aux documents administratifs et aux données instituée par le Code en projet.

L'article 18 (lire : 8) de l'avant-projet prévoit le montant maximum de la rétribution qui peut être demandée pour la délivrance d'une copie, dans l'attente de la détermination, par les autorités administratives, de ce montant. L'article 19 (lire : 9) de l'avant-projet prévoit que les règles de publicité active prévues par le livre B.I du Code en projet s'appliquent aux décisions, actes et documents adoptés après l'entrée en vigueur de ce livre.

Un certain nombre de normes législatives ([3]) sont abrogées six mois après l'entrée en vigueur du décret et ordonnance conjoints à adopter (article 20 (lire : 10) de l'avant-projet).

COMPÉTENCE

4. L'article C.IV.32 du Code en projet s'énonce comme suit :

« Conformément aux compétences matérielles de la Région, de la Commission Communautaire com-

(3) À savoir l'ordonnance du 17 juillet 2020 de la Région de Bruxelles-Capitale « garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité, et portant simplification et harmonisation des formulaires électroniques et papier », le décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française « relatifs à la publicité de l'administration dans les institutions bruxelloises », l'ordonnance du 27 octobre 2016 de la Région de Bruxelles-Capitale « visant à l'établissement d'une politique de données ouvertes (Open Data) et portant transposition de la Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public », l'ordonnance du 8 mai 2014 de la Région de Bruxelles-Capitale « portant création et organisation d'un intégrateur de services régional » et l'Accord de coopération du 28 février 2019 entre la Région de Bruxelles-Capitale et la Commission communautaire commune « portant sur la désignation d'un intégrateur de services commun pour l'échange électronique de données ».

mune, de la Commission Communautaire française, le Gouvernement, le Collège réuni et le Collège exécutent le Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 ».

L'exposé des motifs précise à cet égard ce qui suit :

« Le présent chapitre est volontairement incomplet dans la mesure où il a été introduit afin d'organiser que le cadre légal qui devra être mis en place par la Région, la Cocof et la Cocom afin de décider ou non des conditions d'autorisation des données protégées conformément au Règlement sur la gouvernance de la donnée, devra prendre place à cet endroit du Code.

Les commentaires de l'APD aux points 73 à 85 ont mis en évidence que le cadre légal nécessaire aux autorisations de réutilisation des données protégées devait être mûrement réfléchi notamment au regard des questions de répartitions de compétences entre l'État fédéral et les entités fédérées sur certains motifs qui pourraient être l'origine d'un refus de réutilisation des donnée protégées visées. Ce régime sera inséré à cet endroit du Code, une fois finalisé ».

Comme l'a récemment exposé la section de législation au sujet d'un avant-projet fédéral de texte d'exécution du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 « portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 » ([4]), la mise en œuvre de ce règlement ne relève pas exclusivement de l'autorité fédérale, mais aussi des régions et des communautés, entre autres en ce qui concerne la réutilisation de données liées à leurs compétences matérielles. La Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française peuvent dès lors inclure dans le décret et ordonnance conjoints à adopter des mesures d'exécution de ce règlement, dans les limites de leurs compétences matérielles en la matière.

OBSERVATIONS GÉNÉRALES

A. Observation préalable

5. Le Code en projet procède, pour une très large partie, à la codification de dispositifs existants, sur lesquels la section de législation a déjà eu l'occasion de donner un avis. Il est renvoyé à ces avis dans la mesure où ils seraient restés pertinents.

La circonstance que, le cas échéant, certaines des observations formulées par ces avis ne seraient pas reproduites dans le présent avis, ne saurait être interprétée comme signifiant que ces observations auraient perdu de leur pertinence ([5]).

B. Présentation de l'avant-projet et du Code en projet

6.1. L'avant-projet à l'examen est divisé en paragraphes, chacun reprenant un titre particulier. En guise d'illustration, le « Titre I : Dispositions générales », comprenant un seul article malgré l'emploi

(4) Avis 75.556/1 donné le 6 mars 2024 sur un avant-projet de loi « mettant en œuvre le règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 », *Doc. parl.*, Chambre, 2023 2024, n° 3934/001, pp. 63 81, observation 4.

(5) Voir ainsi l'avis 66.350/4 donné le 8 juillet 2019 sur un avant-projet devenu l'ordonnance de la Région de Bruxelles-Capitale du 17 juillet 2020, *Doc. parl.*, Parl. Rég. Brux. Cap., 2019-2020, n° A-180/1, pp. 16-17; les avis 65.516/2, 65.911/2 et 65.910/2 donnés le 27 mars 2019 sur les avant-projets devenus le décret et ordonnance conjoints de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française du 16 mai 2019, *Doc. parl.*, Parl. Rég. Brux. Cap., 2018-2019, n° A-862/1, pp. 43 57; *Doc. parl.*, Ass. réun. C.C.C., 2018-2019, n° B-172/1, p. 77; *Doc. parl.*, Ass. Comm. comm. fr., 2018-2019, n° 144/1, p. 28; l'avis 59.101/1 donné le 13 avril 2016 sur un avant-projet devenu l'ordonnance de la Région de Bruxelles-Capitale du 27 octobre 2016 « visant à l'établissement d'une politique de données ouvertes (Open Data) et portant transposition de la Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public », *Doc. parl.*, Parl. Rég. Brux.-Cap., 2015-2016, n° A-360/1, pp. 20-24; l'avis 69.186/1 donné le 6 mai 2021 sur un avant-projet devenu l'ordonnance de la Région de Bruxelles-Capitale du 10 décembre 2021 « modifiant l'ordonnance de la Région de Bruxelles-Capitale du 27 octobre 2016 visant à l'établissement d'une politique de données ouvertes (Open Data) et portant transposition de la Directive 2019/1024/UE du Parlement européen et du Conseil du 20 juin 2019 (refonte) concernant les données ouvertes et la réutilisation des informations du secteur public du 10 décembre 2021 », *Doc. parl.*, Parl. Rég. Brux.-Cap., 2021-2022, n° A-407/1, pp. 16-21; l'avis 55.264/2 donné le 3 mars 2014 sur un avant-projet devenu l'ordonnance de la Région de Bruxelles-Capitale du 8 mai 2014 « portant création et organisation d'un intégrateur de services régional », *Doc. parl.*, Parl. Rég. Brux.-Cap., 2013-2014, n° A-531/1, pp. 48-52; l'avis 65.075/4 donné le 14 février 2019 sur un avant-projet devenu l'ordonnance de la Région de Bruxelles-Capitale du 11 juin 2020 « portant assentiment de l'accord de coopération du 28 février 2019 entre la Région de Bruxelles-Capitale et la Commission communautaire commune portant sur la désignation d'un intégrateur de services commun pour l'échange électronique de données », *Doc. parl.*, Parl. Rég. Brux.-Cap., 2019-2020, n° 134/1, pp. 4-8 et l'avis 64.095/VR donné le 25 septembre 2018 sur un avant-projet devenu l'ordonnance de la Commission communautaire commune du 16 mai 2019 « portant assentiment de l'Accord de coopération du 28 février 2019 entre la Région de Bruxelles-Capitale et la Commission communautaire commune portant sur la désignation d'un intégrateur de services commun pour l'échange électronique de données », *Doc. parl.*, Ass. réun. C.C.C., 2018-2019, n° B.168/1, pp. 4-9.

du pluriel dans l'intitulé du titre, est présenté comme étant le paragraphe 1er.

Une telle manière de faire manque de cohérence. Les mentions des paragraphes qui assortissent l'intitulé des titres seront omises.

6.2. La numérotation de l'ensemble de l'avant-projet sera revue. L'article 2 est en effet suivi par un article 13 sans que ne figurent dans l'avant-projet les articles 3 à 12.

6.3. Concernant la clarté structurelle du Code en projet, les auteurs de l'avant-projet devront soumettre sa division à un examen complémentaire et seraient bien avisés de vérifier si, malgré le nombre considérable d'articles qu'il comporte, il ne vaudrait pas mieux opter pour une division moins détaillée – et plus facile à appliquer – du texte (6).

C. Tableaux de transposition

7. Le Code en projet vise notamment à transposer partiellement la directive 2003/4/CE ainsi que la directive (UE) 2019/1024.

Pour contrôler qu'une directive est transposée correctement et complètement, les principes de technique législative établis par la section de législation invitent les auteurs de projets, lors d'une transposition de directive, à établir des tableaux de transposition :

« 191. Établissez deux tableaux de transposition.

191.1. Pour contrôler qu'une directive est transposée correctement et complètement, établissez un tableau de correspondance entre les (subdivisions des) articles de la directive et les (subdivisions des) articles de l'acte de transposition que vous rédigez. Mentionnez également dans ce tableau :

a) les (subdivisions des) articles de la directive qui ont éventuellement déjà été transposés, en correspondance avec les actes de droit interne et les (subdivisions des) articles qui ont procédé à cette transposition;

b) les (subdivisions des) articles de la directive qui doivent encore être transposés par une autre autorité.

191.2. Pour pouvoir lire chaque article de l'acte de transposition à la lumière des exigences de la directive, établissez aussi un tableau de correspondance entre les (subdivisions des) articles de l'acte de transposition et les (subdivisions des) articles de la directive » (7).

Sur ce point, il est rappelé que la confection de tels tableaux lors de la transposition d'une ou plusieurs directives est gage de la qualité de cette transposition et que leur communication, d'emblée, à la section de législation, dès l'envoi de la demande d'avis, facilite l'examen du projet dans les délais impartis.

D. Le principe de légalité inscrit à l'article 22 de la Constitution

8. Conformément à l'article 22 de la Constitution, le respect du principe de légalité formelle s'applique à tout traitement de données à caractère personnel et, plus généralement, à toute ingérence dans le droit au respect de la vie privée. En réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée, l'article 22 de la Constitution garantit à tout citoyen qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue. Une délégation à un autre pouvoir n'est toutefois pas contraire au principe de légalité pour autant que l'habilitation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les « éléments essentiels » sont fixés préalablement par le législateur (8).

Par conséquent, les « éléments essentiels » du traitement de données à caractère personnel doivent être fixés dans la loi elle même. À cet égard, la section de législation considère que, quelle que soit la nature de la matière concernée, constituent, en principe, des « éléments essentiels » les éléments suivants : 1°) les catégories de données traitées; 2°) les catégories de personnes concernées; 3°) la finalité poursuivie par le traitement; 4°) les catégories de personnes ayant accès aux données traitées; et 5°) le délai maximal de conservation des données (9).

---

(6) En ce qui concerne les possibilités sur ce point, voir les *Principes de technique législative – Guide de rédaction des textes législatifs et réglementaires*, www.conseildetat.be, onglet « Technique législative », recommandation n° 62.

(7) *Ibidem*, recommandation n° 193.

(8) Jurisprudence constante de la Cour constitutionnelle : voir notamment C.C., 18 mars 2010, n° 29/2010, B.16.1; C.C., 20 février 2020, n° 27/2020, B.17.

(9) Avis 68.936/AG donné le 7 avril 2021 sur un avant-projet devenu la loi du 14 août 2021 « relative aux mesures de police administrative lors d'une situation d'urgence épidémique », *Doc. parl.*, Chambre, 2020-2021, n° 55-1951/001, p. 119, observation 101. Voir également C.C., 10 mars 2022, n° 33/2022, B.13.1; C.C., 22 septembre 2022, n° 110/2022, B.11.2; C.C., 16 février 2023, n° 26/2023, B.74.1; C.C., 17 mai 2023, n° 75/2023, B.55.2.1.

9. À cet égard, il convient de formuler les observations suivantes en ce qui concerne le Code en projet.

9.1. L'article C.III.13, § 4, du Code en projet dispose que les données d'usage sont conservées pour une durée proportionnelle à leurs finalités et sont protégées par des mesures de sécurité adaptées pour prévenir tout accès non autorisé, perte, altération ou divulgation. Une telle disposition paraphrase le principe de la limitation de la conservation inscrit à l'article 5, paragraphe 1er, e), du RGPD (10), qui implique que les données à caractère personnel doivent être « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées », mais ne suffit pas pour pouvoir fixer de manière juridiquement sûre le délai de conservation visé.

Il convient dès lors de prévoir un régime de délai de conservation maximal suffisamment précis, dans le cadre duquel le pouvoir exécutif peut éventuellement être habilité à fixer par arrêté d'exécution conjoint un délai plus court dans des cas spécifiques.

9.2. L'article C.V.6, alinéa 2, du Code en projet, dispose que les « catégories de données à caractère personnel visées par les traitements et les personnes concernées sont définies par les dispositions légales ou, le cas échéant, réglementaires des Autorités publiques disposant d'un cadre légal organique, ou encore, tout autre document établi conformément au RGPD en cadrant l'activité des autres Autorités publiques ». Les catégories de données traitées et les catégories de personnes concernées constituent cependant des éléments essentiels qui doivent être fixés par le législateur lui-même, conformément au principe de légalité précité. En conséquence, ces éléments essentiels ne peuvent pas être définis dans les règlements des autorités publiques et encore moins être désignés par « tout autre document ». La circonstance qu'un tel document serait établi conformément au RGPD ne change rien à ce constat. Le cas échéant, ces éléments essentiels doivent être fixés dans la législation sectorielle des autorités publiques respectives.

9.3.1. L'article C.V.7, alinéa 2, du Code en projet dispose que les données à caractère personnel qui sont traitées par le centre d'exploitation et d'analyse sont conservées « pour une durée fixée en fonction des finalités déterminées par le responsable de traitement ». La disposition en projet ne comporte pas de délai maximal pour la conservation de données à caractère personnel, et celui-ci n'en découle pas explicitement ou implicitement de façon suffisamment claire. Une simple référence à un délai fixé par le responsable de traitement ne suffit pas à la lumière du principe de légalité précité inscrit à l'article 22 de la Constitution.

Il convient dès lors ici aussi de prévoir un régime suffisamment précis en matière de délai de conservation maximal, dans le cadre duquel le pouvoir exécutif peut éventuellement être habilité à fixer par arrêté d'exécution conjoint un délai plus court dans des cas spécifiques.

9.3.2. L'article C.V.7, alinéa 9, du Code en projet dispose que « [s]ans préjudice d'autres dispositions légales, les données à caractère personnel techniques nécessaires au fonctionnement des autres services de la Plateforme bruxelloise de la donnée sont conservées jusqu'à 6 mois après la fin du traitement. ». On n'aperçoit cependant pas clairement ce qu'il y a lieu d'entendre par la notion de « données à caractère personnel techniques », ni quelles « autres dispositions légales » sont visées.

Le régime de délai de conservation maximal en projet n'est conforme au principe de légalité précité que si ces notions sont précisées.

9.3.3. L'article C.V.7 du Code en projet sera en outre soumis à un examen approfondi sur le plan de la concordance entre le texte à l'examen et le texte néerlandais des avant-projets de décret et ordonnance conjoints de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française « portant le Code de la gouvernance et de la donnée » sur lesquels la section de législation a donné ce jour les avis 75.158/VR et 75.314/VR, afin que les délais de conservation maximaux y soient réglés de manière suffisamment claire et avec toute la sécurité juridique nécessaire.

Il est renvoyé à cet égard à l'observation 9.3.3 des avis 75.158/VR et 75.314/VR.

9.4. L'article C.V.15, alinéa 2, du Code en projet dispose que l'objectif du centre d'exploitation et d'analyse des données est de fournir des services facultatifs fixés par le Gouvernement, le Collège réuni et le Collège. Il ressort de l'exposé des motifs que ces « services facultatifs » visent « plusieurs outils pour stocker, traiter et analyser les données ».

Dans la mesure où ces données peuvent également comprendre des données à caractère personnel, les éléments essentiels de leur traitement doivent être réglés dans le Code en projet lui même.

(10) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ».

E. Délégation de pouvoirs réglementaires

10.1. Le Code en projet renferme des délégations de pouvoir à différents acteurs de la donnée. Ces délégations sont souvent rédigées d'une façon très générale et vague, de sorte qu'on n'aperçoit pas clairement ce qui est visé précisément. Dans certains cas, cela pourrait donner à penser qu'un pouvoir réglementaire est dévolu à ces acteurs de la donnée.

Ainsi, on peut renvoyer à l'article C.VI.11 du Code en projet, qui dispose que le comité de coordination numérique « se prononce stratégiquement sur tous les projets […] ».

L'article C.VI.18, 4°, b), du Code en projet dispose que le bureau de la donnée accompagne la mise en œuvre des obligations du Code au travers de « la proposition de directives, de standards, de cadres et de lignes directrices à faire approuver par le Comité de gouvernance de la donnée ».

Aux termes de l'article C.VI.21, § 1er, alinéa 2, du Code en projet, l'administrateur local de la donnée définit « la stratégie interne de l'Autorité publique ». L'alinéa 3 prévoit que l'administrateur local de la donnée établit le « modèle opérationnel interne à l'Autorité publique », définissant la gouvernance interne ainsi que les rôles et responsabilités des différents acteurs de la donnée.

L'article C.VI.24 du Code en projet dispose que le ClRB est chargé de la mise en place du réseau bruxellois de fibre optique et que, dans ce cadre, il doit désigner une entité chargée, entre autres, de prévoir « le déploiement harmonisé, centralisé et coordonné de toutes nouvelles capacités du réseau de fibre optique ».

10.2. L'attribution d'un pouvoir réglementaire à un organisme public n'est en principe pas conforme aux principes généraux de droit public, en ce qu'il est ainsi porté atteinte au principe de l'unité du pouvoir réglementaire et qu'un contrôle parlementaire direct fait défaut. En outre, les garanties dont est assortie la réglementation classique, telles que celles en matière de publication, de contrôle préventif exercé par le Conseil d'État, section de législation, et de rang précis dans la hiérarchie des normes, sont absentes. Pareilles délégations ne se justifient dès lors que dans la mesure où elles sont très limitées et ont un caractère non politique, en raison de leur portée secondaire ou principalement technique. Les organismes qui doivent appliquer la réglementation concernée doivent être soumis à cet égard tant à un contrôle juridictionnel qu'à un contrôle politique ([11]).

Ainsi, les dispositions en projet précitées peuvent être interprétées en ce sens qu'elles visent uniquement des actes de nature purement préparatoire de gestion et qu'elles ne renferment pas de pouvoir décisionnel, ni *à fortiori* d'actes de pouvoir réglementaire. S'il en était autrement, il conviendrait de remplir les conditions évoquées ci-dessus.

F. Examen du point de vue de la correction de la langue et de la légistique

11. L'avant-projet doit être soumis à un examen approfondi sur le plan de la correction de la langue et de la légistique. En outre, on vérifiera la concordance du texte à l'examen avec le texte néerlandais des avant-projets de décret et ordonnance conjoints de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française, sur lesquels la section de législation a donné les avis 75.158/VR et 75.314/VR.

À titre d'exemple, on peut relever les points suivants :

– l'énumération des définitions utilisées à l'article A.II.2 du Code en projet doit débuter par le point 1) ([12]);

– au point 14), de l'article A.III.1, du Code en projet, les mots « donnée à forte valeur (ensemble de) »

(11) Comparer avec les critères d'évaluation qu'utilise la Cour constitutionnelle pour apprécier les délégations de pouvoir réglementaire par le législateur à une autorité administrative autonome ou à un organisme public décentralisé; voir C.C., 11 juin 2015, n° 86/2015, B.22.4 et C.C., 9 juin 2016, n° 89/2016, B.9.6.4 : « Les articles 33, 105 et 108 de la Constitution ne s'opposent pas à ce que, dans une matière technique déterminée, le législateur confie des compétences exécutives spécifiques à une autorité administrative autonome soumise tant au contrôle juridictionnel qu'au contrôle parlementaire et n'interdisent pas au législateur d'accorder des délégations à un organe exécutif, pour autant qu'elles portent sur l'exécution de mesures dont le législateur compétent a déterminé l'objet, en particulier dans les matières techniques et complexes »; voir C.C., 19 novembre 2015, n° 162/2015, B.8.4 : « L'article 33 de la Constitution et l'article 20 de la loi spéciale du 8 août 1980 de réformes institutionnelles ne s'opposent pas à ce que le législateur confie des compétences exécutives spécifiques à un organisme public décentralisé qui est soumis à une tutelle administrative et à un contrôle juridictionnel ». Voir aussi C.C., 14 mai 2020, n° 67/2020, B.41.2 : « Une délégation à un organisme public décentralisé qui est soumis à une tutelle administrative et à un contrôle juridictionnel n'est toutefois pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur ».

(12) *Principes de technique législative – Guide de rédaction des textes législatifs et réglementaires*, www.conseildetat.be, onglet « Technique législative », recommandation n° 58, b).

seront remplacés par les mots « (ensemble de) donnée(s) à forte valeur »;

– à l'article B.II.9, § 3, du Code en projet, on écrira « règlement d'ordre intérieur » au lieu de « Règlement d'ordre intérieur interne »;

– au paragraphe 3 de l'article B.II.18 du Code en projet, il convient de remplacer les mots « articles B. II.16 à 18, » par les mots « articles B.II.16 à B.II.18, »;

– en ce qui concerne la structure en paragraphes de l'article C.III.3, § 2, du Code en projet, le texte à l'examen sera aligné sur le texte néerlandais des avant-projets de décret et ordonnance conjoints de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française, sur lesquels la section de législation a donné les avis 75.158/VR et 75.314/VR. L'alinéa 3 de l'article C.III.3, § 1er, du Code en projet deviendra le paragraphe 2, qui, lui, deviendra le paragraphe 3;

– à l'article C.III.7, § 2, alinéa 1er, 3°, du Code en projet, on écrira « la sécurité et la protection des données au sens du chapitre 2 du titre 4 du présent livre » au lieu de « la sécurité et la protection des données au sens du chapitre 2 du titre 5 du présent livre »;

– les articles C.III.11, C.III.16 et C.IV.18 du Code en projet échappent à la division en chapitres. Ces dispositions doivent être placées sous un chapitre intitulé « Dispositions introductives » ou « Objet » ([13]);

– à l'alinéa 2 de l'article C.IV.19 du Code en projet, il y a lieu de compléter le numéro d'ordre de la directive (EU) 2019/1024;

– à l'article C.IV.25, § 5, alinéa 1er, du Code en projet, on écrira « Dans les cas visés aux points 1° et 3° du paragraphe 4 » au lieu de « Dans les cas visés aux points 1e et 3e »;

– à l'article C.V.2, alinéa 1er, 7°, du Code en projet, le segment de phrase commençant par les mots « la conception évolutive » doit être inscrit dans un point 8° distinct;

– conformément au texte néerlandais des avant-projets de décret et ordonnance conjoints de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française, sur lesquels la section de législation a donné les avis 75.158/VR et 75.314/VR, le dernier segment de phrase de l'avant dernier tiret de l'article C.V.4 du Code en projet, commençant par les mots « au niveau de Point de contact et d'information », doit être inscrit sous un tiret distinct;

– différentes dispositions du Code en projet présentent de nombreux chevauchements ou répétitions. Ainsi, à titre d'exemple, on peut relever le fait que tant l'article C.V.13, § 1er, 1°, en projet, que l'article C.V.13, § 2, 1°, en projet, disposent que le « Catalogue de données » vise à dresser un inventaire de l'ensemble des données détenues par les autorités publiques;

– à l'article C.VI.1 du Code en projet, le segment de phrase « des Autorités visées au a), b) » sera remplacé par le segment de phrase « des Autorités publiques visées à l'article A.I.3, 1), a) et b) »;

– l'article C.VI.9, § 3, alinéa 2, du Code en projet, renvoie erronément aux autorités publiques autres que celles visées à l'article « B.VI.I ». Il convient de faire référence à l'article C.VI.1;

– au paragraphe 2, 1°, de l'article C.VI.22 du Code en projet, mieux vaut écrire que la mission d'implémentation est « approuvée » plutôt que « validée »;

– tout comme tel est le cas dans l'ensemble du Code en projet, les titres auxquels il est fait référence dans les dispositions finales doivent être indiqués en chiffres arabes et non pas en chiffres romains.

OBSERVATIONS PARTICULIÈRES

INTITULÉ

12. Eu égard à l'article 92*bis*/1, § 1er, alinéa 2, de la loi spéciale du 8 août 1980 « de réformes institutionnelles », l'intitulé mentionnera la dénomination de toutes les entités qui adoptent le décret et ordonnance conjoints ([14]).

On écrira dès lors « Décret et ordonnance conjoints de la Région de Bruxelles-Capitale, de la Commission communautaire commune et de la Commission communautaire française [...] ».

(13) *Ibidem*, recommandation n° 63.

(14) Avis 73.262/VR donné le 16 juin 2023 sur un avant-projet devenu le décret et ordonnance conjoints de la Commission communautaire française et de la Commission communautaire commune du 25 janvier 2024 « relatifs à l'adoption et à la mise en œuvre du Plan social santé intégré bruxellois », *Doc. parl.*, Ass. réun. C.C.C., 2022-23, n° B-157/1, p. 22, observation 5.

Article 1er

13. Les mots « La présente loi » seront remplacés par les mots « Le présent décret et ordonnance conjoints » ([15]).

Article 2

Article A.I.3

14. L'article A.I.3, 7), du Code en projet définit le « CIRB » comme étant le « centre informatique de la Région bruxelloise ». Toutefois, l'ordonnance de la Région de Bruxelles-Capitale du 22 février 2024 « relative à Paradigm » modifie la dénomination du Centre d'informatique de la Région bruxelloise en « Paradigm ». Le Code en projet devra tenir compte de ce changement de dénomination.

15. À l'article A.I.3, 8), du Code en projet les mots « créant Bruxelles Environnement » seront insérés après la date du « 8 mars 1989 ».

Livre A.II et livre A.III

16. Le Livre A.II du Code en projet comprend l'article A.II.1 établissant la liste des définitions à employer pour l'application du Livre B.1. Le livre A. III, comprenant l'article A.III.1, fait de même pour ce qui concerne l'application de la partie C du Code en projet.

Afin d'assurer une plus grande lisibilité du texte, le Code en projet gagnerait à ce que ces deux blocs de définitions, dès lors que celles-ci ne s'appliquent pas à l'ensemble du Code en projet, soient scindés et placés respectivement au début de la partie à laquelle les définitions se rapportent. Les définitions reprises à l'article A.II.1 figureront donc au début du Livre B.1, tandis que les définitions reprises à l'article A.III.1 figureront au début de la partie C.

Article A.III.1

17. Au point 2) de l'article A.III.1 du Code en projet, il convient de choisir une seule et même formule pour désigner le règlement (UE) 2022/868. En l'occurrence, les mots « Règlement sur la gouvernance des données » sont à privilégier et les mots « ou « Data Governance Act » ou « DGA » » seront omis.

L'ensemble du Code en projet sera revu afin que seuls les mots « Règlement sur la gouvernance des données » soient employés pour désigner ce règlement.

Ainsi, on se reportera à titre d'exemple à l'article C.V.17 du Code en projet dont la phrase introductive se réfère au DGA mais dont le point 4° mentionne en toutes lettres « Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données ».

18. La notion de « donnée d'usage », définie au point 23) de l'article A.III.1 du Code en projet fait également l'objet d'une définition au point 102).

Ces deux définitions étant différentes, les dispositions seront revues et la définition superfétatoire sera omise.

19. Compte tenu de la définition reprise au point 30) de l'article A.III.1 du Code en projet, la définition figurant au point 29) est redondante et sera omise.

20.1. En vertu de l'article A.I.2 du Code en projet,

« [l]es définitions formulées à l'article 4 du règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE, s'appliquent au présent Code à l'exception des termes qui reçoivent une définition spécifique dans le cadre des articles A.I.3, A.II.1 et A.II.2 et A.III.1 ».

Les points 103) et 104) de l'article A.III.1 du Code en projet distinguent, d'une part, la « donnée à caractère personnel non confidentielle », définie comme « donnée qui, bien que à caractère personnel, peut être rendue publique pour des objectifs d'intérêt général en vertu de normes législatives » (point 103) et, d'autre part, la « donnée à caractère personnel confidentielle », définie comme la « donnée à caractère personnel qui n'est pas une donnée à caractère personnel non confidentielle » (point 104).

L'exposé des motifs indique à ce sujet :

« Cette définition distingue les informations personnelles qui peuvent être publiées en Open data (ex auteur de livres). Elle oriente les politiques et les pratiques concernant la divulgation des données personnelles, assurant un équilibre entre transparence et protection de la vie privée ».

20.2. Il résulte de l'article A.I.2 du Code en projet que la définition spécifique de la « donnée à caractère personnel non confidentielle » contenue dans l'article A.III.1, 103), pour le Livre C du Code en projet a pour effet d'exclure la définition des « données à caractère personnel » au sens de l'article 4, point 1), du

(15) Voir les articles 42 et 63 de la loi spéciale du 12 janvier 1989 « relative aux Institutions bruxelloises ».

RGPD ([16]), ce qui ne semble pas compatible ni avec la directive 2003/4/CE ou la directive (UE) 2019/1024, ni avec le règlement (UE) 2022/868 ([17]). Les directives et le règlement précités organisent, respectivement, un régime d'accès ou de réutilisation des données à caractère personnel au sens du RGPD, moyennant différentes conditions et exceptions ([18]). Ni ces directives, ni le règlement (UE) 2022/868 ni le RGPD d'ailleurs, n'opèrent une distinction entre la « donnée à caractère personnel non confidentielle » et la « donnée à caractère personnel confidentielle ».

La distinction opérée par les points 103) et 104) de l'article A.III.1 du Code en projet est, à tout le moins, source d'ambiguïté par rapport au respect des exigences du RGPD. Ainsi, en définissant la donnée à caractère personnel non confidentielle, comme celle qui peut être rendue publique « pour des objectifs d'intérêt général en vertu de normes législatives », l'article A.III.1 du Code en projet autorise la publicité de données à caractère personnel pour de simples « objectifs d'intérêt général en vertu de normes législatives » sans davantage de précision, ce qui ne correspond pas aux principes de limitation des finalités, de minimisation des données et de licéité d'un traitement de données à caractère personnel prévus dans les articles 5 et 6 du RGPD.

La disposition sera revue à la lumière de cette observation.

(16) Article 4, point 1), du RGPD : « Aux fins du présent règlement, on entend par : 1) « données à caractère personnel », toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »); est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

(17) L'article 2, 12), de la directive (UE) 2019/1024, de même que l'article 2, 3), du Règlement (UE) 2022/868, définissent les « données à caractère personnel » comme « les données à caractère personnel telles qu'elles sont définies à l'article 4, point 1), du règlement (UE) 2016/679 ». L'article 4, paragraphe 2, alinéa 3, de la directive 2003/4/CE prévoit qu'en ce qui concerne les dérogations au droit d'accès aux informations environnementales, « aux fins notamment de l'application du point f) [relatif à la confidentialité des données à caractère personnel], les États membres veillent au respect des exigences de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ».

(18) Voir les articles 3 et 4 de la directive 2003/4/CE, l'article 4 de la directive (UE) 2019/1024, et l'article 5 du règlement (UE) 2022/868.

Article B.I.4

21.1. Au paragraphe 1er, alinéa 2, 5°, de l'article B.I.4 du Code en projet, il est prévu que la rubrique « transparence » des sites internet des autorités publiques contient au minimum « les décisions de recrutement, de promotion ou de remplacement des emplois des agents de niveau A qu'elles pourvoient, publiées dans les sept jours ouvrables de la décision et pendant soixante jours ».

L'exposé des motifs indique :

« Cet article reprend l'article 6 du décret et ordonnance conjoints du 16 mai 2019.

[…]

La publication des données à caractère personnel dans le cadre de la rubrique transparence apparaît le moyen le plus efficace d'assurer l'information adéquate de tout un chacun au regard des finalités poursuivies. La limitation des durées de publication des données à caractère personnel, relativement courtes, assure le caractère proportionné du traitement. ».

21.2. Les décisions visées à l'article B.I.4, § 1er, alinéa 2, 5°, du Code en projet sont des décisions individuelles concernant le recrutement, la promotion ou le remplacement pour l'ensemble des agents de niveau A des autorités publiques concernées. De telles décisions portent nécessairement sur des données à caractère personnel qui peuvent, le cas échéant, emporter un jugement ou une appréciation sur l'agent concerné, voire sur des tiers candidats évincés.

Le fait que la publication visée soit limitée dans le temps ne permet pas de considérer que la publicité de l'ensemble des éléments contenus dans ces décisions individuelles soit proportionnée au regard du droit au respect de la vie privée, dont le droit à la protection des données à caractère personnel. Les auteurs de l'avant-projet sont invités à examiner si les finalités visées au paragraphe 4 de cet article – pour autant qu'elles soient rendues applicables au paragraphe 1er (voir ci-dessous) – ne peuvent être atteintes par des voies moins attentatoires à la vie privée, telle qu'une liste actualisée mentionnant les nom et fonction des agents concernés, de la même manière que le prévoit l'article B.I.4, § 2, du Code en projet pour les membres des cabinets ministériels.

À cet égard, la mesure en projet apparait d'autant moins proportionnée que, tel que le paragraphe 4 du même article est libellé, les finalités qui y sont mentionnées (alinéa 1er), de même que le droit d'opposition conféré à la personne concernée conformément à l'article 21 du RGPD (alinéa 2), ne visent que les « données à caractère personnel en application des

paragraphes 2 à 3 », de sorte que, d'une part, les finalités des publications visées au paragraphe 1er en projet ne sont pas prévues dans le dispositif et que, d'autre part, sont exclus de toute possibilité d'opposition les agents ou tiers concernés par « les décisions de recrutement, de promotion ou de remplacement » visées au paragraphe 1er, 5°, en projet.

21.3. Le dispositif sera complété en conséquence et, le cas échéant, revu à la lumière de cette observation.

22. Dans le paragraphe 2, alinéa 2, de l'article B.I.4 du Code en projet, on écrira « Le collège des bourgmestre et échevins » au lieu de « Collège communal ».

23. Le commentaire de l'article B.I.4 du Code en projet indique que, conformément à l'avis de l'Autorité de protection des données, cette disposition est notamment complétée afin :

« […] de mentionner le temps de publication de ces données. Ce temps est d'un an pour ce qui concerne les études et les inventaires des subventions vu que le budget est voté annuellement. Le temps de publication est d'une législature pour ce qui concerne les données à caractère personnel publiées dans le cadre de fonctions ou de mandats politiques. Le temps de publication est de soixante jours pour les décisions en matière de fonction publique afin de permettre aux agents qui le souhaitent d'introduire un recours contre ces décisions devant le Conseil d'État; [...] ».

Toutefois, en ce qui concerne le temps de publication des données à caractère personnel dans le cadre de fonctions ou mandats politiques (à l'exception du collège communal (lire : le collège des bourgmestre et échevins) et du président du CPAS), cette modification n'a pas été apportée dans le texte soumis au Conseil d'État, section de législation. En conséquence, les auteurs de l'avant-projet doivent indiquer, pour ce cas également, le temps de publication des données à caractère personnel dans l'article B.I.4 du Code en projet.

24.1. En vertu du paragraphe 3, alinéa 1er, 2°, de l'article B.I.4 du Code en projet, le Gouvernement, le Collège réuni et le Collège diffusent au sein de la rubrique transparence de leur site internet « au plus tard le jour ouvrable qui suit leur réunion, les décisions qu'ils ont adoptées ainsi que les notes sur lesquelles elles se fondent ».

Ainsi formulée, cette disposition n'exclut donc pas la mise en ligne de décisions individuelles (19). Les auteurs de l'avant-projet sont invités à examiner si cette mesure se justifie au regard du principe de limiter les traitements de données au strict nécessaire.

24.2. En outre, la disposition en projet ne définit pas les « notes sur lesquelles [les décisions adoptées] se fondent » ni ne liste ces catégories de documents.

Au sujet d'une disposition analogue, la section de législation a observé :

« Dès lors que l'article 3/1, § 1er, en projet ne définit pas la notion de 'documents y afférents' ni ne liste ces catégories de documents, elle peut être lue comme imposant au Gouvernement de divulguer l'ensemble des documents qui se rapportent, directement ou indirectement, à ses décisions (20).

D'après sa justification, l'amendement « tend à transposer la réglementation flamande au niveau fédéral ».

