



Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 154/2023 van 20 oktober 2023

Betreft: adviesaanvraag over een Gezamenlijk decreet en ordonnantie houdende het Wetboek voor governance en gegevensbeheer en de aanduiding van de cartografische databank URBIS (CO-A-2023-407)

Vertaling

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit"),

Aanwezig: de dames Juline Deschuyteneer en Cédrine Morlière en de heren Bart Preneel en Gert Vermeulen;;

Gelet op de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, met name de artikelen 23 en 26 (hierna "WOG");

Gelet op artikel 25, derde lid, van de WOG, volgens hetwelk de beslissingen van het Kenniscentrum bij meerderheid van stemmen worden aangenomen;

Gelet op Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (hierna "AVG");

Gelet op de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (hierna "WVG");

Gelet op het verzoek om advies van de heer Bernard Clerfayt, Minister van de Brusselse Hoofdstedelijke Regering, belast met Werk en Beroepsopleiding, Digitalisering, de Plaatselijke Besturen en Dierenwelzijn, (hierna: de aanvrager) ontvangen op 25 juli 2023;

Brengt op 20 oktober 2023 het volgend advies uit:

I. Onderwerp en context van de adviesaanvraag

1. De minister heeft bij de Autoriteit een verzoek om advies ingediend over alle bepalingen van een gezamenlijk voorontwerp van decreet en ordonnantie houdende het Brussels Wetboek voor governance en gegevensbeheer (hierna "het ontwerp" genoemd). In zijn adviesaanvraagformulier legt de aanvrager uit dat (de Autoriteit vertaalt) «*het doel van het gezamenlijke voorontwerp van decreet en ordonnantie houdende het Brussels wetboek voor governance en gegevensbeheer is om alle nationale en Europese wet- en regelgeving over gegevens en governance te codificeren*».

II. Onderzoek

Dit advies is als volgt opgebouwd:

II.1. Algemene overwegingen	3
II.1.1. Reikwijdte van het ontwerp en eerdere adviezen van de Autoriteit	4
II.1.2. Algemene en aanzienlijke bezorgdheid veroorzaakt door het ontwerp op het gebied van gegevensbescherming	8
A) Vergemakkelijken van gegevensverwerking, gegevensverkeer tussen overheidsinstanties en gegevensconcentratie	8
B) Het CIBG (PARADIGM), een centrale en essentiële instelling voor gegevensverwerking	11
C) Een bepaalde patrimoniale zienswijze op gegevens met vage concrete gevolgen.....	17
II.1.3. Algemene opmerkingen over het ontwerp.....	20
II.2. Openbaarheid van bestuur	21
II.2.1. Passieve openbaarheid en belang	21
II.2.2. Gegevensmededeling per e-mail	23
II.2.3. Rol van toestemming (milieu-informatie)	24
II.2.4. Gedeeltelijke vrijstelling van openbaarheid van bestuur	25
II.2.5. Openbaarheid van gegevens via internet	26
II.4. Delen van administratieve gegevens (uitwisseling van gegevens tussen overheidsinstanties) (Boek C.IV., Titel 2)	28
II.4.1. Administratief delen in het algemeen.....	29
II.4.2. Authentieke gegevensbronnen	31
II.4.3. Gegevensbank afkomstig uit authentieke bronnen.....	36
II.5. Hergebruik van openbare documenten en openbare gegevens (Boek C.IV, Titel 3)	39
II.5.1. Toepassingsgebied van 2 stelsels van hergebruik.....	39
II.5.2. Omzetting van de Richtlijn hergebruik - artikelen C.IV 17 tot C.IV.30	41
II.5.3. Uitvoering van de verordening data governance - artikelen C.IV.31 tot en met C.IV.32	42
II.5.4. Openbaarmaking van persoonsgegevens	50

II.5.5. Hoofdstuk 4 – ‘Data-altruïsme’	51
II.6. Commissie voor Toegang tot Bestuursdocumenten en Gegevens ("CTBG")	51
II.6.1. Een ander beroeps- en adviesorgaan dan een gegevensbeschermingsautoriteit	51
II.6.2. Systematische gegevensoverdracht naar de CTBG	52
II.6.3. Andere bevoegdheden van de CTBG	52
II.6.4. Advies van de Gegevensbeschermingsautoriteit	53
II.6.5. Openbaarmaking van de beslissingen van de CTBG.....	54
II.7. Gegevensbeheer	55
II.7.1. Toepassingsgebied (onbepaald) en verplichte toepassing van de regels van het wetboek	55
II.7.2. Toepasselijke wettelijke regelingen op gegevens.....	56
II.7.3. Omkeerbaarheid van de gegevens	56
II.7.4. Typologie van gegevenscategorieën	57
II.7.5. Valorisatie van gebruiksgegevens.....	58
II.7.6. Eerbiediging van de rechten van derden bij valorisatie van gegevens - toestemming e.d.	59
II.7.7. Beroep in het kader van gegevensvalorisatie	62
II.7.8. Bijwerken van de gegevens	63
II.7.9. Referentiegegevens.....	64
II.7.10. Analytische modellen, algoritmen en artificiële intelligentie	65
II.8. De verantwoordelijkheden met betrekking tot de verwerking van persoonsgegevens.....	67
II.9. Centrum voor gegevensanalyse en gegevensverwerking.....	69
II.10. Bewaartermijn van de gegevens.....	70
II.11 Aanwijzing van URBIS als gegevensbank afkomstig van authentieke bronnen	73
II.12. Besluit.....	76

II.1. ALGEMENE OVERWEGINGEN

- De Autoriteit merkt van meet af aan op dat de aanpak van de aanvrager gedurfd en innovatief lijkt. In het algemeen staat de Autoriteit positief tegenover initiatieven die gericht zijn op het verbeteren van de kwaliteit van gegevensbeheer en -governance, ook buiten de persoonsgegevens, aangezien een dergelijke aanpak de verwerkingsverantwoordelijken waarschijnlijk bewuster zal maken van de omgang met gegevens in het algemeen en persoonsgegevens in het bijzonder.
- Ondanks erkend wordt dat de nagestreefde doeleinden van dit transversaal ontwerp verdienen zijn, wil de Autoriteit er niettemin op wijzen dat dit ontwerp bepaalde belangrijke problemen opwerpt en een aantal opmerkingen in verband met gegevensbescherming vereist. Met het oog op de

doeltreffendheid concentreert dit advies zich op deze aspecten en kan daarom niet tegelijkertijd alle mogelijke positieve aspecten van het ontwerp opsommen.

II.1.1. Reikwijdte van het ontwerp en eerdere adviezen van de Autoriteit

4. Het Ontwerp regelt, in gecodificeerde vorm, de **bestuurlijke transparantie** (of openbaarheid van bestuur, zowel actief als passief), het **hergebruik van overheidsinformatie, de uitwisseling van gegevens tussen overheidsinstanties** (inclusief authentieke bronnen en gegevensbanken ontstaan uit authentieke bronnen) en de **principes die van toepassing zijn op het beheer van gegevens** door deze instanties (in dit opzicht creëert het ontwerp een nieuw institutioneel landschap). Het voorziet ook in **een gegevensbank ontstaan uit de belangrijkste Brusselse authentieke bronnen**, « *Brussels UrbIS* »¹.

5. Daartoe worden in artikel 20 van het ontwerp **de volgende teksten opgeheven** :
 - Ordonnantie van 17 juli 2020 *houdende verankering van het principe van de unieke gegevensinzameling in de werking van de diensten en instanties die behoren tot of taken uitvoeren voor de overheid en tot vereenvoudiging en gelijkschakeling van elektronische en papieren formulieren*;

 - Gezamenlijk decreet en ordonnantie van 16 mei 2019 van het Brussels Hoofdstedelijk Gewest, de Gemeenschappelijke Gemeenschapscommissie en de Franse Gemeenschapscommissie *betreffende de openbaarheid van bestuur bij de Brusselse instellingen* ;

 - Ordonnantie *ertoe strekkende een opendatabeleid uit te stippelen en houdende omzetting van de Richtlijn 2013/37/EU van het Europees Parlement en de Raad van 26 juni 2013 tot wijziging van Richtlijn 2003/98/EG van het Europees Parlement en de Raad van 17 november 2003 inzake het hergebruik van overheidsinformatie* ;

 - De ordonnantie van 8 mei 2014 *betreffende de oprichting en organisatie van een gewestelijke dienstenintegrator*.

6. Met betrekking tot **openbaarheid van bestuur** en in het bijzonder de openbaarmaking van persoonsgegevens heeft de Autoriteit onlangs haar standpunt samengevat in de volgende twee adviezen :

¹ Namelijk volgens artikel 3, 6° van Titel III van het ontwerp, de «*databank van vectorbestanden en beelden van digitale referentiecarterografie op grote schaal van het grondgebied van het Brussels Hoofdstedelijk Gewest. Maakt deel uit van het UrbIS-product dat door het CIBG wordt verdeeld overeenkomstig het besluit van de Brusselse Hoofdstedelijke Regering van 19 mei 1994 betreffende de opdracht tot promotie, distributie en dienstverlening aan de gebruikers van het product Brussels UrbIS*».

- Advies 131/2023 van 8 september 2023 *met betrekking tot amendement nr. 4 van het wetsontwerp tot wijziging van de wet van 11 april 1994 betreffende de openbaarheid van bestuur en tot opheffing van de wet van 12 november 1997 betreffende de openbaarheid van bestuur in de provincies en gemeenten (CO-A-2022-316) (hierna «**het advies 131/2023**»);*
 - Advies nr. 42/2023 van 9 februari 2023 *met betrekking tot een voorontwerp van wet tot wijziging van de wet van 11 april 1994 betreffende de openbaarheid van bestuur (CO-A-2022-311) (hierna «**het advies 42/2023**»).*
7. Met betrekking tot het **hergebruik van overheidsinformatie** nodigt de Autoriteit de aanvrager uit om vooraf kennis te nemen van de volgende adviezen, waarvan de beginselen van toepassing zijn :
- Advies nr. 144/2023 van 29 februari 2023 *met betrekking tot een voorontwerp van wet tot wijziging van de wet van 4 april 2016 betreffende de openbaarheid van bestuur (CO-A-2023-334) (hierna «**het advies 144/2023**»);*
 - Advies 203/2021 van 25 oktober 2021 over) *ontwerpdecreet nr. 2020/279 van de Franse Gemeenschapscommissie inzake open gegevens en het hergebruik van overheidsinformatie (CO-A-2021-196 (hierna «**het advies 203/2021** »);*
 - Advies 167/2022 van 19 juli 2022 *betreffende een voorontwerp van decreet inzake de verspreiding en het hergebruik van overheidsinformatie en een voorontwerp van decreet inzake de verspreiding en het hergebruik van overheidsinformatie voor aangelegenheden bedoeld in artikel 138 van de Grondwet) ((CO-A-2022-150) (hierna «**het advies 167/2022**»);*
 - Advies 227/2022 van 29 oktober 2022 over *een ontwerpdecreet nr. 227/2022 van de Franse Gemeenschapscommissie over open gegevens en het hergebruik van overheidsinformatie (CO-A-2022-209).*
8. Wat betreft **de uitwisseling van gegevens uit authentieke gegevensbronnen, de dienstintegratoren en de daarmee samenhangende verwerkingsverantwoordelijkheden** inzake persoonsgegevens, verwijst de Autoriteit de aanvrager naar haar advies nr. 143/2023 van 29 september 2023 *betreffende een voorontwerp van decreet houdende instemming met het samenwerkingsakkoord tussen het Waals Gewest en de Franse Gemeenschap tot aanwijzing van de dienstintegrator van het Waals Gewest en de Franse Gemeenschap en een ontwerp van samenwerkingsakkoord met betrekking tot de oprichting van de gemeenschappelijke dienst van de*

Waalse Regeringen en de Franse Gemeenschap, genaamd Banque Carrefour d'échange de données (niet onderworpen aan instemming) (CO-A-2023-375), en betreffende een ontwerp van decreet houdende instemming met het samenwerkingsakkoord tussen het Waals Gewest en de Franse Gemeenschap tot aanwijzing van de dienstintegrator van het Waals Gewest en de Franse Gemeenschap en een ontwerp van samenwerkingsakkoord met betrekking tot de oprichting van de gemeenschappelijke dienst van de Waalse Regeringen en de Franse Gemeenschap, genaamd Banque Carrefour d'échange de données (niet onderworpen aan instemming) (CO-A-2023-376) (hierna «advies 143/2023»)

9. Het ontwerp is **ook gedeeltelijk in lijn met het Europese recht**, en zonder dat het nodig is om alle Europese teksten waarnaar het verwijst op te sommen, kunnen worden aangehaald Richtlijn 2013/37/EU van het Europees Parlement en de Raad van 26 juni 2013 *tot wijziging van Richtlijn 2003/98/EG van het Europees Parlement en de Raad van 17 november 2003 inzake het hergebruik van overheidsinformatie* (hierna, "**de richtlijn hergebruik**"), en Verordening 2022/868 van het Europees Parlement en de Raad van 30 mei 2022 *betreffende Europese datagovernance en tot wijziging van Verordening (EU) 2018/1724 (Datagovernanceverordening)* (hierna "**de verordening data governance**"), die zij gedeeltelijk ten uitvoer legt, waarmee verderop in dit advies rekening zal worden gehouden.
10. Tegen deze achtergrond **geeft het ontwerp meer dan 120 definities**, sommige bestaand, sommige geïnspireerd door Europees recht, federaal recht of, wanneer het ontwerp nieuwe concepten introduceert, door rechtsleer. Ter illustratie worden de volgende concepten gedefinieerd door het ontwerp (vetgedrukte begrippen worden besproken in het vervolg van dit advies en gedefinieerd in een voetnoot): «overheidsinstantie » ; « **derde overheidsinstantie** »² ; « *gegeven* » ; « **beschermd gegeven** »³ ; « *gevoelig gegeven* » ; « **openbaar gegeven** »⁴ ; « *geklasseerd gegeven* » ; « *gegevensset* » ; « **open gegeven** »⁵ ; « *verworven gegeven* » ; « *gereduceerd gegeven* » ; « *afgeleid gegeven* » ; « *gegeven van particuliere herkomst* » ; « *exclusief gegeven* » ; « *gesloten geven* » ; « *vrij verstrekt gegeven* » ; « *waargenomen gegeven* » ;

² hetzij, volgens artikel A.III.1.5 « *openbare entiteit die onder een ander nationaal of internationaal gezagsniveau valt* ».

³ Namelijk volgens artikel A.III.1.9) van het ontwerp:

« *elk gegeven dat beschermd is op een van de volgende gronden:*

(a) *commerciële vertrouwelijkheid, waaronder het handels-, bedrijfs- of beroepsgeheim;*

(b) *statistisch geheim;*

(c) *bescherming van de intellectuele-eigendomsrechten van derden;*

(d) *bescherming van persoonsgegevens* ».

⁴ Namelijk volgens artikel A.III.1.23) van het ontwerp « *elk gegeven dat de Overheidsinstanties bezit en beheert in het kader van hun taken van openbare dienstverlening* ».

⁵ Namelijk, volgens artikel A.III.1.13) van het ontwerp « *elk vrij toegankelijk gegeven* ».

« **gebruiksgegevens** »⁶ ; « *inhoudsgegevens* » ; « **referentiegegevens** »⁷ ; « *metagegeven* » ; « *gegeven afkomstig van een authentieke bron* » ; « **authentieke bron** »⁸ ; « **(gegevens)gebruiker** »⁹ ; « **vertrouwde derde** »¹⁰ ; « *gegevensbankbeheerder* » ; « *databemiddelingsdienst* » ; « *Brussels digitaal ecosysteem* » ; « *Brussels dienstenplatform* » ; « *Brussels integratiecentrum* » ; « *centrum voor gegevensanalyse en gegevensverwerking* » ; « *gegevensproducerende overheidsinstantie* » ; « **valorisatie** »¹¹ ; « *gegevensdeling, mededeling* » ; « **administratieve gegevensdeling** »¹² ; « *mededeling* » ; « *verhulling* » ; « **gegevensintegratie** »¹³ ; « **interoperabiliteit** »¹⁴ ; « *kunstmatige intelligentie* » ; « **digitale partnerschappen** »¹⁵.

11. Gezien de reikwijdte en het zeer brede toepassingsgebied, met inbegrip van de keuzes die met name op het gebied van hergebruik van gegevens zijn gemaakt¹⁶, is het duidelijk dat het ontwerp een **aanzienlijke inbreuk** vormt op de rechten en vrijheden van de betrokken personen.

⁶ Namelijk volgens artikel A.III.1.24) van het ontwerp «*elk gegeven dat voortvloeit uit de activiteit van een gegevensgebruiker en meer bepaald uit diens interactie met gegevens; gebruiksgegevens worden verzameld om informatie over de gebruiker te verstrekken*». Het (gegevens)gebruik wordt in artikel A.III.1.34) als volgt gedefinieerd «*gebruiker in de zin van artikel 2, 9) van de DGA [data governance verordening]*», namelijk «*een natuurlijk persoon of rechtspersoon die rechtmatige toegang heeft tot bepaalde persoonsgegevens of niet-persoonsgebonden gegevens en die het recht heeft, onder meer uit hoofde van Verordening (EU) 2016/679 in het geval van persoonsgegevens, om die gegevens voor commerciële of niet-commerciële doeleinden te gebruiken*».

⁷ Namelijk volgens artikel A.III.1.26) van het ontwerp «*elk gegeven dat door de Overheidsinstantie of door het gebruik ervan als structurerend wordt beschouwd, met name om producten, economische entiteiten, gebieden of natuurlijke en rechtspersonen te benoemen of te identificeren*».

⁸ Zie overweging 47.

⁹ Zie voetnoot 6

¹⁰ Namelijk A.III.1.98) van het ontwerp «*een onafhankelijke entiteit die beschikt over de technische middelen die nodig zijn voor het anonimiseren of pseudonimiseren van persoonsgegevens in het kader van de verwerkingen zoals beschreven in artikel 89 van de AVG*».

¹¹ Namelijk volgens artikel A.III.1.68) van het ontwerp «*de gegevensverwerking met het oog op de exploitatie van de gegevens om de taken van openbare dienstverlening of wettelijke verplichtingen van de Overheidsinstanties te optimaliseren of voor andere doeleinden dan waarvoor zij zijn verzameld*».

¹² Namelijk volgens artikel A.III.1.70) van het ontwerp «*de terbeschikkingstelling of verzending van openbare gegevens tussen Overheidsinstanties, met als enig doel de uitvoering van hun taken van openbare dienstverlening of hun verplichtingen van algemeen belang, met uitzondering van het delen met het CIBG in zijn functie van beheerder van het Brussels Dienstenplatform met betrekking tot de Gegevenscatalogus en met uitzondering van het delen van open data, zonder voorwaarden van hergebruik, beschikbaar in de Open portaal voor openbare gegevens van het Brussels Dienstenplatform*».

¹³ Artikel A.III.1.80) van het ontwerp definieert gegevensintegratie als «*het proces waarbij verschillende gegevenssets worden gecombineerd tot één enkele gegevensset die vollediger en samenhangender is*» Artikel A.III.A.12) van het ontwerp definieert gegevensset als «*samenhangend geheel van bronnen of informatie (gegevensbestanden, toelichtingsbestanden, API, link, ...) en metagegevens (beschrijving, producent, publicatiedatum, trefwoorden, geografische en temporele dekking, ...) over een bepaald thema*».

¹⁴ Namelijk zoals bedoeld in artikel A.III.1.86) van het ontwerp «*het vermogen van verschillende systemen, apparatuur, software of diensten om op een samenhangende manier samen te werken en informatie uit te wisselen*».

¹⁵ « Een digitaal gegevenspartnerschap is elk initiatief waarbij openbare gegevens worden gebruikt of gedeeld en dat juridisch of administratief twee of meer entiteiten binnen dezelfde Overheidsinstantie met elkaar verbindt, of twee of meer entiteiten met rechtspersoonlijkheid, waarvan ten minste één Overheidsinstantie is», artikel C.III.2, § 1, 2de lid van het ontwerp. Het digitale partnerschap kan openbaar of gemengd zijn, afhankelijk van het feit of het al dan niet is afgesloten met een andere overheidsinstantie.

¹⁶ Zie de overwegingen 74-75.

II.1.2. Algemene en aanzienlijke bezorgdheid veroorzaakt door het ontwerp op het gebied van gegevensbescherming

12. Naast het brede toepassingsgebied, en onverminderd latere opmerkingen, is de Autoriteit van mening dat **het ontwerp ook een algemeen en belangrijk probleem op het gebied van gegevensbescherming opwerpt, en wel om de volgende drie redenen :**

- Het ontwerp heeft tot doel **de verwerking van gegevens door de Brusselse overheidsinstanties en, in het bijzonder, het gegevensverkeer tussen deze instanties aanzienlijk te vergemakkelijken**, met name door het nastreven van een concentratiedynamiek op het gebied van gegevensverwerking (integratie van diensten en gegevens, interoperabiliteit, mutualisatie);
- Het **plaatst een essentiële overheidsinstantie in het middelpunt van de gegevensverwerking in het Brussels Hoofdstedelijk Gewest;**
- Vanuit **conceptueel oogpunt lijkt het een bepaalde opvatting van gegevens als patrimonium** (persoonlijk of anderszins) **uit te dukken**, waarvan de praktische gevolgen onduidelijk zijn.

13. Deze redenen moeten worden onderbouwd op basis van het dispositief en de memorie toelichting bij het ontwerp.

A) Vergemakkelijken van gegevensverwerking, gegevensverkeer tussen overheidsinstanties en gegevensconcentratie

14. De volgende elementen geven duidelijk aan dat het ontwerp ernaar streeft de verwerking van persoonsgegevens te vergemakkelijken (vet en onderstreept toegevoegd door de Autoriteit in de onderstaande citaten):

- Naast het reeds in het Belgische (federale en gefedereerde) recht gekende beginsel om een beroep te doen op **authentieke bronnen** van in het ontwerp vastgestelde gegevens, bepaalt artikel C.II.3. van dit ontwerp, gewijd aan het «***beginsel van gegevensdeling***», in paragraaf 1 het volgende «*De overheidsinstanties organiseren standaard de onderlinge administratieve gegevensdeling om de uitvoering van hun taken van openbare dienstverlening en hun verplichtingen van algemeen belang te verbeteren en, in voorkomend geval, de administratieve lasten voor de burgers te verminderen*», artikel C.IV.4 van het ontwerp getiteld «***Standaard administratieve deling en verzoek tot administratieve deling***» is gewijd aan het beginsel dat overheden onderling gegevens delen. De memorie van toelichting

verduidelijkt dit als volgt «*Het gratis karakter van het [administratief] delen wordt gerechtvaardigd door de wens om het delen van gegevens tussen Overheidsinstanties te faciliteren en aan te moedigen*»;

- Het ontwerp voorziet in de mogelijkheid om **databanken op te zetten die zijn afgeleid van authentieke gegevensbronnen**, , namelijk « *superdatabanken* » in de eigenlijke bewoordingen van de memorie van toelichting;
- Het doel van het ontwerp is de **grootst mogelijke interoperabiliteit** te bereiken, zo voeren «*de overheidsinstanties (...) oplossingen in die de gemeenschappelijke standaarden bevorderen*»¹⁷ en de «*De Overheidsinstanties nemen alle nodige (organisatorische, juridische en technische) maatregelen om de interoperabiliteit van de gegevens die zij bezitten te waarborgen, vanaf het ontwerp van hun processen, [zij] maken gebruik van interoperabele systemen die waar mogelijk gebaseerd zijn op nationaal of internationaal erkende normen*»¹⁸; de gegevens die zij bezitten zijn «*geïntegreerd (...) in interoperabele informatiesystemen, als omschreven in artikel C.II.17*»¹⁹;

¹⁷ Artikel C.II.9 van het ontwerp (het *betreft* een "strategisch doel" van data governance)

Over de aanneming van gemeenschappelijke standaarden zegt de memorie van toelichting het volgende :

« *Het stijgende volume aan gegevens en de ontwikkeling van het gebruik ervan brengt het risico met zich mee dat zich verschillende modellen ontwikkelen, waarvan het naast elkaar bestaan leidt tot een afname van de doelmatigheid van het beheer en een aanzienlijke stijging van de kosten.*

Het gebruik van gemeenschappelijke standaarden voor gegevensbeheer bevordert de interoperabiliteit en vergemakkelijkt het delen van gegevens tussen de verschillende betrokken partijen. Dit garandeert ook de consistentie, kwaliteit en compatibiliteit van de gegevens, wat essentieel is voor de integriteit en het effectieve gebruik ervan.

Om een efficiënt beheer te waarborgen en de kosten in verband met het beheer en het gebruik van gegevens te optimaliseren, moeten de Overheidsinstanties dan ook de voorkeur geven aan het gebruik van onderling gedeelde oplossingen. Het delen van de kosten verbonden met de ontwikkeling van nieuwe oplossingen maakt schaalvoordelen mogelijk en versnelt de "data"-transformatie». Het standaardiseren van de tools en de gegevensuitwisselingen vermijdt ook het overlappen van gegevens, wat de naleving van de veiligheidsbeginselen en het respecteren van de individuele rechten ten goede komt. Het delen van gemeenschappelijke oplossingen en standaarden voor data-architectuur maakt ook samenwerking mogelijk in het ontwikkelen van gemeenschappelijke competenties» (onderstreept door de Autoriteit).

¹⁸ Artikel C.II.17 van het ontwerp. Over de **interoperabiliteit** zegt de memorie van toelichting het volgende

« *Opdat gegevens kunnen worden gevaloriseerd, verspreid en uitgewisseld, begrepen en hergebruikt, moeten ze voldoen aan de interoperabiliteitsregels. Het is dus noodzakelijk dat de Overheidsinstanties interoperabele systemen opzetten om de hoogst mogelijke kwaliteit van gegevens te waarborgen.*

[...]

Deze operationele doelstelling loop voorop op de toekomstige toepassing van de verordening voor een interoperabel Europa (momenteel nog Voorstel voor een Verordening van het Europees Parlement en de Raad tot vaststelling van maatregelen voor een hoog niveau van interoperabiliteit van de overheidssector in de Unie, COM (2022) 720 final, aangenomen op 18 november 2022). Naast de kwestie van de interoperabiliteit zelf, bereiden overheden hun deelname voor aan "data spaces". In het kader van de Europese datastrategie verwijzen "data spaces" [...] » (onderstreept door de Autoriteit).

¹⁹ Artikel C.III.16, 2de lid, 3° van het ontwerp.

- Een van de operationele doelstellingen die aan autoriteiten zijn toegewezen in het kader van datagovernance, is dat ze dienen ²⁰ « **over te gaan tot de gegevensintegratie** [21]»²², met andere woorden, centraliseren/concentreren ; het ontwerp stelt dat «**overheidsinstanties gegevens integreren die geïntegreerd kunnen worden** »^{23, 24} ;
- Overheidsinstanties moeten **referentiegegevens**²⁵ identificeren **en het gebruik ervan bevorderen**, en ook «*ervoor zorg(en) dat die gegevens in voorkomend geval gedeeld kunnen worden* »²⁶ ;
- «*De digitale governance heeft tot doel de samenhang en **de mutualisatie** van het Brussels digitaal ecosysteem te optimaliseren* »²⁷, dat in het ontwerp wordt gedefinieerd als «*het netwerk van stakeholders, partners, IT-infrastructuren, informatiesystemen die met elkaar verbonden zijn in een digitale ruimte, evenals netwerken voor elektronische communicatie via kabel en radio in het Brussels Hoofdstedelijk Gewest* »²⁸.