Le « Bestuursdecreet » (décret de gouvernance) du 7 décembre 2018, auquel les auteurs de l'amendement renvoient expressément, énonce en effet une règle similaire en son article II.9 (21).

Les auteurs de l'amendement précisent par ailleurs que

« [c]e décret prévoit une transparence étendue des documents administratifs qui s'étend non seulement, par exemple, à la publicité des décisions du gouvernement, mais aussi à la publicité des dossiers y afférents (avis sur le budget, Inspection des Finances, etc.) ».

Il doit cependant être constaté que les travaux préparatoires relatifs au « Bestuursdecreet » nuancent l'obligation selon laquelle l'ensemble des documents

(19) Ainsi, le paragraphe 1er de l'article II.9 du « Bestuursdecreet » de la Communauté flamande et de la Région flamande du 7 décembre 2018 exclut expressément la publication de décisions à portée individuelle.

(20) *Note de bas de page n° 2 de l'avis cité :* Comme, par exemple, les formalités, obligatoires ou non, qui ont été accomplies (avis, accords ou propositions), les notes au Gouvernement, les échanges entre les membres du Gouvernement ou les membres de leurs cabinets, les versions antérieures de ces décisions voire même des études qui fonderaient la décision adoptée.

(21) *Note de bas de page n° 3 de l'avis cité :* Le paragraphe 1er de l'article II.9 du décret de l'Autorité flamande du 7 décembre 2018 « de gouvernance » énonce ce qui suit :
« À l'exception des décisions à portée individuelle, les décisions du Gouvernement flamand, ainsi que les documents y afférents, sont systématiquement publiés sur le site internet central de l'Autorité flamande ».

relatifs à la décision du Gouvernement doivent être publiés :

« De bepaling van de eerste paragraaf is momenteel ingeschreven in artikel 16/1, § 1, bevoegdheidsbesluit van de Vlaamse Regering (BVR 25 juli 2014). Het is aangewezen deze verplichting decretaal te verankeren met het oog op de continuïteit van deze praktijk die kadert in een transparantere besluitvorming maar ook in ruimere participatie en consultatie. Onder meer ook alle visienota's, conceptnota's, groenen witboeken, principieel goedgekeurde ontwerpregelgeving worden gepubliceerd.

De beslissingen van de VR worden gepubliceerd, samen met de bijhorende documenten :

– de nota's aan de VR en de documenten die door de VR goedgekeurd worden (ontwerpbesluit, (voor) ontwerpdecreet, conceptnota enzovoort);

– de mededelingen aan de VR samen met de documenten die aan de VR voorgelegd worden;

– de adviezen van adviesorganen.

Het is niet wenselijk of nuttig om alle bijlagen bij de nota's aan de VR systematisch te publiceren. De volgende documenten zullen niet worden gepubliceerd :

– interne adviezen en akkoorden (IF, begrotingsakkoord, akkoord minister van bestuurszaken;

– vertrouwelijke documenten, onder andere cv's enzovoort;

– voorgaande versies als er bis-, ter- enzovoort versies zijn;

– documenten bij agendapunten die uitgesteld of ingetrokken werden;

– te omvangrijke documenten, kaarten enzovoort. » ([22]).

L'intention des auteurs de l'amendement apparaît dès lors incertaine en ce qui concerne la portée de l'obligation de publier les documents « afférents » à la décision.

Cette incertitude sera, par souci de sécurité juridique, levée en définissant ce qu'il convient d'entendre par les mots « documents y afférents » ou en énumérant les catégories de documents qui relèvent de cette notion.

Il sera également précisé si, et le cas échéant dans quelle mesure, les exceptions à la publicité des documents administratifs figurant à l'article 6 de la loi du 11 avril 1994 peuvent être invoquées pour restreindre la publicité de certains documents afférents à une décision gouvernementale ([23]). Dans ce cadre, il convient de mettre en balance la nécessité de publier les documents afférents à la décision – en tenant compte de leur nature et de leur portée – et les intérêts protégés par les exceptions précitées.

La disposition examinée sera revue à la lumière de ce qui précède. » ([24]).

La même observation vaut *mutatis mutandis* pour l'article B.I.4, paragraphe 3, alinéa 1er, 2°, du Code en projet.

L'attention des auteurs de l'avant-projet est plus particulièrement attirée sur le fait que, conformément au paragraphe 4, alinéa 2, de l'article B.I.4 du Code en projet, la publicité visée au paragraphe 3, ne peut être limitée que moyennant l'exercice d'un droit d'opposition conformément à l'article 21 du RGPD, avec indication par la personne concernée des « raisons tenant à sa situation particulière », sans aucune autre possibilité de s'opposer à cette publicité active, notamment en raison de la confidentialité des délibérations des pouvoirs publics ([25]) ou en raison d'une obligation de secret ([26]). Il convient notamment d'examiner si la mise en balance entre l'intérêt de la publicité active et la protection d'autres intérêts protégés dans le cadre de la publicité passive ne doit pas être effectuée par l'autorité concernée préalablement à la

(22) *Note de bas de page n° 4 de l'avis cité : Doc. parl.*, Vl. Parl., 2017-2018, n° 1656/1, p. 38.

(23) *Note de bas de page n° 5 de l'avis cité :* Voir, par comparaison, l'article 3/2, § 2, en projet qu'entend insérer l'article 6 de l'avant-projet « modifiant la loi du 11 avril 1994 relative à la publicité de l'administration et abrogeant la loi du 12 novembre 1997 relative à la publicité de l'administration dans les provinces et les communes », qui dispose que les instances administratives informent, de leur propre initiative, sur leurs politiques, réglementations et services, chaque fois que cela est utile, important ou nécessaire « [s]ans préjudice des exceptions prévues à l'article 6 ».

(24) Avis 74.617/2 donné le 6 novembre 2023 sur les amendements nos 14 et 15 à 17 au « projet de loi modifiant la loi du 11 avril 1994 relative à la publicité de l'administration et abrogeant la loi du 12 novembre 1997 relative à la publicité de l'administration dans les provinces et les communes », *Doc. parl.*, Chambre, 2022-2023, n° 55-3217/13, pp. 4 5, observation sous l'amendement n° 14, point 2.

(25) L'article 19, § 2, alinéa 1er, 6°, et § 3, alinéa 1er, 1°, du décret et ordonnance conjoints du 16 mai 2019 prévoit que « la confidentialité des délibérations des autorités publiques » constitue une exception à la publicité passive respectivement des documents administratifs et des informations environnementales. Cette exception est reprise dans l'article B.I.18, § 2, alinéa 1er, 6°, et § 3, alinéa 1er, 1°, du Code en projet.

(26) L'article B.I.18, § 5, du Code en projet prévoit qu'une demande d'accès aux documents administratifs est rejetée si elle porte atteinte à « une obligation de secret instaurée par une ordonnance de la Région de Bruxelles-Capitale, une ordonnance de la Commission communautaire commune ou un décret de la Commission communautaire française ».

mise en ligne de décisions individuelles ou de documents contenant des données à caractère personnel, le cas échéant, en occultant dans ce dernier cas certains éléments de la publicité ([27]).

24.3. La disposition sera revue à la lumière de ce qui précède.

Article B.I.15

25. Au deuxième alinéa de l'article B.I.15 du Code en projet, le renvoi fait à « l'article A.I.1, 4° » est erroné.

La disposition devrait viser, en l'état du texte, l'article A.II.1, 4).

Article B.I.18

26. Au paragraphe 2, alinéa 1er, 5°, de l'article B.I.18 du Code en projet, le renvoi fait à l'article 3, 1° à 9°, est erroné.

La disposition devrait viser, en l'état du texte, l'article B.I.2.

27.1. Le paragraphe 3, alinéa 2, de l'article B.I.18 du Code en projet prévoit :

« [l]'Autorité publique ne peut, en vertu des points 1°, 4°, 5°, 6°, 7°, rejeter une demande lorsqu'elle concerne des informations relatives à des émissions dans l'environnement ».

L'exposé des motifs indique à cet égard :

« La seule hypothèse où l'exception en matière de protection des données à caractère personnel ne pourra pas être invoquée est lorsque la demande d'information portera sur des émissions environnementales, lesquelles ne supposent *a priori* pas, dans la grande majorité des cas, la communication de données à caractère personnel ».

27.2. Ainsi que l'a observé la section de législation,

« Wanneer de Grondwetgever artikel 32 van de Grondwet heeft aangenomen, is benadrukt dat de uitzonderingen op dat recht in beginsel een onderzoek, geval per geval, van de verschillende aanwezige belangen vereisen : « telkens [moet] *in concreto* het belang van de openbaarmaking […] worden afgewogen tegen het belang beschermd door een uitzonderingsgrond » ([28]).

Uit de rechtspraak van het Grondwettelijk Hof lijkt te kunnen worden afgeleid dat die grondwetsbepaling zich weliswaar niet verzet tegen een algemene en absolute uitzondering op het recht op toegang tot bestuursdocumenten, maar enkel voor zover die maatregel evenredig is met het door de decreetgever nagestreefde doel. Inzonderheid moet worden aangetoond waarom er niet mee kan worden volstaan in een procedure te voorzien waarbij het belang van de openbaarheid wordt afgewogen tegen andere motieven van algemeen belang. ([29]) » ([30]).

En prévoyant que la demande ne peut être rejetée pour certains motifs lorsque les informations sont relatives à des émissions dans l'environnement, l'article B.I.18, § 3, alinéa 2, en projet transpose l'article 4, paragraphe 2, deuxième alinéa, troisième phrase, de la directive 2003/4/CE.

L'article 4, paragraphe 2, de la directive 2003/4/CE dispose :

« 2. Les États membres peuvent prévoir qu'une demande d'informations environnementales peut être rejetée lorsque la divulgation des informations porterait atteinte :

a) à la confidentialité des délibérations des autorités publiques, lorsque cette confidentialité est prévue en droit;

b) aux relations internationales, à la sécurité publique ou à la défense nationale;

c) à la bonne marche de la justice, à la possibilité pour toute personne d'être jugée équitablement ou à la capacité d'une autorité publique de mener une enquête à caractère pénal ou disciplinaire;

(27) Voir l'avis 74.483/4 donné le 6 novembre 2023 sur un avant-projet devenu l'ordonnance de la Région de Bruxelles-Capitale du 22 février 2024 « modifiant la Nouvelle loi communale », *Doc. parl.*, Parl. Rég. Brux.-Cap., 2023-2024, n° 808/1, pp. 16-21, observation sous l'article 6 :
« Il ne peut être exclu que les « notes de synthèses explicatives » accompagnant les projets de délibération du conseil communal contiennent des données à caractère personnel.
Il convient alors soit d'exclure explicitement les données à caractère personnel de la publication envisagée, soit d'encadrer le traitement de ces données en fixant dans l'avant-projet d'ordonnance les « éléments essentiels » de ce traitement ».

(28) *Note de bas de page n° 44 de l'avis cité :* Parl.St. Kamer 1992-93, nr. 839/1, 5.

(29) *Note de bas de page n° 45 de l'avis cité :* Zie inzonderheid GwH 19 december 2013, nr. 169/2013, B.15 tot B.27.

(30) Avis 63.130/3 donné le 16 mai 2018 sur un avant-projet devenu le « Bestuursdecreet » de la Communauté flamande et de la Région flamande du 7 décembre 2018, *Doc. parl.*, Parl. fl., 2017-18, n° 1656/1, pp. 783 864, observation 11.2.

d) à la confidentialité des informations commerciales ou industrielles, lorsque cette confidentialité est prévue par le droit national ou communautaire afin de protéger un intérêt économique légitime, y compris l'intérêt public lié à la préservation de la confidentialité des statistiques et du secret fiscal;

e) à des droits de propriété intellectuelle;

f) à la confidentialité des données à caractère personnel et/ou des dossiers concernant une personne physique si cette personne n'a pas consenti à la divulgation de ces informations au public, lorsque la confidentialité de ce type d'information est prévue par le droit national ou communautaire;

g) aux intérêts ou à la protection de toute personne qui a fourni les informations demandées sur une base volontaire sans y être contrainte par la loi ou sans que la loi puisse l'y contraindre, à moins que cette personne n'ait consenti à la divulgation de ces données;

h) à la protection de l'environnement auquel se rapportent ces informations, telles que la localisation d'espèces rares.

Les motifs de refus visés aux paragraphes 1er et 2 sont interprétés de manière restrictive, en tenant compte dans le cas d'espèce de l'intérêt que présenterait pour le public la divulgation de l'information. Dans chaque cas particulier, l'intérêt public servi par la divulgation est mis en balance avec l'intérêt servi par le refus de divulguer. Les États membres ne peuvent, en vertu du paragraphe 2, points a), d), f), g) et h), prévoir qu'une demande soit rejetée lorsque elle concerne des informations relatives à des émissions dans l'environnement.

Dans ce cadre, et aux fins de l'application du point f), les États membres veillent au respect des exigences de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ».

27.3. Au regard de l'article 4, paragraphe 2, troisième alinéa, de la directive 2003/4/CE, il va de soi que, si, ainsi que le prévoit l'article 4, paragraphe 2, deuxième alinéa, troisième phrase, de la directive 2003/4/CE, la demande ne peut pas être rejetée pour le motif prévu au paragraphe 3, alinéa 1er, 5°, de l'article B.I.18 du Code en projet (« la confidentialité des données à caractère personnel et des dossiers concernant une personne physique si cette personne n'a pas consenti à la divulgation de ces informations au public, lorsque la confidentialité de ce type d'information est prévue par le droit régional ou européen »), les autorités concernées doivent néanmoins veiller, dans l'hypothèse où les informations environnementales concernant des émissions dans l'environnement comporteraient des données à caractère personnel, au respect des exigences du RGPD, et dès lors vérifier concrètement si la communication des données à caractère personnel est indispensable à l'intérêt protégé par la communication des informations relatives aux émissions dans l'environnement ([31]).

Article B.I.24

28. L'article B.I.24 du Code en projet dispose que : « Le présent Livre ne préjudicie pas aux dispositions législatives qui prévoient une publicité plus étendue de l'administration ». Ainsi, cette disposition en projet reproduit l'article 37 du décret et ordonnance conjoints de la Région de Bruxelles-Capitale, de la Commission communautaire commune et de la Commission communautaire française du 16 mai 2019 « relatifs à la publicité de l'administration dans les institutions bruxelloises ». Cette dernière disposition reproduisait à son tour l'article 22 de l'ordonnance du 30 mars 1995 « relative à la publicité de l'administration », sur lequel l'avis 23.853/1 a formulé l'observation suivante :

« Selon cet article, l'ordonnance ne préjudicie pas aux dispositions législatives qui prévoient une publicité plus étendue de l'administration. Il est permis de présumer que les « dispositions législatives » visées comportent également les dispositions d'ordonnances et que l'article emporte, par conséquent, que des ordonnances prévoyant une publicité moins étendue de l'administration doivent être réputées être implicitement abrogées, sur ce point, par l'ordonnance relative à la publicité de l'administration (voir, par exemple, l'ordonnance du 29 août 1991 sur l'accès à l'information relative à l'environnement dans la Région de Bruxelles-Capitale). Le Gouvernement devra veiller à vérifier quelles ordonnances ou parties de celles-ci seront ainsi abrogées de manière implicite, afin que les règles en question soient également abrogées de manière explicite en temps utile. » ([32]).

La même observation peut être formulée en ce qui concerne le Code en projet à l'examen.

---

(31) Si tel n'est pas le cas, les données à caractère personnel pourraient être occultées dans le document transmis.

(32) Avis 23.853/1 donné le 24 novembre 1994 sur un avant-projet devenu l'ordonnance de la Région de Bruxelles-Capitale du 30 mars 1995 « relative à la publicité de l'administration », *Doc. parl.*, Parl. Rég. Brux.-Cap., 1994-1995, n° A-353/1, p. 25. Voir également l'avis 65.516/1 du 27 mars 2019, *Doc. parl.*, Parl. Rég. Brux.-Cap., 2018-2019, n° A-862/1 - B-172/1, p. 57.

Article B.II.3

29.1. Le paragraphe 2 de l'article B.II.3 du Code en projet prévoit :

« La Commission peut, d'initiative, émettre des avis sur l'application générale du Livre B.I. portant sur la publicité administrative, le Livre B. II l'instituant et le Livre C. IV en matière de partage administratif et de réutilisation, ainsi que sur les arrêtés d'exécution de ces livres. […]

La Commission peut également remettre des avis à la demande d'une Autorité publique à propos d'une question relative à l'application du Livre B.I. portant sur la publicité administrative, du présent Livre et du Livre C. IV en matière de partage administratif et de réutilisation, ainsi que sur les arrêtés d'exécution de ces livres ».

29.2. Le maintien de la compétence d'avis de la Commission d'accès aux documents administratifs et aux données agissant à la demande d'une autorité publique, qui figure à l'article B.II.3, § 2, alinéa 2, du Code en projet, suppose que soit organisé un mécanisme permettant d'éviter les cas dans lesquels, saisie d'un recours, ladite Commission devrait également donner avis sur la même question à la demande de l'autorité contre la décision de laquelle le recours est introduit ([33]) ([34]).

(33) Voir en ce sens l'avis 64.533/4 donné le 3 décembre 2018 sur des amendements à une proposition devenue le décret de la Communauté française du 14 mars 2019 « modifiant le décret du 22 décembre 1994 relatif à la publicité de l'Administration afin de renforcer le rôle de la Commission d'accès aux documents administratifs de la Communauté française », *Doc. parl*., Parl. Comm. fr., 2017-2018, n° 625/4, pp. 2-5; l'avis 74.617/2, *Doc. parl*., Chambre, 2022-2023, n° 3217/13, pp. 3-15, observation sous l'amendement n° 17, point 5.

(34) Voir le rapport annuel 2023 de la Commission d'accès aux documents administratifs bruxelloise, p. 4 : « Dans un de ses avis (AI. 22.23 du 6 mars 2023 [lequel se réfère à l'avis interprétatif n° 16.22 du 29 novembre 2022 lequel se réfère aux AI 8.21 du 1er avril 2021, 11.21 du 21 mai 2021 et 13.21 du 16 septembre 2021]), la Commission a réitéré le principe important selon lequel il n'est pas de sa compétence d'émettre un avis à l'intention d'une autorité administrative sur une demande d'accès (individuelle) qui est examinée parallèlement par cette autorité. L'émission d'un avis dans un tel contexte constituerait une entorse aux garanties établies par le législateur bruxellois pour mettre en œuvre l'article 32 de la Constitution. En effet, l'intention ne peut être que la Commission émette un avis dans le cadre d'une demande d'accès individuelle qui pourrait par la suite être contestée devant la Commission par le biais d'un recours. Concrètement, la Commission devra donc – le cas échéant vérifier dans chaque cas si la demande d'avis présente un degré d'abstraction suffisamment avéré pour qu'elle puisse émettre un avis général sur l'application/le champ d'application du DOC ».

Le texte sera complété en conséquence ([35]).

Article B.II.5

30. Le paragraphe 3, alinéa 2, de l'article B. II.5 du Code en projet dispose :

« Les deux membres de la chambre, en dehors du Président, sont désignés notamment en raison de leur connaissance approfondie dans le domaine de la gestion des données dans le secteur public et de l'échange de données d'information entre le secteur public et le secteur privé. Ils doivent être titulaires d'un diplôme universitaire de deuxième cycle et justifier une connaissance et d'une expérience suffisantes en matière de gestion des données dans le secteur public. La chambre doit être composée au minimum d'une personne titulaire d'un diplôme universitaire de deuxième cycle en droit et d'une personne démontrant une compétence technique dans le secteur des nouvelles technologies ».

En précisant que les désignations se font « notamment » en raison des connaissances, le paragraphe semble concevoir que d'autres critères puissent être pris en considération. Le commentaire de la disposition ne fournit aucune précision sur ce point. Par ailleurs, il convient de relever que le mot « notamment » est absent du dispositif lorsqu'il énonce les règles de désignation des autres membres de la commission.

La disposition sera revue pour compléter le dispositif à la lumière de l'observation ou, le cas échéant, pour omettre le mot « notamment ».

Article B.II.7

31. Au paragraphe 2, 1°, de l'article B.II.7 du Code en projet, il est fait référence à l'hypothèse où le président ou tout autre membre de la Commission « manque à ses devoirs ».

Dans un souci de sécurité juridique, dès lors que la disposition organise la cessation anticipée des fonctions, il convient de prévoir une disposition spécifique reprenant les devoirs spécifiques dont il est ici question et qui différeraient des autres obligations des membres de la Commission, mentionnées au paragraphe 2, 2° à 4°, du même article.

(35) Par exemple, par la précision, ainsi que le prévoit l'alinéa 1er du paragraphe 2 de l'article B.II.3 du Code en projet, que la demande d'avis porte sur une question relative à l'application « générale » des parties visées du Code en projet.

Articles B.II.16 et B.II.17

32. L'article B.II.16, § 1er, du Code en projet fait double emploi avec l'article B.II.17, § 2, dans la mesure où ces deux dispositions prévoient toutes deux les points de départ des délais envisagés.

Les dispositions seront revues pour assurer leur articulation et, le cas échéant, pour omettre la répétition.

Article B.II.20

33. Au paragraphe 2, 2°, de l'article B.II.20 du Code en projet, il est énoncé qu'

« [e]n l'absence de notification du maintien de son recours par le requérant dans un délai de 15 jours à compter de la réception par la Commission de la notification du médiateur, le requérant est réputé se désister de son recours ».

Toutefois, le texte néerlandais des avant-projets de décret et ordonnance conjoints de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française, sur lesquels la section de législation a donné les avis 75.158/VR et 75.314/VR, énonce cette disposition en ces termes :

« Indien de verzoeker de Commissie niet binnen 15 dagen na ontvangst van de kennisgeving van de Ombudsman meedeelt dat hij het beroep wenst te handhaven, wordt hij geacht het beroep te hebben ingetrokken. ».

Le texte néerlandais permet de déduire que c'est la réception de la notification du médiateur par le requérant qui est visée. En outre, l'intéressé n'a pas connaissance de la réception de la notification du médiateur par la Commission, de sorte que le délai de quinze jours dont il est question dans cette disposition, ne peut raisonnablement pas commencer à courir pour lui à ce moment-là. Eu égard à ce qui précède, on omettra les mots « par la Commission » dans le texte à l'examen.

Article B.II.21

34. L'obligation de motivation formelle résulte déjà de la loi du 29 juillet 1991 « relative à la motivation formelle des actes administratifs ».

Cette obligation ne doit dès lors pas être répétée dans la disposition à l'examen.

L'alinéa 3 de l'article B.II.21 du Code en projet sera donc omis.

Article B.II.25

35. Au paragraphe 2 de l'article B.II.25 du Code en projet, il convient de compléter la disposition de manière telle que le rapport annuel qui y est visé soit simultanément déposé au Parlement de la Région de Bruxelles-Capitale, ainsi qu'à l'assemblée réunie de la Commission communautaire commune et à l'assemblée de la Commission communautaire française.

36. Au paragraphe 4 du même article, il convient, pour éviter toute ambiguïté, de préciser l'objet du bilan que la Commission doit opérer dans les deux ans après l'entrée en vigueur du Livre B.II.

Article C.II.2

37. L'articulation entre le paragraphe 2 et le paragraphe 3, alinéa 2, de l'article C.II.2 du Code en projet, qui semblent en partie redondants ([36]), n'apparaît pas clairement.

La disposition sera adaptée en conséquence.

Article C.II.6

38. La notion de « standards communs », visée au 3° de l'article C.II.6 du Code en projet, n'est nullement définie dans le reste du Code. Or, l'article C.II.9 en projet prévoit que les autorités publiques doivent déployer des solutions qui privilégient ceux-ci.

À cet égard, il y a lieu de s'interroger au sujet de l'articulation de ces « standards communs » avec les « standards reconnus au niveau national ou international » évoqués à l'article C.II.17, alinéa 2, du Code en projet.

---

(36) Le paragraphe 2 en projet prévoit : « Les Autorités publiques sécurisent les données, et plus spécifiquement les données protégées, en toute circonstance, à des fins de qualité et de respect des droits des tiers ». Le paragraphe 3, alinéa 2, en projet prévoit : « Les Autorités publiques garantissent notamment la protection et la sécurisation des données protégées. Plus particulièrement, les Autorités publiques garantissent que les données à caractère personnel ou faisant l'objet de droits de propriété intellectuelle, ou contenant des secrets d'affaires ou commerciaux, ou encore des secrets statistiques, ne peuvent être partagées qu'aux conditions légales ou réglementaires en vigueur. Les Autorités publiques protègent également la vie privée et les droits des personnes concernées par les données à caractère personnel qu'elles détiennent ».

L'article C.II.6 du Code en projet sera revu et la notion sera explicitée pour éviter, le cas échéant, toute confusion.

Article C.II.11

39. L'article C.II.11 du Code en projet dispose que les autorités publiques favorisent la culture de la donnée, entre autres notamment par « la mobilisation » de toutes les parties prenantes. Au lieu de cela, on écrira « l'implication ».

Article C.II.14

40. La portée de la notion d'« espaces européens communs », visée à l'alinéa 2, 2°, de l'article C.II.14 du Code en projet est ambiguë et sera explicitée.

Article C.III.1

41. Aux alinéas 3 et 4 de l'article C.III.1 du Code en projet, les renvois dont il est fait mention seront complétés.

Interrogé à ce sujet, le délégué a indiqué que les alinéas doivent être complétés comme suit :

« Le deuxième palier est soumis au :

Titre 1 du présent livre,

Titre 2 du présent livre,

Titre 3 du présent Livre à l'exception du chapitre 2,

Titre 4 du présent livre,

Le troisième palier est soumis au :

Titre 1 du présent livre

Titre 2 du présent livre

Chapitre 3 du titre 3 du présent livre

Article C.III.16, al. 1 et 2 du titre 4 du présent livre ».

Article C.III.9

42. Le paragraphe 1er, alinéa 1er, de l'article C.III.9 du Code en projet dispose :

« [l]es données publiques d'un partenariat sont catégorisées au minimum conformément au présent titre ».

Interrogé sur la portée de cet alinéa, le délégué a répondu :

« Le paragraphe 1er exprime l'obligation pour les Autorités publiques d'identifier et de classifier les données conformément au présent chapitre. Il est important de préciser que la catégorisation proposée est un cadre minimal sur lequel peuvent venir se greffer d'autres catégories identifiées selon le cas par les Autorités publiques ou tout autre partie. Il est envisageable que de nouvelles classifications, ou de nouveaux types de données apparaissent au fil des usages.

Chaque donnée est identifiée au regard de chacune des classifications proposées en vue de générer les métadonnées telles que prévues par le titre 4. Cela permet de générer des métadonnées (données qui fournissent des informations sur d'autres données) utiles et compréhensibles pour tous puisque les catégories de données sont normalisées au travers de la nomenclature commune. Chaque utilisateur peut donc récupérer les données pertinentes pour ses besoins.

L'approche vise à s'assurer que les métadonnées générées sont compréhensibles et pertinentes peu importe le point de vue de l'utilisateur. Cela signifie que, que l'on soit un analyste, un gestionnaire de données, un décideur, ou un auditeur externe, les métadonnées fournissent une information claire et immédiatement utile sur les données concernées ».

Le segment de phrase selon lequel les données « sont catégorisées au minimum » manque toutefois de clarté et sera reformulé pour mieux traduire l'intention des auteurs de l'avant-projet, telle que celle-ci ressort des explications du délégué.

43. Au sujet du paragraphe 2 du même article, le délégué a indiqué ce qui suit :

« Le paragraphe 2 précise que chaque catégorie de donnée est encadrée par un ensemble de dispositions juridiques et administratives (par exemple le RGPD pour les données à caractère personnel, le respect des droits d'auteurs pour les données protégées par des droits intellectuels, …) ».

Compte tenu de ces explications, la portée normative de ce paragraphe n'est pas certaine dès lors qu'il se contente de répéter que chaque catégorie de données est régie par d'autres dispositions.

Pour éviter toute interprétation erronée, et dès lors que la plus-value de ce paragraphe n'apparaît pas clairement, le paragraphe 2 sera omis.

Article C.III.14

44. L'article C.III.14, § 5, du Code en projet dispose :

« Sans préjudice des droits des personnes concernées et des recours organisés par le RGPD, les Autorités publiques organisent les recours internes permettant aux personnes titulaires de droits sur les données protégées [de] déposer plainte auprès des services ou des personnes compétentes au sein des Autorités publiques dès qu'ils estiment que leurs droits ne sont pas respectés ou sont menacés ».

On n'aperçoit pas ce qu'il y a lieu d'entendre par « les recours internes ». Si les auteurs de l'avant-projet se réfèrent à une procédure de dépôt de plaintes, il est recommandé de le préciser en termes exprès dans la disposition en projet et en outre de développer ce point. Dans la mesure où l'intention serait plutôt d'instaurer une autre voie de recours interne, les principes qui s'y appliqueraient devraient être définis de manière plus circonstanciée dans le dispositif de cette disposition afin de faire apparaître plus clairement l'intention des auteurs de l'avant-projet. Dans ce cas aussi, il y a lieu d'expliciter la voie de recours envisagée.

Article C.III.25

45. Le paragraphe 4 de l'article C.III.25 du Code en projet énonce :

« Conformément avec l'état de l'art, le chiffrement des données protégées en transit est obligatoire, notamment lors de la transmission via des réseaux non sécurisés. ».

Or, le paragraphe 5 du même article répète pour sa part :

« Conformément à l'état de l'art, le chiffrement des données protégées en transit est obligatoire ».

Compte tenu de cette répétition, le paragraphe 5 sera omis, et la numérotation des paragraphes sera adaptée en conséquence dans l'article en projet.

Article C.IV.2

46. Au 5° de l'article C.IV.2 du Code en projet, il convient d'ajouter l'intitulé complet de la directive (UE) 2019/1937, à savoir la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 « sur la protection des personnes qui signalent des violations du droit de l'Union ».

Article C.IV.15

47. Au paragraphe 3, 1°, de l'article C.IV.15 du Code en projet, il convient de remplacer les mots « l'article 2, alinéa 2, de la loi du 8 août 1983 » par les mots « l'article 2, § 3, de la loi du 8 août 1983 ».

Article C.IV.17

48. Dans la phrase liminaire du paragraphe 4, alinéa 1er, de l'article C.IV.17 du Code en projet, les mots « visée au paragraphe 2, 1° et 2° » seront remplacés par les mots « visée au paragraphe 3, 1° et 2° ».

49. Au paragraphe 4, alinéa 2, du même article, les mots « visée au paragraphe 2, 3° » seront remplacés par les mots « visée au paragraphe 3, 3° ».

Article C.IV.18

50. Le 1° de l'article C.IV.18 du Code en projet envisage le régime de réutilisation suivant :

« la réutilisation des documents et des données publiques des Autorités publiques ouverts accessibles librement et des documents partageables accessibles aux conditions décrites dans le présent, titre conformément à la transposition de la Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte) ».

Il convient de relever qu'une disposition de droit interne ne doit pas faire référence à une directive, mais aux dispositions de droit interne qui ont transposé cette dernière.

Article C.IV.21

51. L'alinéa 1er de l'article C.IV.21 du Code en projet ne présente aucun contenu normatif, mais doit être assimilé à un intitulé.

L'alinéa sera omis.

Article C.IV.22

52. À l'alinéa 5 de l'article C.IV.22 du Code en projet, les mots « l'article C.VI.33 » seront remplacés par les mots « l'article C.IV.33 ».

Article C.IV.24

53. Au paragraphe 2 de l'article C.IV.24 du Code en projet, la notion de « normes formelles ouvertes au sens du présent Code » n'est nullement explicitée et manque de précision.

La disposition sera complétée sur ce point.

Article C.IV.25

54. L'article C.IV.25, § 1er, du Code en projet dispose qu'une redevance « peut » être demandée pour la mise à disposition d'un document.

Ainsi, le pouvoir de prélever ou non une redevance est délégué aux autorités publiques auxquelles s'applique l'article C.IV.25.

Même si, comme tel est le cas en l'espèce, la faculté d'exiger une rétribution est inscrite dans une norme européenne, sa mise en œuvre doit prendre en considération le principe de légalité formelle relative au prélèvement de rétributions énoncé à l'article 173 de la Constitution. Conformément à cet article, il appartient au législateur décrétal ou régional bruxellois de préciser les cas qui peuvent donner lieu à la perception d'une rétribution, ainsi que de désigner les redevables ([37]). En outre, c'est au législateur, qui a le pouvoir d'établir une rétribution, qu'il incombe de déterminer également les cas dans lesquels peuvent être accordées les exemptions et réductions ([38]). Il n'est donc pas conforme à cette disposition constitutionnelle de confier au pouvoir exécutif le soin de décider de percevoir ou non une rétribution.

Il convient de réexaminer l'article C.IV.25 du Code en projet au regard de ce qui précède.

Article C.IV.26

55. L'alinéa 4 de l'article C.IV.26 du Code en projet prévoit :

« Pour l'application du présent article, les Autorités publiques utilisent les licences prévues au Chapitre II de l'arrêté du Gouvernement de la Région de Bruxelles-Capitale du 1er février 2018 portant exécution de l'ordonnance du 27 octobre 2016 visant à l'établissement d'une politique de données ouvertes (open data) et portant transposition de la Directive 2013/37/UE du Parlement européen et du conseil du 26 juin 2013 modifiant la Directive 2003/98/CE du Parlement européen et du conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, jusqu'à ce que celui-ci soit abrogé. ».

Cet alinéa s'assimile à une disposition transitoire, laquelle doit prendre place, pour plus de lisibilité, à la fin de l'avant-projet, de manière autonome.

Article C.IV.30

56. L'alinéa 2 de l'article C.IV.30 du Code en projet doit indiquer le numéro d'ordre de la directive (UE) 2019/2024.

Article C.V.2

57. La notion de « cadre documentaire de base », visée à l'alinéa 1er, 3°, de l'article C.V.2 n'est pas définie dans le Code en projet.

La disposition sera complétée pour que la notion soit davantage explicitée.

Article C.V.4

58. D'une manière générale, l'usage de tirets à l'intérieur d'une énumération est à éviter ([39]). Il convient d'utiliser à l'article C.V.4 du Code en projet les subdivisions 1°, 2°, 3° …, elles-mêmes éventuellement subdivisées en a), b), c), etc.

(37) Avis 69.675/3 donné le 20 juillet 2021 sur un projet d'arrêté ministériel flamand « over de toekenning van een verklaring van vrijstelling voor het nemen van een loods of het gebruikmaken van loodsen op afstand », observation 3.2; avis 68.145/3 donné le 10 novembre 2020 sur un projet devenu l'arrêté du Gouvernement flamand « tot vaststelling van de verordening voor het verkeer van havenvoertuigen in de haven van Antwerpen », observation 5.2.3.

(38) Avis 62.411/2/AG donné le 2 mars 2018 sur un avant-projet de loi « instaurant la Brussels International Business Court », *Doc. parl.*, Chambre, 2017-2018, n° 3072/001, pp. 94 148, observation 48 (avec référence à l'avis 46.941/3 donné le 14 juillet 2009 sur un projet devenu l'arrêté royal du 27 octobre 2009 « fixant le montant et le mode de paiement des redevances perçues en application de la réglementation relative à la protection contre les rayonnements ionisants »; avis 47.147/1/V donné le 8 septembre 2009 sur un projet devenu l'arrêté royal du 13 juin 2010 « modifiant l'arrêté royal du 19 avril 1999 fixant les conditions dans lesquelles le Fonds des maladies professionnelles peut émettre des avis en matière d'exposition aux risques de maladie professionnelle dans le cadre de ses missions préventives »; avis 49.269/3 donné le 8 mars 2011 sur un avant-projet devenu le décret de la Région flamande et de la Communauté flamande du 8 juillet 2011 « tot wijziging van verschillende decreten in het kader van de herstructurering van het agentschap Toerisme Vlaanderen » (Tourisme Belgique-Flandre & Bruxelles), *Doc. parl.*, Parl. fl., 2010-2011, n° 1093/1.

(39) *Principes de technique législative – Guide de rédaction des textes législatifs et réglementaires*, www.conseildetat.be, onglet « Technique législative », recommandation n° 58.

La même observation vaut *mutatis mutandis* pour les articles C.V.6 et C.V.8 du Code en projet.