15. Welnu, het lijkt geen twijfel dat het vergemakkelijken van gegevensverwerking en het circuleren van gegevens tussen overheidsinstanties zoals voorzien in het ontwerp, in het bijzonder door de concentratie van gegevens en hun verwerkingsmethoden, voor alle doeleinden samen, een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen : zonder afbreuk te doen aan latere ontwikkelingen, **moeten de noodzaak en evenredigheid ervan eerst worden aangetoond en moeten de passende waarborgen tegen de risico's voor de rechten en vrijheden van de betrokkenen worden bepaald en benadrukt.**²⁹ De Autoriteit herinnert er overigens aan dat het

²⁰ De formulering van de bepaling in ontwerp is evenwel ongewoon. In plaats van een eenvoudige verplichting voor de autoriteiten te formuleren, staat er: «*In het kader van hun taken verbinden de Overheidsinstanties zich ertoe*» (onderstreept door de Autoriteit).

²¹ Zie voetnoot 13

²² Artikel C.II.6^o van het ontwerp.

²³ Artikel C.II.19 van het ontwerp.

²⁴ De memorie van toelichting verduidelijkt dat:

«*Deze doelstelling is erop gericht dat Overheidsinstanties gegevens uit verschillende oorspronkelijke bronnen kunnen combineren om gebruikers één uniforme overzichtswaargave te bieden*» (onderstreept door de Autoriteit).

²⁵ Zie voetnoot 7.

²⁶ Artikel C.II.20 van het ontwerp

²⁷ Artikel VI.2, § 1, ¹ste lid van het ontwerp.

²⁸ Artikel A.III.1.46) van het ontwerp.

²⁹ In **zijn advies 1/2023 van 13 januari 2023 concernant la proposition de règlement pour une Europe Interopérable**, herinnert de Europese Toezichthouder voor Gegevensbescherming er in het kort aan (de Autoriteit vertaalt) :

«*De Europese Toezichthouder voor gegevensbescherming (EDPS) erkent de potentiële voordelen van een grotere interoperabiliteit in de overheidssector en verwelkomt de inspanningen van de Commissie om het proces in deze richting te organiseren en te institutionaliseren. De EDPS wijst er echter ook op dat de interoperabiliteit van netwerken en informatiesystemen in alle sectoren van het openbaar bestuur en op alle bestuursniveaus een van de meest fundamentele beginselen van gegevensbescherming in gevaar brengt, namelijk het doelbindingsbeginsel. Daarom is het van essentieel belang dat de risico's die ontstaan door het wegnemen van technische belemmeringen voor de uitwisseling van informatie in het proces grondiger worden onderzocht*» (vet toegevoegd en onderstreept door de Autoriteit).

Hof van Justitie hierover het volgende stelt «*benadrukt dient evenwel te worden dat de omstandigheid dat aan overheidsinstanties te weinig middelen worden toegekend, in geen geval een legitieme reden kan vormen die vermag te rechtvaardigen dat inbreuk wordt gemaakt op de door het Handvest gewaarborgde grondrechten*»³⁰.

B) Het CIBG (PARADIGM), een centrale en essentiële instelling voor gegevensverwerking

16. Het **CIBG** (« **Centrum voor Informatica voor het Brussels Hoofdstedelijk Gewest**») onlangs omgedoopt tot «**Paradigm**»³¹, blijkt **de centrale instelling te zijn voor gegevensverwerking** in het Brussels Hoofdstedelijk Gewest (de nieuwe naam «*Paradigm*» is in dit opzicht verhelderend). Het betreft een instelling van openbaar nut die is opgericht met artikel 27 van de wet van *21 augustus 1987 tot wijziging van de wet houdende organisatie van de agglomeraties en federaties van gemeenten en houdende bepalingen betreffende het Brusselse Gewest*, die een eigen rechtspersoonlijkheid heeft en dagelijks wordt geleid door een leidende ambtenaar en een adjunct-leidende ambtenaar aangesteld door de Brusselse Hoofdstedelijke Regering. Het CIBG (PARADIGM) lijkt te ressorteren onder een minister (*a priori*, de aanvrager)³².
17. **Het ontwerp illustreert overvloedig de centrale en onvermijdelijke rol van het CIBG (PARADIGM) op alle gebieden van gegevensverwerking in de Brusselse publieke rechtsorde:** verwerkingen verrichten, infrastructuur, technologische keuzes, expertise, enz.) Het ontwerp kent meer concreet de volgende taken toe aan het CIBG (PARADIGM) (vet toegevoegd door de Autoriteit in de citaten hierna):
- Het CIBG (PARADIGM) «*wordt belast met de operationalisering en de inwerkingstelling van de internetsites die het Brusselse webecosysteem vormen*»³³ ;

In overweging 7 van hetzelfde advies benadrukt hij nog eens het volgende (de Autoriteit vertaalt) :

«*De EDPS herinnert eraan dat een technologische omgeving met informatiesystemen die onderling niet interoperabel zijn, veel bescherming heeft geboden tegen de schending van een van de fundamentele beginselen van gegevensbescherming, namelijk het doelbindingsbeginsel. Hoewel onvoldoende interoperabiliteit geen bewuste technische maatregel is om rechtmatige verwerking te garanderen, is het decennialang effectief gebleken. Technische onuitvoerbaarheid heeft het moeilijker gemaakt om grote hoeveelheden gegevens te gebruiken voor andere doeleinden dan waarvoor ze verzameld zijn. Het opheffen van deze technische belemmering vereist meer aandacht voor wettelijke beperkingen en zou ook kunnen zorgen voor nieuwe waarborgen om rechtmatige verwerking en verantwoording te garanderen*» (vet toegevoegd door de Autoriteit).

³⁰ HvJ-EU, (Grote kamer), arrest van 1 augustus 2022, *OT tegen Vyriausioji tarnybinės etikos komisija*, zaak C-28/08, overweging 89.

³¹ Zie <https://paradigm.brussels/fr/paradigm/base-legale-du-cirb>, laatst geraadpleegd op 2 A la connaissance de l'Autorité, l'avant-projet d'ordonnance relatif à Paradigm et qui a donné lieu à l'avis standard de l'Autorité lors de sa séance du 8 septembre 2023 n'a pas encore été voté.

³² «Paradigm ondersteunt via de uitoefening van zijn taak de voogdijminister voor informatica en digitalisering», zie <https://be.brussels/nl/over-het-gewest/structuur-en-organisatie/overzicht-van-de-overheden-en-instellingen-het-gewest/paradigm>, laatst geraadpleegd op 6/10/2023.

³³ Met andere woorden, het aantal en de voorwaarden worden bepaald door de Regering, het Verenigd College en het College. Zie artikel B.I.5, 2de lid van het ontwerp.

- Overheidsinstanties **moeten gegevens uit authentieke bronnen verzamelen bij de** integrator van het Brussels Dienstenplatform³⁴. Dit **platform** is opgezet binnen het **CIBG (PARADIGM)** en het CIBG (PARADIGM) is de «*beheerder*»³⁵ ervan. Hieronder vallen «*het technisch bestuur van het Platform, in het bijzonder met betrekking tot de infrastructuur, de veiligheid, het beheer of de beschikbaarheid van de informatie of, in voorkomend geval, de gegevens*» ; «*in voorkomend geval, de controle van de elektronische identificatieschema's of certificering in de zin van Verordening (EU) nr. 910/2014 (EIDAS)*» ; «*In voorkomend geval, de aanduiding van een onafhankelijke dienstverlener als derde vertrouwenspersoon*» ; «*het verlenen van advies en bijstand aan de Overheidsinstanties die het Platform gebruiken en de coördinatie met hun vertegenwoordigers, met name wat betreft de opleiding over het gebruik van het Platform, het beheer van specifieke projecten of enig ander relevant gebied in verband met het gebruik van het Platform; het evolutief ontwerp van de architectuur van het Platform overeenkomstig de meerjarige gegevensstrategie en de jaarlijkse actieplannen, als bedoeld in artikel C. VI.5, §2*»³⁶ ;
- Het CIBG (PARADIGM) (als dienstenintegrator) kan **verzoeken om een gegevensbron aan te wijzen** als authentieke bron³⁷ ;
- De diensten die via dit platform worden aangeboden zijn toegankelijk op basis van een «*toetredingsovereenkomst*» tussen het CIBG (PARADIGM) en de gebruiker van het platform³⁸, en het is de beheerder van het platform (het CIBG (PARADIGM)) die verantwoordelijk is voor «*de vaststelling van het documentaire basiskader en een toetredingsovereenkomst die het gebruik ervan mogelijk maken, met name met betrekking tot de formaliteiten of modaliteiten voor toetreding tot het Platform en gebruik van zijn diensten* [...]»³⁹ ;
- **In principe moet elke uitwisseling van gegevens met een Brusselse overheidsinstantie via het CIBG (PARADIGM) verlopen.** Op die manier verloopt «*elke administratieve gegevensdeling* [⁴⁰] (...) *via het Brusselse Integratiecentrum, bij gebrek aan specifieke wetgeving die de betrokken administratieve deling specifiek organiseert*»⁴¹

³⁴ Zie de artikelen C.II.3, §2, 2de lid en C.IV.12, §2 van het ontwerp.

³⁵ Artikel C.V.1, §§1 en 2 van het ontwerp.

³⁶ Zie artikel C.V.2 van het ontwerp.

³⁷ Artikelen 15, § 2, 1^o van het ontwerp:

³⁸ Zie artikel C.V.3 van het ontwerp.

³⁹ Zie artikel C.V. 2, eerste lid, ^{3o}, van het ontwerp.

⁴⁰ Zie voetnoot 12.

⁴¹ Artikel C.IV.5, §1 van het ontwerp.

(onderstreept door de Autoriteit), deze regel geldt ook, bij gebrek aan andersluidende wettelijke of reglementaire bepalingen, voor de uitwisseling van gegevens tussen overheidsinstanties en "**derde overheidsinstanties**"⁴²» (d.w.z. federale of andere, en zelfs internationale)⁴³⁴⁴. Wanneer gegevens administratief worden gedeeld met een derde instantie, moet de «*Brusselse dienstintegrator*»⁴⁵ ook controleren of de nodige toestemmingen zijn verkregen voordat het administratief delen wordt toegestaan⁴⁶. Het is via het «*Integratiecentrum*» dat het CIBG (PARADIGM) **de administratieve uitwisseling technisch ondersteunt**⁴⁷ ;

- Het CIBG (PARADIGM) is verantwoordelijk voor het organiseren van **data-altruïsme**⁴⁸ ;
- Het CIBG biedt diensten aan die bestaan uit de **Gegevenscatalogus**⁴⁹, het **Open portaal voor openbare gegevens**, dat «(...) *de voor hergebruik beschikbare gegevens aan(biedt)*»⁵⁰ en het« **Centrum voor gegevensanalyse en gegevensverwerking** »⁵¹ ;
- Als Brussels dienstenintegrator gaat het CIBG meer bepaald over «*tot de **administratieve deling van geïntegreerde gegevens op verzoek van de ontvangende Overheidsinstantie***», wat inhoudt dat de gegevens worden geïntegreerd in het CIBG (PARADIGM) zelf; en het CIBG (PARADIGM) kan «*voor de deelnemende overheidsdiensten **nuttige applicaties ontwikkelen voor de uitwisseling en/of de integratie van gegevens die bewaard worden in de databanken***»⁵² ;
- Het Brussels gegevensplatform omvat ook de **hulp- en ondersteuningsdiensten** bedoeld in artikel 7 van de data governance verordening, waarbij het CIBG (PARADIGM) anders gezegd, een bevoegde instantie is zoals bedoeld in deze bepaling⁵³ ;

⁴² Zie voetnoot 2.

⁴³ Zie voetnoot 2

⁴⁴ «*In dit geval wordt de administratieve deling uitgevoerd via het Brusselse Integratiecentrum en, indien van toepassing, vormt het Brusselse Integratiecentrum het doorgeefluik tussen de Overheidsinstanties en de andere integratoren ten dienste van de derde overheidsorganen*», artikel C.IV.5, §2, 1ste lid van het ontwerp.

⁴⁵ Hetzij volgens artikel A.III.A.1.102) van het ontwerp «*instelling aangewezen in artikel C.V.*». Volgens artikel C.V.7, is het Integratiecentrum opgericht binnen het Brussels dataplatform. Het is artikel C.V.8. van het ontwerp dat bepaalt dat «*het CIBG wordt aangewezen als Brusselse dienstenintegrator in het kader van zijn beheer van het Integratiecentrum*». **Het ontwerp moet bijgevolg op dit punt worden aangepast.**

⁴⁶ Artikel C.IV.5, §2 , 2de lid, van het ontwerp

⁴⁷ Zie artikel C.V.7 van het ontwerp.

⁴⁸ Zie artikel C.I.33 van het ontwerp.

⁴⁹ Zie artikel C.V.9 van het ontwerp.

⁵⁰ Zie artikel C.V.10 van het ontwerp.

⁵¹ Zie artikel C.V.11 van het ontwerp.

⁵² Zie artikel C.V.8 van het ontwerp.

⁵³ Zie artikel C.V.13 van het ontwerp.

- Het **CIBG (PARADIGM)** bevindt zich verder binnen de «*governance-organen*», die door het ontwerp worden opgericht. Zo wordt het **Digitaal Secretariaat** opgericht binnen het CIBG (PARADIGM)⁵⁴. Het CIBG (PARADIGM) verzorgt het secretariaat voor het Digitaal Coördinatiecomité en het Validatiecomité van de Digitale Architectuur.

Het **Validatiecomité van de Digitale Architectuur** is met met name «*belast met de governance van de gewestelijke digitale architectuur met het oog op samenhang en mutualisatie*»⁵⁵.

Het **Bureau voor Digitale Aankopen** wordt opgericht binnen het CIBG (PARADIGM) Het CIBG (PARADIGM) «*verleent alle operationele, juridische of technische ondersteuning aan de Overheidsinstanties*» «*bedoeld in artikel C.I.1 met betrekking tot de procedure van de overheidsopdrachten voor digitale aangelegenheden*»⁵⁶; het is, in het bijzonder bevoegd om de nodige hulp te bieden aan elke overheidsinstantie bij elk wederzijds digitaal aanbestedingsproces dat gevolgen kan hebben voor het Brusselse digitale ecosysteem; het stelt «*de relevante criteria voor de mutualisatie van digitale overheidsopdrachten*» voor aan de Regering, het brengt adviezen uit over ontwerpen die voorgelegd worden aan de digitale zelfevaluatietoets; het brengt *adviezen* uit op eigen initiatief of op verzoek van het Validatiecomité voor de Digitale Architectuur, het Digitale Coördinatiecomité en het Gegevensbureau⁵⁷. Het Digitaal Coördinatiecomité «*neemt strategische beslissingen over alle projecten die voorgelegd worden aan de digitale zelftoets*» die vooraf geanalyseerd zijn door alle of sommige adviesorganen en brengt zelf advies uit over het onderwerp⁵⁸; het kan ook op eigen initiatief of op verzoek advies uitbrengen⁵⁹;

Het **Gegevensbureau** wordt opgericht binnen het CIBG (PARADIGM)⁶⁰. In het bijzonder ondersteunt en stuurt het, in overleg met het Comité voor gegevensbeheer, het Comité voor gegevensbeheer, het stelt adviezen op uit eigen beweging of op verzoek en het heeft een taak als «*van gegevenscoördinator, voorafgaand aan de validatie door het Comité voor gegevensbeheer, met name door [...] de organisatie van een kader voor het beheer van de interoperabiliteit*», het heeft als taak «*het bieden van ondersteuning bij de uitvoering van de verplichtingen van het Wetboek op het gebied van gegevensbeheer, met name via [...] het*

⁵⁴ Zie artikel V.VI.4 van het

⁵⁵ Zie artikel 6.VI.6. van het ontwerp.

⁵⁶ Artikel C.VI.8 van het ontwerp

⁵⁷ Artikel C.VI.9 van het Ontwerp.

⁵⁸ Zie artikel 11.VI.11 van het ontwerp.

⁵⁹ *Ibid.*

⁶⁰ Artikel C.VI.17 van het ontwerp:.

voorstellen van richtlijnen, normen, kaders en richtsnoeren die door het Comité voor Gegevensbeheer moeten worden goedgekeurd», via «het bevorderen van interne beleidsinstrumenten bij de Overheidsinstanties betreffende gegevensbeheer in de zin van hoofdstuk 1 van titel 4 van boek C.III, met inbegrip van het beheer van de analysemodellen, algoritmen en systemen die gebruik maken van kunstmatige intelligentie in de zin van artikel C.III.18», verder heeft het nog de «opdracht om veranderingen op gang te brengen door a) praktijkgemeenschappen op te zetten, [...]», een taak ter «ondersteuning van Overheidsinstanties door deskundigen op het gebied van gegevensbeheer ter beschikking te stellen wanneer Overheidsinstanties niet over voldoende middelen beschikken»⁶¹. Het Gegevensbureau «staat onder de verantwoordelijkheid van een gegevenscoördinator» en zijn strategische doelstellingen worden vastgesteld door de «minister bevoegd voor het CIBG en de ministers bevoegd voor digitale aangelegenheden van het College en het Verenigd College»⁶².

Het CIBG (PARADIGM) maakt deel uit van de samenstelling van het **Comité voor Gegevensbeheer**⁶³ dat met name «de operationele doelstellingen van de Dienst voor Gegevensbeheer vaststelt», het CIBG (PARADIGM) (alweer) beoordeelt en valideert ook «de normen, goede praktijken en modellen die door de Gegevensdienst worden voorgesteld, met name op het gebied van interoperabiliteit», heeft als doelstelling «de operationaliteit van de bepalingen van het Wetboek waarborgen door overeenstemming te bereiken over alle punten die duidelijke verantwoordelijkheden vereisen, met name de aanwijzing in onderlinge overeenstemming van de identiteit van de Overheidsinstantie(s) die belast is/zijn met het beheer van een specifiek gegevensdomein»⁶⁴.

- Het CIBG (PARADIGM) «is belast met de oprichting **van het Brussels glasvezelnetwerk dat de glasvezelnetwerken van bepaalde Overheidsinstanties op het Brussels gewestelijk grondgebied bundelt**. In deze context duidt het CIBG een entiteit aan die verantwoordelijk is voor de taken» beschreven in het ontwerp⁶⁵. Voor wat dit Brussels glasvezelsnetwerk betreft, sluiten «de Overheidsinstanties met een glasvezelnetwerk (...) een overeenkomst met de aangewezen entiteit[...] en het CIBG waarin met name alle technische, operationele en financiële voorwaarden van taken worden vastgelegd» als opgesomd in het ontwerp⁶⁶ ;

⁶¹ Artikel C.VI.18 van het ontwerp.

⁶² Artikel C.VI.19 van het ontwerp.

⁶³ Zie artikel C.VI.14 van het ontwerp.

⁶⁴ Zie artikel C.VI.15 van het ontwerp.

⁶⁵ Artikel C.VI.24, § 1 van het ontwerp, getiteld «Brussels openbaar glasvezelnetwerk».

⁶⁶ Artikel C.VI.24, § 5 van het ontwerp.

- En tot slot, is het opnieuw het CIBG (PARADIGM) dat, in titel 3 van het ontwerp «*verantwoordelijk is voor het verzamelen, valideren, registreren, opslaan, bijwerken en beschikbaar stellen van de gegevens in de databank afkomstig uit authentieke bronnen Brussels UrbIS*» en is aangewezen als «*als beheerder van de databank Brussels UrbIS*»⁶⁷ die een belangrijke reeks categorieën geografische gegevens over het Brussels Hoofdstedelijk Gewest⁶⁸ bevat en met name de mogelijkheid biedt om geografische informatie te combineren, de geografische coördinaten van om het even welke plaats te achterhalen en gegevens uit te wisselen die kunnen worden gekoppeld aan Brussels UrbIS⁶⁹.

18. Bovendien moet, buiten het ontwerp om, in het positieve recht nog steeds het volgende worden benadrukt :

- **Het CIBG (PARADIGM) beheert het Brussels videobeschermingsplatform** (d.w.z. het platform voor het verzamelen van beelden en gegevens van bewakingscamera's) **en is ook lid van het Strategisch Comité**⁷⁰. Het is bevoegd «*voor het beheer van de juridische aspecten in verband met de werking van het Brusselse videobeschermingsplatform en van de technische aspecten in verband met de werking van het systeem voor het gedeelde gebruik van beelden en gegevens en voor het aankoopbeheer*»⁷¹ ;
- Tot slot beheert het CIBG (PARADIGM) de " IRISbox , «*het elektronische loket van het Brussels Hoofdstedelijk Gewest*», «*dat online gewestelijke en lokale diensten aanbiedt*» waar «*Burgers en bedrijven (...) 24/7 online documenten (kunnen) raadplegen en krijgen toegang tot interactieve formulieren om documenten aan te vragen*»⁷².

⁶⁷ Artikel 6 van Titel III van het ontwerp.

⁶⁸ Deze omvatten de namen van gemeenten en straten, huisnummers en busnummer, gebouwen afkomstig uit stedenbouwkundige vergunningen , ligplaatsen, de feitelijke en o rechtstoestanden en feitelijke toestanden voor al de hierboven vermelde gegevens , waaronder de «*verbindingen tussen adressen enerzijds en gebouwen, gebouwwunits, percelen, standplaatsen en ligplaatsen anderzijds*». Zie artikel 10 van Titel III van het ontwerp.

⁶⁹ Zie artikel 5 van Titel III van het ontwerp.

⁷⁰ Zie artikel 2, 12° van de Ordonnantie van 28 mei 2015 *tot oprichting van een instelling van openbaar nut waarin het beheer Gewest is samengebracht en tot oprichting van de Gewestelijke School voor de Veiligheids-, Preventie- en Hulpdienstberoepen - Brusafe*.

⁷¹ Zie artikel 10/9, § 2 van de in voetnoot 70 vermelde ordonnantie. De Autoriteit wijst er terloops op, hoewel zij zich niet uitspreekt over het onderwerp van deze ordonnantie, dat de aanwijzing van verantwoordelijkheden met betrekking tot de verwerking van persoonsgegevens in het kader van deze ordonnantie niet in overeenstemming is met de praktijk van de Autoriteit (zie overweging 166 e.v.).

⁷² Zie <https://irisbox.irisnet.be/irisbox/about>, laatst geraadpleegd op 06/10/2023. Volgens de algemene gebruiksvoorwaarden van IRISbox, «*Het huidige internetportaal is een initiatief van Paradigm, parastatale van categorie « A » opgericht krachtens artikel 27 van de wet van 21 augustus 1987 tot wijziging van de wet houdende organisatie van de agglomeraties en de federaties van gemeenten en houdende bepalingen betreffende het Brusselse Gewest, waarvan de maatschappelijke zetel gevestigd is te 1000 Brussel, Kunstlaan 21 » ; « Voor de website IRISbox is de verwerkingsverantwoordelijke het Centrum voor Informatica voor het Brussels Gewest. De sociale zetel is gevestigd in de Kunstlaan 21 te 1000, Brussel » (wat overigens niet duidelijk is met betrekking tot het "internetportaal" en de diensten die via IRISbox worden aangeboden (bijv. aanvragen van documenten bij lokale autoriteiten, uittreksels uit strafregisters, enz.).*

19. Nogmaals, het is overduidelijk dat het toekennen van al deze bevoegdheden aan één enkele instelling grote risico's met zich meebrengt voor de rechten en vrijheden van de betrokken personen. Nogmaals, **zonder afbreuk te doen aan latere ontwikkelingen, moeten eerst de noodzaak van een dergelijke centraliteit en de evenredigheid ervan worden aangetoond, en moeten passende waarborgen tegen risico's voor de rechten en vrijheden van betrokkenen worden vastgesteld en benadrukt.** In dit verband is het bijzonder belangrijk **om de verantwoordelijkheid van de verschillende betrokken entiteiten vast te stellen en in aanmerking te nemen**⁷³.

C) Een bepaalde patrimoniale zienswijze op gegevens met vage concrete gevolgen

20. Tot slot **lijkt het ontwerp vanuit conceptueel oogpunt de voorkeur te geven aan een patrimoniale visie die gericht is (of toegespitst is) op de gegevens in plaats van op de betrokken persoon** of de burger die de betrokken overheidsdienst ontvangt, **zonder dat de concrete gevolgen van een dergelijke benadering duidelijk naar voren komen**, in ieder geval wat betreft de verwerking van persoonsgegevens. Meer bepaald:

- Artikel C.II.7 van het ontwerp dat voorziet in een «*strategische doel*» voor het gegevensbeheer die «*de gegevens centraal stellen*», luidt als volgt : «*De Overheidsinstanties nemen processen aan die **de gegevens centraal stellen** in het beheer van hun taken van openbare dienstverlening en hun verplichtingen van algemeen belang, alsook in hun governance, **en die gegevens als volwaardige activa beschouwen*** »⁷⁴ (onderstreept door de Autoriteit). De memorie van toelichting spreekt van een «*nieuwe paradigma, waarin het gegeven centraal staat* », en stelt dat de gegevensgerichte aanpak overheden in staat stelt om van gegevensbeheer een prioriteit te maken «*met name door voorrang te verlenen aan krachtige en efficiënte tools, bijvoorbeeld om gegevens intern of extern te raadplegen, op te slaan of te beschermen*», waardoor «*de waarde van gegevens worden gemaximaliseerd door ze te gebruiken op een relevante en strategische manier* » ;
- Onder de operationele doelstellingen die aan overheidsinstanties zijn toegewezen in de context van gegevensbeheer, moeten zij ⁷⁵ « *hun gegevens valoriseren volgens hun prioriteiten* »⁷⁶; en «*om na te gaan over welke digitale middelen zij beschikken en welke zij moeten valoriseren, identificeren de Overheidsinstanties de digitale gegevenspartnerschappen*»⁷⁷

⁷³ Zie de overwegingen 166 e.v.

⁷⁴ Zie voetnoot 82, laatste citaat, over de identificatie van gegevens als activa.

⁷⁵ Zie voetnoot 20

⁷⁶ Artikel C.II.13° van het ontwerp.

⁷⁷ Zie voetnoot 15.

waarbij zij partij zijn »⁷⁸ ; « de valorisatie van de gegevens die de Overheidsinstanties bezitten heeft tot doel het beheer van gegevens **te organiseren als bronnen van waarde en als echte digitale activa** »⁷⁹; de valorisatie van gegevens is met name gebaseerd op de valorisatie van gebruiksgegevens⁸⁰; artikel C.III.10 van het ontwerp bepaalt dat de gegevens tot de volgende categorieën behoren «afhankelijk van hun **eigendomsstructuur**»; de overheden moeten een «**strategie voor de valorisatie** » van de gegevens bepalen als onderdeel van hun taken en verplichtingen⁸¹ ;

- Het ontwerp gaat ook over «**digitale partnerschappen**» en in de memorie van toelichting staat dat «dit begrip als enige bedoeling heeft om de Overheidsinstanties in staat te stellen om de juridische of bestuurlijke banden te kwalificeren die zij onderhouden **en die de valorisatie van gegevens als einddoel hebben** »⁸². In dit opzicht richt het ontwerp zich

⁷⁸ Artikel C.III.2, §1, 1^{ste} lid van het ontwerp.

⁷⁹ Artikel C.III.11 van het Ontwerp

⁸⁰ Zie voetnoot nr. 6 over de definitie over gegevensgebruik⁶.

⁸¹ Zie artikel C.II.14 van het Ontwerp. De memorie van toelichting verduidelijkt dat «Deze doelstelling is gericht op het erkennen van de potentiële waarde van de gegevens die worden gehouden door een Overheidsinstantie en op het bepalen van prioriteiten inzake gebruik en valorisering» (onderstreept door de Autoriteit).

⁸² Verder zegt de toelichting nog:

« Op dit moment weten Overheidsinstanties vaak niet welke gegevens ze houden en op welke manier de verwerking van deze gegevens hen niet alleen in staat zou kunnen stellen om hun openbare dienst opdrachten of hun verplichtingen van algemeen belang meer efficiënt uit te voeren, maar ook hoe die verwerking van belang kan zijn voor andere Overheidsinstanties, de publiekrechtelijke lichamen van het land of ook de sociaal-economische actoren.» (onderstreept door de Autoriteit).

« [...] de Overheidsinstanties stap voor stap moeten nagaan welke van de gegevens waarvan ze de houder zijn, van dien aard zijn om waarde te creëren en hoe deze gegevens kunnen worden gevaloriseerd» (onderstreept door de Autoriteit).