Article C.V.5

59. Le dernier alinéa de l'article C.V.5 du Code en projet n'est revêtu d'aucune valeur normative propre, la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel » et le RGPD devant en tout état de cause être respectés. Le dernier alinéa de cet article est donc superflu et sera omis.

Article C.V.17

60. L'article C.V.17 du Code en projet reproduit partiellement le contenu de l'article 7, paragraphe 4, du règlement sur la gouvernance des données, en particulier en ce qui concerne la nature de l'assistance.

Il y a lieu de rappeler que, conformément à l'article 288, deuxième alinéa, du Traité sur le fonctionnement de l'Union européenne (ci-après : « TFUE »), un règlement est obligatoire dans tous ses éléments et est directement applicable dans tout État membre. Sauf lorsqu'un règlement confie certaines mesures d'exécution aux États membres ou si le règlement concerné laisse une certaine marge pour prendre pareilles mesures, une telle applicabilité directe signifie qu'il n'est pas nécessaire que les États membres interviennent en vue d'intégrer les dispositions du règlement dans leur ordre juridique interne. Les dispositions d'un règlement ne doivent notamment pas être transposées dans le droit interne des États membres. Un tel procédé est non seulement superflu d'un point de vue normatif, dès lors qu'il ne crée aucune nouvelle norme, mais il risque également de semer la confusion quant à la nature juridique de la règle incorporée dans le régime de droit interne et, notamment, en ce qui concerne la compétence de la Cour de justice de l'Union européenne à connaître de tout litige relatif aux règles définies par le règlement. Ce procédé risque aussi de créer une équivoque en ce qui concerne le moment de l'entrée en vigueur des normes concernées ([40]).

Si, dans l'intérêt de la lisibilité ou d'une bonne compréhension de la réglementation en projet ou modifiée, il s'avérait malgré tout nécessaire de reproduire une disposition d'un règlement, il conviendrait de se référer à cette disposition (« conformément ») afin que sa nature juridique demeure identifiable. En outre, il est recommandé de se rapprocher aussi textuellement que possible des dispositions du règlement concernées ([41]).

En ce qui concerne ce point, il convient de noter que l'article C.V.17 du Code en projet reproduit les formes d'assistance énumérées dans l'article 7, paragraphe 4, a), b), d) et e), du règlement sur la gouvernance des données mais pas celle énoncée à l'article 7, paragraphe 4, c), de ce règlement, ce qui peut prêter à confusion.

Dans un souci de sécurité juridique, il est recommandé soit d'omettre l'énumération de l'article C.V.17 du Code en projet et de plutôt faire référence « aux formes d'assistance énumérées dans l'article 7, paragraphe 4, du règlement sur la gouvernance des données », soit de compléter l'article C.V.17 sur ce point.

Article C.VI.6

61. Au paragraphe 3, alinéa 3, de l'article C.VI.6 du Code en projet il est énoncé que « [l]es membres permanents sont obligatoirement présents à chaque réunion du Comité de validation de l'architecture numérique ».

Il n'est toutefois pas précisé si l'absence d'un membre permanent entraîne des conséquences individuelles pour le membre concerné, même en cas de force majeure, ou si une telle absence entraîne l'irrégularité de la composition du comité dans son ensemble.

La disposition sera complétée pour fixer les conséquences de l'absence d'un membre permanent.

La même observation vaut *mutatis mutandis* pour l'article C.VI.11, § 2, alinéa 2, du Code en projet.

Article 20 (LIRE : Article 10)

62. À l'alinéa 1er, les mots « de la Région de Bruxelles-Capitale » seront insérés entre les mots « 17 juillet 2020 » et les mots « garantissant le principe ».

(40) C.J., 7 février 1973, C-39/72, Commission c. Italie, ECLI:EU:C:1973:13, points 16-17; C.J.U.E., 2 février 1977, C-50/76, *Amsterdam Bulb*, ECLI:EU:C:1977:13, points 4-7.

(41) Voir par exemple l'avis 74.481/1 donné le 31 janvier 2024 sur un avant-projet d'ordonnance du Gouvernement de la Région de Bruxelles-Capitale « modifiant l'ordonnance du 27 juillet 2017 visant à promouvoir la recherche, le développement et l'innovation par l'octroi d'aides affectées à des finalités économiques en faveur des entreprises et des organismes de recherche assimilés à des entreprises et l'ordonnance du 27 juillet 2017 visant à promouvoir la recherche, le développement et l'innovation par l'octroi d'aides à finalité non économique en faveur des organisations non-marchandes, des organismes de recherche et des entreprises », observation 3.1.

62. À l'alinéa 3, les mots « de la Région de Bruxelles-Capitale » seront insérés entre les mots « 27 octobre 2016 » et les mots « visant à l'établissement ».

64. À l'alinéa 4, les mots « de la Région de Bruxelles-Capitale » seront insérés entre les mots « 8 mai 2014 » et les mots « portant création et organisation ».

Les chambres réunies étaient composées de

Messieurs	J. VAN NIEUWENHOVE,	président de chambre, président
	B. BLERO,	président de chambre,
	L. CAMBIER,	
	K. MUYLLE,	
Mesdames	G. ROSOUX,	
	E. VAN DE VELDE,	conseillers d'État,
	M. DONY,	
Monsieur	B. PEETERS,	assesseurs,
Mesdames	A. GOOSSENS,	
	A.-C. VAN GEERSDAELE,	greffier.

Les rapports ont été présentés par M. R. WIMMER, premier auditeur, et MM. X. MINY, P. AERTGEERTS et R. VAN CROMBRUGGE, auditeurs adjoints.

Le Greffier, *La Présidente,*

A.-C. VAN GEERSDAELE J. VAN NIEUWENHOVE

ANNEXE 2

AVANT-PROJET DE DÉCRET ET ORDONNANCE CONJOINTS

portant le Code de la gouvernance et de la donnée et la désignation de la base de données cartographiques URBIS

TITRE I
Dispositions générales

Article 1er

La présente loi règle une matière visée à l'article 39, 135 et 135*bis* de la Constitution, ainsi qu'aux articles 127 et 128 de la Constitution en vertu de l'article 138 de celle-ci.

TITRE II
Code

Article 2

Les dispositions suivantes forment le Code de la gouvernance et de la donnée :

PARTIE A
DISPOSITIONS GÉNÉRALES

LIVRE A.I
Champ d'application

Article A.I.1.
Définitions communes au Code

Au sens du présent Code de la gouvernance et de la donnée, on entend par :

1) « Autorité publique » :

a) la Région de Bruxelles-Capitale, la Commission communautaire commune ou la Commission communautaire française;

b) les personnes morales de droit public qui dépendent, directement ou indirectement, de la Région de Bruxelles-Capitale, de la Commission communautaire commune ou de la Commission communautaire française;

c) les communes, les centres publics d'action sociale; les associations visées au Chapitre XII et XII*bis* de la loi du 8 juillet 1976, organique des centres publics d'action sociale;

d) les autorités administratives dépendant de la Région de Bruxelles-Capitale ou de l'Agglomération bruxelloise, dénommées ci-après « autorités administratives régionales ». Pour l'application du présent livre, les organes consultatifs régionaux en matière d'environnement ou d'aménagement du territoire sont assimilés à des autorités administratives régionales;

e) les autorités administratives dépendant de la COCOM et de la COCOF;

f) les autorités administratives communales, en ce compris les organes consultatifs communaux en matière d'environnement ou d'aménagement du territoire;

g) les intercommunales régionales et interrégionales soumises à la tutelle administrative de la Région de Bruxelles-Capitale ainsi qu'à leurs filiales, aux ASBL communales et pluri-communales et aux régies communales autonomes, visées par l'ordonnance du 5 juillet 2018 relative aux modes spécifiques de gestion communale et à la coopération intercommunale. Pour l'application du présent livre, les intercommunales et leurs filiales, les ASBL communales et pluri-communales, et les régies communales autonomes sont assimilées aux « autorités administratives communales »;

h) les personnes, quelles que soient leur forme et leur nature, qui :

– ont été créées pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial;

– sont dotées de la personnalité juridique;

– et dont soit l'activité est financée majoritairement par les Autorité publiques visées au point a),b),c), soit la gestion est soumise à un

contrôle de ces Autorités publique s ou soit plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance sont désignés par ces Autorités publiques;

i) les associations formées par une ou plusieurs Autorités publiques visées au point a), b), c) ou h);

j) toute personne physique ou morale :

a) qui exerce des fonctions administratives publiques, y compris des tâches, activités ou services spécifiques en rapport avec l'environnement ou l'aménagement du territoire;

b) ayant des responsabilités ou des fonctions publiques, ou fournissant des services publics, en rapport avec l'environnement ou l'aménagement du territoire sous le contrôle d'un organe ou d'une personne visée au point d) ou k), 0. Pour l'application du présent livre, ces personnes physiques ou morales sont assimilées à des « autorités administratives régionales »;

2) « COCOF » : Commission communautaire française;

3) « COCOM » : Commission communautaire commune;

4) « Gouvernement » : le Gouvernement de la Région de Bruxelles-Capitale;

5) « Collège réuni » : le Collège réuni de la Commission communautaire commune;

6) « Collège » : le Collège de la Commission communautaire française;

7) « CIRB » : centre informatique de la Région bruxelloise;

8) « Bruxelles Environnement » : l'organisme d'intérêt public créé par l'arrêté royal du 8 mars 1989;

9) « RGPD » :

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogeant la Directive 95/46/CE (règlement général sur la protection des données);

LIVRE A.II
Définitions

TITRE I
Définitions du livre B

Pour l'application du livre B.I., il faut entendre par :

1) « aménagement du territoire » : toutes les matières reprises à l'article 6, § 1er, I, de la loi spéciale de réformes institutionnelles du 8 août 1980;

2) « environnement » : toutes les matières reprises à l'article 6, § 1er, II, III et V de la loi spéciale de réformes institutionnelles du 8 août 1980;

3) « document administratif » : toute information, sous quelque forme que ce soit, dont une Autorité publique dispose;

4) « information environnementale » : toute information disponible sous forme écrite, visuelle, sonore, électronique ou toute autre forme matérielle, concernant :

a) l'état des éléments de l'environnement, tels que l'air et l'atmosphère, l'eau, le sol, les terres, les paysages et les sites naturels, y compris les biotopes humides, la diversité biologique et ses composantes, y compris les organismes génétiquement modifiés, ainsi que l'interaction entre ces éléments;

b) des facteurs, tels que les substances, l'énergie, le bruit, les rayonnements ou les déchets, les émissions, les déversements et autres rejets dans l'environnement, qui ont ou sont susceptibles d'avoir des incidences sur les éléments de l'environnement visés au point a);

c) les mesures, y compris les mesures administratives, telles que les politiques, les dispositions législatives, les plans, les programmes, l'évaluation des incidences environnementales des plans et programmes, les accords environnementaux et les activités ayant ou étant susceptibles d'avoir des incidences sur les éléments et les facteurs visés aux points a) et b), ainsi que les mesures ou activités destinées à protéger ces éléments;

d) les rapports sur l'application de la législation environnementale;

e) les analyses coût-avantages et autres analyses et hypothèses économiques utilisées dans le cadre des mesures et activités visées au point c), et

f) l'état de la santé de l'homme, sa sécurité et les conditions de vie des personnes, les sites culturels et les constructions, pour autant qu'ils soient ou puissent être altérés par l'état des éléments de l'environnement visés au point a), ou, par l'intermédiaire de ces éléments, par l'un des facteurs, mesures ou activités visés aux points b) et c);

g) l'aménagement du territoire;

5) « informations détenues par une Autorité publique » : le document administratif ou l'information environnementale qui est en la possession de cette Autorité et qui a été reçu ou établi par elle. Sauf si elle ne se rapporte manifestement pas à l'exercice des fonctions de l'intéressé, une donnée détenue par un membre du personnel attaché à une Autorité publique ou par un membre d'une instance collégiale constitutive d'une Autorité publique, est une donnée détenue par l'Autorité publique;

6) « demandeur » : toute personne physique ou morale qui demande un document administratif ou une information environnementale;

7) « public » : une ou plusieurs personnes physiques ou morales ainsi que les associations, organisations ou groupes constitués de ces personnes;

8) « jour ouvrable » : celui qui n'est ni un samedi, ni un dimanche, ni un jour férié;

9) « Étude » : travaux de recherche, de mise au point d'une question, d'un projet, réalisés de façon détaillée par des experts au sujet d'une thématique intéressant une ou plusieurs autorités bruxelloises; il peut notamment s'agir d'investiguer une question technique, scientifique, ou juridique, pour autant que l'analyse soit menée de façon approfondie;

10) « subvention » : toute forme de soutien financier, de contribution, d'avantage ou d'aide, quelles que soient sa forme ou sa dénomination, accordée dans une finalité directe ou indirecte d'intérêt général, à une activité organisée par un tiers, quelle que soit la dénomination de cette activité.

11) « Commission » : la Commission d'accès aux documents administratifs et aux données;

12) « partage administratif » : partage visé à l'article A. I.4.70 °;

13) « réutilisation » : réutilisation visées à l'article A.I.4. 71°.

TITRE II
Définitions du livre C

Article A.I.2

Au sens de la partie C du présent Code, on entend par :

1) « Arrêté fixant les seuils numériques » :

Arrêté conjoint du Gouvernement, du Collège et du Collège réuni fixant les seuils numériques, adopté sur la base de l'article C.III.1;

2) « Acte sur la gouvernance des données » ou « Data Governance Act » ou « DGA » :

Règlement 2022/868/UE du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724;

3) « Règlement eIDAS » :

Règlement (UE) 910/2014 du Parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur,abrogeant la Directive 1999/93/CE;

4) « Directive SRI 2 (NIS 2) » :

Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la Directive (UE) 2018/1972 et abrogeant la Directive (UE) 2016/1148 (Directive SRI 2);

5) « Autorité publique tierce » :

pouvoir public relevant d'un autre niveau de pouvoir, à savoir national ou international;

6) « donnée » :

donnée au sens de l'article 2, 1) du DGA;

7) « document » :

tout contenu, quel que soit son support (papier ou forme électronique, enregistrement sonore, visuel ou audiovisuel) ou toute partie de ce contenu;

8) « donnée à caractère personnel » :

donnée à caractère personnel au sens de l'article 4, 1) du RGPD;

9) « donnée protégée » :

toute donnée qui est protégée pour l'un des motifs suivants :

(a) confidentialité commerciale, y compris le secret d'affaires, le secret professionnel et le secret d'entreprise;

(b) secret statistique;

(c) protection des droits de propriété intellectuelle de tiers;

(d) protection des données à caractère personnel;

10) « donnée sensible » :

toute donnée considérée comme confidentielle compte tenu du risque que leur accès ou leur diffusion représenterait pour l'Autorité publique et pour les droits et libertés des personnes, ainsi que toute donnée classifiée;

11) « donnée classifiée » :

donnée nécessitant un degré de protection en matière de sécurité imposé par la loi, par des traités ou des conventions liant la Belgique;

12) « jeu de données » :

ensemble cohérent de ressources ou d'informations (fichiers de données, fichiers d'explications, API, lien …) et de métadonnées (description, producteur, date de publication, mots-clefs, couverture géographique temporelle …) sur un thème donné;

13) « donnée ouverte » :

toute donnée librement accessible;

14) « donnée acquise » :

toute donnée obtenue auprès de tiers au moyen de contrats de licence commerciale ou par des moyens non commerciaux;

15) « donnée à forte valeur (ensemble de) » :

toute donnée qui présente des avantages importants pour la société, l'environnement ou l'économie, en particulier parce qu'elles se prêtent à la création de services possédant une valeur ajoutée, d'applications et de nouveaux emplois convenables tels que définis par l'arrêté ministériel du 26 novembre 1991 portant les modalités d'application de la réglementation du chômage, ainsi qu'en raison du nombre de bénéficiaires potentiels des services et applications à valeur ajoutée fondés sur ces ensembles de données;

16) « donnée déduite » et « donnée dérivée » :

toute donnée générée par analyse ou mise en relation avec d'autres données;

17) « données d'origine privée » :

toute donnée produite par des entités privées;

18) « donnée exclusive » :

toute donnée protégée par des droits de propriété intellectuelle ou commerciaux, dont les droits d'auteur et les secrets commerciaux, ou par des privilèges d'accès et de contrôle;

19) « donnée fermée » :

toute donnée qui n'est en principe pas accessible sauf si la réglementation en vigueur en dispose autrement;

20) « donnée fournies librement » :

toute donnée partagée activement et délibérément par une entité;

21) « données observée » :

toute donnée saisie et enregistrée relative à des activités concernant un utilisateur ou tout phénomène observable;

22) « donnée partageable » :

toute donnée qui peut être partagée de façon contrôlée ou restreinte, notamment au travers d'un cadre réglementaire ou légal;

23) « donnée publique » :

toute donnée détenue et gérée par les Autorités publiques dans le cadre de leurs missions de services publics;

24) « donnée d'usage » :

toute donnée issue de l'activité d'un utilisateur de données et, plus spécifiquement, de son interaction avec des données; les données d'usage sont collectées afin de fournir de l'information sur l'utilisateur;

25) « donnée de contenu » :

toute donnée qui transmet l'essence, la substance, le sens ou le but d'une donnée ou d'une communication informatique stockée ou transmise;

26) « donnée de référence » :

toute donnée considérée comme structurante, par l'Autorité publique ou par l'usage, notamment pour nommer ou identifier des produits, des entités économiques, des territoires ou des personnes physiques et morales;

27) « donnée dynamique » :

tout donnée faisant l'objet d'actualisations fréquentes ou en temps réel, notamment à cause de leur volatilité ou de leur obsolescence rapide; les données émanant de capteurs sont typiquement considérées comme étant des données dynamiques;

28) « données de la recherche » :

toute donnée, autres que des publications scientifiques, qui sont recueillis ou produits au cours d'activités de recherche scientifique et utilisés comme éléments probants dans le processus de recherche, ou dont la communauté scientifique admet communément qu'ils sont nécessaires pour valider des conclusions et résultats de la recherche;

29) « métadonnée » :

toute donnée relative à des données ou à des éléments de données, et décrivant un contenu, en mentionnant par exemple la date de création d'un document, l'auteur, le volume ou le format;

30) « donnée issue de source authentique » :

donnée récoltée et gérée par une Autorité publique désignée comme producteur des données ou récoltée et gérée par une Autorité publique tierce;

31) « source authentique » :

toute base de données comprenant des données qui font foi comme données uniques et originales concernant la personne ou le fait concerné(e) dont la gestion est assurée exclusivement par une Autorité publique ou une Autorité publique tierce, désigné comme producteur de la base de donnée, et dont le contenu est destiné à faire l'objet de partages administratifs obligatoires conformément au principe de la collecte unique;

32) « source authentique bruxelloise » :

source authentique dont l'Autorité publique désignée producteur des données relève de la compétence de la Région, de la COCOM ou de la COCOF;

33) « domaine de données » :

champ spécifique ou relatif à un sujet d'intérêt dans lequel des données sont gérées;

34) « utilisateur (des données) » :

utilisateur défini au sens de l'article 2, 9) du DGA;

35) « administrateur de base de données » :

fonction visant la prise en charge des opérations de surveillance, de maintenance et de gestion des interactions des données avec les applications et processus métiers, disposant de droits privilégiés leur permettant de réaliser leurs tâches d'administration;

36) « administrateur de sécurité informatique » :

fonction visant la prise en charge de la protection des données et des systèmes d'information contre les menaces sur la sécurité;

37) « administrateur réseau » :

fonction portant sur la mise en place, de la maintenance et de la surveillance des réseaux informatiques, également chargé de la configuration des équipements réseau, de l'optimisation des performances, de la sécurité des communications et de la résolution des problèmes relatifs au réseau de communication;

38) « administrateur système » :

fonction visant la prise en charge des systèmes informatiques et de leur bon fonctionnement,

dont les tâches visent l'installation de la maintenance et de la mise à jour des logiciels et des matériels, la sauvegarde et la restauration des données, ainsi que la résolution des problèmes techniques;

39) « organisation altruiste » :

organisation qui a pour mission d'encourager l'altruisme en matière de données;

40) « altruisme en matière de données » :

activité et finalité définie par l'article 2, 16) du DGA;

41) « prestataire de services de confiance » :

prestataire tel que défini à l'article 3, 19) du Règlement eIDAS;

42) « service de confiance » :

service défini à l'article 3, 16) du Règlement eIDAS.

43) « prestataire de services en nuage » :

tout prestataire de service numérique qui permet l'administration à la demande et l'accès large à distance à un ensemble modulable et variable de ressources informatiques pouvant être partagées, y compris lorsque ces ressources sont réparties à différents endroits;

44) « prestataire de services informatiques de stockage » :

prestataire qui fournit des services de stockage de données informatiques pour les entreprises et les organisations;

45) « service d'intermédiation de données » :

service défini à l'article 2, 11) du DGA;

46) « écosystème numérique bruxellois » :

le réseau de parties prenantes, partenaires, infrastructures informatiques, systèmes d'informations qui sont interconnectés dans un espace numérique, ainsi que des réseaux de communication électroniques, filaires et radios, au sein du territoire de la Région de Bruxelles-Capitale;

47) « Plateforme bruxelloise de la donnée » :

plateforme visée à l'article C.V.1;

48) « Centre d'intégration bruxellois » :

Centre d'intégration visé à l'article visé à l'article B.V.7;

49) « Catalogue des données » :

catalogue des données visé à l'article C.V.9;

50) « Portail ouvert des données publiques » :

portail ouvert des données publiques visé à l'article C.V.10;

51) « Centre d'exploitation et d'analyse des données » :

centre d'exploitation et d'analyse des données visé à l'article C.V.11;

52) « Point de contact et d'information » :

service visé à l'article C.V.12;

53) « Service d'appui » :

service visé à l'article C.V.13;

54) « Secrétariat numérique » :

service visé à l'article C.VI.4;

55) « Comité de coordination numérique » :

l'organe visé à l'article C.VI.11;

56) « Bureau de la donnée » :

l'organe visé à l'article C.VI.17;

57) « Comité de validation de l'architecture numérique» :

l'organe visé à l'article C.VI.6;

58) « Comité de gouvernance de la donnée » :

l'organe visé à l'article C.VI.14;

59) « Bureau d'achats numériques » :

l'organe visé à l'article C.VI.8;

60) « administrateur local de la donnée » :

la fonction visée à l'article C.VI.21;

61) « responsable de la donnée » :

la fonction visée à l'article C.VI.22;

62) « conseiller en sécurité de l'information » :

la fonction visée à l'article C.VII.23;

63) « entreprise publique » :

toute entreprise :

i) exerçant des activités dans les domaines définis dans la Directive 2014/25/UE;

ii) agissant en qualité d'opérateurs de services publics conformément à l'article 2 du règlement (CE) n° 1370/2007;

iii) agissant en qualité de transporteurs aériens remplissant des obligations de service public conformément à l'article 16 du règlement (CE) n° 1008/2008;

iv) agissant en qualité d'armateurs communautaires remplissant des obligations de service public conformément à l'article 4 du règlement (CEE) n° 3577/92;

et sur laquelle les autorités publiques peuvent exercer directement ou indirectement une influence dominante du fait de la propriété de l'entreprise, de la participation financière qu'ils y détiennent ou des règles qui la régissent; l'influence dominante des autorités publiques sur l'entreprise est présumée dans tous les cas suivants lorsque ces organismes, directement ou indirectement :

a) détiennent la majorité du capital souscrit de l'entreprise;

b) disposent de la majorité des voix attachées aux parts émises par l'entreprise;

c) peuvent désigner plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance de l'entreprise;

64) « université » :

un organisme du secteur public dispensant un enseignement supérieur post-secondaire sanctionné par des diplômes universitaires;

65) « opérateur privé » :

toute personne physique ou morale ou organisation, ayant une personnalité juridique ou non, et qui n'est pas une Autorité publique;

66) « Autorité publique producteur (de données) » :

Autorité publique qui produit les données qui sont appelées à faire l'objet d'un partage administratif ou d'une réutilisation;

67) « Autorité publique destinataire » :

Autorité publique qui est destinée à recevoir les données dans le cadre d'un partage administratif ou d'une Communication;

68) « valorisation » :

traitement de données en vue de les exploiter de manière à optimiser les missions de services publics ou les obligations légales dont sont chargées les Autorités publiques ou à d'autres fins que celles pour lesquelles elles ont été collectées;

69) « partage de données» :

Partage de données visé à l'article 2, 10) du DGA;

70) « partage administratif » :

mise à disposition ou transmission de données publiques entre Autorités publiques, aux seules fins de l'exercice de leurs missions de services publics ou de leurs obligations d'intérêt général, à l'exclusion des partages avec le CIRB dans sa fonction de gestionnaire de la Plateforme bruxelloise de la donnée par rapport au Catalogue des données et à l'exclusion des partages visant les données ouvertes, sans conditions de réutilisation, disponibles dans le Portail ouvert des données publiques de la Plateforme bruxelloise de la donnée;

71) « Réutilisation » :

Utilisation par des personnes physiques ou morales de documents détenus par :

a) des Autorités publiques, à des fins commerciales ou non commerciales autres que l'objectif initial de la mission de service public pour lequel les documents ont été produits, à l'exception de l'échange de documents entre des Autorités publiques aux seules fins de

l'exercice de leur mission de service public, ou;

b) des entreprises publiques, à des fins commerciales ou non commerciales autres que l'objectif initial de fournir les services d'intérêt général pour lequel les documents ont été produits, à l'exception de l'échange de documents entre des entreprises publiques et des Autorités publiques aux seules fins de l'exercice de leur mission de service public;

72) « Communication » :

la fourniture de données d'un opérateur privé vers une ou plusieurs Autorité (s) publique(s) destinataire(s) à des fins exclusives d'utilisation dans le cadre de l'exécution de ses missions de service public ou d'intérêt général;

73) « Traitement » :

traitement défini à l'article 2, 12) du DGA;

74) « Accès » :

accès défini à l'article 2. 13) du DGA;

75) « Transmission » (dans le cadre d'un partage administratif) :

procédé qui, dans le cadre d'un partage administratif, implique l'envoi ou le déplacement actif d'une donnée depuis l'Autorité publique producteur de la donnée vers l'Autorité publique destinataire de la donnée à un autre, généralement via un réseau de communication;

76) « mise à disposition » (dans le cadre d'un partage administratif) :

procédé qui, dans le cadre d'un partage administratif, permet de rendre les données d'une Autorité publique producteur des données accessibles et utilisables par une Autorité publique destinataire de ces données au moyen d'un accès approprié;

77) « Anonymisation » :

processus de transformation des documents en documents anonymes ne permettant pas de remonter à une personne physique identifiée ou identifiable ou processus consistant à rendre anonymes des données à caractère personnel de telle sorte que la personne concernée ne soit pas ou plus identifiable;

78) « pseudonymisation » :

processus défini à l'article 4.5 du RGPD;

79) « Occultation » :

processus de transformation des documents ou données confidentielles en documents ou données ne permettant pas d'accéder aux données confidentielles ou consistant à masquer les données commerciales sensibles ou confidentielles de sorte qu'elles ne soient plus identifiables;

80) « Intégration des données » :

processus de combinaison de différents jeux de données pour en créer un seul plus complet et plus cohérent;

81) « Profilage » :

profilage défini à l'article 4.4 du RGPD;

82) « Archivage » :

conservation des données compte tenu d'un délai de conservation légal ou de l'utilité administrative caractérisant encore les documents et les données visées;

83) « Base de données » :

recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessibles par des moyens électroniques ou d'une autre manière;

84) « Consentement » :

le consentement au sens de l'article 4, point 11) du RGPD;

85) « Autorisation » :

l'autorisation visées à l'article 2. 6) du DGA

86) « Interopérabilité » :

capacité de différents systèmes, équipements, logiciels ou services à fonctionner ensemble de manière cohérente et à échanger des informations;

87) « (réseau et) Système d'information » :

Cette notion peut désigner :

a) un réseau de communications électroniques au sens de l'article 2, point a), de la Directive 2002/21/CE;

b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques; ou

c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance;

88) « Cas d'usage ou cas d'utilisation » :

manière d'utiliser un système d'information qui a une valeur ou une utilité pour les acteurs impliqués;

89) « Format ouvert » :

format de fichier indépendant des plates-formes utilisées et mis à la disposition du public sans restriction empêchant la réutilisation des documents;

90) « Informatique en nuage (cloud computing) » :

modèle de gestion informatique permettant l'accès via un réseau à des ressources informatiques partagées et configurables;

91) « Modèle opérationnel » :

représentation abstraite de la façon dont une organisation opère à travers des domaines de processus, d'organisation et de technologie afin d'accomplir sa fonction;

92) « Interface de programmation d'application » :

tout ensemble de fonctions, de procédures, de définitions et de protocoles qui permet le transfert de machine à machine et l'échange automatisé de données;

93) « Intelligence artificielle » :

logiciel développé au moyen d'une ou plusieurs techniques et approches telles que l'approche d'apprentissage automatique, l'approche fondée sur la logique et les connaissances ou les approches statistiques, et, qui peut, pour un ensemble donné d'objectifs définis par l'homme, générer des résultats tels que des contenus, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels il interagit;

94) « Licence type » :

une série de conditions de réutilisation prédéfinies dans un format numérique, de préférence compatible avec des licences publiques normalisées disponibles en ligne;

95) « Format lisible par machine » :

un format de fichier structuré de telle manière que des applications logicielles puissent facilement identifier, reconnaître et extraire des données spécifiques, notamment chaque énoncé d'un fait et sa structure interne;

96) « Norme formelle ouverte » :

norme établie par écrit, précisant en détail les exigences relatives à la manière d'assurer l'interopérabilité des logiciels;

97) « Retour sur investissement raisonnable » :

un pourcentage de la redevance globale, en sus du montant nécessaire au recouvrement des coûts éligibles, ne dépassant pas de plus de cinq points de pourcentage le taux d'intérêt fixe de la BCE;

98) « Tiers de confiance » :

le tiers de confiance est une entité indépendante qui dispose des moyens techniques nécessaires à l'anonymisation ou la pseudonymisation des données à caractère personnel dans le cadre des traitements énoncés par l'article 89 du RGPD;

99) « Sécurité de l'information » :

stratégie, règles, procédures et moyens de protection de tout type d'information tant dans les systèmes de transmission que dans les systèmes de traitement en vue de garantir la confidentialité, la disponibilité, l'intégrité, la fiabilité, l'authenticité et l'irréfutabilité de l'information;

100) « Intégrateur de services » :

une institution qui, par ou en vertu d'un traité, d'un règlement, d'une directive, d'une loi, d'un décret ou d'une ordonnance, est chargée de l'in-

tégration de services à un niveau de pouvoir ou dans un secteur déterminé

101) « Intégration de services » :

l'organisation d'échanges mutuels de données électroniques entre Autorités publiques entre elles et entre les Autorités publiques et les intégrateurs de services, ainsi que la mise à disposition intégrée de ces données;

102) « Intégrateur de service bruxellois » :

l'institution désignée à l'article C.V.7.

103) « Commande publique numérique mutualisable » :

commande publique numérique mutualisable : Achat en matière numérique considéré comme mutualisable portant sur des travaux, services ou fournitures ayant un impact sur l'écosystème numérique, qui reprend les besoins similaires des autorités publiques.

PARTIE B
GOUVERNANCE ADMINISTRATIVE

LIVRE B.I.
Publicité administrative

TITRE 1
Dispositions générales

Article A.I.1.
Dispositions générales

Le présent livre a pour objet de renforcer la transparence de l'administration en facilitant l'accès aux documents administratifs et aux informations environnementales.

Il vise également à transposer partiellement la Directive 2003/4/CE du Parlement européen et du Conseil du 28 janvier 2003 concernant l'accès du public à l'information en matière d'environnement et abrogeant la Directive 90/313/CEE du Conseil. À cette fin, il vise à garantir le droit d'accès aux informations environnementales détenues par les Autorités publiques ou pour leur compte, à fixer les conditions de base et les modalités pratiques de ce droit et à veiller à ce que les informations environnementales soient d'office rendues progressivement disponibles et diffusées auprès du public afin de parvenir à une mise à disposition et une diffusion systématique aussi large que possible des informations environnementales auprès du public. Dans ce but, il convient de promouvoir l'utilisation, entre autres, des technologies de télécommunication informatique ou des technologies électroniques, lorsqu'elles sont disponibles.

Le présent livre s'applique sans préjudice des dispositions applicables du règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE et sans préjudice de l'existence d'obligations d'omettre des informations qui doivent être tenues confidentielles en vertu d'une disposition de droit international en vigueur ou d'une norme interne à caractère législatif.

Il s'applique également sans préjudice de l'ordonnance du 4 octobre 2018 relative à l'accessibilité des sites internet et des applications mobiles des organismes publics régionaux et des communes.

Article A.I.2.
Champ d'application ratione personae

Le présent livre s'applique aux Autorités publiques visées à l'article A.I.1°, a), à g) et j).

Le présent livre s'applique également aux autorités administratives autres que celles visées à l'alinéa 1er, mais seulement dans la mesure où elles prohibent ou restreignent la publicité de documents administratifs pour des motifs relevant de la compétence de la Commission communautaire commune, de la Région de Bruxelles-Capitale et de la Commission communautaire française.

Article A.I.3.
Calcul des délais

Les délais prévus dans le présent livre commencent à courir le jour qui suit celui qui constitue le point de départ du délai. Le jour de l'échéance est compris dans le délai. Si ce jour n'est pas un jour ouvrable, le jour de l'échéance est reporté au jour ouvrable qui suit.

TITRE 2
Publicité active

CHAPITRE 1
Dispositions générales

Article A.I.4.
Publications sur les sites internet de chaque Autorité publique

§ 1er. – Les Autorités publiques disposent de sites internet qui comprennent, parmi les éléments de la

page d'accueil, une rubrique « transparence » aisément identifiable.

Cette rubrique contient au minimum :

1° un document décrivant les compétences, l'organisation et le fonctionnement de l'Autorité publique;

2° un inventaire des subventions accordées dans le courant de l'année précédente, mentionnant le bénéficiaire, l'objet de la subvention et son montant;

3° un inventaire des études réalisées pour le compte de l'Autorité publique dans le courant de l'année précédente, pour autant qu'elles aient été réalisées par un partenaire externe. L'inventaire mentionne, pour chaque étude, l'identité de son auteur, c'est-à-dire le nom de la personne morale ou physique à qui l'étude a été confiée, ainsi que son coût et le titre de l'étude;

4° un inventaire des marchés publics conclus dans le courant de l'année précédente, comprenant la mention de l'adjudicataire et le montant engagé;

5° les appels à candidats et les conditions de recrutement, de promotion ou de remplacement de tous les emplois qu'elles entendent pourvoir, publiés dans les sept jours ouvrables de la décision de procéder à un recrutement, une promotion ou un remplacement, ainsi que les décisions de recrutement, de promotion ou de remplacement des emplois des agents de niveau A qu'elles pourvoient, publiées dans les sept jours ouvrables de la décision.

Le document visé à l'alinéa 2, 1°, est mis à jour sans délai dès qu'un changement affecte les compétences, l'organisation ou le fonctionnement de l'Autorité publique. Les inventaires visés à l'alinéa 2, 2° à 4°, sont publiés chaque année au plus tard le 1er avril.

Le Gouvernement, le Collège réuni et le Collège peuvent, conjointement, déterminer les autres documents qui doivent figurer sous la rubrique visée à l'alinéa 1er.

§ 2. – Le Gouvernement, le Collège réuni et le Collège publient au sein de la rubrique transparence de leur site internet la liste actualisée de tous les membres des cabinets ministériels, en mentionnant leur nom et leur fonction.

Le Collège communal publie au sein de la rubrique transparence du site internet de la commune la liste actualisée de tous les membres des cabinets employés au service du bourgmestre et des échevins, en mentionnant leur nom et leur fonction.

Le président du CPAS publie au sein de la rubrique transparence du site internet du CPAS la liste actualisée de tous les membres de son cabinet, en mentionnant leur nom et leur fonction.

§ 3. – Le Gouvernement, le Collège réuni et le Collège diffusent au sein de la rubrique transparence de leur site internet :

1° au plus tard la veille de leurs réunions, l'ordre du jour définitif de celles-ci;

2° au plus tard le jour ouvrable qui suit leur réunion, les décisions qu'ils ont adoptées ainsi que les notes sur lesquelles elles se fondent.

Les publications au sein de la rubrique « transparence » des sites internet des autorités publiques ne constituent pas des publications officielles.

Article A.I.5.
L'écosystème web bruxellois

Le Gouvernement, le Collège réuni et le Collège fixent, chacun dans le cadre de leurs compétences respectives le nombre et les modalités des sites internet qui composent l'écosystème web bruxellois.

Le CIRB est chargé de l'opérationnalisation et de la mise en œuvre des sites internet qui composent l'écosystème web bruxellois.

Article A.I.6.
Désignation de la personne en charge de la publicité active

Les Autorités publiques désignent en leur sein au minimum une personne chargée de recueillir les documents administratifs ainsi que les informations à caractère environnemental devant être publiées sous la rubrique « transparence » de leurs sites internet et de procéder à la publication requise par le présent livre.

Les Autorités publiques transmettent à la Commission d'accès aux documents administratifs et aux données le nom et les coordonnées de cette personne.

Article A.I.7.
Indication de la personne disposant de l'information et des modes de saisine du médiateur bruxellois

§ 1er. – Toute correspondance émanant d'une Autorité publique indique le nom, le prénom, la qualité, l'adresse administrative, le numéro de téléphone et

l'adresse courriel de la personne en mesure de fournir de plus amples informations sur le dossier.

Par dérogation à l'alinéa 1er, les correspondances de même nature envoyées à plus de cent destinataires peuvent se limiter à mentionner l'adresse administrative, le numéro de téléphone et, si elle existe, l'adresse courriel spécifique de l'unité administrative compétente.

§ 2. – Tout acte administratif unilatéral à portée individuelle notifié à un administré indique la possibilité de saisir le médiateur bruxellois, ainsi que les modalités de cette saisine et les voies éventuelles de recours administratifs, les instances compétentes pour en connaître, ainsi que les formes et délais à respecter, faute de quoi le délai de prescription pour introduire le recours ne prend pas cours.

Article A.I.8.
La disponibilité des informations publiées

La publication au sein de la rubrique « transparence » des sites internet des Autorités publiques consiste, soit à rendre le document ou l'information directement disponible à la lecture, à l'impression ou à la réutilisation, soit à renseigner un lien vers un autre site Internet permettant la lecture, l'impression ou la réutilisation du document ou de l'information.

Le Gouvernement, le Collège réuni et le Collège arrêtent, s'il échet conjointement, les modalités techniques et pratiques destinées à permettre une récolte et un traitement aisé des données à publier.

CHAPITRE 2
Dispositions spécifiques aux informations relatives à l'environnement et l'aménagement du territoire

Article A.I.9.
Publications actives spécifiques à Bruxelles Environnement

Bruxelles Environnement publie sur son site internet les textes des traités, conventions et accords internationaux, ainsi que de la législation européenne, fédérale, régionale et locale concernant l'environnement ou s'y rapportant. Il veille à ce que ces textes soient tenus à jour.

Article A.I.10.
Publication active d'informations environnementales

Les Autorités publiques compétentes publient, sous la rubrique « transparence » de leurs sites internet, dans les 30 jours ouvrables de leur adoption, les plans et programmes environnementaux, les plans et schémas d'aménagement du territoire, les règlements d'urbanisme, les lignes de conduite en matière d'environnement ou d'aménagement du territoire qu'elles adoptent, ainsi que le rapport sur les incidences environnementales qui accompagne les informations environnementales précitées.

Article A.I.11.
Publication active des permis d'urbanisme et de lotir ainsi que des rapports et études jointes

Dans les 10 jours ouvrables de leur délivrance, les autorités publiques compétentes publient, sous la rubrique transparence de leur site internet, les permis d'urbanisme, les permis de lotir et leurs modifications qui ont fait l'objet d'un rapport ou d'une étude d'incidences. Ce rapport ou cette étude est joint à la publication. Lorsque la demande de permis d'urbanisme était soumise aux mesures particulières de publicité, les plans de synthèse sont joints à la publication.

Indépendamment de la réalisation d'un rapport ou d'une étude d'incidences, les Autorités publiques compétentes publient, dans le même délai, les permis d'urbanisme, les permis de lotir et leurs modifications lorsque ceux-ci sont susceptibles d'avoir un impact significatif sur l'environnement ou sur l'aménagement du territoire.

Lorsque les documents visés aux alinéas 1er et 2 comportent des éléments relatifs à la vie privée, des éléments faisant l'objet d'un droit de propriété intellectuelle ou des éléments dont la divulgation serait susceptible de porter gravement atteinte à la sécurité publique, l'Autorité publique s'assure, préalablement à la publication, que ces éléments soient omis du document publié.

Article A.I.12.
Publication active des mesures de protection du patrimoine immobilier

Le Gouvernement publie sur son site Internet les mesures de protection du patrimoine immobilier qu'il adopte, dans les 10 jours ouvrables de leur adoption.

Article A.I.13.
Publication active des permis d'environnement

§ 1er. – Dans les 10 jours ouvrables de leur délivrance ou de la décision, les Autorités publiques compétentes publient, sous la rubrique « transparence » de leurs sites internet, les permis d'environnement, les modifications d'autorisation, les scissions de permis

d'environnement, les prolongations de permis d'environnement, les modifications de condition d'exploiter des installations classées ainsi que les suspensions et les retraits de permis d'environnement qui ont fait l'objet d'un rapport ou d'une étude d'incidences. Ce rapport ou cette étude est joint à la publication.

Indépendamment de la réalisation d'un rapport ou d'une étude d'incidences, les autorités publiques compétentes publient, dans le même délai, les documents visés à l'alinéa 1er, lorsque ceux-ci sont susceptibles d'avoir un impact significatif sur l'environnement ou sur l'aménagement du territoire.

Lorsque les documents visés aux alinéas 1er et 2 comportent des éléments relatifs à la vie privée, des éléments faisant l'objet d'un droit de propriété intellectuelle ou des éléments dont la divulgation serait susceptible de porter gravement atteinte à la sécurité publique, l'Autorité publique s'assure, préalablement à la publication, que ces éléments soient omis du document publié.

§ 2. – Bruxelles Environnement publie sur son site Internet :

1° la liste des agréments visés à l'article 78 de l'ordonnance du 5 juin 1997 relative aux permis d'environnement;

2° les rapports d'inspection requis par l'article 19, § 6, de l'arrêté du Gouvernement de la Région de Bruxelles-Capitale du 21 novembre 2013 relatif à la prévention et la réduction intégrées de la pollution due aux émissions industrielles dans les 30 jours ouvrables de leur notification à l'exploitant;

3° les informations qui doivent être tenues à la disposition du public ou publiées en vertu des articles 9 et 10 de l'ordonnance du 5 mars 2009 relative à la gestion et à l'assainissement des sols pollués.

Lorsque les documents visés à l'alinéa 1er comportent des éléments relatifs à la vie privée, des éléments faisant l'objet d'un droit de propriété intellectuelle ou des éléments dont la divulgation serait susceptible de porter gravement atteinte à la sécurité publique, l'Autorité publique s'assure, préalablement à la publication, que ces éléments soient omis du document publié.

Article A.I.14.
Publication active en cas de menace imminente

Les Autorités publiques compétentes publient immédiatement au sein de la rubrique « transparence » de leur site internet, en cas de menace imminente pour la santé humaine ou pour l'environnement résultant d'activités humaines ou de causes naturelles, toutes les informations qui pourraient permettre à la population susceptible d'être affectée de prendre des mesures pour prévenir ou atténuer le dommage lié à la menace en question.

Article A.I.15.
Rapport sur l'état de l'environnement bruxellois

Sans préjudice des obligations de faire rapport découlant d'autres législations, le Gouvernement publie sur son site internet, tous les quatre ans, un rapport détaillé sur l'état de l'environnement bruxellois, qu'il transmet également au Parlement de la Région de Bruxelles-Capitale, et il publie sur son site internet tous les deux ans une note de synthèse comportant les principaux indicateurs environnementaux.

Ce rapport et cette note de synthèse sont établis par Bruxelles Environnement et décrivent la situation des différentes composantes du milieu environnemental, visées à l'article A.I.2, 4°, les pressions qui y sont exercées, le contexte socio-économique, les entreprises, les transports, les changements socio-démographiques et les perspectives d'évolution.

Ils se basent sur des données régionales ou éventuellement locales, dont certaines doivent permettre une comparaison cohérente avec les données rassemblées par diverses institutions internationales dans le cadre de rapports au niveau des pays ou au niveau des régions urbaines et d'autres doivent détailler des spécificités bruxelloises. Ils sont ensuite soumis à l'avis du Conseil de l'Environnement, qui sera également publié sur le site internet du Gouvernement.

Le rapport comprend en outre les indicateurs socio-économiques suivants :

1° structures des entreprises (primaire-secondaire-tertiaire);

2° accidents industriels;

3° évolution des modes de transport.

TITRE 3
Publicité passive

Article A.I.16.
Principes

§ 1er. – Chacun, selon les conditions prévues par le présent livre, peut prendre connaissance sur place de tout document administratif et de toute information environnementale émanant d'une Autorité publique,

obtenir des explications à son sujet et en recevoir communication sous forme de copie.

§ 2. – L'obtention de copies de documents administratifs ou d'informations environnementales peut être soumise à une rétribution, qui ne peut en excéder le prix coûtant. Ces rétributions sont payables au comptant si la copie est reçue par le demandeur auprès de l'Autorité publique. Celle-ci délivre un récépissé à titre de preuve de paiement. Si la copie est transmise au demandeur par la poste ou un autre moyen de transmission, les rétributions sont payées préalablement à cette transmission, par virement ou versement au compte des recettes de l'autorité concernée.

§ 3. – Pour les documents administratifs contenant de l'information se rapportant à une personne physique identifiée ou identifiable, lorsque cette information constitue une appréciation ou un jugement de valeur relatif à cette personne ou lorsqu'elle se rapporte à un comportement de cette personne dont la divulgation peut manifestement lui causer préjudice, le demandeur doit justifier d'un intérêt.

L'alinéa 1er n'est pas applicable aux informations environnementales.

Article A.I.17.
Demande d'accès au document administratif ou à une information environnementale

§ 1er. – La consultation d'un document administratif ou d'une information environnementale, les explications y relatives ou sa communication sous forme de copie ont lieu sur demande. La demande indique clairement la matière concernée et si possible, les documents administratifs ou les informations environnementales concernés et est adressée par envoi postal, électronique ou par porteur à l'Autorité publique compétente.

§ 2. – La demande est irrecevable :

1° si elle n'est pas signée par le demandeur.

Les personnes morales, outre la signature de leur fondé de pouvoir, mentionnent dans leur demande leur numéro d'inscription à la banque-carrefour des entreprises visée à l'article III.15 du code de droit économique ou fournissent une copie de leurs statuts lorsqu'il s'agit d'une personne morale de droit étranger.

En cas d'envoi de la demande par courriel, celui-ci est considéré comme valablement signé lorsque le demandeur, ou le fondé de pouvoir de la demanderesse personne morale, joint à son courriel une photocopie, une photographie ou un scan d'un document d'identité.

Lorsque la demande est signée par un avocat ou qu'elle est transmise par courriel par un avocat, le demandeur ne doit pas y joindre les documents visés par les alinéas précédents;

2° si elle ne précise pas le nom et l'adresse du demandeur;

3° si elle n'est pas adressée à l'Autorité publique de façon à lui assurer une date certaine.

Quand une demande n'est pas recevable, l'Autorité publique compétente doit le faire savoir au demandeur dans les plus brefs délais, pour autant que ce dernier soit identifié dans la demande.

§ 3. – Lorsque la demande de consultation, d'explication ou de communication sous forme de copie est adressée à l'Autorité publique qui n'est pas compétente ou si celle-ci n'est pas en possession du document administratif ou de l'information environnementale, elle en informe sans délai le demandeur et lui communique la dénomination et l'adresse de l'autorité qui, selon les informations dont elle dispose, est compétente ou est détentrice du document administratif. Si l'Autorité publique considère que le document est inexistant, elle le communique également sans délai au demandeur.

§ 4. – Le demandeur veille à indiquer la façon dont il souhaite pouvoir prendre connaissance du document ou de l'information environnementale. À défaut de précisions, la communication d'une copie par courriel est privilégiée.

§ 5. – L'Autorité publique consigne les demandes écrites dans un registre, classées par date de réception.

Article A.I.18.
Rejet des demandes

§ 1er. – L'Autorité publique peut rejeter une demande de consultation, d'explication ou de communication sous forme de copie d'un document administratif ou d'une information environnementale dans la mesure où la demande :

1° concerne un document administratif ou une information environnementale dont la divulgation peut être source de méprise, le document étant inachevé ou incomplet. Le cas échéant, l'Autorité publique désigne l'autorité qui élabore les documents ou les informations en question et indique le délai jugé nécessaire pour les finaliser;

2° concerne un avis ou une opinion communiqués librement et à titre confidentiel à l'autorité;

3° est manifestement abusive;

4° demeure formulée de manière trop générale, même après l'application de l'article B.I.19, § 3.

§ 2. – L'Autorité publique rejette la demande de consultation, d'explication ou de communication sous forme de copie d'un document administratif, si elle constate que l'intérêt de la publicité ne l'emporte pas sur la protection de l'un des intérêts suivants :

1° les libertés et les droits fondamentaux des administrés, en ce compris la vie privée;

2° les relations internationales et la sécurité publique;

3° la bonne marche de la justice, la possibilité pour toute personne d'être jugée équitablement ou la capacité d'un pouvoir public de mener une enquête à caractère pénal ou disciplinaire;

4° le secret de l'identité de la personne qui a communiqué le document ou l'information à l'Autorité publique à titre confidentiel pour dénoncer un fait punissable ou supposé tel;

5° un intérêt économique ou financier de la Commission communautaire commune, de la Région de Bruxelles-Capitale, de la Commission communautaire française, des communes et CPAS ainsi que de l'ensemble des autorités visées à l'article 3, 1° à 9°;

6° la confidentialité des délibérations des pouvoirs publics;

7° la confidentialité des informations commerciales ou industrielles, lorsque cette confidentialité est prévue par le droit régional ou européen afin de protéger un intérêt économique légitime;

8° la protection de l'environnement auquel se rapportent les informations sollicitées, telles que la localisation d'espèces rares;

9° la confidentialité requise en vue de mener des évaluations des membres du personnel de l'Autorité publique concernée et des audits internes.

Le présent paragraphe n'est pas applicable aux informations environnementales.

§ 3. – L'Autorité publique rejette la demande de consultation, d'explication ou de communication sous forme de copie d'une information environnementale si elle constate que l'intérêt du public servi par la publicité ne l'emporte pas sur la protection de l'un des intérêts suivants :

1° la confidentialité des délibérations des pouvoirs publics, lorsque cette confidentialité est prévue par le droit;

2° les relations internationales et la sécurité publique;

3° la bonne marche de la justice, à la possibilité pour toute personne d'être jugée équitablement ou à la capacité pour un pouvoir public de mener une enquête à caractère pénal ou disciplinaire;

4° la confidentialité des informations commerciales ou industrielles, lorsque cette confidentialité est prévue par le droit régional ou européen afin de protéger un intérêt économique légitime;

5° la confidentialité des données à caractère personnel et des dossiers concernant une personne physique si cette personne n'a pas consenti à la divulgation de ces informations au public, lorsque la confidentialité de ce type d'information est prévue par le droit régional ou européen;

6° aux intérêts ou la protection de toute personne qui a fourni les informations demandées sur une base volontaire sans y être contrainte par la loi ou sans que la loi puisse l'y contraindre, à moins que cette personne n'ait consenti à la divulgation de ces données;

7° la protection de l'environnement auquel se rapportent les informations sollicitées, telles que la localisation d'espèces rares.

L'Autorité publique ne peut, en vertu des points 1°, 4°, 5°, 6°, 7°, rejeter une demande lorsqu'elle concerne des informations relatives à des émissions dans l'environnement.

§ 4. – L'Autorité publique rejette la demande de consultation, d'explication ou de communication sous forme de copie d'un document administratif si la publicité porte atteinte à une obligation de secret instaurée par une ordonnance de la Région de Bruxelles-Capitale, une ordonnance de la Commission communautaire commune ou un décret de la Commission communautaire française.

Le présent paragraphe n'est pas applicable aux informations environnementales.

§ 5. – Pour l'application des paragraphes 2 et 3, le rejet de la demande de communication sous forme de copie d'un document administratif ou d'une information environnementale n'implique pas nécessairement le rejet de la demande de consultation de ce

document ou de cette information environnementale ou la demande d'explication à son sujet.

Lorsque, en application des paragraphes 2, 3, et 4, un document administratif ou une information environnementale ne doit ou ne peut être soustrait que partiellement à la publicité, la consultation, l'explication ou la communication sous forme de copie est limitée à la partie restante.

Article A.I.19.
Délais

§ 1er. – Sans préjudice du Titre II et de la faculté, pour une Autorité publique, de les laisser consulter immédiatement sur place, l'autorité saisie d'une demande met les documents administratifs et les informations environnementales à la disposition du demandeur dès que possible ou, au plus tard, dans les 20 jours ouvrables qui suivent la réception de la demande par elle, en tenant compte du délai indiqué par le demandeur dans sa demande écrite et, le cas échéant, de l'urgence invoquée par celui-ci.

§ 2. – Ce délai est porté à 40 jours ouvrables lorsque le volume et la complexité des informations sont tels que le délai de 20 jours ouvrables ne peut être respecté. Dans ce cas, le demandeur est informé dès que possible et en tout état de cause, avant la fin du délai de 20 jours ouvrables, de toute prolongation du délai et des motifs de cette prolongation.

§ 3. – Si une demande est formulée de manière trop vague, l'Autorité publique invite le demandeur, dès que possible et avant l'expiration du délai de 20 jours ouvrables, à la préciser et l'aide à cet effet.

§ 4. – Le demandeur a la faculté de solliciter l'examen de sa demande en urgence. Il doit exposer les raisons qui justifient l'urgence dans sa demande. L'urgence dûment motivée par le demandeur est celle qui rend manifestement inapproprié aux faits de la cause le respect des délais de traitement établi aux paragraphes § 1er et § 2, en raison des inconvénients graves susceptibles d'affecter la situation du demandeur si les délais précités devaient être observés.

Lorsque l'Autorité publique reconnaît l'urgence de la demande, elle y répond dès que possible et au plus tard dans les 7 jours ouvrables qui suivent la réception de la demande.

Lorsque l'Autorité publique considère que l'urgence invoquée n'est pas fondée, elle en informe immédiatement le demandeur par une décision motivée et applique les délais déterminés par les paragraphes § 1er et § 2.

§ 5. – Par dérogation aux paragraphes § 1er à § 4, les demandes sont traitées prioritairement et selon une procédure accélérée lorsque la demande d'accès concerne une décision soumise à une procédure d'enquête publique en cours, en vertu du Code Bruxellois de l'Aménagement du territoire ou des normes prises en exécution de celui-ci, de l'ordonnance du 5 juin 1997 relative aux permis d'environnement ou de l'ordonnance du 18 mars 2004 relative à l'évaluation des incidences de certains plans et programmes sur l'environnement.

Dans ce cas, l'Autorité publique à laquelle la demande est adressée met les documents et informations demandés à disposition du demandeur immédiatement et, si le document ou l'information ne se trouve pas dans les lieux prévus pour la consultation du dossier soumis à l'enquête publique, au plus tard une semaine avant l'expiration du délai de l'enquête publique.

Article A.I.20.
Notification de la décision

Toute décision de refus, total ou partiel, d'accès ou de refus d'accès sous la forme ou dans le format demandé est notifiée au demandeur par écrit, dans les délais visés à l'Article B.I.19, § 1er à § 4, selon le cas.

Si l'Autorité publique à laquelle une demande est formulée dans le cadre d'une enquête publique estime que l'accès au document ou à l'information demandée doit être refusé ou limité en vertu d'un des motifs visés à l'Article B.I.18, elle le notifie au demandeur dans les sept jours ouvrables de la demande.

La notification indique de manière claire, précise et complète, les motifs qui justifient le refus et indique l'existence du recours prévu au livre B.II ainsi que les formes et délais à respecter, de même que la possibilité de saisir le médiateur bruxellois et les modalités de sa saisine.

Le défaut de notification dans les délais visés à l'article B.I.19, § 1er à § 4 équivaut à un refus.

TITRE 4
Correction d'informations inexactes ou incomplètes

Article A.I.21.
Principe

Lorsqu'une personne démontre qu'un document administratif ou une information environnementale émanant d'une Autorité publique comporte des informations inexactes ou incomplètes la concernant,

cette Autorité est tenue d'apporter les corrections requises sans frais pour l'intéressé.

La rectification s'opère à la demande écrite de l'intéressé.

Article A.I.22.
Demande de rectification

L'Autorité publique donne suite à une demande de rectification au plus tard dans un délai d'un mois à compter de la réception de la demande. En cas de refus, elle communique les motifs de rejet.

Ce délai peut être prolongé de deux mois compte tenu de la complexité de la demande ou du nombre de demandes. Dans ce cas, l'Autorité publique en informe l'intéressé dans un délai d'un mois à compter de la réception de la demande.

En l'absence de réponse à l'Autorité publique dans les délais prescrits, la demande est réputée avoir été rejetée.

Article A.I.23.
Renvoi vers l'Autorité publique compétente

Lorsque la demande est adressée à une Autorité publique qui n'est pas compétente pour apporter les corrections, celle-ci en informe immédiatement le demandeur et lui communique la dénomination et l'adresse de l'Autorité qui, selon ses informations, est compétente pour le faire.

I.1 Dispositions finales

Article A.I.24.
Cadres législatifs plus larges

Le présent livre ne préjudicie pas aux dispositions législatives qui prévoient une publicité plus étendue de l'administration.

Article A.I.25.
Qualité des informations environnementales

Les Autorités publiques veillent, dans la mesure où cela leur est possible, à ce que toute information environnementale compilée par elles ou pour leur soit à jour, précise et comparable.

Sur demande, les Autorités publiques répondent aux demandes d'informations environnementales en indiquant, le cas échéant, l'endroit où les indications concernant les procédés de mesure, y compris les procédés d'analyse, de prélèvement et de préparation des échantillons, utilisés pour la compilation des informations, peuvent être trouvées ou en faisant référence à une procédure standardisée.

LIVRE B.II.
La Commission d'accès aux documents administratifs et aux données (CADADO)

TITRE 1
Dispositions générales

Article B.II.1.
Transposition partielle

Le présent livre transpose partiellement la Directive 2003/4/CE du Parlement européen et du Conseil du 28 janvier 2003 concernant l'accès du public à l'information en matière d'environnement et abrogeant la Directive 90/313/CEE du Conseil.

Article B.II.2.
Calcul des délais

Les délais prévus dans le présent livre commencent à courir le jour qui suit celui qui constitue le point de départ du délai. Le jour de l'échéance est compris dans le délai. Si ce jour n'est pas un jour ouvrable, le jour de l'échéance est reporté au jour ouvrable qui suit.

TITRE 2
Composition et organisation de la Commission

Article B.II.3.
Compétences de la Commission et indépendance

§ 1er. – La Commission connaît des recours dirigés contre :

1° les manquements aux obligations de publicité active prévues au titre 2 du livre B.I, à l'exception de l'obligation, visée à l'article Article B. I. 15, d'établir un rapport détaillé sur l'état de l'environnement et une note de synthèse;

2° les rejets des demandes d'accès aux documents administratifs visées au titre 3 du livre B.I;

3° les refus de rectification visés au titre 4 du livre B.I.

4° les décisions d'une Autorité publique visée à l'article C.I.1. Relatives au partage administratif des données ou à la réutilisation des données visés au livre C.IV.

§ 2. – La Commission peut, d'initiative, émettre des avis sur l'application générale du livre B.I. portant sur la publicité administrative, le livre B.II l'instituant et le livre C.IV en matière de partage administratif et de réutilisation, ainsi que sur les arrêtés d'exécution de ces livres. Elle peut soumettre au Parlement ou au Gouvernement de la Région de Bruxelles-Capitale, à l'Assemblée ou au Collège réuni de la COCOM, à l'Assemblée ou au Collège de la COCOF, des propositions relatives à leur application et leur révision éventuelle.

La Commission peut également remettre des avis à la demande d'une Autorité publique à propos d'une question relative à l'application du livre B.I. portant sur la publicité administrative, du présent livre et du livre C.IV en matière de partage administratif et de réutilisation, ainsi que sur les arrêtés d'exécution de ces livres.

§ 3. – La Commission exerce ses missions en toute indépendance et dans le respect de l'impartialité. Elle ne peut recevoir aucune instruction dans l'exercice de ses missions.

Ses membres ne peuvent faire l'objet d'une évaluation ou d'une procédure disciplinaire sur la base des éléments de fait ou de droit motivant une décision de la Commission adoptée conformément aux dispositions du présent livre.

Article B.II.4.
Composition générale

§ 1er. – La Commission est composée d'un secrétariat général et de trois chambres : une chambre relative à l'accès aux documents administratif, une chambre relative au partage administratif de données et une chambre relative à la réutilisation de données.

§ 2. – Le secrétariat général est composé d'un secrétaire principal et d'un secrétaire adjoint qui s'occupent de la gestion administrative et organisationnelle de la Commission. Les secrétaires de la Commission sont désignés par arrêté conjoint du Gouvernement, du Collège réuni et du Collège parmi les membres du personnel statutaire des Autorités publiques. Ils doivent être titulaires d'un diplôme universitaire en droit de deuxième cycle et exercer leur mission à temps plein.

La Commission est composée de treize membres, parmi lesquels est désigné un président qui est membre du Conseil d'État ou de son auditorat, ou magistrat dans l'arrondissement judiciaire de Bruxelles. Le président dirige les débats et signe au nom de la Commission toute correspondance, toutes les recommandations et tous les avis.

Article B.II.5.
Composition des chambres

§ 1er. – La chambre relative à l'accès aux documents administratifs est composée du Président de la Commission, de huit autres membres et d'un membre du secrétariat général.

Quatre des membres de la chambre, en dehors du Président, sont désignés parmi les membres du personnel statutaire des Autorités publiques visées à l'article B.I.2. Les membres désignés en cette qualité doivent être titulaires d'un diplôme universitaire de deuxième cycle en droit et justifier d'une expérience suffisante en matière de publicité de l'administration.

Quatre des membres de la chambre, en dehors du Président, sont désignés en raison de leur connaissance approfondie dans le domaine de la publicité de l'administration. Ils doivent être titulaires d'un diplôme universitaire de deuxième cycle en droit et ne peuvent pas être fonctionnaires au sein d'une Autorité publique visées à l'article B.I.2 ou de toute autre autorité administrative.

§ 2. – La chambre relative au partage des données est composée du Président de la Commission, de deux autres membres, et d'un membre du secrétariat général.

Les deux membres de la chambre, en dehors du Président, sont désignés en raison de leur connaissance approfondie dans le domaine de la gestion des données dans le secteur public. Ils doivent être titulaires d'un diplôme universitaire de deuxième cycle et justifier d'une connaissance et d'une expérience suffisantes en matière de gestion des données dans le secteur public. La chambre doit être composée au minimum d'une personne titulaire d'un diplôme universitaire de deuxième cycle en droit et d'une personne démontrant une compétence technique dans le secteur des nouvelles technologies.

§ 3. – La chambre relative à la réutilisation des données est composée du Président de la Commission, de deux autres membres, et d'un membre du secrétariat général.

Les deux membres de la chambre, en dehors du Président, sont désignés en raison de leur connaissance approfondie dans le domaine de la gestion des données dans le secteur public et de l'échange de données entre le secteur public et le secteur privé. Ils doivent être titulaires d'un diplôme universitaire de deuxième cycle et justifier d'une connaissance et d'une expérience suffisantes en matière de gestion des données dans le secteur public. La chambre doit être composée au minimum d'une personne titulaire d'un diplôme universitaire de deuxième cycle en droit

et d'une personne démontrant une compétence technique dans le secteur des nouvelles technologies.

§ 4. – Le Président et le secrétariat sont communs aux trois chambres. Le secrétaire n'a pas voix délibérative.

§ 5. – Il est désigné pour chacun des membres un suppléant aux mêmes conditions que les membres effectifs.

En cas d'empêchement ou d'absence d'un membre, celui-ci est remplacé par son suppléant.

Le suppléant achève le mandat de son prédécesseur au cas où ce dernier démissionne ou cesse pour une raison quelconque de faire partie de la Commission.

§ 6. – Toutes chambres confondues, la Commission ne comporte pas plus de sept membres du même sexe.

§ 7. – Toutes chambres confondues, la Commission ne comporte pas plus de sept membres du même rôle linguistique, celle-ci étant vérifiée par la langue dans laquelle les diplômes requis pour leur fonction ont été obtenus.

§ 8. – Le Gouvernement, le Collège réuni et le Collège peuvent déterminer conjointement les règles complémentaires relatives à la composition de la Commission.

Article B.II.6.
Experts

Un minimum de trois experts sur des questions spécialisées en matière de partage administratif et de réutilisation de données sont désignés auprès de la Commission, sur la base d'une liste proposée par le Président et les autres membres de la Commission, par arrêté conjoint du Gouvernement, du Collège réuni et du Collège. La désignation de chaque expert a une durée de 5 ans et peut être renouvelée une fois,

Les experts justifient d'une expérience de plus de cinq ans dans les questions relatives au partage administratif et à la réutilisation de données détenues par des Autorités publiques visées à l'article C.I.1. Ils justifient également de plusieurs publications académiques sur ces questions.

Les experts sont désignés par le Président pour des dossiers ou missions spécifiques et ne siègent que pour les nécessités de ces dossiers ou missions. Ils ne possèdent pas de voix délibérative et ne peuvent émettre que des avis sur les dossiers et missions pour lesquels ils sont désignés.

Les paragraphes 2 et 3 de l'article B.II.7 s'appliquent également aux experts.

Article B.II.7.
Mandats des membres

§ 1er. – Les membres de la Commission sont désignés conjointement par le Gouvernement, le Collège réuni et le Collège pour un terme de 5 ans renouvelable une fois.

§ 2. – À la demande du Président ou de tout membre de la Commission, et après l'audition de la personne visée, le Gouvernement, le Collège réuni et le Collège peuvent conjointement mettre fin anticipativement au mandat du Président et de tout autre membre de la Commission dans les cas suivants :

1° S'il ne remplit plus les conditions de désignation au mandat en question ou manque à ses devoirs;

2° S'il porte atteinte à la dignité de sa fonction;

3° S'il ne respecte pas le caractère confidentiel des délibérations ou diffuse des documents confidentiels auxquels il a accès dans l'exercice de son mandat;

4° S'il participe aux délibérations de la Commission alors qu'il se trouve dans une situation de conflit d'intérêt visées au troisième paragraphe.

§ 3. – Il est interdit aux membres de la Commission et aux experts d'être présents à une délibération concernant des dossiers et missions dans lesquelles ils ont un intérêt personnel et direct ou dans lesquelles leurs parents ou alliés jusqu'au quatrième degré ont un intérêt personnel et direct.

Il est en outre interdit aux membres visés à l'article B.II.5. § 1er, alinéa 2, d'être présents à une délibération s'ils ont été impliqués de quelque manière que ce soit dans la décision administrative au sujet de laquelle un recours a été introduit.

Article B.II.8.
Rémunération

§ 1er. – Les membres de la Commission et les experts sont rémunérés par recours visé à l'article B.II.3, § 1er, ou demande d'avis traité. Chaque dossier traité donne droit à un jeton.

Le rapporteur désigné pour chaque dossier reçoit un jeton d'un montant supérieur.

§ 2. – Le Gouvernement, le Collège réuni et le Collège fixent conjointement les modalités et le montant des jetons en faveur des membres, experts et rapporteurs.

Article B.II.9.
Fonctionnement

§ 1er. – Le Président dirige les débats au sein de chaque chambre. Il désigne pour chaque dossier, un membre rapporteur et le cas échéant, un ou plusieurs experts. Il fixe, en concertation avec le secrétaire, la date des réunions, leurs modalités, dont leur tenue en présentiel ou distanciel, et en établit l'ordre du jour.

§ 2. – La Commission se réunit, toutes les chambres réunies, au moins deux fois par an. Le secrétaire envoie au Président, à chaque membre et, le cas échéant, aux experts, pour chacune des réunions de la Commission, une convocation contenant l'ordre du jour, accompagnée de la documentation nécessaire et la modalité de la tenue de la réunion.

Chaque convocation est envoyée au moins trois jours ouvrables avant la date de la réunion.

§ 3. – La Commission doit établir un Règlement d'ordre intérieur interne dans les trois mois de son entrée en fonction, concernant également le fonctionnement des chambres de la Commission.

§ 4. – Le Gouvernement, le Collège réuni et le Collège déterminent conjointement les règles complémentaires relatives au fonctionnement de la Commission.

TITRE 3
Les demandes d'avis

Article B.II.10.
Modalités des demandes d'avis

Conformément à l'article B.II.3, § 2, alinéa 2, les demandes d'avis des Autorités publiques sont soit envoyées via le formulaire en ligne sur le site internet de la Commission, soit adressées au secrétariat de la Commission par courrier électronique. Celle-ci en accuse réception en toute hypothèse.

Article B.II.11.
Information des membres

Chaque fois qu'une demande d'avis est introduite auprès de la Commission, le Secrétariat de la Commission en informe immédiatement l'ensemble des membres de la Chambre concernée par voie électronique.

Article B.II.12.
Délibération de la Commission

§ 1er. – Le secrétariat désigne un rapporteur qui rédige une proposition d'avis. Cette proposition est ensuite soumise à l'approbation de la Chambre concernée.

§ 2. – Chaque chambre de la Commission ne peut délibérer valablement quant à la formulation de l'avis que si le Président ainsi qu'au minimum deux membres de la Chambre concernée sont présents.

Les avis sont adoptés à la majorité simple des suffrages exprimés. En cas de parité des voix, celle du Président est prépondérante.

Article B.II.13.
Délai dans lequel la Commission statue

La Commission statue sur la demande d'avis dans les 60 jours de la réception de la demande d'avis visée à l'article B.II.10.

Article B.II.14.
Secrétariat

§ 1er. – Le secrétariat est chargé de la conservation des documents et des archives de la Commission.

§ 2. – Le secrétariat s'assure de la communication des avis à l'Autorité publique à l'origine de la demande d'avis, ainsi que la publication de cet avis

Article B.II.15.
Publication de l'avis

La Commission publie sur son site internet les avis rendus dans un délai de 15 jours ouvrables à compter de la date à laquelle il est adopté conformément à l'article B.II.13.

TITRE 4
Les recours

Article B.II.16.
Délai pour introduire un recours

§ 1er. – Sous peine d'irrecevabilité, la Commission est saisie d'un recours visé à l'article B.II.3, § 1er, dans les 30 jours de la décision de l'Autorité publique ou dans les 30 jours à compter de la prise de connaissance du manquement visé à l'article B.II.3. § 1er, 1°.

§ 2. – Lorsque le requérant sollicite l'examen de son recours en urgence, le délai pour introduire son recours est réduit à 5 jours ouvrables.

Article B.II.17.
Modalités d'introduction du recours

§ 1er. – Les recours sont introduits par une requête adressée au secrétariat de la Commission par lettre recommandée ou par tout autre moyen conférant date certaine à l'envoi.

§ 2. – Le point de départ des délais est le jour de la prise de connaissance de la décision expresse de l'Autorité publique, ou, à défaut d'une telle décision, le jour de l'expiration du délai dans lequel l'Autorité publique devait se prononcer sur la demande, ou encore la date de la prise de connaissance du manquement visé à l'article B.II.3. § 1er, 1°.

§ 3. – Les délais visés au paragraphe 1er sont interrompus par l'introduction d'une réclamation devant le médiateur bruxellois. Un nouveau délai commence à courir à dater de la réception par le requérant de la notification du médiateur l'informant de la fin de son intervention.

Article B.II.18.
Formalités des recours

§ 1er. – Sous peine d'irrecevabilité, le recours est introduit par une requête qui :

1° est signée par le requérant.