Elders stelt de memorie van toelichting dit:

« dat de valorisatie erop is gericht om bestaande gegevens zodanig te verrijken, te versterken of te verbeteren dat zij een bepaalde waarde krijgen. Dit voordeel kan onder meer een economisch voordeel zijn, in dit geval digitaal van aard De doelstellingen van een project van gegevensvalorisatie zijn zeer uiteenlopend en hangen af van het betrokken toepassingsgebied.

Door de valorisatie van gegevens zullen Overheidsinstanties gegevens omzetten in echte publieke goederen die zullen bijdragen tot de verbetering van de efficiëntie van hun diensten en de uitvoering van hun opdrachten. Tot vandaag genereren veel Overheidsinstanties gegevens zonder zich bewust te zijn van de waarde ervan. Dit gebrek aan kennis van het digitale erfgoed van Brussel kan leiden tot gemiste kansen en financiële verliezen (bijvoorbeeld door onwetendheid over de verwerkingen die onderling gedeeld kunnen worden) of in het geding komen van de aansprakelijkheden na het uitlekken van onvoldoende beveiligde gegevens, omdat geen rekening werd gehouden met het belang of de gevoeligheid ervan.

Titel 3 heeft als doel om de Overheidsinstanties toe te staan om hun capaciteit te vergroten om oplossingen tot stand te brengen op basis van de gegevens waarover zij beschikt of zou kunnen beschikken. In dit kader moeten de Overheidsinstanties een probleemoplossende aanpak hanteren, op basis van data.

De Overheidsinstanties worden aangemoedigd om te investeren in de creatie van processen, competenties en hulpmiddelen om hun gegevens beter te valoriseren.

[...]

«

Op theoretisch vlak kan worden opgemerkt dat de gegevensvalorisatie diverse vormen kan aannemen. De rechtsleer onderscheidt bijvoorbeeld (zie in dit verband L.-D., Benyayerd, S., Chignard, Datanomics, FYP Editions, Parijs, p.49):

- 1° « wanneer de gegevens worden doorverkocht door degenen die ze verzamelen of aggregeren, nemen ze de vorm aan van een grondstof.
- 2° Wanneer ze worden gebruikt zonder vermarkting, bijvoorbeeld om de kosten te verlagen of de inkomsten te verhogen, nemen ze de vorm aan van een hefboomwerking
- 3° wanneer ze een strategisch wapen zijn om een concurrentiepositie te verdedigen of te veroveren, krijgen ze de waarde van activa. »

op de valorisatie van gegevens **zonder echter concreet te illustreren wat dit inhoudt, met uitzondering van de volgende drie voorbeelden**: het geval van «*administratieve deling*», van «*hergebruik*» of nog «*mededeling*», zijn de enige zeer specifieke gegevensvalorisatie- en -uitwisselingsactiviteiten die onder het wetboek vallen en wettelijk geregeld zijn⁸³.

21. In dit verband **benadrukt de Autoriteit van meet af aan dat de valorisatie van gegevens in de zin van het ontwerp op zich geen specifiek verwerkingsdoel vormt**. Met andere woorden, dit doel van het ontwerp alleen kan niet de basis zijn voor de verwerking van persoonsgegevens. De Autoriteit wijst er ook op dat als het gaat om de verwerking van persoonsgegevens, **persoonsgegevens niet los kunnen worden gezien van het doel waarvoor ze worden verwerkt en, meer in het algemeen, van de regels die gelden voor de verwerking ervan. Bovendien kan valorisatie per definitie niet voortvloeien uit een onrechtmatige handeling (in dit geval gegevensverwerking die niet voldoet aan de AVG)**.
22. Ten tweede is de Autoriteit van mening dat **duidelijk moet worden aangegeven welke gevolgen deze doelstelling van valorisatie heeft voor de verwerking van persoonsgegevens, welke mogelijke risico's dit met zich meebrengt voor de rechten en vrijheden van de betrokkenen en welke maatregelen zijn genomen om deze risico's te beperken**. Op dit punt **dient de aanvrager meer fundamenteel na te denken over de toegevoegde waarde van het gebruik van een begrip als valorisatie en de conceptuele consequenties die hij daaraan verbindt**, indien dit begrip in concreto beperkt zou blijven tot het verwijzen, met andere woorden, naar de vervulling door een overheidsinstantie van haar taak van algemeen belang of haar wettelijke

In het geval van Overheidsinstanties hebben de meeste gevallen van valorisatie betrekking op de totstandbrenging van hefboomen. De gegevens gehouden door de Overheidsinstanties worden met name en hoofdzakelijk gebruikt en gedeeld met het oog op:

- 1° het nemen van betere beslissingen en het verlagen van de werkingskosten van de overheid;*
- 2° het aanbieden van betere of nieuwe diensten aan de burgers.*

Men mag echter niet vergeten dat de door de Overheidsinstanties geproduceerde gegevens door privé-operatoren gebruikt kunnen worden voor andere vormen van valorisatie.

Het doel is dus ten minste tweeledig:

- 1° het mogelijk maken van een beter intern beheer van openbare diensten en verplichtingen van openbaar belang van Overheidsinstanties, door een betere valorisatie van gegevens. Het identificeren van de gegevens die een Overheidsinstantie bezit, zal haar toestaan om haar interne processen en haar relatie met haar burgers te optimaliseren, de gegevens beter te beveiligen en het daaruit voortvloeiende vertrouwen te vergroten,*
- 2° het mogelijk maken van echte gegevensdeling in het kader van hergebruik of tussen Overheidsinstanties (open data/hergebruik van beschermde gegevens of toepassing van de "once only") door een beter intern beheer van gegevens die klaar zijn voor gebruik door andere Overheidsinstanties of belangstellende marktdeelnemers. De beginselverklaring zal het mogelijk maken om de grondslagen te leggen (metadata en referentiegegevens) van wat de Gegevenscatalogus van het Brussels Gegevensplatform vormt (zie boek B.V.) »(onderstreept door de Autoriteit).*

⁸³ Er is ook sprake van een digitaal partnerschap wanneer overheidsinstanties besluiten om «*bepaalde tools of ook bepaalde competenties of functies onder elkaar te poolen*», bijvoorbeeld «*een project voor het poolen van gegevens betreffende een intelligent grondgebied, dat betrekking kan hebben op digitale infrastructuren zoals telecommunicatienetwerken, hostingcentra of gegevensverwerkingsplatforms voor een specifiek domein (mobiliteit, landbouw, grondgebruik, enz.)* » (?).

verplichtingen. De nieuwigheid van het ontwerp in het Brusselse rechtssysteem moet worden omschreven, net als de impact ervan op de rechten en vrijheden van de betrokken personen.

II.1.3. Algemene opmerkingen over het ontwerp

23. Op basis van de bovenstaande beschouwingen moeten de volgende drie algemene opmerkingen worden gemaakt.
24. **Ten eerste**, overeenkomstig haar constate adviespraktijk, herinnert de Autoriteit eraan dan in het kader van een verwerking die een **aanzienlijke inmenging in de rechten en vrijheden van de betrokkenen** tot gevolg heeft, de Autoriteit van mening is dat krachtens artikel 22 van de Grondwet, gelezen in combinatie met artikel 8 van het EVRM en artikel 6, lid 3, van de AVG, een norm van wettelijke rangorde moet bepalen onder welke omstandigheden een gegevensverwerking toegelaten is. Overeenkomstig het legaliteitsbeginsel moet deze wetgevingsnorm in ieder geval de essentiële elementen van de verwerking vastleggen. Wanneer de verwerking van gegevens een bijzonder ernstige inmenging vormt in de rechten en vrijheden van de betrokkenen, zoals in het onderhavige geval, is het noodzakelijk dat de volgende essentiële elementen door de wetgever worden vastgesteld: het (de) specifieke doeleinde(n)⁸⁴ uit de lezing waarvan men reeds kan opmaken welke gegevensverwerkingen voor de verwezenlijking ervan zullen plaatsvinden, de identiteit van de verwerkingsverantwoordelijke(n) (indien dit reeds mogelijk is), de (categorieën van) gegevens die nodig zijn voor het verwezenlijken van dat (die) doeleinde(n), de bewaartermijn van de gegevens, de categorieën van betrokkenen van wie de gegevens zullen worden verwerkt, de (categorieën van) ontvangers aan wie de gegevens zullen worden meegedeeld, de omstandigheden waarin zij zullen worden meegedeeld, en de eventuele beperking van verplichtingen en/of rechten bedoeld in de artikelen 5, 12 tot en met 22, en 34 van de AVG.
25. In dit geval moet het ontwerp, **gezien de reikwijdte ervan, in principe worden gelezen in samenhang met het wetgevingskader dat de taken en verplichtingen van de betrokken overheidsinstanties regelt**. Met andere woorden, in verschillende gevallen, bijvoorbeeld met betrekking tot de uitwisseling van gegevens tussen overheidsinstanties, kan het ontwerp op zich geen rechtsgrondslag vormen voor de verwerking van persoonsgegevens.
26. **Ten tweede**, gezien de zeer talrijke verbanden tussen het ontwerp en de regels inzake gegevensbescherming (het ontwerp bevat regels over gegevensclassificatie, rechtsmiddelen, risicoanalyse, verantwoordelijkheden, informatiebeveiliging, naleving, traceerbaarheid en de verantwoordelijkheden van overheidsinstanties, correctie van gegevens, enz.), het feit dat het Ontwerp een lex a posteriori van wettelijke rangorde is, en het feit dat de AVG de lidstaten in

⁸⁴ Zie ook artikel 6.3. van de AVG.

verschillende opzichten speelruimte laat, met name met betrekking tot gegevensverwerking in de overheidssector, **is de Autoriteit van mening dat in een algemene bepaling moet worden gespecificeerd dat het ontwerp de AVG onverlet laat en niet kan worden gelezen als een beperking van de rechten van betrokkenen of de verplichtingen van de verwerkingsverantwoordelijke.**

27. **Ten derde** betreft de Autoriteit dat de aanvrager geen effectbeoordeling van het ontwerp heeft uitgevoerd. Zij is van mening dat **een ontwerp met een dergelijke ambitie⁸⁵ vergezeld moet gaan van een effectbeoordeling die met name ingaat op de algemene bezorgdheid die de Autoriteit zojuist heeft uitgesproken** (zie met name de overwegingen 15, 19, 21 en 22 van dit advies). In dit geval bemoeilijkt het ontbreken van een dergelijke effectbeoordeling het inzicht in de ambities en de reikwijdte van het ontwerp aanzienlijk. De Autoriteit is van mening dat een dergelijke analyse noodzakelijk is met het oog op de organisatie van een doeltreffend parlementair debat over de elementen van het ontwerp die betrekking hebben op de verwerking van persoonsgegevens. De Autoriteit wijst erop dat, in overeenstemming met artikel 23 van de WVG, deze effectbeoordeling de betrokken verwerkingsverantwoordelijken (op zijn minst het CIBG/PARADIGM) niet zal vrijstellen van het uitvoeren van hun eigen effectbeoordelingen op het gebied van gegevensbescherming in overeenstemming met artikel 35 van de AVG.

II.2. OPENBAARHEID VAN BESTUUR

II.2.1. Passieve openbaarheid en belang

28. Artikel artikel B.I.16, § 3 van het ontwerp stelt het volgende «*voor bestuursdocumenten die informatie bevatten over een met naam genoemde of identificeerbare natuurlijke persoon, wanneer deze informatie een beoordeling of een waardeoordeel vormt ten aanzien van deze persoon of wanneer ze*

⁸⁵ Naast bovenstaande beschouwingen merkt de Autoriteit op dat de paradigmaverschuiving die het ontwerp teweegbrengt ook verband houdt met de naleving van de AVG. De Memorie van Toelichting verduidelijkt als volgt:

« *Het implementeren van dit soort governance biedt ook de kans om over te stappen van een "task-centric" naar een "data-centric" model, teneinde de uitwisseling van informatie binnen de overheidsdiensten en dus tussen alle bedrijfsprocessen te vergemakkelijken. Met andere woorden: het implementeren van een goede governance en architectuur voor data- en informatiesystemen kan de manier zijn om een grote kwalitatieve sprong voorwaarts te maken inzake het leveren van een betere dienstverlening aan gebruikers, het verbeteren van de efficiëntie door het rationaliseren van de kosten en het voldoen aan de eis van de AVG die het lastigst is om te halen: privacy by design* ».

Er wordt ook gewezen op de verbetering van de gegevenskwaliteit als gevolg van de voorgestelde nieuwe aanpak en de daarmee samenhangende kostenbesparingen: de gekozen aanpak «*levert het een aanzienlijk rendement op, dit in tegenstelling tot een aanpak van pure naleving, die alleen maar geld kost. Een dergelijke aanpak heeft een dubbel voordeel: ten eerste levert hij de overheidsdienst structureel een zeer groot aandeel van de naleving op met een minimum aan specifieke uitgaven voor de AGV, en ten tweede brengt hij een verandering teweeg die makkelijker op gang te brengen is omdat ze positief bedoeld is, in tegenstelling tot een aanpak van naleving die over het algemeen een verandering onder dwang impliceert* ».

En verder :«*Instappen in dergelijke systeemaanpak, die een combinatie vormt van wendbaarheid, een cultuur van vertrouwen en data governance, betekent het volledig integreren van het principe dat ons het belangrijkste lijkt in de PbD[1] van Ann Kavoukian: "full functionality – Positive-Sum, not Zero-sum »[(« A. BEELEN (dir.), La protection des données pour les institutions publiques, Anthemis, Limal, 2020, p./229-230 »)]* ».

betrekking heeft op een gedrag van deze persoon waarvan het ruchtbaar maken aan die persoon kennelijk nadeel kan berokkenen, is vereist dat de aanvrager een belang aantoon» (onderstreept door de Autoriteit).

29. Met andere woorden, in gevallen waarin andere persoonsgegevens worden geraadpleegd, hoeft de aanvrager geen belang aan te tonen.
30. « *Met betrekking tot het doel en de (categorieën) gegevens in kwestie vestigt de Autoriteit de aandacht van de aanvragers op het feit dat toegang tot persoonsgegevens over het algemeen een afweging van de betrokken belangen vereist en in elk geval een afweging van het doel (belang) dat door de betrokken aanvrager wordt nagestreefd en dat van de wetgeving betreffende de toegang in kwestie. Of dit evenwicht nu wordt bereikt door regelgeving (actieve openbaarheid) of in concreto op basis van individuele verzoeken of in ieder geval voorwaardelijke toegang tot informatie (passieve openbaarheid). De Autoriteit heeft deze principes ook, mutatis mutandis, in herinnering gebracht en toegelicht in de overwegingen 15 tot 22 van haar advies nr. 102/2020 van 19 oktober 2020 over een ontwerpbesluit van de Brusselse Hoofdstedelijke Regering tot wijziging van het Besluit van de Brusselse Hoofdstedelijke Regering van 25 april 2019 tot bepaling van de vorm en van de procedures voor de bekendmaking en de terbeschikkingstelling van de beslissingen, genomen door het college van burgemeester en schepenen, de gemachtigde ambtenaar en de Regering inzake stedenbouwkundige vergunningen, verkavelingsvergunningen en stedenbouwkundige attesten*» ((vet toegevoegd door de Autoriteit in dit advies)⁸⁶.
31. Bijgevolg⁸⁷, en rekening houdend met het feit dat het krachtens artikel 86 van de AVG de taak van de nationale wetgeving is om het recht van het publiek op toegang tot officiële documenten te verzoenen met het recht op bescherming van persoonsgegevens krachtens de AVG, is de Autoriteit van mening dat artikel B.I.16., § 3 van het ontwerp moet worden aangepast om ervoor te zorgen, dat, onverminderd een norm van wettelijke rangorde die voorziet in vrije en onvoorwaardelijke toegang van het publiek tot de betrokken documenten, om toegang te krijgen tot een administratief document dat persoonsgegevens bevat, het doel (legitiem, specifiek, enz.) van het beoogde gebruik (verwerking) van de gegevens, moet rechtvaardigen, wat in sommige gevallen gelijk kan staan aan de eis dat hij een legitiem belang rechtvaardigt.
32. Gelet op de grote verscheidenheid aan documenten en informatie die betrokken zijn bij passieve openbaarheid door de overheid, volstaat het niet, om de betrokken rechten en vrijheden te verzoeken met de overheidsinstantie waarbij een verzoek wordt ingediend, om een belang van de verzoeker te eisen enkel wanneer de betrokken informatie een beoordeling of waardeoordeel « *inhoudt met*

⁸⁶ Advies nr. 167/2022 , overweging 25.

⁸⁷ Zie ook overwegingen 12-14 van het advies 131/2023.

betrekking tot [de betrokken] persoon [of] wanneer zij betrekking heeft op gedragingen van deze persoon waarvan de openbaarmaking hem of haar duidelijk schade zou kunnen berokkenen ».

II.2.2. Gegevensmededeling per e-mail

33. Artikel B.I.17, § 4, van het ontwerp bepaalt dat na een verzoek om toegang tot een administratief document of tot milieu-informatie *«de aanvrager aangeeft op welke manier hij kennis wenst te nemen van het document of van de milieu-informatie. Bij ontstentenis van deze precisering gaat de voorkeur uit naar de verzending van een afschrift per e-mail»* (onderstreept door de Autoriteit).
34. Afhankelijk van de betrokken gegevens kan dit communicatiemiddel echter ongeschikt zijn vanuit het oogpunt van informatiebeveiliging. De Autoriteit heeft al benadrukt dat gevoelige gegevens niet via e-mail mogen worden uitgewisseld, en heeft zich al uitgesproken over de in dit verband te nemen voorzorgsmaatregelen. In de overwegingen 25-27 van haar advies 106/2022 van 3 juni 2022 *betreffende een ontwerpbesluit van de Waalse Regering tot wijziging van het Waalse Wetboek van Sociale Actie en Gezondheid met betrekking tot gezondheidsbevordering, inclusief preventie, in het Waals Gewest (CO-A-2022-090)*, verduidelijkte de Autoriteit het volgende:

« Het is de verantwoordelijkheid van de [verwerkingsverantwoordelijke] om procedures en een communicatiekanaal in te stellen die een beveiligingsniveau bieden dat past bij de aard van de doorgegeven gegevens.

In dit geval vereisen de gegevens betreffende de gezondheid een hoog niveau van vertrouwelijkheid. Naast de in de normen voor informatiebeveiliging opgesomde algemene maatregelen (bijvoorbeeld de normen ISO 27001, 27002, 27701), zouden met name, om een correct niveau van vertrouwelijkheid in de e-mailcommunicatie te bereiken, maatregelen kunnen worden getroffen met betrekking tot zowel het transmissiekanaal als het bericht (en de eventuele bijlagen) zelf, bijvoorbeeld door middel van (niet exhaustief):

- *het gebruik van een online uitwisselingsplatform met veiligheidsnormen overeenkomstig de stand van de techniek . Op internet is het gebruik van het TLS protocol in een versie gelijk aan of hoger dan versie 1.2 een goede praktijk;*
- *een encryptiesoftware die de informatie voor iedereen onbegrijpelijk maakt die niet over de nodige informatie beschikt voor de decryptie (de sleutel), zoals de gratis compressietool "7-zip" waarbij de encryptiestandaard AES-256 wordt gebruikt. Er zij opgemerkt dat twee verschillende communicatiekanalen moeten*

worden gebruikt voor het verzenden van het versleuteld bericht en de overeenkomstige decoderingssleutel (bijvoorbeeld e-mail en daarna telefoon);

- *Als men er zeker van wilt zijn dat de informatie tijdens de overdracht niet is gewijzigd, gebruikt u een hashingtechniek. Net als bij versleuteling moet ervoor worden gezorgd dat alleen erkende en veilige algoritmen worden gebruikt (bijv. SHA-512 en SHA-3). De hashfunctie moet op de platte tekst worden toegepast en aan de platte tekst worden toegevoegd voordat deze wordt versleuteld (niet aan de cijfertekst).*

Naast deze maatregelen is het ook raadzaam om voor elk systeem dat toegang geeft tot gevoelige gegevens (dus ook gegevens met betrekking tot de gezondheid) :

- *de authenticatie met minstens twee factoren te gebruiken (authenticatie bij het platform door een gebruikersnaam en een wachtwoord is niet voldoende)»;*
- *een strikt wachtwoordbeleid te voeren (een willekeurig wachtwoord samengesteld uit ten minste 17 tekens of een willekeurig wachtwoord samengesteld uit alfanumerieke tekens (a-z, A-Z, 0-9,...) van minsten 14 tekens);*
- *van verwerkers en verdere verwerkers eisen dat zij aan dezelfde veiligheidseisen voldoen ».*

35. Bijgevolg is de Autoriteit van mening dat het ontwerp moet worden aangepast om niet systematisch voorrang te geven aan het verzenden van de betrokken informatie via e-mail, en om het gebruik van deze communicatiemethode te beperken tot gevallen waarin dit vanuit het oogpunt van informatiebeveiliging aangewezen is. Met andere woorden, en overigens in overeenstemming met het verantwoordingsbeginsel, moet het ontwerp, afhankelijk van de verwerking van persoonsgegevens in kwestie, en in het bijzonder afhankelijk van de betrokken gegevens, de verwerkingsverantwoordelijke de nodige speelruimte laten om in concreto te bepalen op welke wijze de gegevens worden meegedeeld.

II.2.3. Rol van toestemming (milieu-informatie)

36. Artikel B.I.18, § 3 van het ontwerp bepaalt, en op voorwaarde dat de informatie niet over uitstoot gaat (in welk geval de hierna opgesomde uitzonderingen niet van toepassing zijn), het volgende «*de Overheidsinstantie wijst de aanvraag om inzage, uitleg of mededeling van een afschrift van een milieu-informatie af, wanneer zij heeft vastgesteld dat het openbaar belang van de openbaarmaking niet*

opweegt tegen de bescherming van een van de volgende belangen: met name om : «de vertrouwelijkheid van persoonsgegevens en dossiers betreffende een natuurlijk persoon wanneer deze persoon geen toestemming heeft gegeven voor de openbaarmaking van deze informatie en de vertrouwelijkheid van deze informatie bij de gewestelijke of Europese wetgeving geboden wordt; 6° de belangen of de bescherming van iedere persoon die de gevraagde gegevens op vrijwillige basis heeft verstrekt zonder daartoe te zijn verplicht door de wet of zonder dat de wet hem daartoe kan verplichten, tenzij deze persoon toestemming heeft gegeven voor de openbaarmaking van deze gegevens» (onderstreept door de Autoriteit).

37. Het ontwerp definieert echter niet «*toestemming hebben gegeven*», maar eerder het begrip «toestemming», als toestemming in de zin van artikel 4, 11) van de AVG⁸⁸. De Autoriteit heeft er geen bezwaar tegen dat het ontwerp toegang geeft tot milieu-informatie mits de betrokkene toestemming geeft in de zin van de AVG. Dit gezegd zijnde, moet de wettelijke regeling die van toepassing is op deze toestemming duidelijk worden geregeld. De Autoriteit heeft er reeds herhaaldelijk op gewezen dat, wat de openbaarheid van bestuur betreft, de verstrekking van gegevens door de betrokken Autoriteit een verwerking van persoonsgegevens inhoudt op basis van een wettelijke verplichting, d.w.z. een verwerking die valt onder artikel 6.1.c) van de AVG. In dit opzicht is het aan de aanvrager om de wettelijke regeling van de toestemming te definiëren die wordt behouden in de context van zijn ontwerp (kan deze worden ingetrokken en onder welke voorwaarden ?). Bij gebrek aan een specifieke rechtvaardiging die door de aanvrager moet worden verstrekt, is de Autoriteit van mening dat de bepalingen van het ontwerp moeten voorzien in de volledige toepassing van artikel 7 van de AVG op de situaties waarnaar wordt verwezen in artikel B.I.18, § 3, 5° en 6° van het ontwerp. In het geval dat de aanvrager voorziet in een rechtssysteem dat het niet mogelijk maakt om toestemming in te trekken (ervan uitgaande dat hij dit kan rechtvaardigen met betrekking tot de betreffende verwerking - wat de Autoriteit a priori betwijfelt), dan zou hij ook een bezwaarsysteem moeten implementeren dat de betrokkene in staat stelt om, om redenen die specifiek zijn voor zijn situatie, a posteriori bezwaar te maken tegen de verwerking⁸⁹.

II.2.4. Gedeeltelijke vrijstelling van openbaarheid van bestuur

38. Artikel B.I.18, § 5, 2de lid van het ontwerp bepaalt het volgende «wanneer in toepassing van de paragrafen §2, §3 en §4 een bestuursdocument of milieu-informatie slechts voor een deel aan de openbaarheid moet of mag worden onttrokken, wordt de inzage, de uitleg of de mededeling in afschrift tot het overige deel beperkt».

⁸⁸ Artikel A.III.1.84) van het ontwerp.

⁸⁹ De Autoriteit wijst erop dat het recht om bezwaar te maken onder de AVG ook a priori *kan worden* uitgeoefend, d.w.z. voordat de verwerking wordt uitgevoerd. Dit gezegd zijnde, in het onderhavige geval, aangezien het hier gaat om gegevensverwerking op basis van een wettelijke verplichting waarvoor de toestemming van de betrokkene vereist is, zal deze laatste zich dus altijd tegen de verwerking kunnen verzetten door zijn of haar toestemming niet te geven.

39. Op dit punt wil de Autoriteit erop wijzen dat persoonsgegevens niet langer persoonsgegevens zijn als ze zijn geanonimiseerd. In dit verband kan het verwijderen van gegevens uit een gegevensset soms leiden tot het anonimiseren van de betreffende gegevens, maar dit is niet noodzakelijkerwijs altijd het geval (het hangt af van de betreffende gegevens en de verwijderde gegevens : het kan bijvoorbeeld niet voldoende zijn om de identiteit van een betrokkene te verwijderen om zijn identificatie/heridentificatie of afzondering te voorkomen).

II.2.5. Openbaarheid van gegevens via internet

40. In artikel B.I.4 van het ontwerp wordt een huidige maatregel van actieve openbaarheid door de administratie genoemd, die met name bestaat uit het beschikbaar stellen van informatie met betrekking tot subsidies, studies, overheidsopdrachten en personeel (oproepen voor kandidaten, promoties, enz.).

41. De Autoriteit verwijst eerst en vooral als voorafgaande opmerking, naar haar adviezen 131/2023 en 42/2023 waarvan de overwegingen, mutatis mutandis, hier rechtstreeks van toepassing zijn. In dit verband, moet het ontwerp:

- het doel toelichten van de geïmplementeerde transparantiemaatregel. Ter herinnering: transparantie is op zichzelf geen doel van verwerking. Het voldoet aan een specifiek doel dat overeenkomt met het doel van de verwerking ;
- de periode waarin de betreffende persoonsgegevens beschikbaar worden gesteld via het transparantiedeel van de websites van overheidsinstanties, bepalen en rechtvaardigen;
- Voorzien in een specifiek bezwaarsysteem voor de betrokkene, aangezien het in de praktijk niet kan worden uitgesloten dat een betrokkene, om redenen die specifiek zijn voor zijn situatie, informatie die op hem betrekking heeft, moet intrekken⁹⁰. Deze overweging geldt in dit geval des te meer omdat er ook gegevens worden gepubliceerd over werving, vervanging en promotie. Dit gezegd zijnde, mag deze regeling er ook niet toe leiden dat de brede doelstelling van transparantie die met het ontwerp wordt nagestreefd, in twijfel wordt getrokken;

⁹⁰ Op dit punt wijst de Autoriteit erop dat het recht om bezwaar te maken zowel voor als na de verwerking van de gegevens kan worden uitgeoefend.

- De Autoriteit vestigt ook de aandacht van de aanvrager op het feit dat wanneer de gegevens in kwestie eenmaal via internet beschikbaar zijn gesteld, het over het algemeen illusoir is om te proberen de verdere verspreiding ervan te controleren.