Les personnes morales, outre la signature de leur fondé de pouvoir, mentionnent dans leur requête leur numéro d'inscription à la banque-carrefour des entreprises visée à l'article III.15 du Code de droit économique ou fournissent une copie de leurs statuts lorsqu'il s'agit d'une personne morale de droit étranger.

En cas d'envoi de la requête par courriel, celui-ci est considéré comme valablement signé lorsque le requérant, ou le fondé de pouvoir de la personne morale requérante, joint à son courriel une photocopie, une photographie ou un scan d'un document d'identité. Lorsque la requête est signée par un avocat ou qu'elle est transmise par courriel par un avocat, le requérant ne doit pas y joindre les documents visés par les alinéas précédents;

2° précise le nom et l'adresse du requérant;

3° est adressée à la Commission de façon à lui assurer une date d'envoi certaine;

4° Comprend le cas échéant une motivation de l'urgence invoquée conformément à l'article B.II.16, § 2.

§ 2. – Dans le cas des recours visés à l'article B.II.3, § 1er, 2° à 4°, le recours contient, sous peine d'irrecevabilité, une copie de la demande d'accès, de rectification, de partage administratif ou de réutilisation, ou le cas échéant des conditions de partage administratif et de réutilisation et, si le refus est exprès, une copie de la décision de refus.

§ 3. – Quand un recours est irrecevable pour l'un des motifs visés aux articles B.II.16 à 18, la Commission doit le faire savoir au requérant dans les plus brefs délais, pour autant que celui-ci soit identifié dans le recours.

§ 4. – Lorsqu'elle est saisie d'un recours, la Commission le notifie sans délai à l'Autorité publique concernée.

Article B.II.19.
Délais d'obtention des documents par la Commission

§ 1er. – La Commission dispose de pouvoirs d'investigation et de contrainte.

L'Autorité publique est tenue de lui communiquer, dans les sept jours ouvrables à compter de la réception de la notification visée à l'article B.II.18, § 4, selon l'hypothèse :

1° le document ou l'information environnementale dont l'accès ou la rectification est sollicité, ou

2° les données visées par le partage administratif, ainsi que le protocole d'accord fixant les conditions relatives au partage, ou

3° les données visées par la réutilisation demandée et les conditions de cette réutilisation.

Pour ce qui concerne les Autorités publiques visées à l'article C.I.1, la communication des documents visés à l'alinéa 2 correspond à un partage administratif.

L'Autorité publique peut joindre aux documents visés à l'alinéa 2 une note justifiant son refus d'accéder à la demande initiale. À défaut d'être transmise en même temps que les documents visés à l'alinéa 2, la Commission n'est pas tenue de prendre en considération la note justifiant ledit refus.

Dans l'hypothèse où le Président de la Commission ou le membre qu'il désigne reconnaît l'urgence invoquée par le requérant, le délai de sept jours visé à l'alinéa 2 est réduit à deux jours ouvrables.

Par dérogation à l'alinéa 2, lorsque l'Autorité publique considère que la demande était manifestement abusive ou qu'elle était formulée de façon manifestement trop vague, elle n'est pas tenue de transmettre à la Commission les documents visés à l'alinéa 2. Lorsque l'Autorité n'a pas répondu à la demande initiale, si elle considère celle-ci manifestement abusive ou manifestement trop vague, elle en informe la Commission sans délai par une décision motivée.

Lorsque l'Autorité publique ne transmet pas à la Commission les documents visés à l'alinéa 2 dans les délais établis aux alinéas 2 et 5, la Commission en fait mention dans le rapport annuel visé à l'article A.II.26.

§ 2. – Le Président de la Commission ou le membre qu'il désigne peut se rendre sur place pour prendre connaissance et copie des documents visés au paragraphe 1er, alinéa 2 concernés par le recours et de tout autre document nécessaire au traitement de ce recours, en ce compris en faisant appel à la force publique.

§ 3. – Si, malgré les pouvoirs de la Commission visés aux § 1er et 2, la Commission n'obtient pas les documents visés à l'alinéa 2, elle en informe sans délai selon le cas le Parlement de la Région, l'Assemblée réunie de la COCOM et l'Assemblée de la COCOF, de même que le Gouvernement, le Collège réuni et le Collège, qui fixent immédiatement de nouvelles sanctions et la procédure y afférente.

Article B.II.20.
Délai maximal pour statuer sur le recours

§ 1er. – À partir du moment où elle dispose des documents visés à l'article B.II.19, § 1er, alinéa 2, la Commission en informe le requérant. Elle statue sur le recours dans les 60 jours de la réception du document administratif ou de l'information environnementale.

Lorsque l'Autorité publique considère la demande comme étant manifestement abusive ou manifestement trop vague conformément à l'article B.II.19, § 1er, alinéa 6, la Commission statue dans les 60 jours de la réception du recours.

Si la Commission considère que la demande n'est ni manifestement abusive ni trop vague, elle sollicite de l'Autorité publique qu'elle lui communique sans délai le document administratif ou l'information environnementale et, dans ce cas, le délai de 60 jours commence à courir conformément à l'alinéa 1er.

Si les délais prévus aux alinéas 1er à 3 ne sont pas respectés, le recours est censé être rejeté.

§ 2. – Le délai de 60 jours visé au paragraphe 1er, alinéas 1er à 3, est suspendu :

3° lorsque la Commission a sollicité l'avis de l'Autorité de protection des données, jusqu'à la réception de cet avis;

4° à compter du jour où la Commission reçoit du médiateur bruxellois l'information selon laquelle celui-ci est saisi d'une réclamation dont l'objet est identique à celui du recours introduit devant la Commission. Le médiateur notifie au même moment à la Commission et au requérant la fin de son intervention et les éventuelles recommandations qu'il a formulées. Dans ce cas, il appartient au requérant de notifier à la Commission s'il maintient son recours au terme de l'intervention du médiateur. En l'absence de notification du maintien de son recours par le requérant dans un délai de 15 jours à compter de la réception par la Commission de la notification du médiateur, le requérant est réputé se désister de son recours.

§ 3. – Lorsque l'urgence invoquée par le requérant dans son recours est reconnue par le Président de la Commission ou par le membre qu'il désigne, la Commission statue sur le recours dans un délai de 10 jours ouvrables à compter de la réception du recours. En cas de rejet de l'urgence par le Président de la Commission ou par le membre désigné par le Président, le recours est examiné par la Commission dans le délai ordinaire déterminé au § 1er.

L'urgence dûment motivée par le requérant est celle qui rend manifestement inapproprié aux faits de la cause le respect du délai ordinaire établi par le § 1er, en raison des inconvénients graves susceptibles d'affecter la situation du requérant si le délai précité devait être observé.

§ 4. – Le Gouvernement, le Collège réuni et le Collège peuvent arrêter conjointement des règles de

procédure devant la Commission complémentaires à celles figurant dans le présent livre.

Article B.II. 21.
Délibération de la Commission

La Commission ne peut délibérer valablement que si son Président ainsi qu'au minimum deux membres de la Chambre concernée sont présents.

Les décisions sont prises à la majorité simple des suffrages exprimés. En cas de parité des voix, celle du Président est prépondérante.

Les décisions sont motivées.

Article B.II. 22.
Notification de la décision de la Commission

La Commission notifie dans les plus brefs délais sa décision par écrit aux parties concernées.

Article B.II. 23.
Pouvoirs de réformation de la Commission

§ 1er. – La Commission dispose d'un pouvoir de réformation et peut elle-même accorder l'accès aux documents administratifs, aux informations environnementales ainsi que leur rectification; elle peut elle-même accorder l'accès aux données visées par un partage administratif ou une réutilisation aux conditions qu'elle fixe.

Dans ce cas, la Commission donne l'injonction à l'Autorité publique de se conformer à sa décision et de l'exécuter dans le délai qu'elle établit, lequel ne peut excéder 30 jours.

§ 2. – À l'expiration du délai de 30 jours visé au premier paragraphe, si l'Autorité publique n'a pas respecté la décision de la Commission dans le délai imparti, cette dernière communique elle-même, lorsqu'elle en dispose, la copie du document administratif, l'information environnementale ou les données visées par le partage administratif ou la réutilisation. Dans cette hypothèse, la Commission avertit l'Autorité publique au minimum 15 jours avant la communication faite au requérant.

Lorsque la Commission constate le défaut pour une Autorité publique visée à l'article C.I.1. de satisfaire à une obligation visée au titre 2 du livre B.I, la Commission lui donne l'injonction de satisfaire sans délai à cette obligation.

Article B.II. 24.
Publication des décisions, avis et propositions

La Commission publie sur son site internet visés à l'article B.II.26, dans les 20 jours ouvrables de leur adoption, les décisions, avis et propositions qu'elle adopte.

Sauf consentement préalable du requérant en vue d'une publication nominative, la Commission opère une anonymisation des décisions avant leur publication. Elle omet également toute information qu'elle jugera confidentielle.

TITRE 5
Rapport annuel et site web

Article B.II.25.
Rapport annuel

§ 1er. – La Commission rédige un rapport annuel.

Ce rapport comprend au moins :

1° le nombre de recours introduits et le nombre de décisions adoptées;

2° le nombre de demandes d'avis introduits et le nombre d'avis adoptés;

3° le délai moyen de traitement d'un recours et d'un avis;

4° le nombre de réunions par chambre ou en plénière;

5° une synthèse des principales problématiques auxquelles la Commission a été confrontée, tant sur le fond des affaires que sur le fonctionnement de la Commission elle-même;

6° Un budget prévisionnel pour les deux années à venir et une justification de l'utilisation de la dotation reçue pour l'année faisant l'objet du rapport;

7° une liste répertoriant les cas dans lesquels les délais de commination des documents demandés et faisant l'objet des recours n'ont pas été respectés. Cette liste mentionne l'Autorité publique concernée et le nombre de dépassements des délais.

§ 2. – Le rapport annuel est présenté par le Président de la Commission ou le membre qu'il désigne au Parlement de la Région de Bruxelles-Capitale au plus tard le 31 mars de l'année qui suit celle à laquelle il se rapporte.

§ 3. – Le rapport annuel est publié sur le site internet de la Commission.

§ 4. – La Commission adresse au Gouvernement, au Collège réuni et au Collège un bilan dans les 2 ans après l'entrée en vigueur du présent Livre.

Article B.II. 26.
Site Web

§ 1er. – La Commission doit tenir un site web à destination du public contenant au minimum les informations suivantes :

1° une information sur les missions de la Commission, son fonctionnement et les bases légales qui fondent ses interventions;

2° une information sur les membres et les experts de la Commission;

3° les avis et décisions sur recours qui ont été rendus.

TITRE 6
Dotation

Article B.II.27.
Dotation

§ 1er. – Une dotation est inscrite au budget général de la Région de Bruxelles-Capitale, de la COCOM, de la COCOF pour financer le fonctionnement de la Commission et lui permettre d'exécuter les missions qui lui sont confiées par le présent Code.

§ 2. – Le Gouvernement, le Collège réuni et le Collège déterminent conjointement les modalités relatives à la dotation.

PARTIE C
GOUVERNANCE DE LA DONNÉE

LIVRE C.I
Champ d'application ratione personae

Article C.I.1.
Champ d'application ratione personae

La partie C du présent Code s'applique aux Autorités publiques visées à l'article A.I.1., a), b), c), h), i).

LIVRE C.II
Principes généraux

TITRE 1
Les principes directeurs

Article C.II.1
Les quatre principes directeurs

Dans le cadre de l'exercice de leurs missions de services publics, lorsqu'elles traitent des données, les Autorités publiques doivent respecter les principes directeurs suivants :

1° le principe de protection et de sécurisation;

2° le principe de partage;

3° le principe de transparence;

4° le principe de qualité.

Les Autorités publiques doivent garantir par toute mesure technique et organisationnelle disponible, dès le début du cycle de vie de la donnée, le plus haut niveau de respect des principes applicables. Dans ce cadre, les Autorités publiques tiennent compte de la réglementation particulière applicable aux données, de l'état des connaissances, des coûts de mise en œuvre ainsi que de la nature, de la portée, du contexte, des finalités du traitement des données et des risques qui y sont afférents.

Article C.II.2.
Principe de protection et
de sécurisation des données

§ 1er. – Les Autorités publiques protègent les droits des tiers sur les données qu'elles détiennent.

§ 2. – Les Autorités publiques sécurisent les données en toute circonstance, à des fins de qualité et de respect des droits des tiers.

§ 3. – Le principe de protection et de sécurisation des données appelle une application différenciée en fonction des catégories particulières de données visées à l'article C.III.10.

Les Autorités publiques garantissent notamment la protection et la sécurisation des données protégées. Plus particulièrement, les Autorités publiques garantissent que les données faisant l'objet de droits de propriété intellectuelle, ou contenant des secrets d'affaires ou commerciaux, ou encore des secrets statistiques, ne peuvent être partagées qu'aux conditions légales ou réglementaires en vigueur. Les Autorités publiques protègent également la vie privée et

les droits des personnes concernées par les données à caractère personnel qu'elles détiennent.

Article C.II.3.
Principe de partage

§ 1er. – Par défaut, les Autorités publiques organisent le partage administratif de données entre elles afin d'améliorer l'exercice de leurs missions de services publics et de leurs obligations d'intérêt général, et, d'alléger le cas échéant la charge administrative des citoyens.

§ 2. – Les Autorités publiques utilisent les sources authentiques afin de collecter les données dont elles ont besoin.

Les Autorités publiques collectent les données issues de sources authentiques auprès du Centre d'intégration de la Plateforme bruxelloise de la donnée conformément à la section 2, du chapitre 2 du titre 2 du livre C.IV.

Les Autorités publiques ne peuvent recueillir des données auprès des citoyens qu'en l'absence de données issues de sources authentiques.

§ 3. – Les Autorités publique garantissent également par défaut la réutilisation de leurs données publiques par des opérateurs privés.

Article C.II.4.
Principe de transparence

§ 1er. – Les Autorités publiques gèrent les données qu'elles détiennent dans le cadre de leurs missions de services publics et leurs obligations d'intérêt général conformément à un impératif de transparence.

§ 2. – Les Autorités publiques organisent la réutilisation de leurs données conformément au titre 3 du livre C.IV.

Les Autorités publiques mettent à disposition leurs données ouvertes, en assurant le plus haut degré d'ouverture. À défaut, si cela s'avère impossible, les Autorités publiques adoptent des outils afin de permettre d'extraire et d'exploiter librement tout ou partie des bases de données contenant de telles données.

§ 3. – Conformément au principe de documentation, les Autorités publiques assurent une transparence active par la mise à disposition d'office de la documentation relative aux processus qu'elles mettent en place en vertu des obligations imposées par le Code, sans préjudice des dispositions assurant la protection de certaines données.

Les Autorités publiques assurent une transparence passive en fournissant sur demande toute fonction de support et d'information portant sur la gouvernance des données numériques, nécessaire à leurs propres services et aux tiers.

Article C.II.5.
Principe de qualité

Les Autorités publiques doivent garantir le niveau le plus élevé de qualité des données en fonction des usages qui en sont faits.

La qualité de données se définit sous l'angle de différentes dimensions complémentaires, à savoir notamment :

1° Consistance

2° Exactitude

3° Exhaustivité

4° Vérifiabilité

5° Validité

6° Unicité

7° Intégrité

8° Ponctualité

Les Autorités publiques doivent être en mesure d'évaluer, à tout moment, la qualité des données qu'elles détiennent.

TITRE 2
Les objectifs stratégiques

Article C.II.6.
Six objectifs stratégiques

Dans le cadre de leurs missions, les Autorités publiques appliquent une gouvernance des données qui :

1° met les données au centre de leur action;

2° définit les rôles et responsabilités des parties prenantes;

3° se base sur des standards communs;

4° adopte une gouvernance évolutive;

5° favorise l'éducation numérique de toutes les parties prenantes;

6° exploite les données de manière efficiente et responsable.

Article C.II.7.
Approche centrée sur la donnée

Les Autorités publiques adoptent des processus qui placent les données au centre de la gestion de leurs missions de services publics et de leurs obligations d'intérêt général, de même que de leur gouvernance. Les données des Autorités publiques sont assimilées à des actifs à part entière.

Article C.II.8.
Définition des rôles et responsabilités

Les Autorités publiques désignent en leur sein les organes, services ou personnes responsables de la gestion des données, conformément aux qualifications décrites notamment au chapitre 2 du titre 2 du livre C.III.

Article C.II.9.
Adoption de standards communs

Les Autorités publiques déploient des solutions qui privilégient les standards communs.

Article C.II.10.
Gouvernance évolutive

Les Autorités publiques adoptent un modèle de gouvernance qui permet de s'adapter de manière continue aux évolutions techniques et réglementaires.

Article C.II.11.
Éducation des parties prenantes

Les Autorités publiques favorisent la culture de la donnée, notamment par la mobilisation, l'information, la sensibilisation et la formation de toutes les parties prenantes.

Article C.II.12.
Exploitation efficiente et responsable – économicité

Les Autorités publiques exploitent les données qu'elles détiennent de manière efficiente et responsable tout au long du cycle de vie de la donnée, de la collecte au stockage et à l'archivage.

TITRE 3

Les objectifs opérationnels

Article C.II.13.

Huit objectifs opérationnels

Dans le cadre de leurs missions, les Autorités publiques s'engagent à :

1° valoriser leurs données, le cas échéant en fonction de leurs priorités;

2° identifier le ou les régime(s) juridique(s) applicable(s) à chaque donnée;

3° respecter la confidentialité des données protégées;

4° assurer l'interopérabilité des systèmes;

5° garantir la traçabilité et la réversibilité des données;

6° procéder à l'intégration des données;

7° générer les métadonnées et les données de références de leurs données;

8° contrôler les conditions relatives à l'hébergement des données.

Article C.II.14.

Valorisation des données

Les Autorités publiques identifient les données qu'elles détiennent et définissent une stratégie de valorisation à leur égard dans le cadre de leurs missions de services publics et de leurs obligations d'intérêt général.

Plus particulièrement, les Autorités publiques identifient si les données qu'elles détiennent :

1° sont des données de forte valeur conformément à la liste établir conformément à l' article C.IV.29;

2° sont relatives aux espaces européens communs, dont la thématique relève de leurs compétences.

Article C.II.15.
Identification du ou des régime(s) juridique(s) applicable(s)

Les Autorités publiques identifient le ou les régimes juridiques applicables aux données qu'elles détiennent.

Les Autorités publiques tiennent compte de ces régimes juridiques dans les partenariats numériques visés à l'Article C.III.2 dans lesquelles elles sont impliquées lorsqu'ils concernent tout ou une partie de la gestion des données.

Article C.II.16.
Respect de la confidentialité des données protégées

Les Autorités publiques doivent être en mesure de procéder le cas échéant et en fonction des données concernées, à l'occultation, l'anonymisation ou la pseudonymisation des données lorsque cela s'avère pertinent.

Article C.II.17.
Interopérabilité

Les Autorités publiques prennent toutes les mesures nécessaires (organisationnelles, juridiques et techniques) pour assurer l'interopérabilité des données qu'elles détiennent et ce, dès la conception de leur processus.

Les Autorités publiques recourent à des systèmes interopérables qui s'appuient, chaque fois que cela est possible, sur des standards reconnus au niveau national ou international.

Article C.II.18.
Traçabilité et réversibilité

Les Autorités publiques recourent, lorsque cela est pertinent et de manière proportionnée au regard de l'objectif poursuivi, à la traçabilité et à la réversibilité des données, à l'exception des hypothèses pour lesquelles l'anonymisation est requise conformément à la législation ou à la réglementation applicable.

Les Autorités publiques utilisent les outils informatiques permettant la traçabilité et la réversibilité des données tout en garantissant la protection de celles-ci.

Article C.II.19.
Intégration des données

Les Autorités publiques intègrent les données susceptibles de l'être.

Article C.II.20.
Génération et gestion des métadonnées et données de référence

Les Autorités publiques documentent les données qu'elles détiennent au moyen de métadonnées.

Les Autorités publiques identifient les données de référence et en favorisent l'usage.

Les Autorités publiques établissent des politiques de gestion des données de référence et des métadonnées qui permettent d'identifier les données qu'elles détiennent ainsi que de garantir, le cas échéant, le partage des données.

Article C.II.21.
Contrôle des conditions d'hébergement et de stockage des données

Les Autorités publiques contrôlent les conditions d'hébergement et de stockage des données qu'elles détiennent.

LIVRE C.III
Obligations de gouvernance des Autorités publiques

TITRE 1
Champ d'application ratione personae

Article C.III.1.
Champ d'application du présent livres par palier

Le Gouvernement, le Collège réuni et le Collège déterminent conjointement certaines catégories d'Autorités publiques en fonction de seuils numériques définis. À chaque seuil numérique correspond un palier numérique déterminant l'importance de l'activité numérique et la maturité numérique des Autorités publiques qui y sont regroupées.

Le premier palier est appelé à respecter l'ensemble des obligations du présent livre.

Le deuxième palier est soumis aux articles XXX.

Le troisième palier est soumis aux articles XXX.

TITRE 2
Les partenariats numériques de données

CHAPITRE 1
Principe de partenariats numériques de données

Article C.III.2.
La notion de partenariat numérique de données aux fins de valorisation des données

§ 1er. – Afin d'identifier les ressources numériques dont elles disposent et qu'il leur appartient de valoriser, les Autorités publiques identifient les partenariats numériques de données dont elles sont parties.

Est un partenariat numérique de données toute initiative impliquant la valorisation ou le partage de données publiques et liant juridiquement ou administrativement, soit deux ou plusieurs entités au sein d'une même Autorité publique, soit deux ou plusieurs entités disposant de la personnalité juridique dont au moins une est une Autorité publique.

§ 2. – Lorsque le partenariat numérique de données est conclu entre au minimum une Autorité publique, d'une part, et une personne autre qu'une Autorité publique, d'autre part, il s'agit d'un partenariat numérique mixte de données.

§ 3. – Lorsque le partenariat de données n'est conclu qu'entre des Autorités publiques, ou entre différentes entités au sein d'une même Autorité publique, il s'agit d'un partenariat numérique public de données.

Article C.III.3.
Les partenariats mixtes de données

§ 1er. – Dans le cadre des partenariats numériques mixtes de données, les Autorités publiques s'assurent que :

1° l'autre partie gère les données publiques concernées par le partenariat conformément aux dispositions du présent livre et de ses arrêtés d'exécution;

2° chaque partie soit qualifiée conformément au chapitre 2 du présent livre et soit chargée des responsabilités qui en découlent.

Les conditions visées à l'alinéa 1er sont organisées entre les parties dans le respect du principe de proportionnalité compte tenu de l'importance et de la nature des traitements et des données visées par le partenariat.

Les Autorités publiques exigent de leurs partenaires qu'ils mettent en place les moyens techniques et organisationnels appropriés afin d'être en mesure de vérifier à tout moment le respect des conditions imposées au premier alinéa à l'autre partie.

§ 2. – Les Autorités publiques mettent en œuvre les obligations décrites au paragraphe 1er notamment dans les partenariats qu'ils entretiennent avec :

1° Les prestataires de services d'intermédiation de données;

2° Les prestataires de services informatiques;

3° Les opérateurs de services de plateformes numériques;

4° Les prestataires de services informatiques de stockage;

5° Les organisations altruistes en matière de données reconnues et inscrites au « Registre d'organisations altruistes en matière de données » conformément à l'article 19.1 du DGA.

CHAPITRE 2
Qualification des parties à un partenariat numérique de données

Article C.III.4.
La qualification des parties

Chaque partie dans le cadre d'un partenariat numérique de données est qualifiée conformément au présent titre.

Une même partie peut cumuler différentes qualifications.

Article C.III.5.
Les détenteurs de données

Le détenteur de données est soit producteur de données, soit diffuseur de données.

Article C.III.6.
Les producteurs de données

§ 1er. – Est producteur la personne qui assure la création de données généralement à l'aide d'outils et de techniques informatiques.

§ 2. – Conformément à sa mission organique et sans préjudice des dispositions du présent code et du RGPD, une Autorité publique qui procède à l'intégration des données est considérée comme producteur des données intégrées.

§ 3. – Le producteur de données est responsable :

1° de la qualité des données, en ce compris notamment de la mise à jour des données;

2° de l'identification de l'ensemble des données qu'il détient, de la manière dont elles sont gérées, documentées, décrites, organisées et formatées sous forme de jeux de données, de données de contenu, de données de référence et de métadonnées;

3° de la définition des conditions de l'utilisation ou, éventuellement, des conditions de partage des données.

§ 4. – Sauf si le présent Code, une législation ou une réglementation particulière en dispose autrement, le producteur de données désigne le ou les diffuseurs de données pour chacune des données ou jeux de données qui peuvent être partagés.

§ 5. – Sauf si le présent Code, une législation ou une réglementation particulière en dispose autrement, les producteurs de données sont responsables du traitement des demandes formulées par les utilisateurs finaux ou le cas échéant, orientent les utilisateurs finaux vers le service compétent pour traiter leurs demandes.

Article C.III.7.
Les diffuseurs de données

§ 1er. – Est diffuseur la personne qui met des données à disposition des utilisateurs.

§ 2. – Le diffuseur de données est responsable de :

1° la publication des données;

2° la gestion de la qualité des données au sens du chapitre 1 du titre 4;

3° la sécurité et la protection des données au sens du chapitre 2 du titre 5;

4° la conservation et la récupération des données;

5° la mise en forme et la présentation des données;

6° la mise en place des mécanismes d'accès et de téléchargement des données;

7° des garanties de confidentialité et sécurité des données.

Le diffuseur de données garantit un niveau de performance et de disponibilité proportionnel à la nature des données et de l'objectif poursuivi.

§ 3. – Conformément au principe énoncé à l'article C.II.4, les diffuseurs doivent publier les données dans un format :

1° ouvert;

2° lisible par une machine;

3° accessible, traçable et réutilisable;

4° accompagné des métadonnées.

§ 4. – Dans l'hypothèse où la donnée sollicitée est disponible sous un format répondant aux exigences d'un format ouvert, le diffuseur n'est pas tenu de publier les données sous un format différent de celui qu'il utilise déjà pour satisfaire une demande particulière. Dans le cas contraire, le diffuseur devra procéder aux conversions nécessaires.

§ 5. – En application de l'article C.III.6, § 4, le diffuseur de données doit renvoyer les demandes formulées par les utilisateurs finaux vers le producteur de données, sauf si le présent Code, une législation ou une réglementation particulière en dispose autrement.

Article C.III.8.
Les gestionnaires de données

§ 1er. – Dans tout partenariat numérique de données, les parties définissent :

1° l'administrateur de base de données;

2° l'administrateur de sécurité;

3° l'administrateur système;

4° l'administrateur réseau.

§ 2. – Selon le mode de partage des responsabilités entre les parties au partenariat, les administrateurs peuvent se trouver sous la responsabilité de l'une ou l'autre partie.

§ 3. – Les Autorités publiques qui dans le cadre d'un partenariat n'identifient pas les responsabilités visées à l'alinéa premier sont responsables des prestations informatiques relatives aux données qu'elles traitent.

CHAPITRE 3
La catégorisation des données

Article C.III.9.
La catégorisation des données

§ 1er. – Les données publiques d'un partenariat sont catégorisées au minimum conformément au présent titre.

Les catégories de données énoncées au présent titre constituent les identifiants minimums des métadonnées et des données de référence telles que visées à l'article C.III.17 afin d'être intégrées dans le Catalogue des données de la Plateforme bruxelloise de la donnée.

§ 2. – Chaque catégorie de ces données est régie par des politiques, ensembles de normes ou meilleures pratiques, et processus spécifiques.

§ 3. – Les catégories des données ne s'excluent pas mutuellement et les obligations légales et techniques qui leur sont associées peuvent leur être appliquées concomitamment.

§ 4. – Dans le cas où un jeu de données contiendrait des données relevant de catégories différentes, les Autorités publiques tiennent compte du cadre juridique applicable à chacune des catégories de données concernées ainsi que des mécanismes techniques qu'implique chacune des catégories de données.

Article C.III.10.
Typologie des catégories de données

§ 1er. – Les données appartiennent, en fonction de leur régime de propriété, à l'une des catégories suivantes, qui déterminent les règles concernant leur utilisation :

1° données à caractère personnel;

2° données exclusives;

3° données publiques;

4° données à forte valeur;

5° données d'origine privée.

§ 2. – Les données appartiennent à l'une des catégories suivantes, en fonction du lien entre l'origine des données et le mode de production de la donnée :

1° données fournies librement;

2° données observées;

3° données dérivées et déduites;

4° données acquises.

§ 3. – Les données appartiennent à l'une des catégories suivantes, selon le niveau d'accès à accorder aux données et les possibilités de partages organisées :

1° données ouvertes;

2° données partageables;

3° données fermées.

§ 4. – Les données appartiennent à l'une des catégories suivantes, selon le risque de dommages potentiels liés aux traitements des données :

1° données à risques inexistants;

2° données à risques faibles;

3° données à risques importants.

La détermination du risque conformément à l'alinéa 1er permet la catégorisation de certaines données en tant que données sensibles ou en tant que données classifiées.

§ 5. – D'autres catégories de données peuvent être utilisées en complément des catégories visées par le présent article en fonction des usages des Autorités publiques et des autres parties.

TITRE 3
La valorisation des données détenues par les Autorités publiques

Article C.III.11.
La valorisation des données

La valorisation des données détenues par les Autorités publiques vise à organiser la gestion des données en tant que sources de valeur et véritables actifs numériques.

La valorisation des données repose sur :

1° la déclaration de principes;

2° la valorisation des données d'usage;

3° le respect des droits des tiers sur les données protégées;

4° l'évaluation des risques.

CHAPITRE 1
La déclaration de principes

Article C.III.12.
La déclaration de principes

Les Autorités publiques adoptent une déclaration de principes qui établit et décrit :

1° le modèle opérationnel mis en place pour gérer les données;

2° les bases de données qu'elles détiennent et la manière dont les données qu'elles détiennent sont gérées, documentées, décrites, organisées et formatées sous la forme de jeux de données, de données de contenu, de données de référence et de métadonnées;

3° le cas échéant, la déclaration d'accessibilité visée à l'article 7 de l'ordonnance du 4 octobre 2018 relative à l'accessibilité des sites internet et des applications mobiles des organismes publics régionaux et des communes;

4° la manière dont l'Autorité publique compte atteindre l'objectif stratégique d'exploitation efficiente et responsable visé à l'article C.II.12;

5° en cas de recours à des traitements algorithmiques ou d'intelligence artificielle, une description de la manière dont ils sont utilisés dans l'accomplissement des missions de service public ou d'obligations d'intérêt général;

6° en cas d'application d'une redevance dans le cadre d'une réutilisation de données, conformément à l'article C.IV.24, les modalités de calcul et le montant effectif des redevances;

7° la manière dont sont gérés et documentés les accords d'exclusivité visés aux articles C.IV.29;

8° tout autre élément pertinent présentant une importance particulière au regard de la stratégie numérique mise en place par l'Autorité publique dans le cadre de ses missions.

La déclaration de principes est publiée sur le site de chaque Autorité publique ou disponible à première demande.

CHAPITRE 2
La valorisation des données d'usage

Article C.III.13.
Valorisation des données d'usage

Les Autorités publiques collectent et valorisent les données d'usage notamment en vue :

1° d'identifier des profils d'usage, repérer des modes d'engagement avec les contenus ou les habitudes d'utilisation;

2° d'améliorer la lisibilité et l'accès à leurs services;

3° d'informer d'autres usagers ou citoyens que les usagers ou citoyens identifiés au départ des données d'usage déjà récoltées;

4° d'améliorer la représentation des usagers de leurs services;

5° de protéger la vie privée des usagers en collectant les refus et les consentements en tant que donnée d'usage.

CHAPITRE 3
Le respect des droits sur les données protégées

Article C.III.14.
Le respect des droits des tiers sur les données protégées

§ 1er. – Dans le cadre de la valorisation des données qu'elles détiennent, les Autorités publiques respectent les droits des tiers sur les données protégées.

§ 2. – Sans préjudice de l'article 6 du RGPD pour ce qui concerne les données à caractère personnel, les Autorités publiques recueillent les consentements et les autorisations nécessaires à la valorisation et au partage de données protégées de la part des titulaires de droits sur ces données.

Le cas échéant, et sans préjudice des dispositions d'autres réglementations applicables au traitement des données concernées, les Autorités publiques mettent en place un mécanisme de consentement ou d'autorisation dynamique.

§ 3. – Dans le cadre de la valorisation des données qu'elles détiennent, les Autorités publiques respectent la confidentialité des données protégées.

Sauf disposition contraire applicable ou consentement des personnes concernées, les Autorités publiques adaptent leurs techniques, d'anonymisation ou de pseudonymisation au regard de la nature des

données à caractère personnel traitées et des risques liés à leur valorisation.

Sauf disposition contraire applicable ou autorisation des personnes disposant des droits sur ces données, les données protégées pour des raisons de confidentialité commerciale ou de secrets statistiques, par le secret d'affaires ou pour la protection de droits de propriété intellectuelle doivent être occultées avant tout partage.

§ 4. – Sans préjudice des droits des personnes concernées et des recours organisés par le RGPD, les Autorités publiques organisent les recours nécessaires afin que les titulaires de droits sur les données protégées puissent déposer plainte auprès des services ou des personnes compétentes au sein des Autorités publiques dès qu'ils estiment que leurs droits ne sont pas respectés ou sont menacés.

CHAPITRE 4
L'évaluation des risques

Article C.III.15.
Évaluation des risques

Sans préjudice des articles 35 et 36 du RGPD, les Autorités publiques doivent réaliser une évaluation des risques liés à la protection des données protégées en tenant compte des informations à leur disposition concernant :

1° la nature des données protégées à traiter;

2° le type d'opérations à réaliser;

3° la portée des opérations de traitement et leur contexte;

4° la finalité et la durée des traitements.

TITRE 4
La gestion des données

Article C.III.16.
La gestion des données

Les Autorités publiques mettent en place une gestion efficace et cohérente des données qu'elles détiennent.

Dans ce cadre, les Autorités publiques adoptent les mesures techniques et organisationnelles appropriées et tout processus pertinent afin de vérifier, à tout moment, que les données qu'elles détiennent :

1° font l'objet d'une sécurisation adéquate telle qu'énoncée à l'article C.II.2;

2° ont le niveau de qualité requis pour atteindre les objectifs de valorisation identifiés;

3° sont intégrées dans des systèmes d'information interopérables, tels que décrits à l'article C.II.17;

4° sont réversibles, sans préjudice des dispositions réglementaires qui seraient applicables, tels que décrits à l'article B.II.XX.

Les Autorités publiques définissent la fréquence des mises à jour des données qu'elles détiennent.

En tous les cas, les Autorités publiques :

1° garantissent la plus haute fréquence de mise à jour compte tenu de la nature des données traitées et de l'objectif poursuivi;

2° documentent et publient la fréquence de mise à jour des données qu'elles détiennent;

3° garantissent que les titulaires de droits sur les données protégées puissent mettre à jour ou modifier les données à tout moment.

Les Autorités publiques gèrent les données qu'elles détiennent tout au long du cycle de la vie de la donnée, en tenant compte de leur contexte d'utilisation et de leur cas d'usage, ainsi que des éventuelles modifications.

CHAPITRE 1
La gestion de la qualité des données

SECTION 1
La gestion des données de référence et des métadonnées

Article C.III.17.
La gestion des données de référence et des métadonnées

§ 1er. – Le présent article vise à fournir les outils nécessaires aux Autorités publiques pour atteindre l'objectif opérationnel décrit à l'article C.II.20.

§ 2. – Les Autorités publiques définissent, stockent, distribuent les données de référence et organisent une vue complète, fiable et à jour des données de référence qu'elles détiennent au sein d'un système d'information, indépendamment des canaux de communications, du secteur d'activité ou des subdivisions métiers ou géographiques.

§ 3. – Les Autorités publiques définissent, stockent, et organisent une vue complète, fiable et à jour des métadonnées des données qu'elles détiennent au sein d'un système d'information.

Pour gérer les métadonnées et les données de référence, les Autorités publiques utilisent les outils du Catalogue des données. Les Autorités publiques établissent des métadonnées fiables permettant notamment d'identifier :

1° les types de données à valoriser ou partager;

2° l'utilité que les données représentent en termes d'information;

3° l'origine des données;

4° la localisation des données;

5° la manière dont les données se déplacent dans les systèmes;,

6° l'entité responsable de ces données;,

7° les conditions d'accès aux données;,

8° les partenariats numériques de données en vigueur;

9° la qualité des données en ce compris leur fréquence de mise à jour et leur exhaustivité (complétude).

§ 4. – Les données de référence, les métadonnées et l'identification des données qu'elles décrivent sont transmises au gestionnaire de la Plateforme bruxelloise de la donnée par chaque Autorité publique au moins une fois par an à l'aide de l'outil de gestion du Catalogue des données.

SECTION 2
La gestion des modèles analytiques et la transparence des algorithmes

Article C.III.18.
La gestion des modèles analytiques, des algorithmes et des systèmes exploitant l'intelligence artificielle

Les Autorités publiques adoptent des mesures techniques et organisationnelles appropriées en vue de garantir que tout système qu'elles utilisent et qui recourt à des modèles analytiques, des algorithmes ou des solutions d'intelligence artificielle puisse faire l'objet d'un contrôle. À cet effet, les autorités publiques veillent, notamment, concernant les modèles analytiques, algorithmes et systèmes, à :

1° établir une stratégie de gouvernance ciblée intégrant les risques et bénéfices qui en découlent;

2° développer un inventaire de ceux qu'elles utilisent, notamment pour évaluer l'impact de l'ajout de nouveaux éléments ou de la modification des éléments existants;

3° les concevoir et les tester pour éviter les effets disparates éventuels;

4° garantir la transparence de leurs modèles techniques et commerciaux;

5° évaluer leur résilience, leur sécurité, et s'ils développent des moyens proportionnés aux buts recherchés;

6° mettre en place des mécanismes de contrôle assurant la responsabilité et la transparence de leur fonctionnement et le contrôle de leurs résultats par leurs utilisateurs;

7° instaurer des contrôles opérés par l'administrateur local de la donnée;

8° informer et responsabiliser les personnes physiques qui les utilisent quant au fonctionnement des systèmes et à leurs conséquences potentielles;

9° garantir leur accessibilité à tous.

Sans préjudice de toute obligation découlant d'une réglementation applicable, toute décision individuelle prise à l'aide d'un algorithme doit être accompagnée d'une information sur le caractère automatisé de la décision disponible pour le destinataire de la décision individuelle.

SECTION 3
La gestion des bases de données

Article C.III.19.
La gestion des bases de données

Les Autorités publiques adoptent des mesures techniques et organisationnelles appropriées en vue de garantir la gestion des bases de données. À cet effet, les Autorités publiques veillent notamment à :

1° placer chaque base de données sous la responsabilité d'une personne physique désignée et adopter, dans ce cadre, une politique de gestion qui désigne le ou les administrateurs de la base de données, décrivant les rôles, les fonctions et les niveaux d'accès de ces administrateurs. Cette politique peut également imposer différentes exigences aux

administrateurs relativement à l'exercice de leurs fonctions;

2° notifier, en cas notamment de modification, de fusion ou de transfert d'une base de données, aux personnes concernées et aux titulaires de droits sur d'éventuelles données protégées, les changements intervenus.

CHAPITRE 2
La sécurité et la protection des données

SECTION 1
La gestion des accès et des privilèges associés

Article C.III.20.
Gestion de la sécurité et de la protection des données

Les Autorités publiques assurent la sécurisation et la protection des données qu'elles détiennent au travers de :

1° la gestion des accès et des privilèges associés;

2° la gestion de la sécurité informatique.

Article C.III.21.
Gestion des accès et des privilèges associés

Les Autorités publiques adoptent des processus de contrôle et de gestion des accès.

Tout accès à un système d'information et à ses ressources est contrôlé et seuls les accès autorisés peuvent avoir lieu.

Les accès sont établis en tenant compte notamment de :

1° de la fonction de l'utilisateur;

2° des catégories d'accès par type d'utilisateur;

3° de la catégorisation, telle qu'envisagée au chapitre 3 du titre 2 du présent livre, des données elles-mêmes.

Le Gouvernement, le Collège réuni et le Collège définissent conjointement les modalités de la gestion des accès.

SECTION 2
La gestion de la sécurité informatique

Article C.III.22.
Gestion de la sécurité informatique

Les Autorités publiques garantissent la gestion de la sécurité informatique en lien avec les données qu'elles détiennent.

La gestion de la sécurité informatique recouvre notamment :

1° l'appréciation des risques informatiques;

2° la définition de la politique de sécurité de l'information;

3° la gestion de la sécurité de l'information dans la gestion de projet;

4° la définition des rôles et responsabilités dans la sécurité de l'information;

5° la gestion des relations avec les tiers;

6° la gestion des incidents liés à la sécurité de l'information.

Le Gouvernement, le Collège réuni et le Collège, définissent conjointement l'étendue des obligations et les modalités des Autorités publiques en matière de gestion de la sécurité informatique.

TITRE 5
Le contrôle de la conformité, la traçabilité et la responsabilité des Autorités publiques

Article C.III.23.
Contrôle de la conformité et de la traçabilité

§ 1er. – Les Autorités publiques mettent en place des procédures de contrôle afin de s'assurer qu'elles gèrent les données et leurs accès conformément au présent Code, aux dispositions légales et réglementaires applicables en vigueur, de même que conformément aux politiques et normes qu'elles ont établies.

§ 2. – Les Autorités publiques mettent en place des procédures de contrôle permettant de vérifier et d'archiver les accès et les modifications aux données qu'elles détiennent ainsi que la conformité technique des outils et des systèmes utilisés pour gérer les données.

§ 3. – Les mesures de contrôle ainsi que la vérification de la conformité technique des outils et des systèmes utilisés pour celles-ci sont établies pério-

diquement à des points précis du cycle de vie des données pour évaluer les pratiques et les activités de l'Autorité publique.

Au moins un contrôle annuel est effectué pour chaque jeu de données.

§ 4. – Les Autorités publiques procèdent aux renforcements des capacités et des compétences de leurs agents par la mobilisation, l'information, la sensibilisation et la formation, en vue d'atteindre l'objectif stratégique d'éducation des parties prenantes décrit à l'article C.II.11.

LIVRE C.IV
Partage administratif, réutilisation et communication

TITRE 1
Garanties communes aux partages administratifs, réutilisations, communications

Article C.IV.1.
Secret Professionnel et confidentialité

Toute personne au sein des Autorités publiques qui, en raison de ses fonctions, participe à des opérations de partage administratif, de réutilisation ou de Communication, lesquelles, en vertu de dispositions légales ou réglementaires, seraient couvertes par le secret professionnel, est tenue de respecter ces dispositions légales ou réglementaires.

Article C.IV.2.
Respects de droit des tiers

Les opérations de partage administratif, de réutilisation ou de Communication respectent les droits des tiers tels que définis à l'article C.II.2, à savoir notamment :

1° les droits de propriété intellectuelle conformément à la législation applicable;

2° le secret des statistiques;

3° la protection des secrets d'affaires de tiers telle que visée par le titre 8/1 du livre XI du Code de droit économique;

4° la protection des personnes physiques à l'égard du traitement des données à caractère personnel garanti, en particulier, par le RGPD;

5° la protection des personnes qui signalent des violations du droit de l'Union et du droit national, au sens de la Directive (UE) 2019/1937;

6° les principes de concurrence repris dans le Livre IV du Code de droit économique et la réglementation applicable en matière d'aides d'État.

Article C.IV.3.
Absence de droit de propriété intellectuelle ou sui generis sur les bases de données publiques

Les Autorités publiques ne peuvent pas se prévaloir d'un droit de propriété intellectuelle, ni du droit « *sui generis* » prévu par les articles XI.307 et suivants du Code de droit économique sur les bases de données publiques qu'elles détiennent, produisent ou éditent. Elles ne peuvent, en outre, prendre des mesures restrictives d'accès ou de réutilisation de ces informations, que dans les cas où cela est nécessaire à la sauvegarde des prérogatives des tiers ou à des motifs de sécurité publique.

TITRE 2
Partage administratif

CHAPITRE 1
Principe du partage administratif

Article C.IV.4.
Partage administratif par défaut et demande de partage administratif

Les Autorités Publiques organisent des partages administratifs de données entre elles, gratuitement, sauf si ces partages administratifs sont contraires à une règle de droit ou s'ils portent atteinte aux droits des tiers sur les données soumises au partage administratif.

Les modalités des demandes de partage administratif formulées par les Autorités publiques destinataires sont déterminées par le Bureau de la donnée en concertation avec le Comité de Gouvernance de la donnée.

L'absence de réponse à une demande de partage administratif est assimilée à un refus de partage administratif dans le chef de l'Autorité publique productrice des données.

Article C.IV.5.
Passage par le Centre d'intégration par défaut

§ 1er. – Tout partage administratif est réalisé au travers du Centre d'intégration, en l'absence de législation particulière organisant spécifiquement le partage administratif visé.

§ 2. – En l'absence de toute disposition légale ou réglementaire contraire, les partages entre Autorités publiques et Autorités publiques tierces, sont assimilés à des partages administratifs au sens du présent Code. Dans ces hypothèses, le partage administratif est réalisé au travers du Centre d'intégration et, le cas échéant, le Centre d'intégration constitue le relais obligatoire entre les Autorités publiques et les autres intégrateurs de services des Autorités publiques tierces.

L'intégrateur de services bruxellois vérifie le cas échéant les autorisations nécessaires en vertu d'une disposition législative ou réglementaire dans le chef des parties impliquées, avant de permettre le partage administratif.

Article C.IV.6.
La qualité de la donnée partagée

L'Autorité publique identifiée comme le producteur des données est responsable de la qualité de la donnée partagée administrativement.

L'Autorité publique producteur met en œuvre tous les moyens à sa disposition pour atteindre le plus haut niveau de qualité au regard de l'état de l'art et de l'évolution des technologies, ainsi que conformément aux règles de gouvernance du présent Code et des règles, lignes directrices ou recommandations de qualité adoptées en matière de gouvernance des données par le Comité de gouvernance de la donnée.

Article C.IV.7.
Responsabilité de l'Autorité publique destinataire

L'Autorité publique destinataire assure la confidentialité des données issues du partage administratif transitant par le Centre d'intégration, la gestion des accès à ces données. L'Autorité publique destinataire est responsable des accès sur les données mises à disposition ou transmises.

CHAPITRE 2
Conditions du partage administratif

SECTION 1
Conditions générales

Article C.IV.8.
Conclusion d'un protocole d'accord

§ 1er. – Les Autorités publiques parties au partage administratif concluent un protocole d'accord.

Les Autorités publiques peuvent se faire représenter par leur administrateur local de la donnée.

§ 2. – Chaque protocole d'accord comprend au moins les informations suivantes :

1° l'identité et les coordonnées de l'Autorité publique producteur des données, en ce compris celles de son représentant;

2° l'identité et les coordonnées de l'Autorité publique destinataire, en ce compris celles de son représentant;

3° en application du chapitre 2 du titre 2 du livre C.III, les qualités de chaque partie;

4° les finalités précises pour lesquelles les données font l'objet d'un partage administratif;

5° les catégories de données visées conformément au chapitre 3 du titre 2 du livre C. III et les types de données concernées;

6° le format et le support éventuel de la donnée;

7° l'obligation légale, la mission de services publics qui fonde la demande de partage administratif des données;

8° le niveau de qualité de la donnée et la durée pour laquelle ce niveau est garanti par l'Autorités publique producteur;

9° les modalités techniques de l'opération visée et plus spécifiquement les conditions d'interopérabilité;

10° les normes de sécurité implémentées et les normes techniques et organisationnelles de la base de données concernée;

11° les procédures en cas de fuite de données et non disponibilité des données;

12° les modalités de fin du partage administratif et du Protocole d'accord.

§ 3. – Dans l'hypothèse où le partage administratif vise des données personnelles, le protocole d'accord comprend également au moins les informations suivantes :

1° l'identification du responsable de traitement au sein de chaque Autorité publique, partie au partage administratif;

2° les coordonnées des Délégués à la protection des données et Conseillers en sécurité de l'information

au sein de chacune des Autorités publiques parties au partage administratif;

3° les catégories de données à caractère personnel concernées, dans le respect du principe de minimisation, au sens du RGPD;

4° toute mesure spécifique prise conformément au principe de proportionnalité et aux exigences de protection des données dès la conception et par défaut;

5° les restrictions légales applicables aux droits de la personne concernée et la justification de leur application en l'espèce;

6° les modalités d'exercice des droits de la personne concernée.

Article C.IV.9.
Procédure de conclusion du protocole d'accord

§ 1er. – Le protocole d'accord est conclu préalablement au partage administratif des données dans un délai maximal de quarante jours ouvrables à compter de la réception, par l'Autorité publique producteur des données, de la demande de partage administratif visée à l'article C.IV.4, alinéa 2.

Les parties peuvent de commun accord prolonger d'un mois au maximum le délai prévu à l'alinéa 1er, notamment pour des demandes importantes ou complexes.

§ 2. – Le Bureau de la donnée en concertation avec le Comité de gouvernance de la donnée propose des modèles de protocoles d'accord disponibles sur la Plateforme bruxelloise de la donnée, permettant d'encadrer les partages administratifs.

§ 3. – Le délai de quarante jours ouvrables est suspendu pendant les demandes d'avis visées au paragraphe 4 pour une durée de vingt jours ouvrables maximum et, en cas d'analyse d'impact visée à l'article 35 du RGPD, pour une durée de trente jours ouvrables maximum.

L'absence de conclusion d'un protocole d'accord dans le délai légal est assimilée à un refus de conclusion du Protocole d'accord dans le chef de l'Autorité producteur des données.

§ 4. – Le protocole d'accord est adopté après les avis respectifs du Conseiller en sécurité de l'information et de l'administrateur local de la donnée, et, en cas de partage administratif de données à caractère personnel, du Délégué à la protection des données. Ces avis sont remis dans un délai de vingt jours ouvrables, à compter du jour où le projet de protocole d'accord leur a été envoyé simultanément. À défaut, l'avis sera considéré comme négatif.

Ces avis sont annexés au protocole d'accord.

Lorsqu'un de ces avis n'est pas suivi par les parties, le protocole d'accord mentionne, en ses dispositions introductives, les raisons pour lesquelles cet avis n'a pas été suivi.

Article C.IV.10.
Publicité du protocole d'accord

Les protocoles d'accord sont publiés, dans les meilleurs délais et au plus tard avant tout partage administratif, par les Autorités publiques via le Catalogue des données.

L'Autorité publique producteur des données envoie le protocole d'accord à l'Intégrateur de services bruxellois, au plus tard dans le mois suivant son adoption.

Article C.IV.11.
Recours auprès de la CADADo

Toute personne physique ou morale directement affectée par une décision relative à une demande de partage administratif de données dispose d'un droit de recours devant la CADADo dans les conditions prévues au Livre B.II.

SECTION 2
Conditions particulières relatives à la mise à disposition de données issues de sources authentiques aux fins de collecte unique

SOUS-SECTION 1
Principe de la mise à disposition de données issues de sources authentiques aux fins de collecte unique

Article C.IV.12.
Partage administratif de données issues de sources authentiques aux fins de collecte unique

§ 1er. – Les partages administratifs de données issues de sources authentiques visent la mise à disposition de ces données au profit des Autorités publiques destinataires afin qu'elles n'en organisent plus elle-même la collecte.

§ 2. – Les Autorités Publiques ne collectent les données issues de sources authentiques qu'auprès des Autorités publiques désignées producteur de la

sources authentique, à travers le Centre d'intégration, selon les modalités techniques prévues de ce dernier concernant le canal relatif aux données issues de sources authentiques.

Les Autorités publiques ne peuvent plus réclamer directement les données visées au premier alinéa à d'Autres autorités publiques ou à des personnes, organismes ou institutions.

Le Gouvernement et le Collège réuni et le Collège peuvent suspendre pour des raisons techniques ou organisationnelles, et pour toutes ou certaines Autorités publiques uniquement, l'application du présent paragraphe pour une période transitoire renouvelable qui ne peut excéder cinq ans à dater de la désignation de la source authentique par arrêté, afin de permettre aux Autorités publiques de se connecter de manière effective au Centre d'intégration.

Article C.IV.13.
Clefs d'identification

§ 1er. – Dans le cadre des mises à disposition de données issues de sources authentiques, pour l'identification de personnes physiques, les Autorités publiques utilisent :

1° le numéro du Registre national attribué en exécution de l'article 2, § 3, de la loi du 8 août 1983 organisant un Registre national des personnes physiques;

2° ou le numéro d'identification de la Banque-carrefour attribué en exécution de l'article 4, § 2, alinéa 3, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque de la Sécurité sociale, s'il s'agit de données qui concernent une personne physique non reprise dans le Registre national.

§ 2. – Dans le cadre des partages administratifs de données issues de sources authentiques, pour l'identification de personnes morales, les Autorités publiques utilisent, pour l'exécution de leurs missions légales, le numéro d'entreprise attribué en exécution de l'article III.17 du Code de droit économique.

§ 3. – Dans le cadre de l'accomplissement d'une obligation légale d'information, les personnes physiques et morales utilisent :

1° le numéro du Registre national attribué en exécution de l'article 2, alinéa 2, de la loi du 8 août 1983 organisant un Registre national des personnes physiques, ou

2° le numéro d'identification de la Banque attribué en exécution de l'article 4, § 2, alinéa 3, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la Sécurité sociale et le numéro d'entreprise attribué en exécution de l'article III.17 du Code de droit économique.

§ 4. – Dans le cadre des partages administratifs de données issues de sources authentiques, les Autorités publiques peuvent utiliser, pour l'exécution de leurs missions légales :

1° le numéro d'identification des parcelles cadastrales;

2° les identifiants repris dans les bases de données UrbiS concernant toutes les données à caractère géographique relatives au territoire bruxellois.

SOUS-SECTION 2
Gestion des données issues de sources authentiques

Article C.IV.14.
Qualité des données issues de sources authentiques

§ 1er. – L'Autorité publique désignée comme producteur de la source authentique met tout en œuvre pour garantir aux Autorités publiques destinataires la qualité de la donnée authentique, en assurant notamment son caractère exact et mis à jour au regard des finalités d'utilisation.

§ 2. – Si le destinataire des données issues de sources authentiques constate que ces données sont imprécises, incomplètes ou inexactes, il est tenu d'en informer immédiatement le producteur de la source authentique et l'intégrateur de services bruxellois qui sont tenus d'y donner suite.

§ 3. – Le Gouvernement et le Collège réuni, le Collège peuvent conjointement adopter des normes de qualité ou des lignes conduites en matière de qualité des données issues de sources authentiques.

Article C.IV.15.
Désignation de sources authentiques

§ 1er. Sans préjudice des sources authentiques reconnues par des Autorités publiques tierces, le Gouvernement, le Collège réuni et le Collège, désignent par arrêté, les sources authentiques dont l'Autorité publique désignée comme producteur de la source authentique relève de leur compétence.

§ 2. – Par dérogation à l'alinéa 1er, les sources authentiques comprenant des données à caractère personnel sont désignées par décret ou ordonnance selon la Collectivité publique dont dépend l'Autorité

publique désignée producteur de la source authentique.

§ 2. – La désignation des sources authentiques visées au paragraphe 1er s'effectue :

1° soit sur demande de l'Intégrateur de services bruxellois auprès du Gouvernement, Collège réuni ou Collège;

2° soit sur demande de l'Autorité publique qui se propose comme producteur de la source authentique auprès du Gouvernement, Collège réuni ou Collège;

3°soit d'initiative par le Gouvernement, le Collège réuni ou le Collège.

§ 3. – Sous peine d'irrecevabilité, la demande visée au paragraphe 2, 1° et 2° est soumise préalablement à :

1° l'avis du service compétent de la Région bruxelloise pour la simplification administrative;

2° l'avis du Conseiller en sécurité de l'information de l'Autorité publique proposée comme producteur de la source authentique;

3° l'avis du Délégué à la protection des données de la même Autorité publique;

4° l'avis de l'administrateur local des données de la même Autorité publique.

Dans l'hypothèse visée au paragraphe 2, 3°, le Gouvernement, le Collège réuni et le Collège demandent d'office les avis visés à l'alinéa 1er.

Lorsque la base de données dont la désignation en tant que source authentique est demandée contient des données à caractère personnel, les avis examinent, d'une part, dans quelle mesure la désignation de cette source authentique répond aux critères de nécessités et de proportionnalité qui s'imposent à toute ingérence dans le droit à la protection des données à caractère personnel et, d'autre part, quelles procédures sont envisagées afin de garantir la qualité des données à caractère personnel de la source authentique au sens de l'article C.IV.14.

§ 4. – L'acte de désignation visé au paragraphe 1er indique, notamment, pour chaque source authentique :

1° l'identité de l'Autorité publique producteur de la source authentique, chargé de la collecte des données, de leur mise à jour, de leur mise à disposition et de tout autre traitement pertinent et nécessaire à son maintien, en fonction de l'état de l'art et de l'évolution des technologies;

2° les modalités selon lesquelles sont tenues à jour et rendues accessibles les données dont l'hébergement est confié à l'Autorité publique producteur de la source authentique;

3° la ou les finalités poursuivies par l'Autorité publique producteur par la constitution de la source authentique lors la collecte des données visées;

4° la liste des données contenues dans la source authentique;

5° les modalités particulières de financement de la collecte des données comprises dans la source authentique, de leur mise à jour, de leur mise à disposition et de tout autre traitement pertinent et nécessaire à son maintien.

Pour ce qui concerne la désignation de sources authentiques comprenant des données à caractère personnel, le décret ou l'ordonnance indique également :

– les éléments essentiels du traitement;

– les mesures prévues protégeant les droits des personnes concernées;

– les obligations de transparence prévues à l'intention des personnes concernées.

Article C.IV.16.
Désignation de la Base de données issues de Sources Authentiques

Des bases de données constituées au départ de données issues de sources authentiques sont désignées en tant que base de données issues de sources authentiques par décret ou ordonnance selon la collectivité publique dont dépend l'Autorité publique désignée producteur de la base de données issues de sources authentiques.

L'article C.IV.15, § 2 à 4, s'applique à la procédure de désignation des bases de données issues de sources authentiques *mutatis mutandis*.

Dans le cadre de l'application du Code, les bases de données issues des sources authentiques et les données qui en sont issues, sont assimilées respectivement à des sources authentiques et leurs données, à des données issues de sources authentiques.

TITRE 3
Réutilisations des documents et des données publiques

Article C.IV.17.
Deux régimes de réutilisation

Deux régimes de réutilisation doivent être distingués :

1° la réutilisation des documents ouverts accessibles librement et des documents partageables accessibles aux conditions décrites dans le présent, titre conformément à la transposition de la Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte);

2° la réutilisation des données protégées telles que visées par l'article 3.1. du DGA.

CHAPITRE 1
La réutilisation des documents librement accessibles et partageables

SECTION 1
Champ d'application

Article C.IV.18.
Transposition de la Directive 2019/1024

Le présent titre transpose la Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte).

Les ordonnances, les arrêtés ministériels et toute autre réglementation existante qui font référence à la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public sont présumées faire référence à la Directive (UE) du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte).

Article C.IV.19.
Champ d'application et exceptions

§ 1er. – Le présent chapitre s'applique aux :

1° documents existants détenus par les Autorités publiques;

2° documents existants détenus par les entreprises publiques;

3° données de la recherche, sous réserve des limitations et exceptions prévues par le présent chapitre.

§ 2. – Le présent chapitre ne s'applique pas :

1° aux documents étrangers à la mission de service public dévolue à l'Autorité publique, sous réserve que l'objet des missions de service public soit transparent et soumis à réexamen;

2° aux documents détenus par des entreprises publiques :

a) dont la production ne relève pas de la fourniture des services d'intérêt général au sens de la loi;

b) relatifs aux activités directement exposées à la concurrence et qui, par conséquent, conformément à l'article 34 de la Directive 2014/25/UE, ne sont pas soumises aux règles relatives à la passation des marchés;

3° aux documents sur lesquels des tiers détiennent les droits de propriété intellectuelle;

4° aux documents, tels que les données sensibles, dont l'accès est exclu ou dont l'accès est limité conformément aux règles législatives et réglementaires d'accès, notamment pour les motifs suivants :

a) la protection de la sécurité nationale (c'est-à-dire la sécurité de l'État), la défense ou la sécurité publique;

b) la confidentialité des données statistiques;

c) la confidentialité des informations commerciales (notamment le secret d'affaires, le secret professionnel ou le secret d'entreprise)];

5° aux documents dont l'accès est exclu ou limité pour des motifs d'informations sensibles relatives à la protection des infrastructures critiques au sens de l'article 2, point d), de la Directive 2008/114/CE;

6° aux documents dont l'accès est limité légalement notamment dans les cas où un intérêt personnel ou particulier est requis pour avoir accès aux documents;

7° aux logos, armoiries ou insignes;

8° aux documents dont l'accès est exclu ou limité en application de règles d'accès pour des motifs de protection des données à caractère personnel, et aux parties de documents accessibles en vertu desdites règles qui contiennent des données à caractère personnel dont la réutilisation a été définie par une norme législative comme étant incompatible avec la législation concernant la protection des personnes physiques à l'égard du traitement de données à caractère personnel ou comme portant à atteinte à la protection de la vie privée et de l'intégrité de la personne concernée, en particulier au regard des dispositions de droit de l'Union ou de droit national sur la protection des données à caractère personnel;

9° aux documents détenus par les radiodiffuseurs de service public et leurs filiales et par d'autres organismes ou leurs filiales pour une mission de radiodiffusion de service public;

10° aux documents détenus par des établissements culturels autres que des bibliothèques y compris des bibliothèques universitaires, des musées et des archives;

11° aux documents détenus par les établissements d'enseignement de niveau secondaire et au-dessous et, dans le cas de tous les autres établissements d'enseignement, aux documents autres que ceux pouvant être assimilés à des données de recherche visées au paragraphe 1, 3);

12° aux documents autres que les données de recherches visées au paragraphe 1, 3), détenus par des organismes exerçant une activité de recherche et des organisations finançant une activité de recherche y compris des organisations créées pour le transfert des résultats de la recherche.

SECTION 2
Principe de réutilisation

Article C.IV.20.
Réutilisation des données des Autorités publiques, des entreprises publiques, des bibliothèques, des musées et des archives

Sous réserve des limites fixées à l'article C.IV.19, les documents détenus par les Autorités publiques peuvent être réutilisés à des fins commerciales ou non commerciales.

Les Autorités publiques peuvent soumettre la réutilisation des documents à des conditions, conformément aux dispositions du présent chapitre, plus particulièrement les sections IV et V.

Les documents pour lesquels les bibliothèques, y compris les bibliothèques universitaires, les musées et les archives sont titulaires de droits de propriété intellectuelle et les documents détenus par des entreprises publiques peuvent être réutilisés, lorsque la réutilisation de ces documents est autorisée, à des fins commerciales ou non commerciales, conformément aux conditions du présent chapitre, plus particulièrement les sections IV et V.

SECTION 3
Demande de réutilisation

Article C.IV.21.
Demande de réutilisation

Les Autorités publiques traitent les demandes de réutilisation et mettent le document à la disposition du demandeur en vue de la réutilisation, si possible et s'il y a lieu, sous forme électronique.

Si l'obtention du document requiert l'emploi d'une licence, l'Autorité publique sollicitée par la demande de réutilisation envoie au demandeur une offre de licence.

L'Autorité publique traite la demande et fournit le document au demandeur en vue de la réutilisation ou, si une licence est nécessaire, présente au demandeur l'offre de licence définitive dans un délai maximal de vingt jours ouvrables à compter de la réception de la demande. Ce délai peut être prolongé de vingt jours ouvrables supplémentaires pour des demandes importantes ou complexes. En pareils cas, dans les trois semaines qui suivent la demande initiale, le demandeur est informé qu'un délai supplémentaire est nécessaire pour traiter la demande ainsi que des raisons qui justifient ce délai.

En cas de décision négative, l'Autorité publique communique au demandeur les raisons du refus, notamment lié à l'article C.IV.19, § 2, 1) à 12) ou C.IV.20. En cas de décision négative fondée sur l'article C.IV.19, § 2, 3), l'Autorité publique fait mention de la personne physique ou morale titulaire des droits, si elle est connue, ou, à défaut, du donneur de licence auprès duquel elle a obtenu le document en question. Les bibliothèques, y compris les bibliothèques universitaires, les musées et les archives, ne sont pas tenus d'indiquer cette mention

Toute décision relative à la réutilisation des documents notifiée au demandeur indique les voies de recours contre cette décision auprès de la CADADo, conformément à l'article C.VI.32 et au livre B.II.

Le Bureau de la donnée fournit les informations appropriées en vue de faciliter la réutilisation efficace des documents.

À défaut de ces indications, le délai de prescription pour introduire le recours ne prend pas cours.

Les entités suivantes ne sont pas tenues de se conformer au présent article :

1° les entreprises publiques;

2° les établissements d'enseignement, les organismes exerçant une activité de recherche et les organisations finançant une activité de recherche.

SECTION 4
Conditions de réutilisation

Article C.IV.22.
Publicité des conditions

Les conditions applicables à la réutilisation des documents doivent être rendues publiques préalablement, et de préférence par voie électronique.

Article C.IV.23.
Formats disponibles

§ 1er. – L'Autorité publique et les entreprises publiques mettent à disposition leurs documents sous une forme et une langue préexistante, et, si possible, sous forme électronique, sans que cela entraîne d'obligation de créer, d'adapter ou de fournir des extraits de documents qui engendrerait des efforts disproportionnés dépassant la simple manipulation.

§ 2. – Dans toute la mesure du possible, l'Autorité met à disposition les documents dans des formats ouverts et lisibles par machine, accessibles, traçables, réutilisables et accompagnés de leurs métadonnées conformément à l'article C.III.7, § 3. Ces formats et métadonnées doivent répondre à des normes formelles ouvertes au sens du présent Code.

§ 3. – Les Autorités publiques ne sont pas tenues de poursuivre la production de documents en vue de leur réutilisation. Toutefois, elles sont tenues de rendre leurs décisions publiques dans les meilleurs délais.

§ 4. – Les Autorités publiques mettent les données dynamiques à disposition aux fins de réutilisation aussitôt qu'elles ont été recueillies, en recourant à des API appropriées et, le cas échéant, sous la forme d'un téléchargement de masse.

Lorsque la mise à disposition des données dynamiques aux fins de réutilisation ayant eu lieu immédiatement après la collecte, comme prévu à l'alinéa 1er, excéderait les capacités financières et techniques de l'Autorité publique, en imposant de ce fait un effort disproportionné, ces données dynamiques sont mises à disposition aux fins de réutilisation dans un délai ou avec des restrictions techniques temporaires qui ne portent pas indûment atteinte à l'exploitation de leur potentiel économique et social.

§ 5. – Les paragraphes 1er à 4 s'appliquent aux documents existants détenus par des entreprises publiques qui sont disponibles aux fins de réutilisation.

§ 6. – Les ensembles de données de forte valeur dont la liste est établie conformément à l'article C.IV.29, sont mises à disposition à des fins de réutilisation dans des formats lisibles par machine, en recourant à des API appropriées et, le cas échéant, sous la forme d'un téléchargement de masse.

Article C.IV.24.
Principe de tarification

§ 1er. – Une redevance peut être demandée pour la mise à disposition d'un document.

§ 2. – Lorsqu'une redevance est prélevée, elle ne peut couvrir que les coûts marginaux de reproduction, de mise à disposition et de diffusion d'anonymisation de données à caractère personnel et des mesures prises pour protéger des informations confidentielles à caractère commercial.

§ 3. – Lorsque l'Autorité publique applique un système de redevance type pour la réutilisation des documents, le montant effectif et la base de calcul doivent être préalablement fixés et publiés, de préférence par voie électronique.

En l'absence de redevance type, les facteurs pris en compte dans le calcul desdites redevances sont d'emblée indiqués. Le demandeur peut, sur simple demande, être informé par l'Autorité publique concernée de la manière dont la redevance a été calculée dans le cadre d'une demande particulière de réutilisation.

Si les documents sont disponibles en ligne, la publication du système de redevance doit être assurée également par voie électronique.

§ 4. – La restriction visée au § 2 ne s'applique pas aux :

1° Autorités publiques qui sont tenues de générer des recettes destinées à couvrir une part substantielle

des coûts liés à l'accomplissement de leurs missions de service public;

2° bibliothèques, y compris aux bibliothèques universitaires, aux musées et aux archives;

3° entreprises publiques.

Le Gouvernement, le Collège réuni et le Collège publient une liste des Autorités publiques visées au paragraphe 4, 1°.

§ 5. – Dans les cas visés aux points 1e et 3e, le montant total des redevances est calculé selon des critères objectifs, transparents et vérifiables définis par arrêté du Gouvernement, du Collège réuni et du Collège.

Le total des recettes provenant de la fourniture et des autorisations de réutilisation des documents pendant la période à calculer ne dépasse pas le coût de la collecte, de la production, de la reproduction, de la diffusion, et du stockage des données, tout en permettant un retour sur investissement raisonnable, ainsi que, le cas échéant, d'anonymisation de données à caractère personnel et des mesures prises pour protéger des informations confidentielles à caractère commercial.

Dans les cas visés au point 2° du paragraphe 4, le total des recettes provenant de la fourniture et des autorisations de réutilisation pendant la période comptable appropriée ne dépasse pas le coût de collecte, de production, de reproduction, de diffusion, de stockage de données, de conservation et de l'acquisition des droits, ainsi que, le cas échéant, d'anonymisation de données à caractère personnel et des mesures prises pour protéger des informations confidentielles à caractère commercial, tout en permettant un retour sur investissement raisonnable.

§ 6. – Le calcul des redevances s'effectue conformément aux principes comptables applicables aux Autorités publiques concernées.

§ 7. – La réutilisation des éléments suivants est gratuite pour l'utilisateur :

1° sous réserve de l'article C.IV.29, les ensembles de données de forte valeur, dont la liste est établie conformément à l'alinéa 1er dudit article;

2° les données de la recherche visées à l'article C.IV.19, § 1er, 3°.

Article C.IV.25.

Licences

Les Autorités peuvent autoriser une réutilisation inconditionnelle de documents ou imposer des conditions, si nécessaire par le biais d'une licence.

Les conditions contenues dans la licence ne limitent pas indûment les possibilités de réutilisation et ne sont pas utilisées pour restreindre la concurrence. Les conditions fixées par les licences doivent être objectives, proportionnées, non discriminatoires et justifiées sur la base d'un objectif d'intérêt général.

Les différentes licences types seront fixées par le Gouvernement, le Collège réuni et le Collège, par arrêté conjoint ou non dans le cadre de leur compétences respectives. Les licences types peuvent être adaptées à des demandes de licence particulières.

Pour l'application du présent article, les Autorités publiques utilisent les licences prévues au Chapitre II de l'arrêté du Gouvernement de la Région de Bruxelles-Capitale du 1er février 2018 portant exécution de l'ordonnance du 27 octobre 2016 visant à l'établissement d'une politique de données ouvertes (open data) et portant transposition de la Directive 2013/37/UE du Parlement européen et du conseil du 26 juin 2013 modifiant la Directive 2003/98/CE du Parlement européen et du conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, jusqu'à ce que celui-ci soit abrogé.

Article C.IV.26.

Données de la recherche

Sans préjudice de l'article C.VI.19, § 2, 3°, les données de la recherche sont réutilisables à des fins commerciales ou non commerciales, conformément au présent titre, dans la mesure où elles sont financées au moyen de fonds publics et où des chercheurs, des organismes exerçant une activité de recherche ou des organisations finançant une activité de recherche les ont déjà rendues publiques par l'intermédiaire d'une archive ouverte institutionnelle ou thématique. À cette fin, il est tenu compte des intérêts commerciaux légitimes, des activités de transmission des connaissances et des droits de propriété intellectuelle préexistants.

SECTION 5
Non-discrimination et commerce équitable

Article C.IV.27.
Non-discrimination

§ 1er. – Toute condition applicable en matière de réutilisation des documents ne peut être discriminatoire pour des catégories comparables de réutilisation ou de demandeurs.