42. Verder herinnert de Autoriteit aan overweging 12 van haar advies 131/2023, dat het volgende stelt:

« Het Hof van Justitie van de Europese Unie heeft een aantal uitspraken gedaan op het gebied van administratieve transparantie⁹¹ , en hetgeen volgt is met name gebaseerd op zijn jurisprudentie. Het is aan de opsteller van de norm in ontwerp om aan te tonen dat de beoogde gegevensverwerking een juist evenwicht vormt tussen het nagestreefde doel en de rechten en vrijheden in kwestie, en niet verder gaat dan nodig is. Er moet een verband zijn tussen de ernst van de inmenging en het nagestreefde doel van algemeen belang. Het nagestreefde doel mag niet redelijkerwijs op een even doeltreffende manier kunnen worden bereikt met andere middelen die minder inbreuk maken op de grondrechten van de betrokkenen, en beperkingen op gegevensbescherming moeten beperkt blijven tot wat strikt noodzakelijk is. In het bijzonder met betrekking tot de publicatie van gegevens via het internet is het belangrijk dat de wetgever een analyse uitvoert om te bepalen of publicatie via het internet zonder enige beperking van de toegang strikt noodzakelijk is om de nagestreefde doelen te bereiken, in plaats van bijvoorbeeld een beperktere toegang tot dergelijke gegevens voor personen die zichzelf identificeren of, in voorkomend geval, die ook een gerechtvaardigd belang hebben bij toegang tot de gegevens⁹²(nummering van de voetnoten gewijzigd in dit advies door de Autoriteit) ».

43. Artikel B.1.4, § 1, 1ste lid, 5°, van het ontwerp bepaalt dat de volgende gegevens worden gepubliceerd via de transparantierubrieken van de websites van elke overheidsinstantie :

« de oproepen tot kandidaten en de voorwaarden inzake aanwerving, bevordering of vervanging voor alle betrekkingen die zij willen invullen, openbaar gemaakt binnen zeven werkdagen na de aanwervings-, bevorderings- of vervangingsbeslissing, evenals de

⁹¹ « Zie met name : HvJ-EU (Grote arrest van 29 juni 2010 Commissie tegen The Bavarian Lager), zaak C-28/08; HvJ-EU, (Grote kamer), arrest van 22 november 2022, WM en Sovim SA tegen Luxembourg Business Registers, zaken C-37/20 en C-601/20 (informatie over de uiteindelijke begunstigen van entiteiten zoals bedrijven); HvJ-EU (Grote kamer), arrest van 9 november 2010, scheke, Eifert tegen Land Hessen, zaken C-92/09 en C-93/09 (informatie over landbouwsubsidies en -fondsen); HvJ-EU (Grote kamer), arrest van 5 april 2022, G.D. tegen The Commissioner of the Garda Síochána e.a., zaak C-140/20; HvJ-EU (Grote kamer), 1 augustus 2022, OT tegen Vyriausioji tarnybinės etikos komisija, zaak C-184/20 (informatie over belangenverklaringen); HvJ-EU, (Grote kamer), arrest van 22 juni 2021, B-Points de pénalité, zaak C-439/19 (informatie over verkeersovertradingen). ».

⁹² « Zie de artikelen 4 en 6 van de wet van 11 april 1994 betreffende de openbaarheid van bestuur. Over de mogelijke noodzaak om een gerechtvaardigd belang te rechtvaardigen, de noodzaak om persoonsgegevens beschikbaar te stellen, zie bijvoorbeeld het HvJ-EU (Grote kamer), arrest van 29 juni 2010 Commissie tegen The Bavarian Lager), zaak C-28/08; HvJ-EU, (Grote kamer), arrest van 22 november 2022, WM en Sovim SA tegen Luxembourg Business Registers, zaken C-37/20 en C-601/20, overwegingen 68-74 en 85. HvJ-EU, (Grote kamer), arrest van 22 juni 2021, B-Points de pénalité, zaak C-439/1, overwegingen 119-122. ».

beslissingen tot aanwerving, bevordering of vervanging voor de betrekkingen van de ambtenaren van niveau A die zij invullen, openbaar gemaakt binnen zeven werkdagen vanaf de beslissing» (onderstreept door de Autoriteit)

44. De memorie van toelichting bij het gemeenschappelijk decreet en de ordonnantie van het Brussels Hoofdstedelijk Gewest, de Gemeenschappelijke Gemeenschapscommissie en de Franse Gemeenschapscommissie van 16 mei 2019 betreffende de openbaarheid van bestuur in de Brusselse instellingen preciseert het volgende over deze bepaling :

*« de beslissingen inzake aanwerving, promotie of vervanging. Gelet op het proportionaliteitsbeginsel lijkt dit overmatig te zijn aangezien deze regel ook betrekking zou hebben op de ambtenaren waarvan het niet de bedoeling is dat hun benoeming gepubliceerd wordt in het Belgisch Staatsblad. Bijgevolg verzoekt de GBA de aanvrager om deze bepaling te beperken tot enkel de personen die via deze weg worden benoemd ongeacht of zij een overheidsmandaat uitoefenen⁹³. In dit verband wijst de doctrine erop dat het gebruikelijk is dat besluiten tot aanstelling van personeel van niveau 1 in het Belgisch Staatsblad worden bekendgemaakt" (Jean Sarot et al., *Précis de fonction publique*, Bruylant, Brussel, 1994, blz. 194) »⁹⁴(onderstreept door de Autoriteit).*

45. Volgens de Autoriteit is deze rechtvaardiging voor de verwerking in de ontwerpbeepaling ontoereikend. Het is in de eerste plaats aan de aanvrager om na te gaan volgens welke regels en met welk(e) doel(en) de betrokken aanwervings-, bevorderings- en vervangingsbesluiten in het Belgisch Staatsblad worden bekendgemaakt. Dit maakt het mogelijk om, indien nodig, het verschil in verwerking tussen betrokkenen te rechtvaardigen op basis van hun functieniveau, als onderdeel van de initiële publicatie van de gegevens in het Belgisch Staatsblad. Ten tweede moet het ontwerp rechtvaardigen waarom aanvullende publicatie via de transparantierubrieken van de websites van de overheidsinstanties noodzakelijk is met het oog op het doel dat met het ontwerp zelf wordt nagestreefd.

II.4. DELEN VAN ADMINISTRATIEVE GEGEVENS (UITWISSELING VAN GEGEVENS TUSSEN OVERHEIDSINSTANTIES) (BOEK C.IV., TITEL 2)

⁹³ Overweging 13 van haar advies 59/2018 van 4 juli 2018 *over een ontwerp van gezamenlijk decreet en ordonnantie betreffende de openbaarheid van bestuur* bij de Brusselse instellingen (CO-A-2018-038), verduidelijkte de Autoriteit inderdaad het volgende: *« In artikel 17 van het ontwerp wordt, naast de mededeelbare informatie, melding gemaakt van de beslissingen inzake aanwerving, promotie of vervanging. Gelet op het proportionaliteitsbeginsel lijkt dit overmatig te zijn aangezien deze regel ook betrekking zou hebben op de ambtenaren waarvan het niet de bedoeling is dat hun benoeming gepubliceerd wordt in het Belgisch Staatsblad. Bijgevolg verzoekt de GBA de aanvrager om deze bepaling te beperken tot enkel de personen die via deze weg worden benoemd ongeacht of zij een overheidsmandaat uitoefenen ».*

⁹⁴ Brussels Parlement, gewone zitting 2018-2019, 4 april 2019, doc. A-862/1, B-172,

II.4.1. Administratief delen in het algemeen

46. Artikel C.IV.4 van het ontwerp met als titel «*Standaard administratieve deling en verzoek tot administratieve deling*», bepaalt :

« De Overheidsinstanties organiseren de onderlinge administratieve deling van gegevens kosteloos, tenzij deze administratieve deling in strijd is met een rechtsregel of inbreuk maakt op de rechten van de derden op de gegevens waarop de administratieve uitwisseling betrekking heeft.

De voorwaarden voor verzoeken van ontvangende Overheidsinstanties om administratieve deling worden vastgesteld door de Dienst voor Gegevensbeheer in overleg met het Comité voor Gegevensbeheer.

Indien niet wordt gereageerd op een verzoek om administratieve gegevensdeling, wordt dit beschouwd als een weigering van administratieve gegevensdeling door de Overheidsinstantie die de gegevens heeft geproduceer» (onderstreept door de Autoriteit).

47. Artikel C.II.3, § 1 van het ontwerp volgt dezelfde logica door het volgende te bepalen «*de Overheidsinstanties organiseren standaard de onderlinge administratieve gegevensdeling^[95] om de uitvoering van hun taken van openbare dienstverlening en hun verplichtingen van algemeen belang te verbeteren ^[96]en, in voorkomend geval, de administratieve lasten voor de burgers te verminderen ^[97]*»(onderstreept door de Autoriteit)⁹⁸.

48. De Autoriteit is van mening dat deze bepalingen in principe het juridische paradigma omverwerpen dat momenteel van toepassing is op de verwerking van persoonsgegevens naar Belgisch recht, in overeenstemming met de beginselen van rechtmatigheid en voorspelbaarheid die zijn vastgelegd in artikel 8 EVRM en artikel 22 van de Grondwet. Op die manier zet het ontwerp de logica van het verwerken van gegevens uit authentieke gegevensbronnen om in elke gegevensuitwisseling waaraan een Brusselse overheidsinstantie⁹⁹ deelneemt, waarbij deze laatste daartoe een

⁹⁵ Zie voetnoot 12 voor de definitie van het begrip administratieve deling.

⁹⁶ De Autoriteit merkt overigens op dat dit geen welbepaald doel is.

⁹⁷ De Autoriteit merkt overigens op dat dit geen welbepaalde doel is.

⁹⁸ In de memorie van toelichting staat hierover het volgende :

« De Overheidsinstanties zijn gehouden om hun onderling administratief delen te organiseren overeenkomstig de bepalingen van deze titel, dit omwille van de redenen uiteengezet in de memorie van toelichting, namelijk ter verlichting van de administratieve lasten voor burgers, ter totstandbrenging van synergieën en ter verbetering van de kwaliteit van de openbare diensten en diensten van algemeen belang, het poolen van bepaalde werkingskosten enz., ».

⁹⁹ De Autoriteit vraagt zich met de invoering van een dergelijk beginsel ook af of het nuttig zou zijn om authentieke Brusselse bronnen te implementeren. De Autoriteit merkt terloops ook op dat er, voor zover haar bekend, geen authentieke gegevensbron in de Brusselse positieve wetgeving bestaat zoals bedoeld in de Ordonnantie van 8 mei 2014 betreffende de *oprichting en de organisatie van een gewestelijke dienstenintegrator*.

samenwerkingsakkoord moet sluiten¹⁰⁰. Overwegende dat persoonsgegevens in beginsel en in alle gevallen alleen mogen worden verwerkt wanneer daarvoor een rechtsgrondslag bestaat in het kader van de uitoefening van een bevoegdheid of het nakomen van een verplichting die aan een overheidsinstantie is opgedragen (gegevensverwerking door overheidsinstanties vindt bijna altijd plaats in de gevallen bedoeld in artikel 6.1.c) en d)) en waarvan de wezenlijke bestanddelen worden bepaald door een norm van wettelijke rangorde. met dien verstande dat, afhankelijk van de betrokken gegevensverwerking, het kader dat wordt geboden door een norm van wettelijke rangorde, niet mag worden overschreden¹⁰¹. Met andere woorden, om een gegevensverwerking uitvoerbaar te maken, is het niet voldoende dat er geen specifieke bepaling is die dit verhindert.

49. Volledigheidshalve wijst de Autoriteit er ook op dat een protocolakkoord in geen geval volstaat als rechtsgrondslag voor de uitwisseling van gegevens tussen overheidsinstanties¹⁰².

¹⁰⁰ Zie artikel C.IV.8 van het ontwerp.

¹⁰¹ De adviezen van het Kenniscentrum van de Autoriteit bieden een overvloed aan voorbeelden van hoe deze beginselen kunnen worden toegepast (zie ook, in het algemeen, standaardadvies nr. 65/2023 van 24 maart 2023 *betreffende de redactie van normatieve teksten*).

¹⁰² De Autoriteit heeft dit standpunt herhaald en verwijst hier naar haar Aanbeveling nr. 02/2020 van 31 januari 2020 *over de reikwijdte van de verplichting om een protocol te sluiten om de mededeling van persoonsgegevens door de federale overheidssector te formaliseren*, blz. 9-10 :

« Volgens artikel 20 van de WVG bestaat **de verplichting om een protocol af te sluiten** alleen wanneer de mededeling van persoonsgegevens door een federale overheid **noodzakelijk is om te voldoen aan een wettelijke verplichting** waaraan de verwerkingsverantwoordelijke is onderworpen, of wanneer de mededeling **noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag** dat aan de verwerkingsverantwoordelijke is opgedragen, met dien verstande dat de wettelijke verplichting of taak van algemeen belang die de mededeling van persoonsgegevens rechtvaardigt, zowel bestaat voor de verwerkingsverantwoordelijke die de persoonsgegevens meedeelt als de verwerkingsverantwoordelijke die de persoonsgegevens ontvangt

Deze eis moet worden opgevat in het licht van het beginsel van de toekenning van administratieve bevoegdheden, het beginsel van de specialiteit van rechtspersonen en het legaliteitsbeginsel, dat de voorwaarden bepaalt waaronder de administratie zich kan mengen in het recht op bescherming van de persoonlijke levenssfeer, waarvan het recht op bescherming van persoonsgegevens deel uitmaakt¹⁰³. Volgens het principe van de toekenning van administratieve bevoegdheden, dat is vastgelegd in artikel 105 van de Grondwet en artikel 78 van de Bijzondere wet tot hervorming der instellingen van 8 augustus 1980 hebben de administratieve autoriteiten geen andere bevoegdheden dan die welke formeel aan hen zijn toegekend door de Grondwet en de wetten en decreten die in het kader daarvan zijn uitgevaardigd. Voorts bepaalt het specialiteitsbeginsel van rechtspersonen dat elke instelling met rechtspersoonlijkheid alleen mag optreden om het doel of de doelen te bereiken waarvoor zij is opgericht, met dien verstande dat alleen een wetgevende norm een rechtspersoon met een opdracht van openbare dienst kan belasten. Trouwens, zoals de Raad van State in zijn advies over het voorontwerp van wet "betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens" heeft opgemerkt, is "het doorgeven van gegevens van een overheidsinstantie aan een andere een vorm van inmenging in het recht op de bescherming van de persoonlijke levenssfeer van de betrokkenen. Krachtens artikel 8 van het Europees Verdrag voor de rechten van de mens en artikel 22 van de Grondwet, zoals dat wordt geïnterpreteerd in de vaste rechtspraak van het Grondwettelijk Hof, moet een dergelijke inmenging inzonderheid een wettelijke grondslag hebben, evenredig zijn ten opzichte van de nagestreefde doelstelling en op voldoende duidelijke wijze georganiseerd zijn opdat ze voorzienbaar is voor de burger¹⁰⁴. Een overheidsinstantie mag alleen persoonsgegevens verwerken -en dus meedelen - als deze mededeling noodzakelijk is voor de naleving van een verplichting die door of krachtens een wettelijke bepaling aan een van de verwerkingsverantwoordelijken is opgelegd of als deze mededeling noodzakelijk is voor de uitvoering van een taak van algemeen belang die aan een van de verwerkingsverantwoordelijken is toegewezen door of krachtens een wet. Zoals de CBPL in haar advies over het voorontwerp van wet "betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens" heeft opgemerkt, moet de mededeling van persoonsgegevens door de openbare sector een rechtsgrondslag hebben, met dien verstande dat "een uitwisselingsprotocol nooit de rechtsgrondslag voor een gegevensverwerking kan zijn¹⁰⁵."

Deze grondwettelijke eis houdt in dat in de overgrote meerderheid van de gevallen de mededeling van persoonsgegevens door overheden "noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust" (A) of "noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen" (B). Het kan echter niet worden uitgesloten dat in bepaalde, zeer zeldzame omstandigheden een mededeling van persoonsgegevens door de openbare sector kan berusten op een andere rechtsgrond vastgesteld in artikel 6 van de AVG. Volgens artikel 20 van de WVG hoeven dergelijke mededelingen niet te worden geformaliseerd aan de hand van een protocol (C)". (voetnoten in dit advies weggelaten door de Autoriteit).

50. Nog afgezien van deze juridische bezwaren met betrekking tot de wetgeving inzake gegevensbescherming, wordt in de memorie van toelichting niet concreet uitgelegd waarom een dergelijke verandering van aanpak nodig zou zijn¹⁰³.

II.4.2. Authentieke gegevensbronnen

51. Artikel C.II.3, § 2, 1ste lid van het ontwerp bepaalt «*de Overheidsinstanties gebruiken authentieke bronnen om de gegevens te verzamelen die zij nodig hebben om hun taken of verplichtingen te vervullen*» (onderstreept door de Autoriteit).
52. In overeenstemming met de beginselen van evenredigheid en minimale gegevensverwerking die zijn vastgelegd in artikel 5.1.c), van de AVG, mogen overheidsinstanties alleen gegevens verwerken die noodzakelijk zijn voor de uitvoering van hun taken van openbaar belang of hun wettelijke verplichtingen. Het ontwerp moet daarom dienovereenkomstig worden aangepast, vooral omdat het enigszins vaag is in die zin dat het de valorisatie van gegevens vereist.
53. Artikel C.IV.12 van het ontwerp met als titel «*Administratieve deling van authentieke gegevens met het oog op een unieke gegevensinzameling*» (onderstreept door de Autoriteit) bepaalt in paragraaf 1:

¹⁰³ Over artikel C.II.3, zegt de memorie van toelichting het volgende:

« Paragraaf 1 bevat het beginsel van het delen door standaardinstellingen, tussen Overheidsinstanties, van gegevens waarbij dat toegestaan is. Dit beginsel van delen is de algemene doelstelling van het mechanisme voor administratief delen in de zin van het Wetboek, dat een specifieke definitie en nadere uitvoeringsregels krijgt in boek C.IV

Dit beginsel heeft tot doel de instellingen aan te zetten tot uitwisselingen om de administratieve lasten voor de Brusselse burgers te verlichten

Een dergelijk beginsel is noodzakelijk voor meer efficiëntie van de aan de Overheidsinstantie toevertrouwde opdrachten en het vereenvoudigen van het leven van de burgers.

Paragraaf 2 bevat het beginsel van de unieke gegevensinzameling, het zogenoemde "once only"-beginsel

De bekrachtiging van de gegevens afkomstig uit authentieke bronnen, zoals georganiseerd door het Wetboek, maakt het mogelijk de uitwisseling van deze gegevens tussen Overheidsinstanties zodanig te organiseren dat de burger de gegevens die hij reeds aan andere Overheidsinstanties heeft verstrekt, niet opnieuw hoeft te geven. Het gaat erom een unieke gegevensinzameling te organiseren – het once only-beginsel – op basis van gegevens waarvan de kwaliteit wordt gewaarborgd door het wettelijk kader dat erop van toepassing is, en dat wordt beschreven in boek C.IV.

Tot slot voert paragraaf 3 ook het beginsel in van het extern delen van openbare gegevens in het kader van het hergebruik» (onderstreept door de Autoriteit).

Verder preciseert de memorie van toelichting, eraan herinnerend dat «het van belang is om gegevensdeling tussen Overheidsinstanties makkelijker en efficiënter te maken» dat «uit een aantal studies in opdracht van het Federaal Agentschap voor Administratieve Vereenvoudiging (immers zeer duidelijk) blijkt (...) dat het delen van beschikbare gegevens kan leiden tot een aanzienlijke verlichting van administratieve lasten [(met verwijzing naar « Nota aan de Brusselse Hoofdstedelijk Regering over een Brusselse datastrategie»)], en dat «de toepassing van het beginsel van unieke gegevensinzameling ook een positief effect op het functioneren en de efficiëntie van de Overheidsinstanties in het kader van de uitvoering van hun opdrachten [...] ».

In de memorie van toelichting wordt verder nog op het volgende gewezen:

« *De algemene gedachte achter dit boek is dat gegevensstromen alleen kunnen plaatsvinden in overeenstemming met het wettigheidsbeginsel. Boek C.IV vormt de rechtsgrondslag voor de stromen die het reguleert en dit onverminderd, in voorkomend geval, het aannemen van specifieke regels voor elke stroom.* » (onderstreept door de Autoriteit). Deze analyse kan niet worden gevolgd om de redenen die in het dispositief van dit advies worden uiteengezet.

« *De administratieve deling van gegevens uit afkomstig uit authentieke bronnen is bedoeld om de terbeschikkingstelling van deze gegevens aan de ontvangende Overheidsinstanties te regelen, zodat zij de verzameling ervan niet meer zelf organiseren*» (onderstreept door de Autoriteit).

54. Ten eerste benadrukt de Autoriteit dat het gebruik van authentieke gegevensbronnen niet alleen gerechtvaardigd is om te voorkomen dat overheidsinstanties de verzameling van gegevens van betrokkenen zelf moeten organiseren¹⁰⁴. De kwaliteit van de verwerkte gegevens¹⁰⁵ is ook een doorslaggevende factor om het gebruik van authentieke gegevensbronnen te rechtvaardigen, en een centrale factor bij de identificatie van dergelijke gegevensbronnen¹⁰⁶. *Bovendien vereist de vaststelling van een authentieke gegevensbron dat de wetgever en de verwerkingsverantwoordelijke bijzondere aandacht besteden aan de beveiliging van de gegevensmededeling, aangezien het de bedoeling is dat een dergelijke bron wordt hergebruikt en dus aanleiding geeft tot frequente gegevensmededeling.*
55. Bovendien wijst de Autoriteit erop dat de verankering van het *only once*) beginsel in een wet (in dit geval een ordonnantie) de wetgever en overheidsinstanties niet ontslaat van de verplichting om de toepassing van artikel 6.4 van de AVG te waarborgen: het indirect verzamelen van gegevens blijft een verdere verwerking van gegevens waarop artikel 6.4 van de AVG van toepassing is¹⁰⁷.

¹⁰⁴ Hierbij moet worden benadrukt dat de bepaling niet expliciet verwijst naar het verzamelen van gegevens *bij de betrokkene*. En zou dat wel moeten.

¹⁰⁵ Nauwkeurigheid en bijgewerkt zijn, in overeenstemming met artikel 5.1.d) van de AVG.

¹⁰⁶ Zie in dit verband het recente advies 143/2023, overweging 39.

¹⁰⁷ Dus in die zin, volgens de Europese Toezichthouder voor gegevensbescherming :

« *Le RGP 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*¹.

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 1». 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 1, point d) ou en lien avec la perception des impôts en vertu du point e) de la même disposition).

L'allègement 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 1, 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 1, 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 1, 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» (onderstreping en verwijzingen weggelaten door de Autoriteit), CEPD, Avis n° 8/2017 sur la proposition de règlement établissant un portail numérique unique et sur le principe 'une fois pour toutes', blz. 11-12.

56. Artikel C.IV.13 van het ontwerp betreft de «identificatiesleutels» die gebruikt moeten worden. Lid 1 bepaalt dat de overheidsinstanties bij het beschikbaar stellen van gegevens uit authentieke bronnen het rijksregisternummer moeten gebruiken om natuurlijke personen te identificeren¹⁰⁸. Paragraaf 3 bepaalt dan weer:

« In het kader van de uitvoering van een wettelijke informatieplicht gebruiken de natuurlijke en rechtspersonen :

1° het nummer van het Rijksregister, toegekend overeenkomstig artikel 2, lid 2, van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, of

2° het identificatienummer van de Kruispuntbank, toegekend overeenkomstig artikel 4, § 2, lid 3, van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid, en het ondernemingsnummer dat is toegekend overeenkomstig artikel III.17 van het Wetboek van Economisch Recht» (onderstreept door de Autoriteit).

57. De Autoriteit begrijpt de reikwijdte van deze bepaling niet, die niet wordt uitgelegd in de memorie van toelichting. Met andere woorden, deze bepaling moet worden weggelaten of verduidelijkt. De Autoriteit schort haar analyse hierover op.
58. Aangaande de aanduiding van authentieke gegevensbronnen, bepaalt artikel C.IV.15, § 1¹⁰⁹ van het ontwerp het volgende:

« Onverminderd door Derde Overheidsinstanties erkende authentieke bronnen wijzen de Regering, het College en het Verenigd College via een besluit de authentieke bronnen aan waarvan de Overheidsinstantie aangeduid als producent van de authentieke bron onder hun bevoegdheden valt.

In afwijking van lid 1 worden authentieke bronnen die persoonsgegevens bevatten bij besluit of ordonnantie aangewezen, afhankelijk van de openbare collectiviteit waartoe de Overheidsinstantie behoort die als producent van de authentieke bron is aangewezen» (onderstreept door de Autoriteit).

¹⁰⁸ De Memorie van toelichting vermeldt het volgende: «Deze verplichting wil eigenlijk de omstandigheid verhelpen dat sommige Brusselse Overheidsinstanties nog niet de nodige vergunningen hebben aangevraagd voor het gebruik van deze nummers. Het ontbreken van toestemming kan dus niet langer worden gebruikt als excuus voor het niet administratief delen van de in de betrokken authentieke bron beschikbare gegevens». Voor wat de motivering betreft ivm het gebruik van het rijksregisternummer, zie overwegingen 31-33 van het advies 143/2023.

¹⁰⁹ De paragraaf staat vernoemd als § 3 in het ontwerp is in werkelijkheid het 1ste lid van paragraaf 1 van artikel C.IV.15.

59. De Autoriteit wijst erop dat het, in overeenstemming met de beginselen van voorspelbaarheid en rechtmatigheid waarnaar hierboven wordt verwezen en die zijn vastgelegd in normen die hiërarchisch boven de ordonnantie staan (d.w.z. de grondwet en het EVRM), niet voldoende is dat de authentieke bron van gegevens wordt aangewezen door een norm van wettelijke rangorde (in dit geval een decreet of ordonnantie) : alle essentiële elementen van de gegevensverwerking die verband houden met deze authentieke bron moeten worden vastgelegd in een norm van wettelijke rangorde.
60. Zij herinnert er verder aan dat artikel 4.1) van de AVG een persoonsgegeven als volgt definieert «*alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene“); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon*» (onderstreept door de Autoriteit). Het is dus duidelijk dat opdat een authentieke bron persoonsgegevens zou "omvatten", het niet nodig is dat de betrokkene rechtstreeks wordt geïdentificeerd (met naam of via zijn of haar nationaal registratienummer). Deze opmerking is belangrijk met betrekking tot een informatiesysteem zoals UrbIS, waarin informatie kan worden gekoppeld aan adressen en kadastrale perceelnummers¹¹⁰. Doorslaggevend voor de toepassing van de beginselen van transparantie en rechtmatigheid die zijn vastgelegd in artikel 8 EVRM en artikel 22 van de Grondwet, is dat in het kader van de verwerking van persoonsgegevens wordt gestreefd naar de authentieke bron van de gegevens.
61. Bovendien benadrukt de Autoriteit dat de definitie van "Brusselse authentieke bron" moet worden aangepast om te voldoen aan artikel C.IV.15, § 1 van het ontwerp « als de Brusselse *authentieke bron* persoonsgegevens "omvat", moet deze worden aangewezen bij decreet of ordonnantie.
62. In deze context voorziet artikel C.IV 15, §4, van het ontwerp het volgende:

« *Het aanwijzingsbesluit bedoeld in lid 1 vermeldt voor elke authentieke bron met name:*

1° de identiteit van de Overheidsinstantie die de authentieke bron produceert, belast met de verzameling van de gegevens, de bijwerking, de terbeschikkingstelling en elke andere verwerking ervan die relevant en noodzakelijk is voor de handhaving ervan, overeenkomstig de stand van de techniek en de evolutie van de technologieën;

¹¹⁰ Zie overweging 15. laatste streepje.