§ 2. – Lorsqu'une Autorité publique réutilise des documents dans le cadre de ses activités commerciales étrangères à sa mission de service public, les conditions tarifaires et autres applicables à la fourniture des documents destinés à ces activités sont les mêmes que pour les autres utilisateurs qui ne sont pas des Autorités publiques.

Article C.IV.28.
Accord d'exclusivité

§ 1er. – Les accords d'exclusivité de réutilisation sont interdits, à moins qu'ils ne s'avèrent nécessaires pour la prestation d'un service d'intérêt général.

Excepté pour ce qui concerne la numérisation des ressources culturelles, lorsqu'un droit d'exclusivité est accordé dans l'intérêt général, le bien-fondé de celui-ci fait l'objet, tous les trois ans au moins, d'un réexamen.

Les accords d'exclusivité en vigueur le 16 juillet 2019 ou après cette date sont rendus publics en ligne au moins deux mois avant leur prise d'effet. Ces accords sont transparents et rendus publics en ligne à l'initiative de l'autorité qui l'accorde.

§ 2. – La période d'exclusivité accordée pour la numérisation des ressources culturelles ne dépasse pas, en général, dix ans. Lorsque ladite durée est supérieure à dix ans, elle fait l'objet d'un réexamen au cours de la onzième année et ensuite, le cas échéant, tous les sept ans.

Les accords d'exclusivité visés au premier alinéa sont transparents et sont rendus publics en ligne deux mois avant leur prise d'effet.

Dans le cas d'un droit d'exclusivité visé au premier alinéa, une copie des ressources culturelles numérisées est adressée gratuitement à l'autorité publique dans le cadre des accords conclus. À l'expiration de la période d'exclusivité, ladite copie est mise à disposition à des fins de réutilisation.

Les dispositifs juridiques ou pratiques qui, sans accorder expressément de droit d'exclusivité, visent à restreindre la disponibilité de documents à des fins de réutilisation par des entités autres que l'opérateur privé partie au dispositif, ou qui peuvent raisonnablement être considérés comme susceptibles de la restreindre, sont rendus publics en ligne au moins deux mois avant leur entrée en vigueur. L'effet de tels dispositifs juridiques ou pratiques sur la disponibilité des données à des fins de réutilisation fait l'objet, tous les trois ans au moins, d'un réexamen.

§ 3. – Les accords d'exclusivité en vigueur le 17 juillet 2013, hormis ceux bénéficiant de l'exception visée au § 1er et 2, prennent fin à l'échéance du contrat ou, en tout état de cause, au plus tard le 18 juillet 2043.

Les accords d'exclusivité en vigueur le 16 juillet 2019 qui ne relèvent pas des exceptions prévues aux paragraphes 1er et 2 prennent fin à la date d'échéance du contrat ou, en tout état de cause, au plus tard le 17 juillet 2049.

SECTION 6
Ensembles de données de forte valeur

Article C.IV.29.
Catégories thématiques d'ensembles de données de forte valeur

Afin de mettre en place des conditions soutenant la réutilisation d'ensembles de données de forte valeur, une liste des catégories thématiques d'ensembles de données de forte valeur est incluse à l'annexe du Code.

Le Gouvernement, le Collège réuni, le Collège établit les modalités de publication et de réutilisation des ensembles de données de forte valeur relevant des catégories figurant à l'annexe du présent Code basées sur la liste d'ensemble de données de forte valeur dressée par la Commission Européenne conformément à l'article 14 de la Directive (UE) du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public.

SECTION 7
Recours auprès de la CADADo

Article C.IV.30.
Recours auprès de la CADADo

Toute personne physique ou morale directement affectée par une décision relative à une demande de réutilisation de données visées par le présent chapitre dispose d'un droit de recours devant la CADADo dans les conditions prévues au Livre A.II.

L'absence de réponse à une demande de réutilisation de données visées par le présent chapitre est assimilée à un refus de réutilisation dans le chef de l'Autorité publique.

CHAPITRE 2
La réutilisation des données protégées conformément au règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 (DGA)

Article C.IV.31.
Dispositions générales

§ 1er. – Sans préjudice de dispositions particulières, le présent titre exécute le Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724.

§ 2. – Les Autorités publiques permettent la réutilisation, à des fins commerciales ou non commerciales, des données protégées qu'elles détiennent et qui ont été produites aux seules fins de l'exercice de leurs missions de service public ou de leurs obligations d'intérêt général.

Article C.IV.32.
Recours après de la CADADo

Toute personne physique ou morale directement affectée par une décision relative à une demande de réutilisation de données protégées dispose d'un droit de recours devant la CADADo dans les conditions prévues au Livre B.II.

L'absence de réponse à une demande de réutilisation de données protégées est assimilée à un refus de réutilisation dans le chef de l'Autorités publique.

TITRE 4
Communication

Article C.IV.33.
Dispositions générales

§ 1er. – Sans préjudice de dispositions particulières, le présent titre exécute partiellement le Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724.

§ 2. – Par l'intermédiaire du Point de contact de la Plateforme bruxelloise de la donnée, le gestionnaire de la Plateforme bruxelloise de la donnée organise l'altruisme en matière de données pour l'ensemble des Autorités publiques par la Communication des données à caractère personnel ainsi que toutes autres données qui seraient volontairement mises à disposition à des fins d'intérêt général.

LIVRE C.V
La plateforme bruxelloise de la donnée

TITRE 1
Principes de la Plateforme bruxelloise de la donnée

Article C.V.1.
Création et objectif de la Plateforme bruxelloise de la donnée

§ 1er. – Il est créé une Plateforme bruxelloise de la donnée, institué au sein du CIRB.

La Plateforme bruxelloise de la donnée offre notamment des services destinés à permettre le partage administratif de données, la réutilisation de données ou la Communication de données décrites au livre C.IV.

§ 2. – Le CIRB est désigné en qualité de gestionnaire de la Plateforme bruxelloise de la donnée.

Article C.V.2.
Missions du gestionnaire de la Plateforme bruxelloise de donnée

Le gestionnaire de la Plateforme bruxelloise da la donnée est chargée des missions suivantes :

1° l'administration technique de la Plateforme, notamment en ce qui concerne l'infrastructure, la sécurité, la gestion ou la disponibilité des informations ou, le cas échéant, des données;

2° la promotion de l'utilisation et de l'usage efficace de la Plateforme, notamment en ce qui concerne la qualité et l'interopérabilité des données proposées;

3° l'établissement du cadre documentaire de base et d'accord d'adhésion permettant son utilisation, notamment en ce qui concerne les formalités ou les modalités d'adhésion à la Plateforme et d'utilisation de ses services, ou la mise à disposition des modèles de Protocoles d'accord;

4° le cas échéant, le contrôle des schémas d'identification électronique ou de la certification au sens du Règlement (UE) No 910/2014 (EIDAS);

5° Le cas échéant, la désignation d'un prestataire indépendant en qualité de tiers de confiance;

6° la documentation du fonctionnement de la Plateforme, notamment en ce qui concerne les processus mis en place, et les statistiques d'utilisation notamment au regard des données d'usage spécifiques de la Plateforme;

7° le conseil et l'assistance aux Autorités publiques utilisatrices ainsi que la coordination avec leurs représentants, notamment en ce qui concerne la formation à l'utilisation, la prise en charge de projets particuliers, ou tout autre domaine pertinent en relation avec l'utilisation de la Plateforme; la conception évolutive de l'architecture de la Plateforme conformément à la stratégie pluriannuelle de la donnée ainsi que les plans d'actions annuels, visés à l'article C.VI.15, § 2.

Le Gouvernement, le Collège réuni et le Collège peuvent définir conjointement les modalités d'organisation des missions visées ci-dessus.

TITRE 2
Les services de la Plateforme bruxelloise de la donnée

CHAPITRE 1
Dispositions générales

Article C.V.3.
Accord d'adhésion

§ 1er. – La mise à disposition des services de la Plateforme bruxelloise de la donnée fait l'objet d'un accord d'adhésion entre le gestionnaire de la Plateforme et l'utilisateur de la plateforme.

L'utilisateur de la Plateforme marque son accord de manière électronique, préalablement à l'utilisation de la Plateforme.

Le cas échéant, l'accord d'adhésion mentionne les conditions particulières qui s'appliquent en fonction du ou des services que l'utilisateur souhaite utiliser.

§ 2. – Le cas échéant, l'utilisateur concluant l'accord d'adhésion pour une entité dispose du mandat nécessaire pour ce faire.

Article C.V.4.
Qualification conformément au RGPD

Le gestionnaire de la Plateforme bruxelloise de la donnée agit en tant que responsable de traitements pour les traitements des données à caractère personnel nécessaires à la gestion technique de la Plateforme ainsi que pour l'ensemble des traitements du Centre d'intégration.

Le gestionnaire de la Plateforme bruxelloise de la donnée agit pour le compte des Autorités publiques en tant que sous-traitant pour les services du Catalogue, du Portail ouvert des données publiques et du Centre d'exploitation et d'analyse des données.

Le gestionnaire de la Plateforme gère ses bases de données conformément à la loi 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ainsi qu'au RGPD

En ce qui concerne les données à caractère personnel nécessaires à la gestion technique de la Plateforme ainsi que pour l'ensemble des traitements des données à caractère personnel réalisés par le Centre d'intégration, les données sont conservées 10 ans après la fin du traitement.

Sans préjudice d'autres dispositions légales notamment relatives à l'archivage historique, les données techniques nécessaires au fonctionnement des autres services de la Plateforme sont conservées 6 mois après la fin du traitement.

Les données sont détruites à l'échéance des délais précités sauf si celles-ci sont nécessaires dans le cadre d'un examen de suivi ou à des fins historiques, statistiques ou scientifiques dans le respect de la législation relative à la vie privée.

Pour ce faire, les données à caractère personnel sont rendues anonymes dès que leur individualisation n'est plus nécessaire pour la réalisation des finalités pour lesquelles elles ont été collectées.

Les données pourront être communiquées à toute institution désignée par le Gouvernement, le Collège réuni et le Collège en vue de leur traitement ultérieur à des fins historiques, statistiques et scientifiques.

Article C.V.5.
Traçabilité des accès aux données

Le gestionnaire de la Plateforme assure la traçabilité des accès aux services du Centre d'intégration pour chaque Autorité publique. Il appartient ensuite à celle-ci d'organiser la traçabilité des accès internes par ses services et ses agents.

La traçabilité des accès aux données du Catalogue et au Portail ouvert des données est assuré par le gestionnaire de la Plateforme.

La traçabilité des accès aux services proposés par le Centre d'exploitation et d'analyse des données est organisé au cas par cas par le gestionnaire de la Plateforme ou par l'Autorité publique utilisatrice.

Article C.V.6.
Financement

§ 1er. – Le CIRB, en sa qualité de gestionnaire de la Plateforme bruxelloise de la donnée, exerce ses missions dans les limites des redevances éventuellement perçues et du budget octroyé par le Gouvernement, le Collège réuni et le Collège, proportionnellement à l'activité de la Plateforme consacrée aux Autorités publiques relevant de leurs compétences respectives.

Le Gouvernement, le Collège réuni et le Collège établissent conjointement les modalités de calcul des redevances éventuelles pour l'utilisation des services de la Plateforme bruxelloise de la donnée et arrêtent conjointement leurs modalités de financement

Les redevances appliquées dans le cadre des réutilisations de données, notamment concernant les frais de diffusion des données, sont calculées conformément à l'article C.IV.24.

L calcul de la redevance est publié par le gestionnaire sur la Plateforme bruxelloise de la donnée.

CHAPITRE 2
Le Centre d'intégration

Article C.V.7.
Création et objectif

§ 1er. – Il est créé un Centre d'intégration au sein de la Plateforme bruxelloise de la donnée.

L'objectif du Centre d'intégration est d'assurer techniquement les partages administratifs.

§ 2. – À chaque partage administratif, le Gestionnaire de la Plateforme détermine le canal correspondant au type de données visées :

1° soit le canal correspondant aux partages administratifs visant des données issues de sources authentiques ou des données à caractère personnel;

2° soit le canal correspondant aux partages administratifs visant tous les autres types de données.

Le Gouvernement, le Collège réuni et le Collège peuvent déterminer conjointement les modalités techniques et opérationnelles des canaux du Centre d'intégration visés à l'alinéa 1er.

Article C.V.8.
La fonction d'intégrateur de services bruxellois

Le CIRB est désigné en qualité d'intégrateur de services bruxellois dans le cadre de sa gestion du Centre d'intégration.

L'intégrateur de services à pour missions :

1° recevoir et donner, s'il y a lieu, suite aux demandes de consultation et de demande de partage des données enregistrées dans une ou plusieurs base(s) de données;

2° promouvoir et veiller à l'homogénéité des droits d'accès aux bases de données;

3° élaborer les modalités techniques visant à développer les canaux d'accès de la manière la plus efficace et là plus sûre possible;

4° promouvoir une politique de sécurité coordonnée pour le réseau;

5° procéder au partage administratif de données intégrées à la demande de l'Autorité publique destinataire.

6° développer pour les services publics participants des applications utiles à l'échange et/ou l'intégration de données conservées dans les banques de données;

7° organiser la collaboration avec d'autres intégrateurs de services.

CHAPITRE 3
Le Catalogue des données

Article C.V.9.
Création et objectifs

§ 1er. – Il est créé un Catalogue des données au sein de la Plateforme bruxelloise de la donnée.

Le Catalogue des données est un service composé :

1° d'un outil de gestion des métadonnées et des données de référence générées par les Autorités publiques, qui permet de dresser un inventaire des données détenues par les Autorités publiques, afin d'organiser une partie du Catalogue des données mise à la disposition des Autorités publiques par le gestionnaire de la Plateforme, et;

2° d'un outil de publication de la liste des données publiques et de leur catégorisation au regard de

la typologie présentée au chapitre 3, du titre 2 du livre C.III, afin d'organiser une partie publique au Catalogue des données.

§ 2. – L'objectif du Catalogue des données est :

1° d'en réaliser un inventaire de l'ensemble des données détenues par les Autorités publiques permettant notamment d'identifier :

a) les données;

b) l'Autorité publique qui les détient;

c) leur catégorisation au regard de la typologie présentée au chapitre 3 du titre 2 du livre C.III;

d) les déclarations de principe visées à l'article C.III.12;

e) le cas échéant, les protocoles d'accord relatifs à des partages administratifs;

2° de fournir un glossaire;

3° de publier tout ou une partie de l'inventaire des données détenues par chaque Autorité Publique via l'outil de publication visé au paragraphe 1er, alinéa 2;

§ 3. – Les Autorités publiques utilisent l'outil de gestion du Catalogue des données afin de dresser l'inventaire des données qu'elles détiennent sous forme de métadonnées et de données de références qui peuvent être utilisées par le gestionnaire de la Plateforme en vue de leur intégration dans le Catalogue des données et sa partie publique.

CHAPITRE 4
Le Portail ouvert des données publiques

Article C.V.10.
Création et objectifs

§ 1er. – Il est créé un Portail ouvert des données publiques au sein de la Plateforme bruxelloise de la donnée.

Le Portail ouvert des données publiques propose les données disponibles à la réutilisation, notamment le cadastre des subsides, des marchés publics et des études visés à l'article B.I.4.

§ 2. – Les licences ouvertes ou les licences type relatives aux données réutilisables proposées par le Portail ouvert des données publiques sont disponibles dans le Portail ouvert des données publiques.

§ 3. – Pour chaque jeu de données ayant fait l'objet d'une réutilisation, le Portail ouvert des données publiques indique le nombre et l'identité des ré-utilisateurs.

CHAPITRE 5
Le Centre d'exploitation et d'analyse des données

Article C.V.11.
Création et objectifs

Il est créé un Centre d'exploitation et d'analyse des données.

L'objectif du Centre d'exploitation et d'analyse des données est de proposer, notamment aux Autorités publiques, des services facultatifs visant la collecte, le stockage, le traitement et la consommation de données.

CHAPITRE 6
Point de Contact et d'information

Article C.V.12.
Point de contact et d'information visé à l'article 8 du DGA

Conformément à l'article 8 du DGA, il est créé un Point de contact et d'information au sein de la Plateforme bruxelloise de la donnée.

L'objectif du Point de contact est de fournir des informations complètes et précises sur les données disponibles, les modalités de réutilisation et de fourniture de données ainsi que faciliter la Communication de données par des entités privées relevant notamment de l'altruisme de données

CHAPITRE 7
Service d'appui

Article C.V.13.
Service d'appui visé à l'article 7 du DGA

Les services d'appui et d'assistance visés à l'article 7 du DGA sont intégrés à la Plateforme bruxelloise de la donnée, à savoir :

1° fournir une assistance technique en mettant à disposition un environnement de traitement sécurisé pour donner accès à la réutilisation de données via la Plateforme bruxelloise de la donnée;

2° fournir des orientations et une assistance technique sur la meilleure manière de structurer et de

stocker les données pour les rendre facilement accessibles;

3° aider les Autorités publiques, le cas échéant, à fournir une assistance aux ré-utilisateurs pour demander le consentement des personnes concernées à la réutilisation ou l'autorisation des détenteurs de données conformément à leurs décisions spécifiques, y compris en ce qui concerne le territoire où le traitement des données est prévu et à aider les Autorités publiques à mettre en place des mécanismes techniques permettant la transmission des demandes de consentement ou d'autorisation des ré-utilisateurs, lorsque cela est réalisable en pratique;

4° fournir aux Autorités publiques une assistance lorsqu'il s'agit d'évaluer l'adéquation des engagements contractuels pris par un ré-utilisateur en vertu de l'article 5, paragraphe 10 du Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données.

LIVRE C.VI
Les structures administratives de la gouvernance

TITRE 1
La gouvernance numérique

CHAPITRE 1
Champ d'application

Article C.VI.1.
Les Autorités publiques visées par le titre 1

Le présent titre s'applique aux Autorités publiques visées à l'article A.I.1, 1), a), b), et H) et les associations formées par l'une ou plusieurs des Autorités visées au a), b) et H).

CHAPITRE 2
Objectifs

Article C.VI.2.
La gouvernance numérique

§ 1er. – La gouvernance numérique a pour objectif d'optimiser la cohérence et la mutualisation de l'écosystème numérique bruxellois.

Dans ce cadre, la gouvernance numérique :

1° vérifie la conformité des projets et des achats ayant un impact sur l'écosystème numérique bruxellois par rapport à l'architecture numérique commune à la Région, la COCOM et la COCOF, ainsi que la potentielle mutualisation de ces projets et achats;

2° identifie les projets stratégiques qui comportent des composantes numériques ayant un impact sur l'écosystème numérique bruxellois à des fins de cohérence et de mutualisation pour la Région, la COCOM et la COCOF.

§ 2. – Les organes de gouvernance de l'écosystème numérique bruxelloise sont :

1° le Comité de coordination numérique;

2° le Comité de validation de l'architecture numérique.

Deux organes assurent un rôle support à la gouvernance numérique :

1° le Secrétariat numérique;

2° le Bureau des achats numériques.

CHAPITRE 3
Test d'autoévaluation numérique

Article C.VI.3.
Test d'autoévaluation numérique

§ 1er. – Afin de déceler et de faciliter les projets des Autorités publiques visées à l'article C.VI.1 qui comprennent une composante numérique ayant un impact sur l'écosystème numérique bruxellois et de recueillir l'avis des organes participant à la gouvernance numérique organisés dans le cadre du présent titre, un test est réalisé par lesdites Autorités publiques sous la forme d'un formulaire d'autoévaluation numérique.

Ce test est dénommé « test d'autoévaluation numérique ».

§ 2. – Sont soumis au test d'autoévaluation numérique, les projets des Autorités publiques visées à l'article C.VI.1 :

1° visant l'adoption de décisions relatives à l'écosystème numérique bruxellois soit par le Gouvernement, le Collège réuni et le Collège, en ce compris les avant-projets d'ordonnance, de décret ou d'arrêté, soit par l'organe de gestion des Autorités publiques visées à l'article C.VI.1;

2° ou visant une procédure de commande publique relative à l'écosystème numérique bruxellois et dont le montant estimé global est au minimum visé à l'article 5, 10°, 1), 7e tiret de l'arrêté du 18 juillet 2000 de la Région de Bruxelles-Capitale por-

tant règlement de son fonctionnement et réglant la signature des actes du Gouvernement.

Le contenu du test d'autoévaluation numérique ainsi que la procédure associée à ce test sont fixés conjointement par le Gouvernement de la Région de Bruxelles Capitale, le Collège réuni et le Collège.

Les résultats des tests sont ensuite transmis au Secrétariat numérique pour examen.

CHAPITRE 4
Les organes de la gouvernance numérique

SECTION 1
Le Secrétariat numérique

Article C.VI.4.
Création et missions du Secrétariat numérique

§ 1er. – Le Secrétariat numérique, créé au sein du CIRB, assure le secrétariat du Comité de coordination numérique et du Comité de validation de l'architecture numérique.

Il assure l'interface entre ces deux comités, d'une part, et les Autorités publiques visées à l'article C. VI.1, d'autre part.

§ 2. – Le Secrétariat numérique reçoit les tests d'autoévaluation visés à l'article C.VI.3 et en examine les résultats.

En fonction de l'examen qu'il aura réalisé des résultats du test d'autoévaluation, le Secrétariat numérique sollicite l'avis de l'un ou de plusieurs des organes consultatifs suivants :

1° le Bureau d'achat numérique;

2° le Comité de validation de l'architecture numérique;

3° le Bureau de la donnée.

À la demande d'avis du Secrétariat numérique, est joint le test d'autoévaluation complété et le projet ou achat visé à l'article C.VI.3, § 2, qui y a été soumis, de même que, le cas échéant, une brève analyse des résultats de ce test réalisé par le Secrétariat numérique pour justifier sa demande d'avis à l'un ou plusieurs des organes visés à l'alinéa 2.

Le Secrétariat numérique rassemble ensuite les avis de chaque organe visé à l'alinéa 2 consulté et les transmet d'office au Comité de coordination numérique, accompagnés des résultats du test d'autoévaluation et du projet visé à l'article C.VI.3, § 2, qui y a été soumis.

Article C.VI.5.
Financement et contrôle

§ 1er. – Le Secrétariat numérique effectue ses missions au service des Autorités publiques visées à l'article C.VI.1.

§ 2. – Le Secrétariat numérique transmet tous les deux ans un rapport d'activités au Ministre compétent à l'égard du CIRB et aux Ministres compétents en matière de gouvernance numérique du Collège réuni et du Collège.

Ce rapport d'activités est également adressé au Comité de coordination numérique.

SECTION 2
Le Comité de validation de l'architecture numérique

Article C.VI.6.
Compétence et composition du Comité de validation de l'architecture numérique

§ 1er. – Le Comité de validation de l'architecture numérique est responsable de la gouvernance de l'architecture numérique régionale à des fins de cohérence et de mutualisation.

§ 2. – Afin de réaliser sa mission visée au paragraphe 1er, le Comité de validation de l'architecture numérique :

1° remet des avis sur les projets visé à l'article C.VI.3, § 2, soumis au test d'autoévaluation numérique qui lui ont été transmis par le Secrétariat numérique conformément à l'article C.VI.4, § 2, alinéa 2;

2° remet des avis sur les demandes adressées par le Bureau d'achats numériques conformément à l'article C.VI.9, § 4;

3° remet, d'initiative ou à la demande, des avis au Comité de coordination numérique, au Bureau d'achats numériques et au Bureau de la donnée.

§ 3. – Le Comité de validation de l'architecture numérique est composé par :

des membres permanents que sont les dix institutions régionales ayant le budget IT le plus important de la Région Bruxelloise et de la COCOF;

1° des membres non permanents qui représentent les autres Autorités publiques visées à l'article C.VI.1, en dehors des 10 membres permanents.

Les membres permanents ou non permanents sont représentés, au sein du Comité de validation

de l'architecture numérique, par des représentants désignés par chaque membre en fonction du point à l'ordre du jour de la réunion. Les membres désignent les personnes présentant la plus grande compétence technique en la matière.

Les membres permanents sont obligatoirement présents à chaque réunion du Comité de validation de l'architecture numérique.

Les membres non permanents sont invités aux réunions. Ils informent préalablement le Secrétariat numérique de leur participation.

Les membres du Comité de validation de l'architecture numérique peuvent inviter toute personne physique, personne morale de droit public ou de droit privé, dont la présence est jugée pertinente en fonction de l'ordre du jour des réunions.

Le Comité de validation de l'architecture numérique adopte son règlement d'ordre intérieur afin de définir son fonctionnement.

Article C.VI.7.
Rapport d'activités

Le Comité de validation de l'architecture numérique transmet tous les deux ans un rapport d'activités au Gouvernement, au Collège réuni et au Collège.

Ce rapport d'activités est également adressé au Comité de coordination numérique.

SECTION 3
Le Bureau d'achats numériques

Article C.VI.8.
Le Bureau d'achats numériques

Le Bureau d'achats numériques, créé au sein du CIRB, fournit tout appui opérationnel, légal ou technique, aux Autorités publiques visées à l'article C.I.1, concernant les processus de commande publique numérique mutualisable.

Article C.VI.9.
Les missions du Bureau d'achats numériques

§ 1er. – Le Bureau d'achats numériques a pour mission générale :

1° de fournir une assistance nécessaire à toute Autorité publique dans le cadre de tout processus de commande publique numérique mutualisable susceptible d'affecter l'écosystème numérique bruxellois;

2° de proposer au Gouvernement, au Collège Réuni et au Collège qui les arrêtent conjointement, les critères de mutualisation pertinents en matière de commande publique numérique dans le cadre de l'écosystème numérique bruxellois ainsi que les modalités applicables aux commandes publiques numériques jugées mutualisables;

3° d'analyser les déclarations de besoins numériques pluriannuels visés au paragraphe 2 et les formulaires de besoins numériques visés au paragraphe 3 au regard des critères de mutualisation arrêtés conjointement par le Gouvernement, le Collège réuni et le Collège et en déterminer leur caractère mutualisable conformément à ces critères;

4° de recommander aux Autorités publiques les modalités applicables aux commandes publiques numériques mutualisables conformément à l'arrêté conjoint visés au point 2°;

5° De remettre des avis sur les projet soumis au test d'autoévaluation numérique qui lui ont été transmis par le Secrétariat numérique conformément à l'article C.VI.4, § 2, alinéa 2;

6° de remettre, d'initiative ou à la demande, des avis au Comité de validation de l'architecture numérique, au Comité de coordination numérique et au Bureau de la donnée.

§ 2. – Les Autorités publiques visées à l'article C.VI.1 transmettent au Bureau d'achats numériques leurs déclarations de besoins numériques pluriannuelles.

Les Autorités publiques visées à l'article C.I.1, autres que les Autorités publiques visées à l'article C.VI.1, peuvent transmettre d'initiative au Bureau d'achats numériques leurs déclarations de besoins numériques pluriannuelles.

La déclaration de besoins numériques pluriannuelles soumise par une Autorité publique, visée à l'alinéa 1er et 2, au Bureau d'achats numériques peut être mise à jour à tout moment, et doit être mise à jour au minimum une fois par an.

§ 3. – Lorsqu'un projet de commande publique numérique n'est pas repris dans la déclaration de besoins numériques pluriannuelles, les Autorités publiques visées à l'article C.VI.1 doivent transmettre au Bureau d'achats numériques dès que possible, ce projet de commande publique au travers d'un formulaire de besoins numériques, à déterminer par le

Bureau d'achats numériques, décrivant de manière circonstanciée le besoin numérique auquel elle est confrontée en dehors de sa déclaration de besoins numériques pluriannuelle.

Lorsqu'un projet de commande publique numérique n'est pas repris dans la déclaration de besoins numériques pluriannuelles, les Autorités publiques visées à l'article C.I.1, autres que celles visées à l'article B.VI.1, peuvent transmettre, à tout moment, d'initiative, un ou plusieurs besoins numériques au travers d'un formulaire de besoins numériques, décrivant de manière circonstanciée le besoin numérique auquel elle est confrontée en dehors de sa déclaration de besoins numériques pluriannuelle.

§ 4. – Dans le cadre de son analyse des déclarations de besoins numériques pluriannuelles et des formulaires de besoins numériques conformément au paragraphe 1er, 3e tiret, le Bureau d'achats peut demander l'avis :

1° du Comité de validation de l'architecture numérique;

2° du Bureau de la donnée;

3° du Comité de coordination.

§ 5. – Dans l'hypothèse où le Bureau d'achats numériques confirme auprès des Autorités publiques concernées le caractère mutualisable de leur projet, il peut recommander l'application d'un test d'autoévaluation numérique conformément à l'article C.VI.3 si les critères visés à l'article C.VI.3, § 2, sont rencontrés.

Article C.VI.10.
Financement et contrôle

§ 1er. – La Région bruxelloise, la COCOM et la COCOF participent au financement du Bureau des achats numériques proportionnellement à l'importance de l'activité du Bureau en faveur des Autorités publiques visées à l'article C.I.1 ou à l'article C.VI.1 relevant de leurs compétences respectives.

Le Gouvernement, le Collège réuni et le Collège arrêtent conjointement les modalités relatives au financement du Bureau d'achats numériques à charge de la Région, de la COCOM et de la COCOF et, le cas échéant, des Autorités publiques visées à l'article C.I.1 ou à l'article C.VI.1 qui en dépendent.

§ 2. – Le Bureau d'achats numériques transmet annuellement un rapport d'activités au Ministre compétent à l'égard du CIRB et aux Ministres compétents en matière numérique du Collège réuni et du Collège.

Ce rapport d'activités est également adressé au Comité de coordination.

SECTION 4
Le Comité de coordination numérique

Article C.VI.11.
Compétences et composition
du Comité de coordination numérique

§ 1er. – Le Comité de coordination numérique se prononce stratégiquement sur tous les projets visés à l'article C.VI.3, § 2, soumis au test d'autoévaluation numérique visés qui ont été préalablement analysés par le Bureau d'achats numériques, le Comité de validation de l'architecture numérique, et le Bureau de la donnée, ou seulement par certains de ces organes consultatifs.

Le Comité de coordination numérique remet, selon le cas, au Gouvernement, au Collège réuni, au Collège, ou aux organes de gestions compétents, des avis relatifs aux projets pour lesquels il a été saisi ainsi que les procès-verbaux de ses réunions.

Il peut remettre, d'initiative ou à la demande, des avis aux autres organes de gouvernance numérique, au Gouvernement, au Collège réuni, au Collège, et aux organes de gestion des Autorités publiques visées à l'article C.VI.1.

§ 2. – Le Comité de coordination numérique est composé par :

1° des membres permanents qui sont représentés, parmi les Autorités Publiques visées à l'article C. VI.1, les dix pouvoirs publics de la Région, de la COCOM et de la COCOF disposant des plus grands budgets en matière d'achats numériques tels qu'établis par la procédure organisée à l'article 2 de l'arrêté fixant les seuils numériques.

2° des membres non permanents qui représentent les autres Autorités publiques visées à l'article C.VI.1, en dehors des 10 membres permanents.

Les membres permanents sont obligatoirement présents à chaque réunion.

Les membres non permanents sont invités aux réunions et informent préalablement le Secrétariat numérique de leur participation.

Les membres permanents et non permanents du Comité de coordination numérique sont représentés par la personne compétente pour d'engager stratégiquement en matière numérique l'Autorité publique concernée.

Les membres du Comité de coordination numérique peuvent inviter toute personne physique, personne morale de droit public ou de droit privé, dont la présence est jugée pertinente en fonction de l'ordre du jour des réunions.

Le Comité de coordination numérique adopte son règlement d'ordre intérieur.

Article C.VI.12.
Rapport d'activités

Le Comité de la coordination numérique transmet tous les deux ans un rapport d'activités au Gouvernement, au Collège réuni et au Collège.

TITRE 2
La gouvernance de la donnée

CHAPITRE 1
Objectifs

Article C.VI.13.
Objectifs

La gouvernance de la donnée se centre sur la mise en œuvre quotidienne, pratique et opérationnelle du Code.

CHAPITRE 2
Les organes de la gouvernance de la donnée

SECTION 1
Le Comité de gouvernance de la donnée

Article C.VI.14.
Composition du Comité de gouvernance de la donnée

§ 1er. – Le Comité de gouvernance de la donnée est le lieu de concertation entre les Autorités publiques visées à l'article C.I.1 quant à l'implémentation du Code.

§ 2. – Le Comité de gouvernance de la donnée est composé :

1° du coordinateur de la donnée du Bureau de la donnée visé à l'article C.VI.19, § 1er;

2° des Administrateurs locaux de la donnée au sein des Autorités publiques visées à l'article C.I.1 enregistrées auprès du Bureau de la donnée conformément à l'arrêté fixant les seuils numériques et reprises dans les paliers 1 et 2 visés par le même arrêté;

3° d'un ou plusieurs représentant(s) du service compétent pour la simplification administrative;

4° des représentants du gestionnaire de la Plateforme bruxelloise de la donnée.

Les membres du Comité de gouvernance de la donnée peuvent inviter toute personne physique, personne morale de droit public ou de droit privé, dont la présence est jugée pertinente en fonction de l'ordre du jour des réunions.

Afin d'organiser la discussion sur des thématiques précises, le Comité de gouvernance de la donnée peut instituer en son sein des groupes de travail ne comprenant que certains de ses membres et le cas échéant des invités *ad hoc*.

Article C.VI.15.
Missions

§ 1er. – Le Comité de gouvernance de la donnée a pour objectifs :

1° de fixer les objectifs opérationnels du Bureau de la donnée;

2° de communiquer au Bureau de la donnée les besoins et les priorités des Autorités publiques visées à l'article C.I.1;

3° de susciter le partage d'expérience et la présentation des projets réalisés au sein des Autorités publiques visées à l'article C.I.1;

4° de revoir et valider les standards, bonnes pratiques et modèles soumis pour proposition par le Bureau de la Donnée, notamment en matière d'interopérabilité;

5° de s'assurer de l'opérationnalité des dispositions du Code en se concertant sur l'ensemble des points nécessitant des responsabilités claires, notamment la désignation de commun accord de l'identité de la ou des Autorités publiques investies de la responsabilité de la gestion d'un domaine spécifique de données.

§ 2. – Le Comité de gouvernance de la donnée élabore la stratégie pluriannuelle de la donnée ainsi que les plans d'action annuels en concertation avec le Bureau de la donnée.

La stratégie pluriannuelle de la donnée ainsi que les plans d'actions annuels sont approuvés conjointement par le Gouvernement, le Collège réuni et le Collège.

§ 3. – Par arrêté conjoint, le Gouvernement, le Collège réuni et le Collège peuvent attribuer d'autres missions complémentaires aux missions visées au paragraphe 1er. Le Gouvernement de la Région bruxelloise, le Collège réuni et le Collège définissent conjointement les conditions selon lesquelles le Comité de gouvernance de la donnée exerce ces missions complémentaires.

Article C.VI.16.
Fonctionnement

§ 1er. – Le Comité de gouvernance de la donnée se réunit au moins huit fois par an et à chaque demande conjointe d'au minimum cinq membres de cinq Autorités publiques différentes.

§ 2. – Le Comité de gouvernance de la donnée adopte un règlement d'ordre intérieur.

SECTION 2
Le Bureau de la donnée

Article C.VI.17.
Création du Bureau de la donnée

Il est créé un Bureau de la donnée au sein du CIRB.

Le Bureau de la donnée coordonne et supervise la mise en œuvre transversale et opérationnelle de la gouvernance de la donnée décrite par le Code au sein des Autorités publiques et entre elles.