- 2° de wijze waarop de gegevens waarvan de hosting is toevertrouwd aan de Overheidsinstantie die de authentieke bron produceert, worden bijgewerkt en toegankelijk gemaakt;
- 3° de doelstelling(en) die de Overheidsinstantie die de authentieke bron produceert bij de verzameling van de betrokken gegevens nastreeft
- 4° de lijst van de in de authentieke bron opgenomen gegevens;
- 5° de specifieke modaliteiten voor de financiering van de verzameling van de in de authentieke bron opgenomen gegevens, de bijwerking, de terbeschikkingstelling en elke andere verwerking ervan die relevant en noodzakelijk is voor de handhaving ervan.

Met betrekking tot de aanwijzing van authentieke bronnen die persoonsgegevens bevatten, worden in het besluit of de ordonnantie tevens de volgende elementen vermeld:

- de essentiële elementen van de verwerking;
- de voorzien maatregelen ter bescherming van de rechten van de betrokkenen;;
- de verplichtingen inzake transparantie voor de betrokkenen (onderstreept door de Autoriteit)

63. De Autoriteit wijst erop dat deze bepalingen in ieder geval geen afbreuk doen aan de hiërarchisch hogere normen waarnaar zij verwijzen, althans gedeeltelijk, namelijk de normen die voortvloeien uit de toepassing van artikel 8 EVRM, artikel 22 van de Grondwet en de rechtstreeks toepasselijke AVG zelf. In voorkomend geval zal dus in de aanwijzingsbesluiten naar specifieke beschermingsmaatregelen en transparantieverplichtingen worden verwezen, aangezien alle verplichtingen van de AVG rechtstreeks toepasselijk zijn en niet in nationaal recht kunnen worden omgezet¹¹¹. De Autoriteit is van mening dat de memorie van toelichting dit punt van de hiërarchie van normen, moet benadrukken, en dat dit nogmaals moet worden benadrukt in de memorie van toelichting voor aanwijzingsbesluiten (decreet of ordonnantie) van authentieke bronnen die betrekking hebben op de verwerking van persoonsgegevens.

64. Verder is de Autoriteit van mening dat het ontwerp de criteria moet bepalen op basis waarvan een gegevensbank kan worden aangewezen als een authentieke gegevensbron, met bijzondere aandacht voor de kwaliteit van de gegevens (nauwkeurigheid, bijgewerktheid, enz.) en de relatie daarvan met

¹¹¹ De Autoriteit wijst erop dat de rechtstreekse toepasselijkheid van Europese verordeningen betekent dat ze niet kunnen worden omgezet in nationale wetgeving, aangezien een dergelijke procedure dubbelzinnigheid zou *kunnen creëren over zowel de juridische aard van de toepasselijke bepalingen als het tijdstip van hun inwerkingtreding* (HvJEU, arres van 7 februari 1973, Commissie vs/Italië, zaak C-39/72, overweging 17, zie ook HvJEU, arrest van 10 oktober 1973, Fratelli Variola S.p.A. vs/Italiaanse administratie van Financiën, zaak C-34/73, overweging 11; HvJEU, arrest van 31 januari 1978, Ratelli Zerbone Snc vs/Amministrazione delle finanze dello Stato, zaak. C-94/77, overwegingenb 24-26).

de taak van algemeen belang die is toevertrouwd aan de beheerder van de authentieke bron¹¹². Hiertoe bevat het ontwerp nuttige begrippen onder het gegevenskwaliteitsbeginsel vastgelegd in Artikel C.II.5, volgens welke «*gegevenskwaliteit wordt gedefinieerd onder verschillende complementaire dimensies, namelijk in het bijzonder : 1° Consistentie, 2° Juistheid, 3° Volledigheid, 4° Verifieerbaarheid, 5° Geldigheid, 6° Uniekheid, 7° Integriteit, 8° Actualiteit*».

II.4.3. Gegevensbank afkomstig uit authentieke bronnen

65. Artikel C.IV.16 van het ontwerp voorziet in de mogelijkheid om gegevensbanken die zijn opgezet op basis van gegevens uit authentieke bronnen, aan te merken als gegevensbanken afkomstig uit authentieke bronnen. Meer precies zijn dit de bewoordingen van dit artikel:

*« De gegevensbanken op basis van gegevens uit authentieke bronnen worden bij decreet of ordonnantie aangewezen als gegevensbanken uit authentieke bronnen, afhankelijk van de openbare instantie die verantwoordelijk is voor de Overheidsinstantie die is aangewezen als producent van de gegevensbank op basis van gegevens uit authentieke bronnen
Artikel C. IV. 15, §2 tot en met 4 zijn van toepassing op de procedure voor de aanwijzing van de gegevensbanken uit authentieke bronnen mutatis mutandis
Voor de toepassing van het Wetboek worden de gegevensbanken uit authentieke bronnen en de daaruit afkomstige gegevens gelijkgesteld met respectievelijk authentieke bronnen en authentieke gegevens ».*

66. De memorie van toelichting die niet rechtvaardigt waarom het noodzakelijk is dat dergelijke gegevensbanken worden opgezet, preciseert «*Deze wetgevingsprocedure beoogt dus de aanwijzing van superdatabanken met dezelfde waarde als de authentieke bronnen waaruit zij uitsluitend bestaan*» (onderstreept door de Autoriteit).
67. Volgens de Autoriteit is deze aanpak dubbel problematisch.
68. Ten eerste, in overweging 13 van haar advies 65/2019 van 27 februari 2019 *betreffende een ontwerp van samenwerkingsakkoord tot wijziging van het samenwerkingsakkoord van 23 mei 2013 tussen het Waalse Gewest en de Franse Gemeenschap over het opstarten van een gemeenschappelijk initiatief om gegevens te delen en over het gemeenschappelijk beheer van dit initiatief (CO-A-2019-014 + CO-A-2019-044)* vroeg de Autoriteit zich af wat het (equivalent) begrip was van een gegevensbank afkomstig uit authentieke bronnen : «*eerst en vooral, zoals de Commissie voor de Bescherming van de Persoonlijke Levenssfeer reeds stelde , is de Autoriteit immers van mening dat de authentieke*

¹¹² Zie in dit verband de overwegingen 38-39 van het advies

*gegevensbron in principe uniek is en niet moet worden gekopieerd*¹¹³. Voor een betere bescherming van het privéleven van de betrokkenen heeft dezelfde Commissie een duidelijk standpunt ingenomen ten voordele van de integratie van diensten¹¹⁴. , veeleer dan de integratie van gegevens Met andere woorden, om deze redenen zou de toevlucht tot gegevensbanken ontstaan uit authentieke bronnen moeten uitgesloten zijn» (nummering van voetnoten gewijzigd in dit advies en onderstreping toegevoegd in dit advies). Hoewel het concept van een gegevensbank die is ontstaan uit authentieke gegevensbronnen bestaat in de positieve Brusselse wetgeving (hoewel er, voor zover de Autoriteit weet, tot op heden geen dergelijke gegevensbank bestaat¹¹⁵), zijn deze overwegingen evenzeer van toepassing in dit advies.

69. Het concept van gegevensbanken die zijn ontstaan uit authentieke bronnen is in strijd met het principe en de definitie (het doel) van authentieke gegevensbronnen. Zo definieert het dispositief van het ontwerp in zijn artikel A.III.1.31), de authentieke broek terecht als (gedeeltelijk vertaald door de Autoriteit) «*elke databank die gegevens bevat die authentiek zijn als unieke en originele gegevens met betrekking tot de betrokken persoon of het betrokken feit en die uitsluitend wordt beheerd door een overheidsinstantie of een derde overheidsinstantie die is aangewezen als producent van de databank, en waarvan de inhoud bestemd is voor verplichte administratieve gegevensdeling tussen Overheidsinstanties volgens het beginsel van een unieke gegevensverzameling*» (onderstreept door de Autoriteit)¹¹⁶. Het concept van een gegevensbank ontstaan uit authentieke bronnen is in verschillende opzichten problematisch:

- breekt met de zojuist uiteengezette logica, aangezien authentieke gegevens nu toegankelijk zouden zijn in twee verschillende bronnen die bovendien beide worden gepresenteerd als authentiek (van dezelfde waarde) en dit terwijl de verantwoordelijke voor de gegevensbank van gegevens uit authentieke bronnen per definitie een slechtere relatie zal hebben met de betrokken gegevens (doel van de oorspronkelijke verzameling, relatie tussen de publieke taak en de betrokken gegevens en bijgevolg deskundigheid en ervaring met betrekking tot de gegevens, relatie in voorkomend geval met de betrokkene, enz.), wat in strijd is met het doel van het gebruik van authentieke bronnen ;

¹¹³ « In die zin, zie Advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, nr. 29/2012 van 12 september 2012, punt 94 en Aanbeveling nr. 09/2012 van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, van 23 mei 2012, punten 5, a en en c., 9 en 15. ».

¹¹⁴ «Aanbeveling uit eigen beweging van de Commissie voor de bescherming van de persoonlijke levenssfeer 03/2009 van 1 juli 2009 in verband met integratoren in de overheidssector, punten 5-12».

¹¹⁵ Zie verder de beschouwingen over UrbIS.

¹¹⁶ De memorie van toelichting bij het ontwerp herinnert overigens nog aan het volgende «Aangezien de gegevens afkomstig uit authentieke bronnen slechts door één enkele overheidsdienst zullen worden beheerd, hebben zij een unieke en oorspronkelijke waarde in het hele Brusselse ecosysteem ». Een authentieke bron is een specifieke databank waaraan een bijzondere waarde wordt toegekend door het feit dat zij wordt beheerd door één enkele Overheidsinstantie die wordt gekwalificeerd als producent, in de betekenis daaraan gegeven in dit Wetboek». De bepalingen van het ontwerp geven bovendien geen specifieke definitie voor het concept van gegevensbanken die zijn ontstaan uit authentieke gegevensbronnen.

- Naast dit principiële probleem dat rechtstreeks verband houdt met de kwaliteit van de gegevens, verhoogt de integratie van authentieke gegevens uit verschillende bronnen in dezelfde gegevensbank om andere redenen de risico's voor de rechten en vrijheden van de betrokkenen. Zoals de Commissie voor de bescherming van de persoonlijke levenssfeer al eerder aangaf, betekent het toestaan van de integratie van gegevens (in dit geval authentieke gegevens) het toestaan van de vermenigvuldiging van kopieën van gegevens die in omloop zijn, wat leidt tot het probleem van het bijwerken van gegevens. De Autoriteit merkt echter ook op dat deze aanpak vragen kan oproepen met betrekking tot het beginsel van minimale gegevensverwerking ;
- Zoals de Commissie voor de bescherming van de persoonlijke levenssfeer al heeft aangegeven, verhoogt de concentratie van gegevens (in dit geval authentieke gegevens) in één informatiesysteem de risico's voor de informatiebeveiliging ;
- Tot slot brengt het gebruik van een gegevensbank die is ontstaan uit authentieke bronnen een aanzienlijk risico met zich mee op doelverschuiving en een controleverlies van de authentieke gegevensbron over de verwerking van de gegevens die het zou moeten meedelen. Er moet aan worden herinnerd dat de verwerkingsverantwoordelijke van de authentieke gegevensbron verantwoordelijk is voor het doorgeven van de gegevens aan de overheidsinstanties die van plan zijn de daar toegankelijke gegevens te verwerken. Met name in technisch en administratief opzicht verliest deze instantie de controle over de uitwisseling van gegevens (in het bijzonder de verificatie van de ontvanger, het doel en de noodzakelijke gegevens) zodra de gegevens elders, via een andere gegevensbank, beschikbaar zijn. In de praktijk leidt dit tot een verdere verwatering van verantwoordelijkheden en een toename van het aantal actoren voor de betrokken persoon. En deze risico's zijn des te groter wanneer de authentieke bron en de gegevensbank die is ontstaan uit authentieke bronnen onder verschillende bevoegdheidsniveaus vallen. Het ontwerp wil echter ook authentieke bronnen uit andere bevoegdheidsniveaus raadplegen.

70. Ten tweede is het op dit punt expliciet duidelijk uit de definities in het ontwerp dat gegevensbanken die afkomstig zijn uit authentieke bronnen, gegevens kunnen bevatten die afkomstig zijn uit authentieke bronnen van een ander bestuursniveau (bijvoorbeeld de federale staat). Welnu, de Autoriteit haalt overweging 14 aan van haar bovenvermeld advies 65/2019: *In die context stelt de Autoriteit zich enerzijds vragen bij de bevoegdheid en bijgevolg de legitimiteit, van een gewestelijke entiteit om op die wijze een gegevensbank te kopiëren die opgericht en georganiseerd is door een andere entiteit die geen deel uitmaakt van het samenwerkingsakkoord*^[117]. *Een verantwoording geval*

¹¹⁷ in dit geval gesloten tussen het Waals Gewest en de Franse Gemeenschap.

per geval zal op dit punt noodzakelijk zijn. Hoe dan ook, anderzijds kan een dergelijke duplicatie en het daaropvolgende hergebruik van de gegevens alleen worden uitgevoerd als het toepasselijke normatieve kader (inclusief uitvoeringsbepalingen) voor de betreffende externe authentieke bron dit zou toelaten. Voor het overige, als het aan de Raad van State is om de aanvrager te bepalen over de kwestie van de bevoegdheidsverdeling, ziet de Autoriteit niet in waarom, in het kader van de impliciete bevoegdheden, een gefedereerde entiteit bevoegd zou moeten zijn om de authentieke gegevens van een ander bevoegdheidsniveau (waartoe ze per definitie toegang heeft) te dupliceren¹¹⁸).

71. Concluderend is de Autoriteit op dit punt van mening dat het concept van een gegevensbank die is ontstaan uit authentieke gegevensbronnen moet worden losgelaten.
72. Overigens verwijst de Autoriteit, in het verlengde van de bovenstaande overwegingen over de bevoegdheidsverdeling, wat betreft de noodzaak om een beroep te doen op de Brusselse dienstenintegrator naar overweging 43 van haar advies nr. 143/2023, die het volgende zegt : «[...] *Wat dit laatste punt betreft, is de Autoriteit, gelet op de regels inzake de bevoegdheidsverdeling (waarover de Raad van State en het Grondwettelijk Hof zich uiteindelijk zullen moeten uitspreken), van mening dat het ontwerp de regels inzake authentieke bronnen die onder de bevoegdheid van een andere federale of gefedereerde entiteit vallen, onverlet moet laten en met name geen specifieke verplichtingen mag opleggen aan de personen die belast zijn met de verwerking van dergelijke bronnen*[...]» (verwijzingen weggelaten door de Autoriteit in dit advies).

II. HERGEBRUIK VAN OPENBARE DOCUMENTEN EN OPENBARE GEGEVENS (BOEK C.IV, TITEL 3)

II.5.1. Toepassingsgebied van 2 stelsels van hergebruik

73. Titel 3 van Boek C.IV. is gewijd aan het hergebruik van overheidsdocumenten¹¹⁹ en betreft overeenkomstig artikel C.IV.17 van het ontwerp 2 stelsels van hergebruik: een eerste stelsel dat van toepassing is op vrij toegankelijke deelbare documenten, in overeenstemming met de omzetting van de richtlijn inzake hergebruik; een tweede systeem dat betrekking heeft op beschermde gegevens, die onder de Verordening data governance vallen.
74. Meer in het algemeen bepaalt artikel C.II.3, § 3 van het ontwerp «*De Overheidsinstanties garanderen ook standaard het hergebruik van hun openbare gegevens*¹²⁰ door particuliere marktdeelnemers» (onderstreept door de Autoriteit). Artikel C.II.4, § 2 van het ontwerp bepaalt «*De Overheidsinstanties organiseren het hergebruik van hun gegevens overeenkomstig titel 3 van boek C.IV De*

¹¹⁸ Anders zou hij ze niet kunnen dupliceren.

¹¹⁹ Zie voetnoot 4

¹²⁰ Zie voetnoot 4

overheidsinstanties stellen hun open data ter beschikking¹²¹], en garanderen hierbij de hoogste graad van openheid. Zoniet, indien dit onmogelijk blijkt, gebruiken de Overheidsinstanties instrumenten om toe te laten dat het geheel of een deel van de gegevensbanken die dergelijke gegevens bevatten, opgehaald en vrij gebruikt kunnen worden».

75. Het ontwerp is daarom gericht op maximaal hergebruik, zoals zal blijken uit de volgende overwegingen. Met andere woorden, in plaats van na te denken over het openstellen van gegevens voor hergebruik (door het omzetten van de richtlijn inzake hergebruik of het implementeren van de verordening inzake data governance), zal de Brusselse wetgever bij het opstellen van wetgeving moeten overwegen of het nodig is om het hergebruik van documenten waarop de aangenomen wetgeving betrekking heeft, te voorkomen.
76. De eerdere adviezen van de Autoriteit moeten vooraf en voor contextuele doeleinden worden geraadpleegd met betrekking tot het eerste stelsel voor hergebruik.
77. het tweede stelsel is gekoppeld aan de Data Governance Verordening, die ook van toepassing is op gegevensbescherming. Als inleidend punt met betrekking tot dit laatste verwijst de Autoriteit naar het (kritische) advies dat gezamenlijk is uitgebracht door het Europees Comité voor gegevensbescherming en de Europese Toezichthouder voor gegevensbescherming: EDPS-EDPB Joint Opinion 03/2021 *on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, 10 maart 2021 (hierna « het gezamenlijk advies EDPB-EDPS »)¹²².
78. Drie kenmerken van deze verordening verdienen bijzondere aandacht.
79. Ten eerste wordt het toepassingsgebied van de verordening data governance gedefinieerd in relatie tot het toepassingsgebied van de richtlijn hergebruik van gegevens¹²³. Met betrekking tot het hergebruik van persoonsgegevens is de richtlijn inzake hergebruik alleen van toepassing op persoonsgegevens die (onvoorwaardelijk) vrij toegankelijk zijn voor het publiek, zonder beperking. De verordening datagovernance gaat verder door van toepassing te zijn op het hergebruik van andere persoonsgegevens die worden aangetroffen in documenten die in het bezit zijn van overheidsinstanties, d.w.z. de "beschermde gegevens" waarnaar wordt verwezen in artikel 3.1 van de verordening data governance.

¹²¹ Zie voetnoot 5

¹²² Beschikbaar op:

https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_en, laatst geraadpleegd op 4 oktober 2023.

¹²³ Zie de artikelen 1, 2^o en 3.1, d) en overweging 10 van de verordening data governance.

80. Ten tweede, hoewel deze verordening verder gaat dan het toepassingsgebied wat betreft het hergebruik van persoonsgegevens, houdt zij geen verplichting in om het hergebruik van deze beschermde gegevens toe te staan: het is aan de nationale wetgeving om het hergebruik daarvan te regelen¹²⁴.
81. Ten derde doet de data governance verordening geen afbreuk aan de AVG en de nationale wetgeving inzake gegevensbescherming en wordt bovendien expliciet bepaald dat in geval van strijdigheid met de AVG en de nationale wetgeving inzake gegevensbescherming, deze twee laatste voorrang hebben¹²⁵.

II.5.2. Omzetting van de Richtlijn hergebruik - artikelen C.IV 17 tot C.IV.30

82. Voor de betrokken documenten vloeit het toepassingsgebied van de bepalingen van het ontwerp tot omzetting van de richtlijn hergebruik (artikelen C.IV.17 tot en met C.IV.30), voort uit de artikelen C.IV.17, 1°, en C.IV.19. In het bijzonder bepaalt artikel C.IV.19, § 2, 6° en 8°, dat het hoofdstuk in kwestie niet van toepassing is op de volgende twee soorten documenten : «*documenten waartoe de toegang wettelijk beperkt is, met name in gevallen waarin een persoonlijk of specifiek belang vereist is om toegang tot de documenten te krijgen* » ; «*documenten waartoe de toegang is uitgesloten of beperkt op grond van toegangsregels ter bescherming van persoonsgegevens alsmede op delen van documenten waartoe op grond van die regels toegang is verleend en die persoonsgegevens bevatten waarvan het hergebruik door een wettelijke bepaling onverenigbaar is verklaard met de wetgeving betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens of afbreuk doet aan de bescherming van de persoonlijke levenssfeer en de integriteit van de betrokkene, met name gelet op de bepalingen van het recht van de Unie of het nationale recht inzake de bescherming van persoonsgegevens*» (onderstreept door de Autoriteit).
83. Gezien de bestaande relatie tussen de regels inzake toegang tot documenten in het bezit van overheidsinstanties en de regels inzake het hergebruik van dergelijke documenten, verwijst de Autoriteit naar haar eerdere opmerking over de noodzaak om een belang te kunnen aantonen in het kader van passieve openbaarmaking van de administratie. Op dit punt moet het dispositief van het ontwerp worden aangepast om duidelijk aan te geven welke persoonsgegevens kunnen worden hergebruikt op grond van de regels die de richtlijn inzake hergebruik omzetten: Dit zijn gegevens die vrij toegankelijk zijn voor het grote publiek, zonder enige beperking¹²⁶, d.w.z. onvoorwaardelijk

¹²⁴ Zie artikel 5, 1, van de verordening datagovernance. In overweging 11 van de verordening datagovernance staat duidelijk «*elke lidstaat (moet) daarom kunnen beslissen of gegevens toegankelijk wordengemaakt voor hergebruik, en over het doel en de reikwijdte van die toegang.*».

¹²⁵ Zie artikel 1.3 van de verordening data governance.

¹²⁶ De gevallen die onder de richtlijn hergebruik vallen, waarin specifieke wetgeving het hergebruik van de betrokken gegevens zou classificeren als onverenigbaar met de oorspronkelijke wetgeving op basis waarvan de gegevens vrij toegankelijk zijn, moeten worden opgenomen in de gevallen van beperking.

toegankelijk. Andere persoonsgegevens vallen binnen het toepassingsgebied van de verordening data governance. Opmerking : het lijkt erop dat de werkingssfeer van het ontwerp voor dit doel kan worden opgesteld aan de hand van het concept van «*open gegevens*»¹²⁷, desgevallend aangepast, zoals vastgelegd in artikel A.III.1.13) van het ontwerp. Dit moet door de aanvrager worden geverifieerd¹²⁸.

84. Voor het overige lijkt de Autoriteit uit het dispositief van het ontwerp op te maken dat het beschikbaar stellen van gegevens voor hergebruik een "valorisatie" van de gegevens in de zin van het ontwerp vormt¹²⁹, en dat het bijgevolg aan de verwerkingsverantwoordelijke is om te bepalen of de gegevens moeten worden geanonimiseerd, gepseudonimiseerd of anderszins, overeenkomstig artikel C.III.14., § 3 van het ontwerp, aangezien de bepalingen met betrekking tot het hergebruik van documenten geen wettelijke regeling voor de verwerking van persoonsgegevens in deze context bevatten.
85. In dit verband moet het dispositief van het ontwerp in de eerste plaats duidelijk maken dat de mededeling van gegevens voor hergebruik inderdaad een «*valorisatie*» is dat onderworpen is aan de regeling van artikel C.III.14, § 3, tweede lid, van het ontwerp. Ten tweede moet deze bepaling worden verduidelijkt, zodat er geen twijfel bestaat over de gegevensbeschermingsregeling die de verwerkingsverantwoordelijke moet toepassen¹³⁰.
86. Afhankelijk van het vastgesteld stelsel vestigt de Autoriteit de aandacht van de aanvrager, mutatis mutandis, ook op de overwegingen 23-24 van haar advies nr. 144/2023. Overweging 24 preciseert met name het volgende «*Aangezien de anonimisering of pseudonimisering van gegevens in beginsel een gegevensverwerking vereist die verder gaat dan «een eenvoudige handeling», is de Autoriteit van mening dat het ontwerp de relatie moet verduidelijken tussen enerzijds de verplichting van een overheidsinstantie om geanonimiseerde of gepseudonimiseerde documenten beschikbaar te stellen voor hergebruik en anderzijds de afwezigheid van enige verplichting van diezelfde instantie om documenten beschikbaar te stellen in een vorm die een onevenredige inspanning zou vergen en die verder gaat dan een eenvoudige handeling [...]*» (vet in dit advies weggelaten door de Autoriteit)

II.5.3. Uitvoering van de verordening data governance - artikelen C.IV.31 tot en met C.IV.32

87. Met betrekking tot het hergebruik van andere persoonsgegevens, in overeenstemming met de Data Governance Verordening, wijdt het ontwerp twee bepalingen hieraan, namelijk artikel C.IV.31 dat

¹²⁷ Zie voetnoot 5

¹²⁸ Artikel C.IV.17, 1° van het ontwerp is enigszins dubbelzinnig omdat het als volgt luidt : «*het hergebruik van vrij toegankelijke open documenten en onder de in deze titel beschreven voorwaarden toegankelijke deelbare documenten overeenkomstig de omzetting van Richtlijn (EU) 2019/1024 van het Europees Parlement en de Raad van 20 juni 2019 inzake open data en het hergebruik van overheidsinformatie (herschikking)*» (ondertreep door de Autoriteit).

¹²⁹ Zie overweging 20, laatste streepje en de definitie van het begrip "valorisatie" onder voetnoot 11.

¹³⁰ Dit punt wordt verder besproken in de overwegingen 141 en volgende.

hieronder is weergegeven, en artikel C.IV.32 dat een beroepsmogelijkheid organiseert. Zie artikel C.IV.31 van het ontwerp:

« § 1 . Onverminderd bijzondere bepalingen geeft deze titel uitvoering aan 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

§2. De Overheidsinstanties staan het hergebruik toe, voor commerciële of niet-commerciële doeleinden, van de beschermde gegevens die in hun bezit zijn en die uitsluitend zijn geproduceerd met het oog op de uitvoering van hun taken van openbare dienstverlening of verplichtingen van algemeen belang» (onderstreept door de Autoriteit).

88. Met andere woorden, de bepalingen van het ontwerp verplichten overheidsinstanties in zeer algemene zin, en zonder te verwijzen naar de regels inzake toegang tot informatie, om de persoonsgegevens die zij verwerken in het kader van de uitoefening van hun taken beschikbaar te stellen voor hergebruik, waarbij het aan hen is om a priori te bepalen onder welke voorwaarden¹³¹ (zie hierover overweging 84, die mutatis mutandis van toepassing is op artikel C.III.14, § 3, lid 2, van het ontwerp).

89. In de beperktere context van het toepassingsgebied van de richtlijn hergebruik overwoog de Autoriteit het volgende in de overwegingen 9-11 van haar bovenvermeld advies nr. 203/2021:

« In deze context sluit de richtlijn in principe niet uit dat persoonsgegevens "hergebruikt" kunnen worden^[...]. Met andere woorden, principieel kan het de weg vrijmaken voor twee hoofdcategorieën van gegevensverwerking : enerzijds het anonimiseren van persoonsgegevens om hergebruik van documenten mogelijk te maken ; anderzijds het hergebruik van documenten die persoonsgegevens bevatten (al dan niet gepseudonimiseerd). Deze twee categorieën van verwerking van persoonsgegevens vormen systematisch verdere gegevensverwerkingen die moeten voldoen aan de voorwaarden van artikel 6.4 van de AVG.

Een wetsontwerp zoals dat waar dit advies over gaat, zou naar Belgisch recht een grondslag kunnen bieden voor de verwerking van gegevens door het betrokken overheidsorgaan, die erin bestaat documenten met persoonsgegevens te anonimiseren zodat ze beschikbaar kunnen worden gesteld voor hergebruik. Zodra de geanonimiseerde gegevens buiten het

¹³¹ De memorie van toelichting zegt over artikel C.IV.31 het volgende «d eze bepaling vraagt niet om een specifieke toelichting» Nogmaals, de wettelijke regeling die van toepassing is op hergebruik op grond van de verordening zou voortvloeien uit de toepassing van artikel C.III.14, § 3, voor zover enerzijds het beschikbaar stellen van gegevens voor hergebruik op grond van de *verordening* datagovernance een veronderstelling van "valorisatie" van de gegevens vormt en anderzijds de regels voor hergebruik op grond van deze verordening geen wettelijke regeling voor gegevensbescherming bepalen. Zie overweging 20, laatste streepje en de definitie van het begrip "valorisatie" onder voetnoot 11.

toepassingsgebied van de AVG vallen, is het niet langer nodig om het hergebruik van de gegevens door de aanvrager te onderwerpen aan speciale voorwaarden met betrekking tot gegevensbescherming. En het anonimiseringsproces van de gegevens zal te rechtvaardigen zijn in het licht van de vereisten van artikel 6.4, van de AVG^[...].

Het ontwerp kan ook, of ad-hocbepalingen die zijn opgenomen in wetgeving die meer sectorspecifiek kan zijn, een complexer evenwicht nastreven, waarbij de voorwaarden worden vastgesteld waaronder persoonsgegevens mogen worden hergebruikt door natuurlijke of rechtspersonen die daarom verzoeken, waarbij zo nodig ook gevallen worden uitgesloten waarin het hergebruik van persoonsgegevens onverenigbaar wordt geacht met de bescherming van de rechten en vrijheden van de betrokkenen. In principe zal echter systematisch en concreet moeten worden beoordeeld of aan de voorwaarden van artikel 6.4, van de AVG (verenigbaarheidsanalyse) is voldaan^[...], rekening houdend met eventuele specifieke regels^[...]. Hergebruik zal dan onderworpen zijn aan voorwaarden aan de regels voor gegevensbescherming, en persoonsgegevens zullen, desgevallend, gepseudonimiseerd worden om hergebruik mogelijk te maken» (verwijzingen weggelaten en onderstreept door de Autoriteit in dit advies).

90. Aangezien de aanvrager duidelijk de bedoeling heeft om met de bovengenoemde bepaling de doelstelling van een zo ruim mogelijk hergebruik van informatie in het bezit van overheidsinstanties te ondersteunen, ook wanneer deze informatie persoonsgegevens bevat, verzoekt de Autoriteit de aanvrager kennis te nemen van de overwegingen 38-45 van haar advies 167/2022, die eveneens betrekking hebben op de omzetting van de richtlijn inzake hergebruik. In de overwegingen 46 tot en met 48 van dit advies heeft de Autoriteit het volgende verduidelijkt, in een geval waarin het hergebruik van gegevens wordt overwogen ingevolge de toepassing van de regels inzake de toegang tot dergelijke gegevens :

« Ten tweede vereist hoofdstuk 4 van het ontwerp dat de verspreide of beschikbaar gestelde informatie wordt hergebruikt. In deze fase van de gegevensverwerking, wanneer het hergebruik van gegevens wordt overwogen, volgt uit de regels voor toegang of uit de regels voor de verspreiding van informatie (met inachtneming van de voorgaande overwegingen) dat de aanvrager toegang kan krijgen tot alle of een deel van de gewenste informatie.

In een dergelijke context is de Autoriteit van mening dat ontwerp nr. 1 principieel de verantwoordelijkheid kan laten aan de overheidsinstantie om bij de tenuitvoerlegging van de AVG en in het bijzonder van de beginselen van doelbinding en minimalisering van de betrokken gegevens, te bepalen of de betrokken gegevens kunnen worden hergebruikt onder pseudonimisering of anonimisering, of zelfs zoals ze zijn. ^[...],

Zij wijst er echter van meet af aan op dat deze instantie in dit stadium een potentieel complexe en belangrijke verantwoordelijkheid heeft en vestigt de aandacht van de aanvrager en de betrokken verwerkingsverantwoordelijken op de volgende beginselen betreffende anonimisering en pseudonimisering» (verwijzing weggelaten en onderstreept door de Autoriteit in dit advies).

91. Met betrekking tot dit punt van de afstemming tussen de regels voor toegang en die voor hergebruik, bepaalt artikel 3.3.b) van de verordening data governance dat de verordening het Unierecht en het nationale recht inzake de toegang tot documenten onverlet laat. In dit geval moeten de bepalingen van het dispositief van het ontwerp duidelijk aangeven of het voorziet in een nieuw kanaal voor toegang tot documenten (optie 1) met het oog op hergebruik, of dat hergebruik alleen mogelijk is na de uitoefening van een reeds bestaand kanaal voor toegang tot gegevens (optie 2) .
92. De Autoriteit wijst erop dat in de tweede zienswijze (optie 2 - reeds bestaand toegangskanaal) de verantwoordelijkheid van de betrokken overheidsinstantie tweeledig is :
- Het is zijn verantwoordelijkheid om de toepassingsvoorwaarden van de wetgeving te controleren met betrekking tot de toegang tot de persoonsgegevens in kwestie (kan de aanvrager bijvoorbeeld toegang krijgen tot de nominatieve lijst van afdelingshoofden van een directoraat-generaal van een overheidsinstantie ; kan hij toegang krijgen tot een volledige gerechtelijke beslissing waarin een overheidsinstantie partij was; kan hij toegang krijgen tot het dossier met de lijst van buitenlandse dienstreezen van de directeur van een administratie ; etc.) ; en
 - na te gaan of het geplande hergebruik van gegevens in overeenstemming is met artikel 5.1.b) en artikel 6.4 van de AVG (met dien verstande dat het ontwerp, dat hergebruik slechts op een algemene manier toestaat¹³²), niet kan worden gelezen als een bepaling die zou voldoen aan de doelstellingen van artikel 23 van de AVG). Met andere woorden, er moet een verenigbaarheidsanalyse worden uitgevoerd, waarbij rekening wordt gehouden met het doel dat wordt nagestreefd door de wetgeving die de toegang regelt.

93. In de eerste benadering (optie 1 - nieuw en specifiek toegangskanaal voor hergebruik) zou het hergebruik van documenten niettemin een verdere verwerking van gegevens blijven. Dit gezegd

¹³² Als het al nodig zou zijn om te herinneren aan de verordening data governance, bevestigt overweging 53 van bovengenoemd gezamenlijk advies van EDPB en EDPS dat « *in light of the objective and content of the Proposal, the EDPB and the EDPS consider that the Proposal cannot be invoked as Union law constituting a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1) of the GDPR in order to ground the processing for a purpose other than that for which the personal data has been initially collected, where such processing is not based on consent, as per Article 6(4) of the GDPR* ».

hebbende, zal bij de uit te voeren verenigbaarheidsanalyse rekening moeten worden gehouden met het doel dat de overheidsinstantie nastreeft met de verwerking van de betreffende gegevens (met andere woorden, haar taak van openbaar belang).

94. In overweging 77 van het gezamenlijke EDPB-EDPS-advies gingen de Europese instellingen zo ver om te stellen dat « *the EDPB and EDPS strongly recommend to amend the Proposal so as to clarify that the re-use of personal data held by public sector bodies may only be allowed if it is grounded in Union or Member State law which lays down a list of clear compatible purposes for which the further processing may be lawfully authorised or constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23 of the GDPR* » (onderstreping en vet door de Autoriteit).
95. De Autoriteit benadrukt dat een dergelijke aanpak wat zij eerder al aangaf ¹³³, de verdienste heeft dat het meer rechtszekerheid biedt voor verwerkingsverantwoordelijken (overheidsinstanties en hergebruikers) en betrokkenen.
96. Meer recentelijk, met betrekking tot de vraag of persoonsgegevens gepseudonimiseerd of anoniem gemaakt moeten worden voordat ze opnieuw gebruikt mogen worden, heeft de Autoriteit het volgende standpunt ingenomen in de overwegingen 10-12 van haar advies nr. 144/2023 :

« Dit gezegd zijnde, vestigt de Autoriteit ook de aandacht van de aanvrager op de overwegingen 17- 19 van haar advies nr. 203/2021 van 25 oktober 2021 (Nederlandse vertaling niet beschikbaar) concernant un projet de décret n° 2020/279 de la Commission communautaire française relatif aux données ouvertes et à la réutilisation des informations du secteur public (betreffende een ontwerpdecreet nr. 2020/279 van de Franse Gemeenschapscommissie inzake open gegevens en het hergebruik van overheidsinformatie) (CO-A-2021-196), volgens welke:

« [...] het is belangrijk om te benadrukken dat de stand van de techniek en de anonimiseringstechnieken evolueren, net als de (al dan niet openbaar) beschikbare gegevens die de gegevens identificeerbaar zouden maken vanuit het oogpunt van de ontvangers van de geanonimiseerde gegevens (bijv. nieuwe mogelijkheden om betrokkenen opnieuw te identificeren in geval van een datalek, publicatie van andere gegevensreeksen die nog niet beschikbaar waren op het moment van anonimisering, enz.[...]). In een dergelijke context zal de al dan niet geanonimiseerde status van gegevens die niettemin "anoniem" zijn en als zodanig worden meegedeeld (d.w.z. als

¹³³ Zie overweging 89, 4de lid.

vallend buiten de werkingssfeer van de AVG) in de loop van de tijd variëren. Op een zodanige manier dat anonimisering van persoonsgegevens op basis van "de-identificatie" van de gegevens (op basis van een van de technieken die hierboven zijn genoemd - randomisatie, enz.), ie vervolgens als zodanig worden meegegeed aan de aanvragers voor hergebruik van gegevens, ertoe kan leiden dat de aanvrager gegevens deelt die opnieuw identificeerbaar worden zonder dat de aanvrager - a posteriori - de verspreiding ervan kan beperken.

Bovendien kunnen deze technieken de verwerkingsmogelijkheden (en dus het nut) van "geanonimiseerde" gegevens voor de aanvragers van hergebruik en de samenleving als geheel beperken (mogelijk te strikt, afhankelijk van de aard van de oorspronkelijke gegevens en rekening houdend met het doel van het betrokken hergebruik - wat per geval moet worden bekeken).

Daarom vestigt de Autoriteit de aandacht van de aanvrager op andere bestaande technische mogelijkheden die ook zouden kunnen bijdragen tot het hergebruik van de betrokken gegevens, in voorkomend geval op een efficiëntere manier, door bindende technische voorwaarden voor het gebruik van de gegevens te handhaven die door de aanvrager kunnen worden overwogen en door de manier waarop de gegevens ter beschikking van de aanvragers worden gesteld anders te organiseren, zoals bijvoorbeeld via diensten¹³⁴]], (onderstreept door de Autoriteit in dit advies).

Vanuit een meer algemeen perspectief op het hergebruik van overheidsinformatie vestigt de Autoriteit de aandacht van de aanvrager op het belang om rekening te houden met dergelijke andere mogelijkheden. In dergelijke gevallen worden, in plaats van persoonsgegevens (onbewerkt, gepseudonimiseerd of geanonimiseerd) te verstrekken aan de aanvrager die de gegevens opnieuw wil gebruiken, beveiligde toegangsdiensten tot de betreffende gegevens aangeboden door een derde partij (die een vertrouwde derde partij kan zijn) aan[...1]_de aanvrager. Op deze manier kan zowel vanuit normatief oogpunt (gegevensverwerking blijft onderworpen aan de AVG) als vanuit technisch oogpunt een betere controle op gegevensverwerking worden gegarandeerd, terwijl de betreffende gegevens toch kunnen worden hergebruikt. Dergelijke diensten zouden daarom kunnen helpen om zowel de mogelijkheden voor hergebruik van gegevens als de garanties voor de rechten en vrijheden van de betrokkenen te maximaliseren.

¹³⁴ « Zie bijvoorbeeld <https://www.casd.eu>», laatst geraadpleegd op 20/09/2023. Zie ook PARL. GADOUCHE, « The Secure Data Access Centre (CASD), a Service for Datascience and Scientific Research », 22/06/2021, beschikbaar op <https://www.insee.fr/en/information/5014754?sommaire=5014796>, laatst geraadpleegd op 20/09/2023. ».

Gezien de stand van de techniek en de complexiteit van de tenuitvoerlegging van een optimaal anonimiseringsproces van gegevens met betrekking tot de risico's van heridentificatie, is de Autoriteit van mening dat dit type dienst voor gegevenstoegang met het oog op hergebruik voorrang moet krijgen op de verstrekking van (gepseudonimiseerde of geanonimiseerde) gegevenssets, aangezien dit een effectievere methode is om zowel de controle over de verwerking van gegevens als de mogelijkheden voor hergebruik te waarborgen. (verwijzing in dit advies weggelaten)

97. De Autoriteit merkt terloops op dat artikel 5.3 van de verordening data governance, de lidstaten speelruimte laat (en de daarmee gepaard gaande verantwoordelijkheid) om een reeks vereisten vast te stellen om het beschermde karakter van de gegevens te bewaren (toegang na anonimisering, toegang via een beveiligde omgeving die door de betrokken overheidsinstantie ter beschikking wordt gesteld of door haar wordt gecontroleerd, toegang op de locatie waar de beveiligde omgeving zich bevindt, enz). Artikel C.V.13. 1° van het ontwerp kan desgevallend worden uitgebreid om de de mogelijkheid van beveiligde gegevenstoegangsdiensten te organiseren.
98. Hoewel dit concept niet is opgenomen in de regels van het ontwerp voor hergebruik, merkt de Autoriteit op dat het ontwerp niettemin het concept van vertrouwde derde partij¹³⁵ definieert. Zij vestigt de aandacht van de aanvrager op de overwegingen 13-17 van haar advies nr. 144/2023. Meer bepaald overweging 17 van dit advies luidt als volgt:

« Meer in het bijzonder, in het licht van de bovengenoemde normatieve kaders, en onverminderd eventuele overwegingen die de Autoriteit nuttig kan achten om in de toekomst over dit onderwerp uit te brengen, is de Autoriteit van mening dat de volgende elementen relevant zijn bij het uitwerken van dergelijke bepalingen en het denkproces ter zake, onder voorbehoud van de mogelijkheid van hun tenuitvoerlegging onder Europees recht (wat aan de aanvrager is om te verifiëren) :

- *Het vaststellen van voorwaarden met betrekking tot de relatie tussen de betrokken overheidsinstantie en de aanvrager enerzijds en de vertrouwde derde anderzijds. In dit opzicht moet de vertrouwde derde partij in het bijzonder onafhankelijk zijn van de overheidsinstantie en de aanvrager van het hergebruik ;*
- *Bepalen van de verantwoordelijkheden van de betrokken partijen met betrekking tot gegevensverwerking (pseudonimisering, anonimisering of beveiligde gegevenstoegangsdienst). Met name in dit verband, gezien de onafhankelijkheid van de*

¹³⁵ Zie voetnoot 10.

vertrouwde derde partij, de gespecialiseerde deskundigheid die van haar wordt verwacht en de specifieke verplichtingen die op haar zouden rusten op dit gebied, het feit dat zij de essentiële kenmerken zal bepalen (ook al is het niet uitgesloten dat de betrokken overheidsinstantie ook bepaalde beslissingen moet nemen in het kader van bijvoorbeeld de tenuitvoerlegging van een anonimiseringsproces) van de diensten die zij aanbiedt, is de Autoriteit van mening dat de vertrouwde derde partij moet worden beschouwd als de gezamenlijke verantwoordelijke voor de verwerking van gegevensanonimisering of pseudonimisering, samen met de betrokken overheidsinstantie ;

- *Het vastleggen van voorwaarden met betrekking tot de aangeboden dienst/gegevensverwerking. Er kan bijvoorbeeld een verplichting zijn om gegevens te vernietigen zodra ze anoniem zijn gemaakt, een principieel verbod om gegevens te verwerken met de bedoeling de betrokkenen opnieuw te identificeren, een verbod om gegevens voor andere doeleinden te verwerken en een verplichting om aan een hoog betrouwbaarheidsniveau te voldoen. In dit verband is de Autoriteit zich bewust van de moeilijkheid om de toepassing van technische en, waar nodig, procedurele garanties op hoog niveau te waarborgen binnen het kader van een certificeringstelsel, en tegelijkertijd de ontwikkeling van innovatie op dit gebied mogelijk te maken, zodat overheidsinstanties over een relevant en toereikend aanbod van (vertrouwde) diensten kunnen beschikken. Meer in het algemeen is het aan de aanvrager om ervoor te zorgen dat de voorwaarden die hij stelt het beste evenwicht vormen tussen een hoog garantieniveau en de mogelijkheid om te innoveren en diensten te ontwikkelen op het gebied van pseudonimisering, anonimisering of beveiligde toegang tot gegevens. ;*
- *Het bepalen van transparantieverplichtingen. Dergelijke verplichtingen kunnen bijvoorbeeld betrekking hebben op de verklaring/kennisgeving van vertrouwde derden en de publicatie van hun identiteit, en het uitvoeren van externe¹³⁶ audits. Wat anonimisering betreft, zijn transparantieverplichtingen met betrekking tot het anonimiseringsproces en de maatregelen die zijn geïmplementeerd om de risico's van heridentificatie te beperken, evenals de compromissen die in dit kader zijn gesloten, relevant;*
- *Voorwaarden vaststellen voor aanbieders van vertrouwde derde partijdiensten. Dergelijke voorwaarden hebben met name betrekking op het expertiseniveau in gegevensverwerking (pseudonimisering, anonimisering, veilige toegang tot gegevens), de stand van de techniek en de financiële draagkracht».*

¹³⁶ Op gebied van sociale verkiezingen, zie bijvoorbeeld overweging 14 van het advies 32/2023 van 9 maart 2023 betreffende een voorontwerp van wet tot wijziging van de wet van 4 december 2007 betreffende de sociale verkiezingen, van de wet van 20 september 1948 houdende organisatie van het bedrijfsleven en van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk (CO-A-2023-030).

99. Concluderend, en gezien de ambities van het ontwerp, is de Autoriteit van mening dat de wettelijke regeling voor het hergebruik van gegevens zoals uiteengezet in artikel C.IV.31 van het ontwerp moet worden uitgewerkt in het licht van de bovenstaande overwegingen.

II.5.4. Openbaarmaking van persoonsgegevens

100. Artikel C.V.10, §3 van het ontwerp bepaalt «*voor elke gegevensset die hergebruikt wordt, vermeldt het Open portaal voor openbare gegevens het aantal en de identiteit van de hergebruikers*».

101. De Autoriteit verwijst eerst en vooral naar overweging 42 van dit advies, betreffende de openbaarmaking van persoonsgegevens.

102. De Autoriteit is van mening dat de openbaarmakingmaatregel in het ontwerp a priori kan worden gerechtvaardigd met betrekking tot het hergebruik van gegevens in de zin van de richtlijn inzake hergebruik en de verordening data governance, gezien de mogelijkheden die deze teksten bieden. Een dergelijke transparantiemaatregel zal waarschijnlijk de uitvoering van de gegevensbeschermingsregels effectief versterken (ook wanneer persoonsgegevens anoniem zijn gemaakt voor hergebruik), met inbegrip van het verstrekken van informatie aan de betrokkene. Het doeleinde, dat moet worden gespecificeerd, zou daarom op zijn minst erin moeten bestaan de betrokkenen te informeren over het hergebruik dat wordt verricht om de uitoefening van hun rechten onder de AVG te vergemakkelijken.

103. Met dit in gedachten definieert artikel A.III.1.71 het begrip «*hergebruik*»¹³⁷ zonder uitdrukkelijke verwijzing naar de omzetting van de richtlijn hergebruik en de toepassing van de verordening data governance, of met andere woorden, zonder uitdrukkelijke verwijzing naar verzoeken om hergebruik die binnen de werkingssfeer van deze Europese wetgevingen vallen¹³⁸. Bijgevolg kan niet worden uitgesloten dat het "*gebruik door natuurlijke personen*" van documenten die zijn verkregen op grond van de regels inzake toegang tot administratieve documenten (passieve administratieve openbaarheid) binnen het toepassingsgebied valt van de openbaarheidsmaatregel waarin het ontwerp voorziet. Omgekeerd zou een dergelijke algemene openbaarheidsmaatregel onevenredig lijken. Alternatieve

¹³⁷ Als volgt:

« *het gebruik door natuurlijke personen of rechtspersonen van documenten die in het bezit zijn van:*

a) Overheidsinstanties voor andere commerciële of niet-commerciële doeleinden dan de oorspronkelijk doelstelling binnen de taak van openbare dienstverlening waarvoor de documenten zijn geproduceerd, met uitzondering van de uitwisseling van documenten tussen Overheidsinstanties uitsluitend met het oog op de vervulling van hun taak van openbare dienstverlening, of

b) overheidsbedrijven, voor andere commerciële of niet-commerciële doeleinden dan de oorspronkelijk doelstelling om de diensten van algemeen belang te leveren waarvoor de documenten zijn geproduceerd, met uitzondering van de uitwisseling van documenten tussen overheidsbedrijven en Overheidsinstanties, uitsluitend met het oog op de vervulling van hun taak van openbare dienstverlening ».

¹³⁸ De toelichting stelt niettemin dat de definitie in kwestie «*een omzetting is van artikel 2, 11, van de richtlijn PSI*».

maatregelen, waaronder een individueel recht op toegang voor betrokkenen, zouden voldoende kunnen zijn om voldoende transparantie voor betrokkenen te waarborgen.

104. De Autoriteit schort haar analyse van een dergelijke mogelijkheid op, maar lijkt uit de logica van het ontwerp te begrijpen dat het niet de bedoeling van de auteur is om deze in het ontwerp op te nemen. Met andere woorden, de aanvrager zou zich kunnen beperken tot het beperken van de reikwijdte van de voorgestelde openbaarmakingsmaatregel zoals aangegeven in overweging 102.

II.5.5. Hoofdstuk 4 – 'Data-altruïsme'

105. Tot slot behandelt artikel C.IV.33 van het ontwerp de kwestie van data altruïsme. Het bepaalt dat:

« § 1 . Onverminderd bijzondere bepalingen geeft deze titel uitvoering aan 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

§ 2. Via het Contactpunt van het Brussels Gegevensplatform organiseert de platformbeheerder het data-altruïsme voor alle Overheidsinstanties door persoonsgegevens en alle andere gegevens die vrijwillig ter beschikking zouden worden gesteld voor doeleinden van algemeen belang mee te delen. ».

106. De Autoriteit benadrukt dat de tenuitvoerlegging van de verordening op dit punt onvolledig is en dat data altruïsme niet kan worden geïmplementeerd met de huidige bepalingen van het ontwerp. Het is immers aan het nationale recht van de lidstaten om de doelstellingen van algemeen belang vast te stellen waarvoor data altruïsme kan worden toegestaan¹³⁹.

II.6. COMMISSIE VOOR TOEGANG TOT BESTUURSDOCUMENTEN EN GEGEVENS ("CTBG")

II.6.1. Een ander beroeps- en adviesorgaan dan een gegevensbeschermingsautoriteit

107. Het CTBG is een onafhankelijke en onpartijdige administratieve autoriteit waarvan de leden worden benoemd door de uitvoerende macht¹⁴⁰. Het bestaat uit drie kamers, één voor de toegang tot bestuursdocumenten, één voor het hergebruik van gegevens en één voor het delen van bestuursgegevens. Het project geeft het CTBG een reeks beroepsbevoegdheden (in het bijzonder

¹³⁹ Zie artikel 2, 16 van de Verordening Data Governance. Cf. eveneens artikel 16 van dezelfde Verordening.

¹⁴⁰ Zie artikel B.II.3, § 3 van het ontwerp over onafhankelijkheid en onpartijdigheid en artikel B.II.7. dat het volgende bepaalt «De leden van de Commissie worden gezamenlijk benoemd door de Regering, het Verenigd College en het College voor een termijn van 5 jaar, die eenmaal kan worden verlengd».

tegen afwijzingen van verzoeken om toegang tot documenten, tegen weigeringen om gegevens te rectificeren, tegen besluiten van een overheidsinstantie met betrekking tot het administratief delen van gegevens of het hergebruik van gegevens) en adviesbevoegdheden (ook met betrekking tot het administratief delen van gegevens en het hergebruik van gegevens)¹⁴¹. Het heeft ook de bevoegdheid om beslissingen van de overheid te herzien, de bevoegdheid om zelf gegevens of documenten door te geven¹⁴² en onderzoeks- en dwangbevoegdheden¹⁴³. In de memorie van toelichting legt uit dat het ontwerp « (...) *de functie van het CTBG (organiseert) als hoedster van de rechtmatigheid van de gegevensstromen binnen het Brussels Hoofdstedelijk Gewest*» (vet toegevoegd door de Autoriteit).

108. De Autoriteit neemt nota van het feit dat het ontwerp de laatstgenoemde niet aanwijst als een gegevensbeschermingsautoriteit in de zin van de AVG en dat het de Brusselse controlecommissie afschaft waarin de artikelen 31 en volgende voorziet van de Brusselse ordonnantie van 8 mei 2014 *betreffende de oprichting en organisatie van een gewestelijke dienstenintegrator*.

II.6.2. Systematische gegevensoverdracht naar de CTBG

109. Artikel B.II.19 van het ontwerp voorziet in een verplichting voor de overheidsinstanties die betrokken zijn bij de bij CTBG ingediende beroepen, het CTBG systematisch en binnen 7 werkdagen te informeren over het document of de milieu-informatie waarvoor toegang of rectificatie wordt gevraagd, of de gegevens die vallen onder de gevraagde administratieve uitwisseling of de gegevens die vallen onder het gevraagde hergebruik.

110. De Autoriteit is van mening dat een dergelijke systematische mededeling van gegevens, wanneer het om persoonsgegevens gaat, onevenredig is. In overeenstemming met de beginselen van doelbinding en minimale gegevensverwerking is het aan het CTBG om de mededeling van gegevens te eisen indien en wanneer dit noodzakelijk is voor de uitvoering van zijn taken. Het kan niet worden uitgesloten (integendeel) dat de feitelijke mededeling van de betreffende persoonsgegevens in concreto niet noodzakelijk is voor het CTBG om zijn taken uit te voeren.

111. Hetzelfde commentaar geldt *mutatis mutandis* voor artikel B.II.20, § 1, 3de lid van het ontwerp.

II.6.3. Andere bevoegdheden van de CTBG

112. Artikel B.II.19, §3 van het ontwerp bepaalt: «*Indien de Commissie, ondanks de in § 1 en § 2 bedoelde bevoegdheden, de in lid 2 bedoelde documenten niet verkrijgt, stelt zij het Parlement van het Gewest,*

¹⁴¹ Zie artikel B.II.3 van het ontwerp.

¹⁴² Zie artikel B.II.23 van het ontwerp.

¹⁴³ Zie artikel B.II.19 van het ontwerp.

van de Franse Gemeenschapscommissie en van de Gemeenschappelijke Gemeenschapscommissie, alsmede de Regering, het College en het Verenigd College daarvan onverwijld in kennis, die onmiddellijk nieuwe sancties en de procedure daaromtrent vaststellen» (onderstreept door de Autoriteit).

113. De Autoriteit is er niet zeker van dat zij de reikwijdte van deze bepaling volledig begrijpt. Het wijst er in elk geval op dat als de bevoegdheden en sancties in kwestie een nieuwe verwerking van persoonsgegevens inhouden (bijvoorbeeld de bevoegdheid om persoonsgegevens te laten meedelen, om betrokkenen te ondervragen, enzovoort), de essentiële elementen daarvan in een ordonnantie of decreet moeten worden vastgelegd.

II.6.4. Advies van de Gegevensbeschermingsautoriteit

114. Met betrekking tot de termijn om uitspraak te doen over beroepen die bij haar worden ingesteld, bepaalt artikel B.II.20, § 2, 1^o, van het ontwerp dat de termijn van 60 dagen wordt opgeschort «*wanneer de Commissie om het advies van de Gegevensbeschermingsautoriteit heeft gevraagd, tot de ontvangst van dat advies*».

115. In dit verband wijst de Autoriteit erop dat zij alleen kan worden geraadpleegd volgens de procedures van de WOG. Verzoeken om advies kunnen worden ingediend bij het Kenniscentrum van de Autoriteit onder de voorwaarden van artikel 23 van de WOG (wat het geval is bij voorliggend advies). De CTBG behoort echter niet tot de autoriteiten die bevoegd zijn om overeenkomstig deze bepaling een adviesaanvraag bij de Autoriteit in te dienen.

116. Anderzijds kan het Algemeen Secretariaat van de Autoriteit ook een advies uitbrengen aan een verwerkingsverantwoordelijke, zij het in het beperkte geval van een gegevensbeschermingseffectbeoordeling, na raadpleging door de verwerkingsverantwoordelijke van de Gegevensbeschermingsautoriteit¹⁴⁴, wanneer de betrokken verwerking ondanks de door de verwerkingsverantwoordelijke geplande risicobeheersmaatregelen nog steeds een hoog restrisico inhoudt¹⁴⁵.