Article C.VI.18.
Missions du Bureau de la donnée

Le Bureau de la donnée est investi des missions suivantes exercées en concertation avec le Comité de Gouvernance de la donnée :

1° une mission d'appui administratif, de secrétariat et d'animation du Comité de gouvernance de la Donnée conformément aux objectifs opérationnels fixé par le Comité de gouvernance de la donnée en vertu de l'article C.VI.15, § 1er, 1°;

2° une mission d'intégration de la gouvernance de la donnée au sein de la gouvernance numérique par la rédaction d'avis :

a) d'initiative ou à la demande du Bureau d'achats numériques, du Comité de validation de l'architecture numérique ou, du Comité de gouvernance de la donnée ou du Comité de coordination numérique;

b) sur les projet soumis au test d'autoévaluation numérique qui lui ont été transmis par le Secrétariat numérique conformément à l'article C. VI.4, § 2, alinéa 2;

3° une mission de coordinateur de la donnée, avant validation par le Comité de gouvernance de la donnée, notamment au travers de :

a) la proposition de modèles standard de documents en matière de déclaration de principes visée à l'article C.III.12, de protocole d'accord visé à l'article C.IV.8;

b) La proposition de licences de licences types au Gouvernement, Collège réuni et Collège conformément à l'article C.IV.25;

c) l'organisation d'un cadre pour la gestion de l'interopérabilité au sens de l'article C.II.17;

4° une mission d'accompagnement à la mise en œuvre des obligations du Code en matière de gestion de la donnée notamment au travers de :

a) la contribution à la compréhension par tous les acteurs et opérateurs de la Plateforme bruxelloise de la donnée des enjeux de la sécurité et de la protection des données au sens du chapitre 2 du titre 4 du livre C.III;

b) la proposition de directives, de standards, de cadres et de lignes directrices à faire approuver par le Comité de gouvernance de la donnée;

c) la promotion d'instruments de politiques internes aux Autorités publiques concernant la gestion des données au sens du chapitre 1 du titre 4 du livre C.III, en ce compris la gestion des modèles analytiques, des algorithmes et des systèmes exploitant l'intelligence artificielle au sens de l'article C.III.18;

5° une mission d'initiateur du changement au travers de :

a) la mise en place de communautés de pratiques;

b) l'organisation de formations visant à améliorer les compétences régionales en matière de gestion des données;

c) l'organisation d'événements visant à augmenter la culture des données au sein de la Région bruxelloise, de la COCOM et de la COCOF;

6° une mission de support aux Autorités publiques au travers de la mise à disposition d'experts en gouvernance de la donnée lorsque les Autorités

publiques ne disposent pas des ressources suffisantes;

7° une mission de veille et d'explication pour l'ensemble des Autorités publiques, notamment en ce qui concerne le suivi de la réglementation et des initiatives, projets et financements européens, et leur transposition ou leur implémentation éventuelle au niveau national ou bruxellois.

Article C.VI.19.
Fonctionnement, contrôle et financement

§ 1er. – Le Bureau de la donnée est placé sous la responsabilité d'un coordinateur de la donnée.

§ 2. – Le Bureau de la donnée effectue ses missions au service des Autorités publiques de la Région bruxelloise, de la COCOM et de la COCOF.

Le Ministre compétent à l'égard du CIRB et les Ministres compétents en matière numérique du Collège réuni et du Collège définissent conjointement les objectifs stratégiques du Bureau de la donnée et en vérifient annuellement l'application.

§ 3. – La Région bruxelloise, la COCOM et la COCOF participent au financement du Bureau de la donnée proportionnellement à l'importance de l'activité du Bureau en rapport avec les Autorités publiques relevant de leurs compétences respectives.

Le Gouvernement, le Collège réuni et le Collège arrêtent conjointement les modalités relatives au financement du Bureau de la donnée à charge de la Région, de la COCOM et de la COCOF ou des Autorités publiques qui en dépendent.

Le Bureau de la donnée communique au moins deux fois par an l'état d'avancement de ses travaux au Comité de coordination numérique.

§ 4. – Le Bureau de la donnée transmet et présente annuellement un rapport d'activités au Ministre compétent à l'égard du CIRB et aux Ministres compétents en matière numérique du Collège réuni et du Collège.

TITRE 3
Les ressources de la gouvernance de la donnée au sein des Autorités publiques

Article C.VI.20.
Création des fonctions de gouvernance de la donnée

Chaque Autorité publique désigne :

1° un administrateur local de la donnée visé à l'article C.VI.21;

2° un ou plusieurs responsables de la donnée visés à l'article C.VI.22;

3° un conseiller de sécurité de l'information visé à l'article C.VI.23.

Un groupe d'Autorités publiques peut désigner conjointement les personnes assurant les fonctions visées au premier alinéa pour autant que cela ne compromette par le respect du Code et l'implémentation du Plan stratégique visé à l'article C.VI.15, § 2, et que cela soit cohérent par rapport à la structure organisationnelle et à la taille des Autorités publiques concernées.

Les personnes en charge des fonctions visées au premier alinéa peuvent être un membre du personnel de l'Autorité publique ou un sous-traitant, ou exercer ses missions sur la base d'un contrat de service.

Pour les Autorités publiques faisant partie du palier 3 défini par l'arrêté fixant les seuils numériques, la fonction d'administrateur local de la donnée et la fonction de conseiller de sécurité de l'information peuvent être cumulées par la même personne.

Article C.VI.21.
L'administrateur local de la donnée

§ 1er. – L'Administrateur local de la donnée est le pivot et principal organisateur de la gouvernance des données au sein de l'Autorité publique qui l'a désigné.

Il identifie les besoins et définit la stratégie interne de l'Autorité publique, en adéquation avec la stratégie pluriannuelle de la donnée et les plans d'actions annuels visés à l'article C.VI.15, § 2, et veille à son implémentation.

Il définit et veille à l'implémentation du modèle opérationnel interne à l'Autorité publique définissant la gouvernance interne ainsi que les rôles et responsabilités des différents acteurs de la donnée tel que décrit dans la déclaration de principes visées à l'article C.III.12

§ 2. – L'administrateur local de la donnée est investi des missions suivantes :

1) une mission à l'égard de l'Autorité publique qui l'a désigné, sous réserve, le cas échéant, d'une vali-

dation par l'organe légalement compétent en la matière, au regard de :

a) l'identification des besoins et la définition d'une stratégie interne à l'Autorités publique, en adéquation avec la stratégie pluriannuelle de la donnée ainsi que les plans d'action annuels visés à l'article C.VI.15;

b) la détermination des domaines de données gérés par l'Autorité publique;

c) la mise en œuvre des objectifs stratégiques rappelés aux articles C.II.6 et suivants;

d) la mise en œuvre des obligations relatives à la gestion de la donnée visées aux articles C.III.16 et suivants, en ce compris en organisant la répartition des responsabilités entre les parties et en collaborant avec le responsable de la donnée et le Conseiller en sécurité de l'information;

e) la proposition de toute mesure technique ou organisationnelle pertinente concernant l'infrastructure ou l'architecture des données;

f) la documentation de l'ensemble des processus et règles opérationnelles, protocoles d'accord, déclaration de principes propres à l'Autorité publique qui l'a désigné afin d'alimenter le Catalogue des données, le cas échéant en collaboration avec le responsable de la donnée de chacun des domaines de données concernés;

2) une mission à l'égard des tiers à l'Autorité publique qui l'a désigné, en matière d'organisation d'un point de contact unique en matière de gouvernance de la donnée;

3) une mission à l'égard du Bureau de la donnée, au regard de :

a) la fourniture de toute information pertinente, d'initiative ou sur demande, quant à l'exercice de ses missions;

b) la collecte de l'information mise à disposition par le Bureau concernant les processus, les normes et les meilleures pratiques que l'administrateur local de la donnée se chargera de transmettre au responsable de la donnée;

4) une mission à l'égard des autres Autorités publiques visées par le présent Code, le cas échéant au travers du Comité de Gouvernance de la donnée quant à :

a) l'assurance d'une harmonisation horizontale des domaines de données qui concernent plusieurs Autorités publiques;

b) la communication, si nécessaires, de la documentation établie par lui;

c) la collaboration et le dialogue entre les administrateurs locaux de la donnée;

§ 3. – L'Autorité publique peut confier à l'administrateur local de la donnée toute autre mission complémentaire aux missions énoncées au premier paragraphe.

Article C.VI.22.
Le responsable de la donnée

§ 1er. – Le responsable de la donnée est chargé d'un ou plusieurs domaines de données.

Le responsable de la donnée travaille sous la supervision de l'administrateur local de la donnée et en collaboration avec le Délégué à la protection des données et le Conseiller en sécurité de l'information.

§ 2. – Le responsable de la donnée est investi des missions suivantes concernant le ou les domaines de données desquels il est chargé :

1° une mission d'implémentation, notamment au regard de la stratégie interne définie par l'Administrateur local de la donnée et validée par l'organe légalement compétent, ou de toute autre mesure technique ou organisationnelle pertinente;

2° une mission d'évaluation continue des mesures mises en place au regard des politiques, normes et meilleures pratiques dans chacun du ou des domaines de données, en vue de leur amélioration;

3° une mission de contrôle du respect des mesures mises en place dans chacun du ou des domaines de données, par toute personne;

4° une mission de promotion et de diffusion des politiques, normes et meilleures pratiques mises en place par l'Autorité publique qui l'a désigné;

5° une mission de maintenance et de supervision des ressources nécessaires à la gestion des données relevant du ou des domaines de données concernés;

6° une mission de documentation, notamment à l'égard de toute mesure opérationnelle mise en place.

Article C.VI.23.
Le conseiller en sécurité de l'information

§ 1er. – Chaque Autorité publique désigne un conseiller en sécurité de l'information.

Le conseiller en sécurité de l'information travaille en collaboration avec l'administrateur local de la donnée, le Délégué à la protection des données et le responsable de la donnée.

§ 2. – Le conseiller en sécurité est investi de missions qui concernent notamment les obligations relatives à la sécurité et à la protection des données telles que définies au chapitre 2 du titre 4 du livre C.III.

1. une mission d'analyse de risque et d'implémentation de toute mesure opérationnelle pertinente, toute norme ou toute obligation en matière de sécurité;

2. une mission de vérification de la mise en œuvre effective de toute mesure opérationnelle pertinente, toute norme ou toute obligation en matière de sécurité;

3. une mission d'alerte concernant tout risque pour la sécurité et leur incidence sur la confidentialité, l'intégrité et la disponibilité des ressources d'information;

4. une mission d'avis, d'initiative ou sur demande, concernant toute question relative à la sécurité des données;

5. une mission de collaboration avec les conseillers en sécurité d'autres Autorités publiques, le cas échéant au travers du Comité de gouvernance de la donnée;

6. une mission de sensibilisation, au sein de son Autorité publique et à l'égard de tout tiers, concernant la sécurité et la protection des données.

TITRE 4
Réseau public bruxellois de fibre optique

Article C.VI.24.
La gestion des réseaux de fibre optique publics

§ 1er. – Le CIRB est chargé de la mise en place du réseau bruxellois de fibre optique mutualisant les réseaux de fibre optique dont disposent certaines Autorités publiques sur le territoire régional bruxellois. Dans ce cadre, le CIRB désigne une entité chargée des missions décrites au § 2.

§ 2. – L'entité chargée du déploiement de la fibre optique est investie des missions suivantes :

a) la mise en place d'un cadastre des réseaux existants de fibre optique et des infrastructures passives au sens de l'article 2, 87°, de la loi du 13 juin 2005 relative aux communications électroniques;

b) l'intégration des réseaux publics de fibre optique existants, en imposant une interopérabilité aux Autorités publiques concernées;

c) le déploiement harmonisé, centralisé et coordonné de toutes nouvelles capacités du réseau de fibre optique;

d) la facilitation de l'accès aux infrastructures passives des Autorités publiques concernées par toute autre Autorité publique, entité ou personne privée qui en ferait la demande;

e) la valorisation et l'exploitation des capacités non utilisées du réseau de fibre optique à des fins commerciales, notamment auprès des tiers;

f) la mise en place d'un guichet unique à disposition de toute Autorité publique ou de toute entité ou personne privée.

§ 3. – Les Autorités publiques disposant d'un réseau de fibre optique octroient à l'entité désignée en vertu du § 1er, un droit d'utilisation exclusif, gratuit et de longue durée sur la capacité non utilisée des réseaux de fibre optique et gaines qu'ils détiennent, en vue de leur valorisation et de leur exploitation.

§ 4. – Toute Autorité publique ou toute entité ou personne privée disposant d'un réseau de fibre optique ou souhaitant développer un réseau de fibre optique s'adresse, préalablement à l'extension ou au développement de leur réseau, au guichet unique mentionné au § 2, dernier tiret, en vue de la coordination des développements envisagés.

§ 5. – Les Autorités publiques disposant d'un réseau de fibre optique concluent avec l'entité désignée en vertu du § 1er et le CIRB une convention arrêtant notamment toute modalité technique, opérationnelle et financière des missions listées aux §§ 2 à 4.

TITRE III
URBIS

CHAPITRE I[ER]
Dispositions générales

Article 3

Pour l'application du présent titre, on entend par :

1° « L'ordonnance » : l'ordonnance du 8 mai 2014 portant création et organisation d'un intégrateur de services régional;

2° « Donnée authentique » : donnée récoltée et gérée par un service public dans une banque de données et qui fait foi comme donnée unique et originale concernant la personne ou le fait de droit concerné, de sorte que d'autres instances ne doivent plus collecter cette même donnée;

3° « Source authentique » : banque de données dans laquelle sont conservées des données authentiques.

La source authentique doit notamment être :

– complète;

– utile;

– garantir une qualité de l'information;

– correcte et actualisée (mise à jour);

– accessible gratuitement en ce qui concerne les sources authentiques régionales;

4° « Portail régional » : point d'entrée centralisé pour l'ouverture et le partage des données et services régionaux;

5° « CIRB » : organisme d'intérêt public instauré par la loi du 21 août 1987 modifiant la loi organisant les agglomérations et les fédérations de communes et portant des dispositions relatives à la Région bruxelloise, modifiée par l'ordonnance du 20 mai 1999 portant réorganisation du Centre d'Informatique pour la Région bruxelloise;

6° « Brussels UrbIS » : banque de données de fichiers vectoriels et images de cartographie numérique de référence à grande échelle du territoire de la Région de Bruxelles-Capitale faisant partie du produit UrbIS distribué par le CIRB conformément à l'arrêté du Gouvernement de la Région de Bruxelles-Capitale du 19 mai 1994 relatif à la mission de promotion, de distribution et de services aux utilisateurs du produit Brussels UrbIS;

7° « Accord de coopération du 17 juillet 2019 » : l'accord de coopération du 17 juillet 2019 entre l'État fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale concernant l'unification de la manière de référencer les adresses et de la mise en relation des données d'adresses;

8° « Banque de données issues de sources authentiques » : banque de données instituée par une ordonnance, regroupant un ensemble de données issues de sources authentiques ou de liens entre des données issues de sources authentiques et dont la collecte, le stockage, la mise à jour et la destruction sont assurés exclusivement par un service public déterminé, appelé gestionnaire de banque de données issues de sources authentiques, et qui sont destinées à être réutilisées par les services publics;

9° « Données à caractère personnel » : les données à caractère personnel visées à l'article 4, point 1), du règlement général sur la protection des données et de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel;

10° « Le règlement général sur la protection des données (RGPD ou le Règlement) » : Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (« règlement général sur la protection des données »);

11° « Gestionnaire » : une autorité publique chargée de la collecte, du stockage, de la mise à jour et de la destruction des données d'une source authentique ou d'une banque de données issues de sources authentiques;

12° « Initiateur » : une autorité publique ou tierce partie qui a reçu, par ou en vertu du présent titre ou par ou en vertu d'une disposition légale, la responsabilité finale et exclusive concernant la création, la modification, et la suppression d'une ou plusieurs données authentiques;

13° « Adresse » : l'information permettant de référencer, de manière unique et structurée une « unité de bâtiment », un « poste d'amarrage », un « emplacement » ou une « parcelle », sur la base du nom de la « commune », du « nom de rue » ou dans certains cas de la « zone d'adresses », du « numéro de police » éventuellement complété d'une « sous-adresse », d'un « numéro de boîte » ainsi que d'un « code postal »;

14° « Directive INSPIRE » : Directive 2007/2/CE du Parlement Européen et du Conseil du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne (INSPIRE)

15° « Comité d'adresses » : le Comité constitué conformément à l'article 8, § 1er, de l'accord de coopération du 17 juillet 2019;

16° « Situation de droit » : situation qui découle d'une décision administrative officielle, telle qu'un permis d'urbanisme, une décision du collège ou du conseil communal ou une réglementation urbanistique;

17° « Situation de fait » : situation observée sur le terrain mais qui n'est pas une situation de droit.

CHAPITRE 2
Désignation de Brussels UrbIS comme banque de données issues de sources authentiques

Article 4

Conformément à l'article 5, § 2, de l'ordonnance du 8 mai 2014 portant création et organisation d'un intégrateur de services régional, il est créé, selon les modalités déterminées par ou en vertu de du présent titre, une banque de données issues de sources authentiques relatives aux objets situés sur le territoire de la Région de Bruxelles-Capitale, dénommée « Brussels UrbIS ».

CHAPITRE 3
Les finalités poursuivies par Brussels UrbIS en tant que banque de données issues de sources authentiques

Article 5

Brussels UrbIS en tant que banque de données issues de sources authentiques, est le référentiel cartographique de base en Région de Bruxelles-Capitale, permettant de :

– Superposer des informations géographiques entre elles;

– Connaître les coordonnées géographiques de n'importe quel lieu, qu'il s'agisse d'un point précis ou de n'importe quel objet géographique situés sur le territoire de la Région;

– Numériser des données métiers et les localiser sur un même référentiel;

– Échanger des données pouvant être reliées à Brussels UrbIS;

– Réduire les charges administratives dans le cadre du présent titre.

CHAPITRE 4
Gestion et modalités de mise à jour et de mise à disposition des données contenues dans la banque de données Brussels UrbIS

Article 6

Le Centre d'Informatique pour la Région Bruxelloise est l'organisme chargé de la collecte, de la validation, de l'enregistrement, du stockage, de la mise à jour et de la mise à disposition des données contenues dans la banque de données issues de sources authentiques Brussels UrbIS.

Le CIRB est désigné gestionnaire de la banque de données Brussels UrbIS.

Cette mission comprend en particulier les tâches suivantes :

1° l'attribution des identifiants de toutes les données;

2° la coordination et l'assistance lors de la création et la mise à jour des données;

3° le traitement et l'intégration dans Brussels UrbIS des données des initiateurs;

4° la coordination et l'assistance lors de l'utilisation de Brussels UrbIS;

5° la coordination du contrôle de la qualité relative à toutes les initiatives afférentes à Brussels UrbIS;

6° la coordination et l'organisation de l'accès des utilisateurs à Brussels UrbIS;

7° la mise en place d'une procédure permettant à quiconque de communiquer des changements et des anomalies constatés;

8° la promotion de Brussels UrbIS;

9° les formations à l'utilisation de Brussels UrbIS;

10° le développement et la mise à disposition de services et applications utilisant les données Brussels UrbIS;

11° le développement et la mise à disposition de services et applications utilisant les données Brussels UrbIS;

12° la fixation du cadre technique et organisationnel pour le traitement coordonné des données cartographiques qu'elle contient;

13° la mise sur pied d'une coopération entre le gestionnaire et les initiateurs;

14° la mise à jour régulière des données de Brussels UrbIS et le respect de l'application des spécifications convenues entre les parties à l'accord de coopération du 17 juillet 2019;

15° la mise à disposition de documentations et spécifications correctes concernant les données au bénéfice des utilisateurs, des gestionnaires et des tierces parties autorisées à traiter les données dans le respect du Règlement.

Article 7

La validation en continu des données s'appuie sur des processus automatiques dans un environnement logiciel de production UrbIS et sur des procédures manuelles telles que la vérification des données sur le terrain. Ces procédures sont mises en place par le CIRB.

Un environnement logiciel de production spécifique est également mis en place. Il a pour fonction d'assurer en continu la mise à jour et la correction des données ainsi que la confection des livrables UrbIS.

Le CIRB assure l'évolution permanente de l'environnement de production UrbIS afin de tenir compte des changements technologiques, de l'évolution des besoins des utilisateurs ainsi que de l'évolution du cadre réglementaire tel que celui imposé par la Directive INSPIRE.

Des mécanismes d'historisation sont mis en place au sein de l'environnement de production UrbIS et ont pour objectif de rendre les données disponibles dans le temps quelles que soient les modifications subies.

Le système d'identification d'UrbIS permet de distinguer de manière univoque chaque donnée sans aucune confusion possible.

Les mécanismes d'historisation et d'identification sont mis en œuvre et tiennent compte des standards internationaux tels qu'ils sont définis et utilisés dans le cadre de la mise en œuvre de la Directive INSPIRE.

Article 8

Le portail régional donne accès aux données de la banque de données Brussels UrbIS, dans des formats ouverts et lisibles par machine, par voie électronique à des fins de réutilisation.

Les données de Brussels UrbIS seront réutilisées conformément aux conditions telles que définies par les standards européens en matière de licences open data.

La mise à disposition des données de Brussels UrbIS est gratuite pour les administrations.

CHAPITRE 5
Protection des données à caractère personnel

Article 9

À l'égard des traitements de données à caractère personnel en exécution du présent titre, le gestionnaire est responsable de traitement au sens de l'article 4, 7), du Règlement.

En application de l'article 24 du Règlement, le gestionnaire met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au Règlement, en vue du traitement sûr des données à caractère personnel contenues dans Brussels UrbIS.

Le gestionnaire met en place les mesures techniques nécessaires garantissant le respect des droits des personnes concernées, conformément au Règlement.

CHAPITRE 6
Les données contenues dans la banque de données issues de sources authentiques Brussels UrbIS

Article 10

Les données suivantes sont sous l'autorité d'initiateurs autres que le CIRB :

– Chaque commune bruxelloise :

- Noms des communes et des rues
- Numéros de police et boîtes
- Bâtiments extraits des permis d'urbanisme
- Postes d'amarrage
- Emplacements

- Situations de fait et de droit pour toutes les données susmentionnées

– Bruxelles Mobilité :

- Typologie des gestionnaires des voiries

– Bruxelles Environnement :

- Cartographie des parcs

– Perspective – IBSA :

- Quartiers du monitoring

– SPF Économie – StatBel :

- Secteurs statistiques

– SPF Finances – AGDP :

- Limites administratives : Région, communes

- Parcelles cadastrales

– SPF Intérieur :

- Zones de police

– Zones de police :

- Secteurs, divisions et quartiers de police

– Le prestataire du service postal universel :

- Codes postaux

- Zones postales

Sont également initiateurs pour la communication de données créées et mises à jour concernant des situations de fait, les entités suivantes :

– Les sociétés de distribution et les gestionnaires de réseaux de distribution qui ont des points de distribution dans les bâtiments de la Région bruxelloise :

- Adresses

– L'Agence Régionale pour la Propreté

– La Société du Logement de la Région de Bruxelles-Capitale

– Service public régional de Bruxelles Fiscalité

– Urban Brussels (anciennement Bruxelles Urbanisme et Patrimoine)

– Le Service d'Incendie et d'Aide Médicale Urgente

– La Société de Transports Intercommunaux de Bruxelles

Toute autre entité peut être initiateur pour la communication de données collectées ou créées et mises à jour, pour autant que ces données répondent à la définition de donnée authentique, reprise à l'article 2, 2°, et ce, conformément aux modalités reprises à l'article 10 du présent titre.

Le CIRB est initiateur de toutes les autres données de Brussels UrbIS.

Les liaisons entre certaines données de Brussels UrbIS font partie de la banque de données issue de sources authentiques. Sont visées en particulier les liaisons entre d'une part les adresses et d'autre part, les bâtiments, unités de bâtiments, parcelles, emplacements et postes d'amarrage.

Brussels UrbIS se conforme aux spécifications déterminées par le Comité d'adresses. Les spécifications sont les dispositions techniques relatives à l'insertion, la mise à jour, la gestion et la communication de composants d'une adresse.

Chaque initiateur, chacun pour ce qui concerne ses données, et toute autre personne désignée initiateur par le Comité d'adresses, agit en tant qu'initiateur.

Il contribue à la création et à la mise à jour de ses propres données et veille en particulier à ce que le gestionnaire puisse intégrer de façon correcte ces données dans Brussels UrbIS.

Cette mission comprend les tâches suivantes :

1° L'établissement de toutes ses données;

2° La communication de ses données en vue de leur intégration dans Brussels UrbIS;

3° La communication de chaque modification et correction de ses données au gestionnaire en vue de leur mise à jour et de l'amélioration de la qualité de Brussels UrbIS;

4° L'examen de questions ou de notifications de la part du gestionnaire relatives à ses données en vue de l'amélioration de la qualité de Brussels UrbIS.

Des protocoles de collaboration seront conclus entre le gestionnaire et les initiateurs pour régler la mise en œuvre des modalités de cette mission après avis du Comité Brussels UrbIS.

CHAPITRE 7
Gouvernance

Article 11

Par le présent chapitre, il est créé un Comité Brussels UrbIS chargé de contribuer à la stratégie d'évolution de Brussels UrbIS.

Composition

Chaque initiateur cité à l'article 9 du présent titre désigne au minimum un représentant pour siéger dans ce Comité;

Le Comité peut élargir sa composition en intégrant d'autres membres.

Le Comité comprendra un représentant du cabinet du Ministre dont le CIRB relève.

Missions

– Proposer de nouvelles données ou de nouvelles banques de données authentiques à intégrer dans Brussels UrbIS;

– Proposer de nouveaux services portant sur ces données;

– Proposer des évolutions de données, banques de données et services;

– Proposer des modalités pour collecter, améliorer, mettre à jour et distribuer les données de Brussels UrbIS;

– Veiller à ce que le produit UrbIS réponde aux besoins de tous les utilisateurs.

Fonctionnement

Le Comité règle son fonctionnement dans un règlement d'ordre intérieur qu'il établit lors de sa première réunion.

Lors de cette même réunion, sur proposition du CIRB, le Comité établit la liste détaillée des données faisant partie du produit Brussels UrbIS.

Le Comité peut ajouter de nouvelles données à cette liste ou en modifier les données existantes.

CHAPITRE 8
Financement

Article 12

Dans les limites des crédits budgétaires, le Gouvernement alloue annuellement au gestionnaire de la banque de données Brussels UrbIS, les moyens nécessaires à l'exercice de ses missions telles que fixées par le présent titre.

Les moyens couvrent :

1° les frais de personnel;

2° les frais de fonctionnement, en ce compris les frais liés aux développements, à la mise à jour, à l'élaboration de nouvelles données et à l'exploitation informatique spécifique.

TITRE IV
Dispositions finales

Article 13

Les livres B.I. et B.II entrent en vigueur six mois après la publication des présents décret et ordonnance conjoints.

Article 14

Les livres C.IV et C.V entrent en vigueur six mois après la publication des présents décret et ordonnance conjoints pour les Autorités publiques regroupées dans les paliers n° 1 et 2 définis par l'arrêté fixant les seuils numériques.

Le titre II du livre C.III et le chapitre 2 du titre IV du même livre du Code de la gouvernance et de la donnée entrent en vigueur un an après la publication des présents décret et ordonnance conjoints pour les Autorités publiques regroupées dans les paliers n° 1 et 2 définis par l'arrêté fixant les seuils numériques.

Le chapitre I du titre III du livre C.III du Code de la Gouvernance et de la donnée entre en vigueur deux ans après la publication des présents décret et ordonnance conjoints pour les Autorités publiques regroupées dans les paliers n°1 et 2 définis par l'arrêté fixant les seuils numériques.

Article 15

Les livres C.II., C.III, C.IV, à l'exception du titre III, C.V, et C.VI du Code de la gouvernance et de la donnée entrent en vigueur deux ans après la publication

des présents décret et ordonnance conjoints pour les Autorités publiques regroupées dans le palier n° 3 défini par l'arrêté fixant les seuils numériques.

Seul le titre III du livre C.IV entre en vigueur six mois après la publication des présents décret et ordonnance conjoints pour les Autorités publiques regroupées dans le palier n° 3 défini par l'arrêté fixant les seuils numériques.

Article 16

Toutes les compétences dévolues à la Commission d'accès aux documents administratifs instituée par les Décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française relatifs à la publicité de l'administration dans les institutions bruxelloises sont exercées dès son entrée en vigueur par la Commission d'accès aux documents administratifs et aux données, dénommée la CADADo et instituée par le livre B.II du Code de la gouvernance et de la donnée.

La CADADo reprend l'ensemble des droits et obligations précédemment détenues par la CADA.

Les membres de la Commission d'accès aux documents administratifs instituée par les décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française relatifs à la publicité de l'administration dans les institutions bruxelloises poursuivent leur mandat au sein de la chambre relative à l'accès aux documents administratifs de la Commission d'accès aux documents administratifs et aux données instituée par le livre B.II du Code de la gouvernance et de la donnée.

Le Gouvernement, le Collège réuni et le Collège désignent conjointement conformément à l'article B.II. 8 quatre nouveaux membres pour former la chambre relative au partage administratif de données et la chambre relative à la réutilisation de données, dans les six mois suivants la publication du présent décret et ordonnance conjoints. Les mandats de ces nouveaux membres s'achèvent en même temps que celui des membres visés à l'alinéa 3 qui poursuivent leur mandat.

Le secrétariat de la CADADo visé à l'article B.II.5 est désigné dans les six mois suivants la publication du présent décret et ordonnance conjoints.

Les experts visés à l'article B.II.7 doivent également être désignés dans les six mois suivants la publication du présent décret et ordonnance conjoints.

Les recours et les demandes de consultation introduits avant la date d'entrée en vigueur des livres B.I, B.II, C.IV et C.V. devant la Commission d'accès aux documents administratifs instituée par les décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française relatifs à la publicité de l'administration dans les institutions bruxelloises, visés à l'article 25 desdits décret et ordonnance conjoints du 16 mai 2019, de même que les recours introduits avant la même date et visés à l'article 7 de l'ordonnance du 27 octobre 2016 visant à l'établissement d'une politique de données ouvertes (Open Data) et portant transposition de la Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, sont poursuivis par la chambre relative à l'accès aux documents administratifs de la CADADo visée dans le livre A.II du Code de la gouvernance et de la donnée.

Article 17

Les membres de la Commission d'accès aux documents administratifs instituée par les Décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française relatifs à la publicité de l'administration dans les institutions bruxelloises, devenus les membres de la Chambre d'accès aux documents administratifs de la CADADo après l'entrée en vigueur des livres B.I et B.II, perçoivent des jetons conformément à l'article A. II.9 pour l'ensemble des dossiers clôturés après l'entrée en vigueur des livres A.I et A.II du Code, mais introduits avant l'entrée en vigueur desdits livres.

Article 18

Dans l'attente de la détermination, par les autorités administratives, de la rétribution qui peut éventuellement être exigée pour la délivrance d'un document administratif ou d'une information environnementale sous forme de copie, les montants maximum suivants sont applicables :

– 0,01 euro, par face, pour un document au format A4 en noir et blanc;

– 0,02 euro, par face, pour un document supérieur au format A4, mais ne dépassant pas le format A3, en noir et blanc;

– 0,04 euro, par face, pour un document au format A2, en noir et blanc;

– 0,08 euro, par face, pour un document au format A1, en noir et blanc.

Les montants précités sont triplés pour les copies en couleur.

Si une rétribution est exigée, le prix de la copie plus celui du coût de sa communication sur place ou par envoi postal ou autre moyen de transmission est fixé à un minimum de 1 euro.

Article 19

Les décisions, les actes et les documents qui doivent faire l'objet d'une publicité active en vertu du livre B.I du Code de la gouvernance et de la donnée sont ceux qui sont adoptés après l'entrée en vigueur dudit livre.

Article 20

L'ordonnance du 17 juillet 2020 garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité, et portant simplification et harmonisation des formulaires électroniques et papier, est abrogée six mois après l'entrée en vigueur des présents décret et ordonnance conjoints.

Les décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française relatifs à la publicité de l'administration dans les institutions bruxelloises sont abrogés six mois après l'entrée en vigueur des présents décrets et ordonnances conjoints.

L'ordonnance du 27 octobre 2016 visant à l'établissement d'une politique de données ouvertes (Open Data) et portant transposition de la Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public est abrogée six mois après l'entrée en vigueur des présents décrets et ordonnances conjoints.

L'ordonnance du 8 mai 2014 portant création et organisation d'un intégrateur de services régional est abrogée six mois après l'entrée en vigueur des présents décrets et ordonnances conjoints.

ANNEXE 3

Rapport d'évaluation de l'impact sur la dimension genre

Rapport d'évaluation de l'impact sur la dimension genre

Etabli le 30 aout 2023 en vertu de l'article 3, alinéa 1er, 2° du décret du 21 juin 2013 portant intégration de la dimension genre dans les lignes politiques de la Commission communautaire française.

Objet : Avant-projet de Décret et Ordonnance conjoints de la Région Bruxelles-Capitale, de la Commission communautaire commune, de la Commission communautaire française portant le Code Bruxellois de la Gouvernance et de la Donnée

L'article 3, alinéa 1, 2° du décret du 21 juin 2013 stipule que « pour chaque projet d'acte législatif ou réglementaire, chaque Membre du Collège établit un rapport d'évaluation de l'impact du projet sur la situation respective des femmes et des hommes ».

L'avant-projet de Décret et Ordonnance conjoints de la Région Bruxelles-Capitale, de la Commission communautaire commune, de la Commission communautaire française portant le Code Bruxellois de la Gouvernance et de la Donnée a pour objet principal de codifier à droit constant les législations bruxelloises en matière numérique et de réguler la gestion et la circulation des données intra-bruxelloises entre les Autorités Publiques.

Cet avant-projet prévoit également l'abrogation du décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française, relatifs à la publicité de l'administration dans les institutions bruxelloises, de l'ordonnance du 27 octobre 2016 Ordonnance visant à l'établissement d'une politique de données ouvertes et portant transposition de la Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, de l'ordonnance du 13 février 2014 relative à la communication par voie électronique dans le cadre des relations avec les autorités publiques de la Région de Bruxelles-Capitale, de l'ordonnance du 17 juillet 2020 garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité, et portant simplification et harmonisation des formulaires électroniques et papier et de l'ordonnance du 08 mai 2014 portant création et organisation de l'intégrateur de services régional.

Dans la mesure où cet avant-projet de décret et ordonnance conjoints a pour objet l'unification de la législation bruxelloise en matière numérique et la régulation de la gestion et de la circulation intra-bruxelloise des données entre les Autorités Publiques, ce projet de décret et ordonnance conjoints est considéré comme :

N'ayant pas d'impact sur la dimension genre.

ANNEXE 4

Rapport d'évaluation de l'impact sur la situation des personnes handicapées

Rapport d'évaluation de l'impact sur la situation des personnes handicapées

Etabli le 30 aout 2023 en vertu de l'article 4, §3 du décret du 15 décembre 2016 portant intégration de la dimension handicap dans les lignes politiques de la Commission communautaire française.

Objet : Avant-projet de Décret et Ordonnance conjoints de la Région Bruxelles-Capitale, de la Commission communautaire commune, de la Commission communautaire française portant le Code Bruxellois de la Gouvernance et de la Donnée.

L'article 4, §3 du Décret du 15 décembre 2016 stipule que chaque membre du Collège évalue tout projet d'acte législatif ou réglementaire au regard du principe de handistreaming relevant de ses compétences.

L'avant-projet de Décret et Ordonnance conjoints de la Région Bruxelles-Capitale, de la Commission communautaire commune, de la Commission communautaire française portant le Code Bruxellois de la Gouvernance et de la Donnée a pour objet principal de codifier à droit constant les législations bruxelloises en matière numérique et de réguler la gestion et la circulation des données intra-bruxelloises entre les Autorités Publiques.

Cet avant-projet prévoit également l'abrogation du décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française, relatifs à la publicité de l'administration dans les institutions bruxelloises, de l'ordonnance du 27 octobre 2016 Ordonnance visant à l'établissement d'une politique de données ouvertes et portant transposition de la Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, de l'ordonnance du 13 février 2014 relative à la communication par voie électronique dans le cadre des relations avec les autorités publiques de la Région de Bruxelles-Capitale, de l'ordonnance du 17 juillet 2020 garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité, et portant simplification et harmonisation des formulaires électroniques et papier et de l'ordonnance du 08 mai 2014 portant création et organisation de l'intégrateur de services régional.

Dans la mesure où cet avant-projet de décret et ordonnance conjoints a pour objet l'unification de la législation bruxelloise en matière numérique et la régulation de la gestion et de la circulation intra-bruxelloise des données entre les Autorités Publiques, ce projet est considéré comme :

N'ayant pas d'impact sur la dimension handicap.