117. De overheidsinstantie die betrokken is bij het beroep dat wordt ingediend bij de CTBG handelt als een verwerkingsverantwoordelijke wanneer ze beslist over toegang tot een bestuursdocument of tot milieu-

¹⁴⁴ Artikel 20, §1, 3^o van de WOG.

¹⁴⁵ Zie hiervoor <https://www.gegevensbeschermingsautoriteit.be/professioneel/acties/dpia-voorafgaandelijke-raadpleging>, en de handleiding die de Autoriteit publiceerde op volgend adres <https://www.gegevensbeschermingsautoriteit.be/publications/handleiding-gegevensbeschermingseffectbeoordeling.pdf>, laatst geraadpleegd op 08/09/2023.

informatie, wanneer ze administratieve gegevens deelt of wanneer ze beslist over een verzoek tot hergebruik van informatie.

118. De hoedanigheid van de CTBG als verwerkingsverantwoordelijke met betrekking tot de verwerkingen in de dossiers die aan CTBG zijn voorgelegd, is *a priori* echter minder duidelijk. Deze laatste is onpartijdig en onafhankelijk en artikel B.II.23, § 1 van het ontwerp bepaalt dat :

« De Commissie heeft een herzieningsbevoegdheid en kan zelf toegang verlenen tot bestuursdocumenten, milieu-informatie en de verbetering daarvan. Ze kan toegang verlenen tot de gegevens bedoeld door een administratieve deling of hergebruik aan de voorwaarden die zij vastlegt. In dat geval gelast de Commissie de Overheidsinstantie zich te voegen naar haar beslissing en deze uit te voeren binnen de door haar vastgestelde termijn van ten hoogste 30 dagen».

119. Onder deze voorwaarden kan de CTBG ook worden beschouwd als verwerkingsverantwoordelijke voor het administratief delen en meedelen van gegevens na een verzoek om toegang of hergebruik. Afhankelijk van de manier waarop zij handelt, hetzij alleen met behulp van de gegevens die eerder door de overheidsinstantie zijn verstrekt, hetzij in overleg met de betrokken overheidsinstantie waaraan zij een bevel richt, kan zij worden beschouwd als verwerkingsverantwoordelijke of als medeverantwoordelijke voor de verwerking (voor zover zijn bevel reikt). In deze context kan de CTBG een verzoek indienen bij de Gegevensbeschermingsautoriteit onder de voorwaarden van artikel 20, § 1, 3° van de WOG.

II.6.5. Openbaarmaking van de beslissingen van de CTBG

120. Het voornoemd artikel B.II.24 bepaalt het volgende:

« De Commissie maakt op haar website als bedoeld in artikel B.II.26 de beslissingen, adviezen en voorstellen die zij aanneemt binnen 20 werkdagen na de aanneming ervan bekend.

Tenzij de aanvrager vooraf toestemming heeft gegeven voor een openbaarmaking met naam en toenaam, voert de Commissie voor de openbaarmaking een anonimisering uit van de beslissingen. Zij laat tevens alle gegevens weg die zij als vertrouwelijk beschouwt» (onderstreept door de Autoriteit).

121. Nogmaals, het is aan het dispositief van het ontwerp om de wettelijke regeling vast te stellen die van toepassing is op de toestemming in kwestie, alhoewel het ontwerp het begrip toestemming definieert

door te verwijzen naar de AVG¹⁴⁶. Opnieuw vestigt de Autoriteit de aandacht van de aanvrager op het feit dat het van cruciaal belang zal zijn om de betrokkenen hierover naar behoren te informeren, met name gezien het feit dat wanneer de betrokken gegevens eenmaal via internet beschikbaar zijn gesteld, het over het algemeen illusoir zal zijn om te proberen de verdere verspreiding ervan te controleren.

122. Vervolgens is deze anonimiseringsmaatregel (of toestemmingsmaatregel) alleen van toepassing op CTBG "*beslissingen*". Het is de verantwoordelijkheid van de aanvrager om na te gaan of de "*adviezen*" of "*voorstellen*" van CTBG waarschijnlijk persoonsgegevens bevatten en, zo ja, om vergelijkbare waarborgen voor de rechten en vrijheden van de betrokkenen te implementeren.

II. 7. GEGEVENSBEHEER

II.7.1. Toepassingsgebied (onbepaald) en verplichte toepassing van de regels van het wetboek

123. Deel C van het wetboek is gewijd aan gegevensbeheer en het toepassingsgebied *ratione personae* is gedefinieerd in het licht van het toepassingsgebied van de richtlijn inzake hergebruik, zoals uitgelegd in de memorie van toelichting.
124. Bovenal moeten de opschriften van de verschillende titels of bepalingen worden verduidelijkt, zodat er geen twijfel bestaat over de bindende reikwijdte van de regels in deel C van het wetboek. Zo bevat Boek C.II algemene beginselen, of : leidende beginselen die volgens de memorie van toelichting «*interpretatiesleutels aan(geven) voor de bepalingen, rechten en verplichtingen die worden verleend door het Wetboek*»; strategische doelstellingen, namelijk volgens de memorie van toelichting «*de standaarden, uitgedrukt in termen van aanpak en governance, die de overheden op lange termijn moeten bereiken door de toepassing van de bepalingen van het Wetboek*», of operationele doelstellingen, dwz volgens de memorie van toelichting «*de concrete initiatieven die de Overheidsinstanties moeten nemen met het oog op het bereiken van de strategische doelstellingen*». In principe zijn de relevante bepalingen opgesteld als verplichtingen.
125. Boek C.III, getiteld «*Governanceverplichtingen van de overheidsinstanties*», beschrijft verschillende verplichtingen waarvan de toepassing afhangt van de digitale categorie waarop een overheidsinstantie zich bevindt, in overeenstemming met de beslissing van de Regering, het Verenigd College en het College. Het behoren tot een van de drie categorieën zal afhangen van digitale drempels die moeten worden vastgesteld door de regering, het Verenigd College en het College. Het ontwerp bepaalt echter niet welke bepalingen van toepassing zullen zijn op de verschillende categorieën (met uitzondering

¹⁴⁶ Zie overwegingen 35--37 (ook betreffende eventuele noodzaak om daarbij een recht van bezwaar in te voeren) en de overwegingen 14 ev.

van de eerste categorie, waarop alle verplichtingen van toepassing zijn) en is op dit punt uitdrukkelijk onvolledig¹⁴⁷. De Autoriteit maakt daarom nog geen analyse van dit onderwerp.

II.7.2. Toepasselijke wettelijke regelingen op gegevens

126. Artikel C.II.15/15 van het ontwerp luidt als volgt:

« Wanneer dit relevant is en in verhouding tot de nagestreefde doelstelling staat, maken de Overheidsinstanties gebruik van traceerbaarheid en de omkeerbaarheid van gegevens, met uitzondering van de aannames waarvoor de anonimisering is vereist, overeenkomstig de toepasselijke wet- of regelgeving » (onderstreept door de Autoriteit).

127. De Autoriteit is van mening dat een dergelijke bepaling in een gezamenlijk decreet en ordonnantie (d.w.z. een norm van wettelijke rangorde) een bron van rechtsonzekerheid kan zijn. De Autoriteit is van mening dat overheidsinstanties de relevante wettelijke regelingen moeten naleven wanneer ze digitale partnerschappen aangaan.

II.7.3. Omkeerbaarheid van de gegevens

128. Artikel C.II.18 van het ontwerp luidt als volgt:

« Wanneer dit relevant is en in verhouding tot de nagestreefde doelstelling staat, maken de Overheidsinstanties gebruik van traceerbaarheid en de omkeerbaarheid van gegevens, met uitzondering van de aannames waarvoor de anonimisering is vereist, overeenkomstig de toepasselijke wet- of regelgeving

De Overheidsinstanties gebruiken de informatica-instrumenten die de opspoorbaarheid en omkeerbaarheid van de gegevens en tegelijkertijd de bescherming ervan toelaten» (onderstreept door de Autoriteit).

¹⁴⁷ Artikel C.III.1 van het ontwerp luidt als volgt:

« Toepassingsgebied van dit boek per categorie

De Regering, het College en het Verenigd College stellen gezamenlijk de bepalingen van dit boek vast die van toepassing zijn op bepaalde categorieën van Overheidsinstanties, ingedeeld aan de hand van digitale drempels. Elke digitale drempel heeft een bijbehorend digitale categorie dat de omvang van de digitale activiteit en de digitale maturiteit van de overheidsinstanties binnen die drempel bepaalt.

De eerste categorie moet aan alle verplichtingen van dit boek voldoen

Voor de tweede categorie gelden de artikelen XXX.

Voor de derde categorie gelden de artikelen XXX. ».

129. Eerst en vooral is de Autoriteit van mening dat het ontwerp moet verduidelijken wat "*omkeerbaarheid*" van gegevens inhoudt. Technisch gezien zijn het niet de gegevens zelf die 'omkeerbaar' zijn, maar de functie (verwerking) die de gegevens transformeert. Dit gezegd hebbende, begrijpt de Autoriteit uit het ontwerp dat het doel zou zijn om de vorige staat van een gegeven terug te kunnen halen wanneer het tijdens zijn levenscyclus is veranderd en daardoor is aangepast. Met andere woorden, het gaat erom de historiek van de gegevens te waarborgen.
130. In dit licht, en meer dan waarin het dispositief van het ontwerp voorziet, is de Autoriteit van mening dat de omkeerbaarheid van gegevens ook niet mogelijk is wanneer de gegevens moeten worden vernietigd krachtens de toepasselijke wetgeving of zelfs wanneer zij niet langer kunnen worden verwerkt door de overheidsinstantie die verwerkingsverantwoordelijke is. Meer in het algemeen en fundamenteeler wil de Autoriteit erop wijzen dat het feit dat een gegeven omkeerbaar is in de zojuist beschreven zin, niet betekent dat de vorige toestand in elk geval kan worden hersteld. In het algemeen vormen met name het bewaren van gegevens in de vorige staat of het terugbrengen van gegevens naar een vorige staat een verwerking van persoonsgegevens die in concreto moet worden gerechtvaardigd in overeenstemming met de AVG (en het toepasselijke Brusselse of andere regelgevingskader).
131. Artikel C.III.16, lid 2, 4° van het ontwerp lijkt in overeenstemming te zijn met deze logica, hoewel het onvolledig is in die zin dat het bepaalt dat gegevens die in het bezit zijn van overheidsinstanties «*omkeerbaar zijn, onverminderd de toepasselijke wettelijke bepalingen, als omschreven in artikel B.II.XX*». » (Sic).

II.7.4. Typologie van gegevenscategorieën

132. Artikel C.III.10, §1 van het ontwerp bepaalt :,

« De gegevens behoren tot een van de volgende categorieën, afhankelijk van hun eigendomsstructuur, die de regels voor het gebruik ervan bepalen:

1° persoonsgegevens;

2° exclusieve gegevens;

3° openbare gegevens;

4° hoogwaardige gegevens;

5° gegevens van particuliere herkomst» (onderstreept door de Autoriteit).

133. De Autoriteit benadrukt dat deze categorieën gegevens elkaar niet uitsluiten. Persoonsgegevens kunnen bijvoorbeeld openbare gegevens zijn in de zin van het ontwerp. Met andere woorden, de ontwerpbevestiging moet worden aangepast om rekening te houden met het feit dat gegevens tot

verschillende gegevenscategorieën kunnen behoren, afhankelijk van de manier waarop ze worden gebruikt.

134. Voor het overige is het aan de aanvrager om de nodige conclusies te trekken bij de implementatie van het ontwerp.

II.7.5. Valorisatie van gebruiksgegevens

135. Artikel C.III.13 van het ontwerp luidt als volgt:

« *De Overheidsinstanties verzamelen en valoriseren de gebruiksgegevens onder meer om:*

- 1° gebruiksprofielen in kaart te brengen, die wijzen van betrokkenheid bij inhoud of gebruiksgewoonten aangeven; ;*
- 2° de leesbaarheid van en de toegang tot hun diensten te verbeteren;*
- 3° andere gebruikers of burgers te informeren dan de gebruikers of burgers die uit de reeds verzamelde gebruiksgegevens zijn geïdentificeerd;*
- 4° de vertegenwoordiging van de gebruikers van hun diensten te verbeteren ;*
- 5° de privacy van de gebruikers te beschermen door weigeringen en toestemmingen te verzamelen als gebruiksgegevens »¹⁴⁸(onderstreept door de Autoriteit).*

136. Ten eerste wil de Autoriteit, voor zover deze bepaling een grondslag kan vormen voor het verzamelen van persoonsgegevens, erop wijzen dat zij, in overeenstemming met de beginselen van voorspelbaarheid en rechtmatigheid die zijn vastgelegd in artikel 8 van het EVRM en artikel 22 van de Grondwet, de essentiële elementen van de verwerking die zij toestaat, uitputtend moet beschrijven. Ten eerste moet het woord "onder meer" uit de bepaling worden weggelaten.

137. Ten tweede merkt de Autoriteit op dat de bepaling in kwestie niet duidelijk is en niet voldoet aan de eisen die voortvloeien uit de zojuist genoemde beginselen. Zij moet worden uitgewerkt en de Autoriteit schort haar analyse ervan op. De uitgangspunten waarnaar wordt verwezen in 3° en 4° zijn bijzonder vaag. Naast het doel van de bepaling, dat voor alle betrokken verwerkingen uitputtend moet worden omschreven, moeten ook de categorieën betrokkenen duidelijk worden geïdentificeerd, aangezien de begrippen "gebruiker" in de Franse versie "utilisateur", gebruiker(in de Franse versie "usager") of burger verschillend lijken te zijn¹⁴⁹.

¹⁴⁸ Zie voetnoot 3 voor de begrippen "données d'usage et d'6.

¹⁴⁹ De memorie van toelichting verduidelijkt als volgt: «*Gebruiksgegevens kunnen worden gebruikt door Overheidsinstanties die deze in de eerste plaats verzamelen ter verbetering van de kwaliteit van hun digitale diensten en de manier waarop deze worden aangeboden.*

Dankzij de valorisatie van gebruiksgegevens kunnen Overheidsinstanties hun digitale diensten personaliseren en meer ergonomisch of "user friendly" maken, met het oog op een voortdurende verbetering van de openbare dienst of de

138. In dit verband merkt de Autoriteit op dat het begrip gebruiker in de definitie van gebruiksgegevens (d.w.z. de persoon die toegang heeft tot de gegevens) verschilt van het begrip gebruiker in de bovengenoemde bepaling, die verwijst naar betrokkenen wier gegevens worden gebruikt (verwerkt) door hun gebruiker (een verwerkingsverantwoordelijke).
139. De Autoriteit merkt op dat het begrip toestemming in de AVG, waarnaar in het ontwerp wordt verwezen, in beginsel wordt gedefinieerd als «*elke vrije specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt*» (onderstreept door de Autoriteit). Met andere woorden, in principe zal de betrokkene die geen toestemming geeft of onverschillig blijft, passief zijn in plaats van "weigeren", zodat het ontbreken van toestemming in plaats van de weigering het relevante gegeven zal zijn.
140. Bovendien is de Autoriteit, in overeenstemming met de beginselen van minimale gegevensverwerking en verantwoordingsplicht, van mening dat de relevante en noodzakelijke gegevens die moeten worden verzameld, de geuite toestemmingen zijn en, indien van toepassing, in een later stadium van de verwerking, afhankelijk van de wettelijke regeling die van toepassing is op toestemming, de intrekking van toestemming of het bezwaar tegen gegevensverwerking. Het verzamelen van persoonsgegevens over "weigeren" of het ontbreken van toestemming lijkt niet noodzakelijk.

II.7.6. Eerbiediging van de rechten van derden bij valorisatie van gegevens - toestemming e.d.

141. Artikel C.III.14 van het ontwerp bepaalt het volgende «*bij de valorisatie van de gegevens die zij bezitten, moeten Overheidsinstanties de rechten van derden op de beschermde gegevens eerbiedigen*». Meer specifiek, met betrekking tot gegevensbescherming in het bijzonder, luidt § 3 van deze bepaling als volgt :

« In het kader van de valorisatie van de gegevens die zij bezitten, nemen de Overheidsinstanties de vertrouwelijkheid van de beschermde gegevens in acht.

Tenzij anders bepaald in de toepasselijke wetgeving of toestemming van de betrokken personen, passen de overheidsinstanties hun technieken voor anonimisering of pseudonimisering aan de aard van de verwerkte gegevens en de aan het gebruik ervan verbonden risico's aan ».

verplichtingen van algemeen belang die ze verzekeren» (onderstreept door de Autoriteit). De Autoriteit merkt terloops op dat het ontwerp het begrip "digitale dienst" niet definieert. ».

142. Deze bepaling lijkt van bijzonder belang voor zover zij de wettelijke regeling bepaalt die van toepassing is op het hergebruik van persoonsgegevens¹⁵⁰. Meer in het algemeen lijkt het zelfs de wettelijke regeling voor gegevensbescherming te zijn die, bij gebrek aan specifieke wetgeving, van toepassing is op de mogelijke valorisaties van gegevens.
143. De Autoriteit is daarom van mening dat de formulering moet worden verduidelijkt om een ondubbelzinnige handelwijze van de verwerkingsverantwoordelijke aan te geven. Zoals het is geformuleerd, zou artikel C.III.14 van het ontwerp in feite kunnen impliceren dat, tenzij anders bepaald, de verwerkingsverantwoordelijke geen niet-gepseudonimiseerde of geanonimiseerde persoonsgegevens openbaar mag maken met het oog op (bijvoorbeeld) hergebruik. De memorie van toelichting lijkt deze aanpak echter niet te ondersteunen, en laat de keuze om ruwe, gepseudonimiseerde of geanonimiseerde persoonsgegevens al dan niet openbaar te maken over aan de verwerkingsverantwoordelijke¹⁵¹. Met andere woorden, het dispositief van het ontwerp moet duidelijk maken dat de verwerkingsverantwoordelijke moet bepalen of de betrokken gegevens gepseudonimiseerd of geanonimiseerd moeten worden en de gegevensverwerking (pseudonimisering of anonimisering) moet aanpassen aan de risico's van de beoogde gegevensverwerking, tenzij een specifieke regelgevende bepaling van toepassing is.
144. In dit geval verzoekt de Autoriteit de aanvrager echter om het nut van de ontwerpbevestiging te overwegen en deze te benadrukken: de rechtstreekse toepassing van de regels van de AVG vereist al dat de verwerkingsverantwoordelijke bepaalt of gegevens gepseudonimiseerd of geanonimiseerd moeten worden om gegevensverwerking uit te voeren, met name met het oog op de risico's voor de rechten en vrijheden van de betrokkenen. Bij gebrek aan een specifiek vereiste kan men zich afvragen wat het nut is van artikel C.III.14, dat bij wijze van toelichting in de voorbereidende werkzaamheden zou moeten worden opgenomen in plaats van in de wetstekst.
145. Het is ook in deze context dat rekening moet worden gehouden met de opmerkingen van de Autoriteit over de mogelijke invoering van beveiligde gegevenstoegangsdiensten¹⁵².
146. Artikel C.III.14, § 2, 2de lid van het ontwerp bepaalt hierover met betrekking tot de toestemming het volgende *«in voorkomend geval, en onverminderd de bepalingen van andere regelgevingen die van toepassing zijn op de verwerking van de betrokken gegevens, stellen de Overheidsinstanties een*

¹⁵⁰ Zie de overwegingen 81 e.v..

¹⁵¹ Er wordt uitgelegd «de AVG definieert deze twee begrippen, maar zegt niet in welke gevallen men er beroep op dient te doen voor de toepassing van dit Wetboek en in de context van gegevensvalorisatie, moeten deze methoden worden toegepast naargelang de risico's verbonden met het gebruik of hergebruik van de betrokken gegevens. Zo houdt het administratief delen tussen Overheidsinstanties niet dezelfde risico's in als een hergebruik».

¹⁵² Zie overweging 96..

dynamisch toestemmingsmechanisme in» (onderstreept door de Autoriteit). In de memorie van toelichting wordt nog op het volgende gewezen:

« Lid 2 voorziet in de invoering van een zogenaamde "dynamische" methode van toestemming.

Deze methode, die ook in andere delen van de wereld wordt toegepast (zie met name het Canadese voorbeeld in 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 60 e.v.) zorgt voor een correct hergebruik van gegevens in de loop van de tijd Dit mechanisme voor het verkrijgen va toestemming_of toelating in de loop van meerdere fasen van gegevensinzameling en -verwerking biedt in het algemeen granulaire opties op verschillende momenten in de levenscyclus van de gegevens. Op verschillende momenten in de levenscyclus van de gegevens dient toestemming of toelating gevraagd voor het gebruik (of hergebruik) van hetzelfde geheel aan persoonsgegevens of andere beschermde gegevens (bv. bedrijfsgeheimen of commerciële informatie) telkens wanneer er een verandering optreedt in de doeleinden voor het verzamelen, verwerken en delen van deze gegevens.

Wanneer Overheidsinstanties deze mogelijkheid aanbieden, waken zij erover dat deze "dynamische" methode van toestemming of toelating voldoet aan de vereisten van de AVG of de DGA wanneer het delen gaat om beschermde gegevens. . Wanneer een Overheidsinstantie de intentie heeft om de beschermde gegevens te delen voor een ander doel dan datgene waarvoor de gegevens zijn ingezameld, stelt zij de houders van de rechten op de gegevens daarvan vooraf in kennis en beschrijft zij de nieuwe risico's die voortvloeien uit deze secundaire deling. De personen moeten hun toestemming of toelating kunnen intrekken indien zij niet of niet langer gunstig staan tegenover het secundair delen van hun gegevens » (onderstreept door de Autoriteit).

147. De Autoriteit neemt nota van deze bepaling en deze uitleg, die aanleiding geven tot de volgende zes opmerkingen. Ten eerste moet de toestemming van de betrokkene niet alleen opnieuw worden gevraagd als het doel van de verwerking verandert, maar ook voor elke verwerking van persoonsgegevens op basis van toestemming. Met andere woorden, in het geval van bijvoorbeeld hergebruik van gegevens is het niet voldoende dat de betrokkene toestemming geeft voor een specifiek verwerkingsdoel (hij kan er bijvoorbeeld mee instemmen dat de verwerking wordt uitgevoerd door verwerkingsverantwoordelijke A, maar niet door verwerkingsverantwoordelijke B).

148. Ten tweede is de AVG cumulatief van toepassing met de Data Governance Verordening, wanneer de beschermde gegevens in kwestie persoonsgegevens zijn.

149. Ten derde wijst de Autoriteit erop dat het delen van administratieve gegevens, d.w.z. de uitwisseling van gegevens tussen overheidsinstanties, niet kan worden gebaseerd op de toestemming van de betrokkene (artikel 6.1.a), van de AVG)¹⁵³, hoewel niet kan worden uitgesloten dat in bedoelde gevallen rekening wordt gehouden met de wilsautonomie van de betrokkene in de gevallen bedoeld in artikel 6.1., onder c) en e), van de AVG), teneinde de evenredigheid van de beoogde gegevensverwerking te waarborgen en een passende waarborg ten gunste van de betrokkenen ten uitvoer te leggen. Ook in een dergelijk geval moet de wettelijke regeling die van toepassing is op de overeenkomst in kwestie worden bepaald door de betreffende specifieke norm.¹⁵⁴
150. Ten vierde en zoals hierboven al is aangegeven, moet het dispositief van het ontwerp de wettelijke regeling bepalen die van toepassing is op de (intrekking van de) toestemming¹⁵⁵.
151. Ten vijfde is de Autoriteit van mening dat het dispositief van het ontwerp zelf de verplichting moet bevatten om de betrokkene te informeren, in het bijzonder «*beschrijft zij de nieuwe risico' die voortvloeien uit deze secundaire deling*». Dit is een nuttige garantie voor de eerbiediging van de rechten en vrijheden van de betrokken personen.
152. Ten zesde beveelt de Autoriteit aan dat de aanvrager het "*dynamisch toestemmingsmechanisme*" voor de verwerking van persoonsgegevens in het dispositief van het ontwerp definieert, rekening houdend met bovenstaande overwegingen.

II.7.2. Beroep in het kader van gegevensvalorisatie

153. Artikel C.III.14, § 4 van het ontwerp bepaalt het volgende:

« Onverminderd de rechten van de betrokkenen en de door de AVG georganiseerde beroepsmiddelen, organiseren de Overheidsinstanties de nodige beroepsmiddelen zodat de houders van rechten op beschermde gegevens een klacht kunnen indienen bij de bevoegde diensten of personen binnen de Overheidsinstanties zodra zij menen dat hun rechten niet worden geëerbiedigd of worden bedreigd» (onderstreept door de Autoriteit)

154. De Autoriteit maakt uit de memorie van toelichting op dat het niet de bedoeling is dat deze bepaling van toepassing is op geschillen in verband met de verwerking van persoonsgegevens. Volgens de

¹⁵³ Zie de overwegingen 45--46.

¹⁵⁴ Zie voor een recente toepassing het advies 83/2023 van de Autoriteit van 27 april 2023 *over een Voorontwerp van ordonnantie tot wijziging van de ordonnantie van 4 april 2019 betreffende het elektronisch uitwisselingsplatform voor gezondheidsgegevens (CO-A-2023-147)*, overweging 26-28.

¹⁵⁵ Zie ook overweging 37.

memorie van toelichting laat deze bepaling dus niet alleen de rechten van betrokkenen en de door de AVG georganiseerde rechtsmiddelen tegen verwerkingsverantwoordelijken onverlet, maar is zij ook niet van toepassing op klachten over de verwerking van persoonsgegevens. Het dispositief moet in deze zin worden verduidelijkt.

155. Voor het overige vestigt de Autoriteit de aandacht van de aanvrager op de beginselen van voorspelbaarheid en rechtmatigheid die zijn vastgelegd in artikel 8 van het EVRM en artikel 22 van de Grondwet, volgens welke de essentiële elementen van de verwerking van persoonsgegevens moeten worden vastgelegd in een bepaling van wettelijke rangorde. In het onderhavige geval biedt de ontwerpbeeping, gezien het specifieke toepassingsgebied ervan, een zekere mate van voorspelbaarheid met betrekking tot het doel van de verwerking (beroep om rechten te doen gelden op beschermde gegevens), de (categorieën van) verwerkte gegevens (gegevens met betrekking tot de indiener van het beroep, de houder van de betrokken rechten, de betrokken verwerkingsverantwoordelijken) en de ontvangers van de gegevens (de betrokken verwerkingsverantwoordelijken, met inbegrip van de betrokken overheidsinstantie).

156. Niettemin is de Autoriteit enerzijds van mening dat ten minste één regelgevende norm de beoogde rechtsmiddelen moet vaststellen (en niet alleen de overheidsinstanties, die geen normatieve bevoegdheid hebben).

157. En ten tweede moet het dispositief van het ontwerp ook duidelijk maken wat de relatie is tussen de voorgestelde rechtsmiddelen en eventuele andere rechtsmiddelen die beschikbaar zijn voor de betrokken rechthebbenden, en duidelijk de betrokken handelingen aangeven waarop de voorgestelde rechtsmiddelen van toepassing zijn, evenals de autoriteit tot wie de rechtsmiddelen moeten worden gericht. Dit zijn essentiële elementen die verband houden met het doel van het rechtsmiddel in kwestie en die ook doorslaggevend zijn vanuit het oogpunt van de betrokkene, die op basis van zijn verplichtingen en strategie moet beslissen of en welk rechtsmiddel hij tegen een nadelige handeling wil instellen.

158. Het is dus in de eerste plaats aan de Raad van State om te beslissen over de te bieden rechtsmiddelen, met dien verstande dat deze niet van toepassing zijn op klachten over gegevensverwerking.

II.7.8. Bijwerken van de gegevens

159. Artikel C.III.16, 3de en 4de lid luiden als volgt:

« De Overheidsinstanties bepalen de frequentie waarmee de gegevens die zij bezitten worden bijgewerkt.

De Overheidsinstanties zorgen in elk geval voor:

- 1° de garantie van de hoogste bijwerkingsfrequentie, rekening houdend met de aard van de verwerkte gegevens en de beoogde doelstelling ervan ;*
- 2° de documentatie en de openbaarmaking van de bijwerkingsfrequentie van de gegevens die zij bezitten;*
- 3° de garantie dat de houders van rechten op de beschermde gegevens de gegevens te allen tijde kunnen bijwerken of wijzigen» (onderstreept door de Autoriteit).*

160. De Autoriteit benadrukt dat een dergelijke bepaling op zichzelf geen grondslag kan vormen voor het verzamelen van gegevens (of het kruisen van gegevens) met het oog op het bijwerken van de betrokken gegevens, tenzij in een dergelijke gegevensverzameling (of gegevensvergelijking) reeds is voorzien door de regels die van toepassing zijn op de taak van algemeen belang (of wettelijke verplichting) van de betrokken overheidsinstantie die de grondslag vormt voor de gegevensverwerking krachtens artikel 6.1 van de AVG. Ter illustratie: dit beginsel is met name relevant in gevallen waarin betrokkenen worden *gescreend*¹⁵⁶, een situatie waarin de verwerkingsverantwoordelijke in de verleiding zou kunnen komen om een aanvullende gegevensverwerking te initiëren op grond van het feit dat de betrokken gegevens bijgewerkt moeten worden in toepassing van de AVG.

161. Met andere woorden, de Autoriteit is van mening dat artikel C.III.16 van het ontwerp ook moet specificeren dat het bijwerken van gegevens alleen mag worden georganiseerd binnen de grenzen die zijn toegestaan door de regels die gelden voor de taak van algemeen belang of de wettelijke verplichting waarop de gegevensverwerking in kwestie is gebaseerd. In deze context is het zeer waarschijnlijk dat de overheidsinstantie niet in staat zal zijn om bijvoorbeeld op eigen initiatief gegevens te verzamelen met een door haar vastgestelde frequentie (van de betrokkene bijvoorbeeld door periodiek hierom te verzoeken) om de gegevens bij te werken die zij verwerkt.

II.7.9. Referentiegegevens

162. Artikel C.III.17 bepaalt met name dat de overheidsinstanties de referentiegegevens "*verspreiden*". Aangezien de referentiegegevens betrekking kunnen hebben op natuurlijke personen¹⁵⁷, schort de Autoriteit haar analyse op van deze bepaling, waarvan de reikwijdte niet is vastgesteld en die moet worden verduidelijkt (wat wordt bedoeld met "verspreiden", aan wie en met welk doel).

¹⁵⁶ Zie bijvoorbeeld in een ander domein, het advies *245/2022 van 21 oktober 2022 van de Autoriteit met betrekking tot een voorontwerp van wet betreffende de gemeentelijke bestuurlijke handhaving, de instelling van een gemeentelijk integriteitsonderzoek en houdende oprichting van een Directie Integriteitsbeoordeling voor Openbare Besturen (CO-A-2022-248)*, overwegingen 51 en 56, advies *231/2021 van 3 december met betrekking tot een voorontwerp van ordonnantie betreffende de interoperabiliteit van elektronische tolheffingssystemen voor het wegverkeer (CO-A-2021-227)*, overwegingen 62-63.

¹⁵⁷ Zie voetnoot 7.

163. Artikel C.III.17 bepaalt ook dat overheidsinstanties betrouwbare metagegevens moeten opstellen waarmee met name de soorten gegevens die worden gevaloriseerd of gedeeld¹⁵⁸, de locatie van de gegevens, de oorsprong van de gegevens, enz. kunnen worden vastgesteld, evenals «*de entiteit die verantwoordelijk is voor de gegevens*». Gezien de reikwijdte van deze bepaling is de Autoriteit van mening dat ook moet worden voorzien in de identificatie van verwerkingsverantwoordelijken.

II.7.10. Analytische modellen, algoritmen en artificiële intelligentie

164. Artikel C.III.18 van het ontwerp handelt over «*het beheer van de analytische modellen, algoritmen en systemen die gebruik maken van artificiële intelligentie*». In dit verband zal de Autoriteit zich beperken tot het verwijzen naar het voorstel van verordening van het Europees Parlement en de Raad *tot vaststelling van geharmoniseerde regels betreffende kunstmatige intelligentie (wetgeving inzake kunstmatige intelligentie) en tot wijziging van bepaalde wetgevingshandelingen van de Unie*, en naar daarmee verband houdende debatten¹⁵⁹, en tot het innemen van bepaalde standpunten die zij reeds heeft ingenomen over besluitvorming uitsluitend op basis van geautomatiseerde verwerking als bedoeld in artikel 22 van de AVG en het gebruik van algoritmen, met inbegrip van met name :

- de overwegingen 15-17 van het advies 231/2022 van 29 september 2022 *betreffende een voorontwerp van wet houdende diverse fiscale en financiële bepalingen, Titel 9 - Wijzigingen van de wet van 16 december 2015 tot regeling van de mededeling van inlichtingen betreffende financiële rekeningen, door de Belgische financiële instellingen en de FOD Financiën, in het kader van een automatische uitwisseling van inlichtingen op internationaal niveau en voor belastingdoeleinden, artikel 85 (CO-A-2022-226)*, waarin de Autoriteit in het bijzonder het volgende stelt «*een met een algoritme uitgevoerde voorselectie van belastingplichtigen met het oog op een grondigere controle, een geautomatiseerd besluit blijft met name wanneer de beoogde menselijke tussenkomst beperkt blijft tot de eenvoudige systematische bekrachtiging van de voorselectie door een ambtenaar. In een dergelijke situatie houdt de menselijke tussenkomst immers geen verband met het besluitvormingsproces, waarvoor het algoritme exclusief verantwoordelijk is*»; en overweging 18 van datzelfde advies waar de Autoriteit nog het volgende opmerkt «*met betrekking tot de verwerking van de selectiegegevens die zal worden ingevoerd (d.w.z. de risicoanalyse en de criteria die tot een controle leiden) [is het] wenselijk parameters [...] en combinaties daarvan te gebruiken waarvan vaststaat dat zij een duidelijke correlatie hebben met de beoogde fraude. Dit is doorslaggevend voor de evenredigheid van de beoogde verwerking en voor de kwaliteit van de verwerkte gegevens, aangezien de verwerking doeltreffend moet zijn bij in het verwezenlijken van haar doel*.

¹⁵⁸ Opgemerkt moet worden dat delen een geval van valorisatie zou zijn.

¹⁵⁹ COM(2021) 206 final. Zie ook <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence>, laatst geraadpleegd op 10/10/2023).

Bijvoorbeeld, verkeerde fraudeindicatoren bepalen om belastingplichtigen te identificeren waarvoor een grondige controle nodig is, impliceert dat, in strijd met artikel 5, lid 1, punt c), van de AVG, ontoereikende en niet-relevante gegevens worden verwerkt. In deze context is het noodzakelijk te voorzien in een testfase, voorafgaand aan de invoering van de verwerking» (vet weggelaten in dit advies).

- Overweging 13 van het advies 203/2022 van 9 september 2022 *m.b.t. een voorontwerp van wet houdende diverse fiscale en financiële bepalingen – artikel 76 (CO-A-2022-158)* benadrukt het belang van transparantie met betrekking tot de persoonsgegevens die worden verwerkt om het algoritme te trainen, de kwaliteitscriteria die zullen worden gebruikt en de concrete gevolgen voor betrokkenen wanneer zij worden verdacht van mogelijke fraude (in dit geval ging het om belastingfraude) op basis van de resultaten van de algoritmen ;
- Overweging 46 van het advies 135/2020 van de Autoriteit van 11 september 2020 *over het wetsvoorstel (Parl. Doc., 55, 0642/006) tot wijziging van de wet van 13 juni 2005 betreffende de elektronische communicatie met betrekking tot de automatische toekenning van het sociaal tarief (CO-A-2020-13)*, waarin een andere passende maatregel wordt geïllustreerd (in dit geval een *opt-outsysteem*) om de rechten en vrijheden van betrokkenen op een bepaald gebied te waarborgen.

165. In dit verband wijst de Autoriteit erop dat artikel 22.1 van de AVG in de context van gegevensverwerking door overheidsinstanties op zich niet van toepassing is wanneer het nationale recht (of het Unierecht) dit toestaat en wanneer daarin maatregelen zijn vastgesteld om de rechten en vrijheden en gerechtvaardigde belangen van de betrokkenen te waarborgen. In dit verband is het duidelijk dat, hoewel artikel C.III.18 van het ontwerp bijdraagt tot de uitvoering van dergelijke maatregelen, het op zichzelf niet kan volstaan als bepaling die een afwijking van artikel 22.1 van de AVG toestaat.

166. In dit opzicht moet het ontwerp altijd worden gelezen in samenhang met het regelgevingskader waarin de opdracht van algemeen belang of de wettelijke verplichting die op de betrokken overheidsinstantie rust, wordt gedefinieerd, met dien verstande dat dit regelgevingskader het nemen van geautomatiseerde individuele besluiten al dan niet zal toestaan en zal omkaderen met aanvullende maatregelen die specifiek zijn voor het gebied dat het regelt (in aanvulling op artikel C.III.18 van het ontwerp) en die van dien aard zijn dat de rechten en vrijheden van de betrokken personen worden gewaarborgd.

II.8. DE VERANTWOORDELIJKHEDEN MET BETREKKING TOT DE VERWERKING VAN PERSOONSGEGEVENS

167. Als inleidend punt herinnert de Autoriteit aan haar adviespraktijk met betrekking tot het vaststellen van verantwoordelijkheden met betrekking tot de verwerkingsverantwoordelijke van persoonsgegevens: een overheidsinstantie is in beginsel verantwoordelijk voor de gegevensverwerking die noodzakelijk is voor de vervulling van de haar toevertrouwde taak van algemeen belang (of van een taak in het kader van de uitoefening van het openbaar gezag dat aan haar is verleend)¹⁶⁰ of die noodzakelijk is om te voldoen aan de wettelijke verplichting¹⁶¹ die op haar rust krachtens de norm in kwestie¹⁶². Onlangs heeft zij deze beginselen opnieuw toegepast op de uitwisseling van gegevens tussen overheidsinstanties, in overweging 7 en volgende van haar advies 143/2023.

168. De Autoriteit is van mening dat de transversale reikwijdte van het ontwerp dat bedoeld is om van toepassing te zijn op alle in het Brusselse rechtsstelsel vastgestelde gegevensverwerkingen, zich ertoe kan lenen om in het dispositief van het ontwerp het beginsel op te nemen van de identificatie van de verwerkingsverantwoordelijken, zoals zojuist door de Autoriteit in herinnering is gebracht, onverminderd toepasselijke decreten of ordonnanties¹⁶³. In het kader van het ontwerp en de regelgeving die er gelijktijdig op zal worden toegepast, zal de betrokken overheidsinstantie, waar van toepassing, specifieke verplichtingen hebben met betrekking tot de gegevensverwerking zelf, of, meer in het algemeen, persoonsgegevens moeten verwerken voor het uitvoeren van haar taken van openbaar belang, die op hun beurt verband kunnen houden met de gegevensverwerking.

¹⁶⁰ Artikel 6, lid 1, punt e), van de AVG.

¹⁶¹ Artikel 6, lid 1, punt c), van de AVG.

¹⁶² Zie met name: advies nr. 83/2023 van de Autoriteit van 27 april 2023 over een voorontwerp van ordonnantie tot wijziging van de ordonnantie van 4 april 2019 betreffende het elektronisch uitwisselingsplatform voor gezondheidsgegevens (CO-A-2023-147), overweging 11; advies nr. 129/2022 van 1 juli 2022 betreffende de artikelen 2 en 7 tot en met 47 van een ontwerp van wet houdende diverse bepalingen inzake Economie, overwegingen 42 e.v.; het advies 227/2022 van 29 september 2022 concernant un avant-projet de décret relatif aux données ouvertes et à la réutilisation des informations du secteur public (CO-A-2022-209), overwegingen 17-23 (geen NI vertaling beschikbaar), advies 131/2022 van 1 juli 2022 met betrekking tot een wetsontwerp tot oprichting van de Kunstwerkcommissie en ter verbetering van de sociale bescherming van de kunstwerkers (CO-A-2022-129), overwegingen 55 en volgende, advies nr. 112/2022 van 3 juni 2022 met betrekking tot een ontwerp van wet tot wijziging van het Sociaal Strafwetboek met het oog op de invoering van het eDossier-platform, overwegingen 3-41 en 87-88; advies nr. 231/2021 van 3 december 2021 met betrekking tot een voorontwerp van ordonnantie betreffende de interoperabiliteit van elektronische tolheffingssystemen voor het wegverkeer, overwegingen nrs. 35-37; advies nr. 37/2022 van 16 februari 2022 "oncernant un avant-projet de décret instituant la plateforme informatisée centralisée d'échange de données 'E-Paysage" (niet beschikbaar in het Nederlands), overweging 22; advies nr. 13/2022 van 21 januari 2022 met betrekking tot een ontwerp van besluit van de Brusselse Hoofdstedelijke Regering betreffende de toekenning van premies voor de verbetering van het woonmilieu en een ontwerp van besluit van de Brusselse Hoofdstedelijke Regering tot wijziging van het besluit van de Brusselse Hoofdstedelijke Regering van 9 februari 2012 betreffende de toekenning van financiële steun voor energie, overwegingen 9-17.

¹⁶³ Een dergelijke aanpak helpt ook de volgende zorg weg te nemen die in de toelichting wordt verwoord :

« De persoonsgegevens worden verwerkt in het kader van de diensten van het Platform. Het is nodig, in het licht van de terzake geldende bepalingen en met name de AVG, om de rol te voorzien die de beheerder vervult

Deze rol is qua functie niet dezelfde in functie van de beoogde diensten en is bij uitstek casuïstisch: het zou buiten proportie zijn om een opsomming te geven van elk van de verwerkingen die in het kader van het Platform worden uitgevoerd met daarbij de overeenkomstige rol in het kader van dit Wetboek» (onderstreept door de Autoriteit). De Autoriteit is het niet eens met deze analyse en verwijst in dit verband naar de opmerkingen in het corpus van het advies over de aanwijzing van verwerkingsverantwoordelijken.

169. Het ontwerp zelf bevat een reeks bepalingen waarin verplichtingen/verantwoordelijkheden met betrekking tot gegevensverwerking worden vastgesteld, zonder echter systematisch de verantwoordelijkheden met betrekking tot de verwerkingsverantwoordelijke vast te stellen. Wat echter wel moet gebeuren met betrekking tot de rol van eenieder die is gedefinieerd in het ontwerp¹⁶⁴.
170. Het geval van het CIBG (PARADIGM) is een goed voorbeeld van een instelling waaraan verplichtingen en opdrachten zijn toevertrouwd die rechtstreeks verband houden met de gegevensverwerking, zozeer zelfs dat het ontwerp bij die gelegenheid het CIBG (PARADIGM) een verantwoordelijkheid oplegt met betrekking tot de persoonsgegevensverwerking (bijvoorbeeld met betrekking tot de verwerkingen van het Integratiecentrum)¹⁶⁵. en gezien zijn centrale en essentiële rol mag het ontwerp geen twijfel laten bestaan over de verantwoordelijkheden van het CIBG (PARADIGM) met betrekking tot de verwerking van persoonsgegevens, wat met name inhoudt dat altijd moet kunnen worden vastgesteld of en in welke mate het CIBG gehouden is de instructies van de betrokken overheidsinstanties met betrekking tot de verwerking van persoonsgegevens op te volgen.
171. De Autoriteit herinnert eraan dat op grond van de AVG de verwerker namens de verwerkingsverantwoordelijke optreedt, gegevens alleen verwerkt op de gedocumenteerde instructie van de verwerkingsverantwoordelijke en het doel van en de middelen voor de verwerking niet kan bepalen (tenzij hij als verwerkingsverantwoordelijke wordt geherclassificeerd)¹⁶⁶. Wanneer het ontwerp de verantwoordelijkheid als verwerker aan het CIBG (PARADIGM)¹⁶⁷ toewijst, moet het dit op een precieze en consistente manier doen en ervoor zorgen dat het CIBG (PARADIGM) voor de implementatie ervan verplicht is te handelen, in het kader van de verwerking van persoonsgegevens, in overeenstemming met de instructies van de overheidsinstanties die gebruik maken van zijn diensten

¹⁶⁴ Die in voorkomend geval ook de aangestelde verwerkingsverantwoordelijke kan zijn.

¹⁶⁵ Het eerste en tweede lid van artikel C.V.4 is als volgt geformuleerd:

«de beheerder van het Brussels Gegevensplatform treedt op als verwerkingsverantwoordelijke van de persoonsgegevens die nodig zijn voor het technisch beheer van het Platform en voor alle verwerkingen in het Integratiecentrum.

De beheerder van het Brussels Gegevensplatform treedt namens de Overheidsinstanties op als onderaannemer voor de diensten van de Catalogus, het Open portaal voor openbare gegevens en het Centrum voor gegevensanalyse en gegevensverwerking ».

De memorie van toelichting verduidelijkt als volgt:

«anderzijds, voor wat betreft het Integratiecentrum in het bijzonder, bepaalt de beheerder ook de middelen voor het gebruik van de diensten. Daarom is hij, uitsluitend voor dit deel van het Platform, ten minste medeverantwoordelijk of verantwoordelijk voor de verwerking ».

Het Integratiecentrum valt onder artikel C.V.7 van het ontwerp en maakt administratief delen mogelijk. De functie van de Brusselse dienstenintegrator wordt gedefinieerd in artikel C.V.8. van het ontwerp. Zie overweging 12 van Advies 143/2023 **over de gezamenlijke verantwoordelijkheid van een dienstenintegrator en de verwerkingsverantwoordelijke van een authentieke gegevensbron**.

¹⁶⁶ Artikel 4.1.8) van de AVG en 10 van de AVG.

¹⁶⁷ De enige hypothese die door de Autoriteit wordt genoemd, wordt in voetnoot 168 165.

(Gegevenscatalogus¹⁶⁸, Open Portaal voor gegevens¹⁶⁹ en Centrum voor gegevensanalyse en gegevensverwerking¹⁷⁰).

172. Tot slot, aangezien het ontwerp niet voorziet in de algemene toepassing van de definities van de AVG, moet het de toepassing van de definities van de begrippen verwerkingsverantwoordelijke en verwerker als bedoeld in artikel 4, leden 7 en 8, van de AVG nader specificeren.

II.9. CENTRUM VOOR GEGEVENSANALYSE EN GEGEVENSVERWERKING

173. Het is artikel C.V.11 dat de "Aanmaak en doelstellingen" van het Centrum voor gegevensanalyse en gegevensverwerking vaststelt:

« Er wordt een Centrum voor gegevensanalyse en gegevensverwerking aangemaakt

Het doel van het Centrum voor gegevensanalyse en gegevensverwerking is het aanbieden van facultatieve diensten aan Overheidsinstanties voor de verzameling, de opslag, de verwerking en het verbruik van gegevens» (onderstreept door de Autoriteit)¹⁷¹.

174. Een dergelijke bepaling voldoet duidelijk niet aan de vereisten van voorspelbaarheid en rechtmatigheid die zijn vastgelegd in artikel 8 van het EVMR en artikel 22 van de Grondwet en kan daarom niet worden gebruikt als grondslag voor de verwerking van persoonsgegevens. Om de verwerking van persoonsgegevens toe te staan, zou de voorgestelde bepaling aanzienlijk moeten worden gewijzigd en de Autoriteit schort haar analyse op dit punt op.

¹⁶⁸ Dit is bepaald in artikel C.V.9 van het ontwerp. **Niets in deze bepaling wijst er echter op dat deze catalogus persoonsgegevens zal bevatten**, en de Autoriteit gaat ervan uit dat dit het geval is. Zij is er dan ook niet zeker van dat zij de noodzaak ziet om het CIBG (PARADIGM) als verwerker van de gegevenscatalogus te identificeren.

¹⁶⁹ Als bedoeld in artikel C.V.10 van het ontwerp.

¹⁷⁰ Aangaande dit centrum in het bijzonder, zie de overwegingen 173 en volgende. Hoewel de Autoriteit hierover geen standpunt inneemt, aangezien het ontwerp op dit punt moet worden uitgewerkt, betwijfelt de Autoriteit dat het CIBG (PARADIGM) in deze context als een eenvoudige verwerker optreedt.

¹⁷¹ De memorie van toelichting stelt het volgende:

« Het Centrum voor gegevensanalyse en gegevensverwerking bundelt alle facultatieve diensten en oplossingen die het CIBG aan de overheid aanbiedt. Het bestaat uit verschillende tools voor de opslag, verwerking en analyse van gegevens.

In dit stadium gaat het om hostingoplossingen, diensten voor de analyse van het gebruik (analytics) en diensten o. De platformbeheerder biedt echter uitsluitend diensten aan. Vragen over de aard van de gegevens, de beveiliging en de toegang vallen onder de exclusieve verantwoordelijkheid van de Overheidsinstantie die gebruik maakt van de aangeboden facultatieve diensten.

Wel staat het CIBG, gezien zijn technologische expertise, de overheid bij in de keuzes die moeten worden gemaakt naargelang van de aard van de uit te voeren operatie.

Het is evenwel de bedoeling dat het Centrum voor gegevensanalyse en gegevensverwerking in de toekomst nieuwe facultatieve diensten aanbiedt. In het geval dat diensten verplicht worden gesteld, lijkt een wijziging van dit Wetboek zich op te dringen» (onderstreept door de Autoriteit).

De Autoriteit benadrukt dat het facultatieve karakter van de betrokken diensten de Brusselse wetgever niet ontslaat van de verplichting om de essentiële elementen van de beoogde verwerking van persoonsgegevens vast te leggen.

II.10. BEWAARTERMIJN VAN DE GEGEVENS

175. De transversale aard van het ontwerp betekent dat het over het algemeen niet het enige zal zijn waarmee rekening moet worden gehouden als het gaat om de bewaartermijnen van gegevens. Met dit in gedachten, en indien nodig door te verwijzen naar bepalingen die elders van toepassing zijn (bijvoorbeeld naargelang de administratieve gegevensdeling), moet de auteur van het ontwerp in staat zijn om de bewaartermijnen van gegevens door het CIBG (PARADIGM), de centrale speler in het systeem, vast te stellen voor alle verwerkingen die door laatstgenoemde worden uitgevoerd, zelfs als dit op een functionele basis is¹⁷².

176. Artikel C.V.4 van het ontwerp bepaalt het volgende met betrekking tot de bewaartermijn van gegevens door het CIBG (PARADIGM) (d.w.z. de beheerder van het Brussels Gegevensplatform) :

« [...] »

Met betrekking tot de persoonsgegevens die nodig zijn voor het technisch beheer van het Platform, evenals voor alle verwerkingen van persoonsgegevens die worden uitgevoerd door het integratiecentrum, worden de gegevens gedurende 10 jaar na het einde van de verwerking bewaard.

Onverminderd andere wettelijke bepalingen, in het bijzonder met betrekking tot historische archivering, worden de technische gegevens die nodig zijn voor de werking van de andere diensten van het Platform tot 6 maanden na het einde van de verwerking bewaard.

De gegevens worden vernietigd na het verstrijken van de bovengenoemde termijnen, tenzij ze nodig zijn in het kader van een vervolgonderzoek of voor historische, statistische of wetenschappelijke doeleinden in overeenstemming met de privacywetgeving.

Hiertoe worden de persoonsgegevens geanonimiseerd zodra ze niet meer individueel geïdentificeerd hoeven te worden om de doelen te bereiken waarvoor ze verzameld zijn.

De gegevens kunnen worden meegedeeld aan elke instelling aangewezen door de Regering, het Verenigd College en het College voor verdere verwerking voor historische, statistische en wetenschappelijke doeleinden» (onderstreept door de Autoriteit).

177. De Memorie van Toelichting geeft aan deze bepaling de volgende uitleg:

¹⁷² Dat wil zeggen, in voorkomend geval, door verwijzing naar de regels die gelden voor de betreffende gegevensverwerking.

« Er wordt echter een onderscheid gemaakt in archiveringstijd tussen technische gegevens die betrekking hebben op de werking van het Integratiecentrum en deze van andere diensten.

Gezien de persoonlijke aard van de gegevens die door het Integratiecentrum beschikbaar worden gesteld, is een langere bewaartermijn voor toegangsgegevens gerechtvaardigd als een inbreuk op deze gegevens zou kunnen leiden tot grotere risico's voor de betrokkenen.

Deze periode is korter (6 maanden) als het gaat om toegang tot datasets die geen echte bedreiging vormen voor de privacy (bijv. open data) ».

178. De Autoriteit benadrukt van meet af aan dat de ontwerpbeplanning onduidelijk is en dat het ontwerp de daarin vastgestelde bewaartermijn van gegevens niet rechtvaardigt. De Autoriteit schort haar analyse van de gegevensbewaartermijn door het CIBG (PARADIGM) in het kader van de werking van de diensten van het Brussels gegevensplatform dan ook op. De ontwerpbeplanning moet verduidelijkt worden en moet het mogelijk maken om een duidelijk onderscheid te maken tussen de bewaartermijnen (indien van toepassing, maxima) van de gegevens door het CIBG (PARADIGM), naargelang de betrokken diensten, en, in het kader van een specifieke dienst, naargelang enerzijds de bewuste gegevens het voorwerp uitmaken van de verwerking van persoonsgegevens door de betrokken overheidsinstantie en het CIBG (PARADIGM) in het kader van de dienst, of anderzijds gegevens zijn die in het kader van deze verwerking worden verzameld, met name om de tenuitvoerlegging te garanderen van technische en organisatorische maatregelen die het mogelijk maken de veiligheid van de verwerking te garanderen (logbestanden en toegang, etc.).

179. Als het integratiecentrum bijvoorbeeld technisch zorgt voor administratieve deling via een kanaal dat het op verzoek van een overheidsinstantie instelt¹⁷³¹⁷⁴, is er *a priori* geen reden waarom het de uitgewisselde persoonsgegevens langer zou bewaren dan nodig is voor de uitwisseling *in concreto* tussen de overheidsinstanties. Zodra de gegevens zijn ontvangen, is het delen voltooid. Anderzijds moeten gegevens over de traceerbaarheid van verwerkingsactiviteiten¹⁷⁵ (in dit geval gegevensuitwisseling - die van cruciaal belang zijn voor de doeltreffende tenuitvoerlegging van de gegevensbeschermingsregels en de controle van het betrokken informatiesysteem - langer worden bewaard. Daarom is een bewaartermijn van minstens 10 jaar gerechtvaardigd.

180. Het ontwerp moet ook verduidelijken wat een "*vervolgonderzoek*" is, aangezien dit concept niet gedefinieerd is. Zoals de zaken er nu voor staan, kan een dergelijk doel het bewaren van de gegevens

¹⁷³ Artikel C.V.7. van het ontwerp.

¹⁷⁴ Artikel C.V.8, 2de lid, 5° van het ontwerp.

¹⁷⁵ Toegang tot het gegevens, wijziging van het gegeven, etc;

na de oorspronkelijke bewaartermijn niet rechtvaardigen. De Autoriteit schort haar analyse van dit punt dan ook op.

181. Gezien de aanzienlijke inmenging die het ontwerp met zich meebrengt in de rechten en vrijheden van de betrokkenen en de centrale rol van het CIBG (PARADIGM), benadrukt de Autoriteit in de eerste plaats dat zij voorstander is van de in het ontwerp gevolgde aanpak, die inhoudt dat de gegevens moeten worden vernietigd zodra de bewaartermijn (verwerkingstermijn) is verstreken. Dit is een essentiële garantie voor het behoud van de rechten en vrijheden van de betrokkenen. Deze garantie, die bestaat uit de vernietiging van de gegevens aan het einde van een (of meer) duidelijk in de wet vastgelegde periode(n), is des te belangrijker omdat het CIBG (PARADIGM) een centrale speler is op het gebied van gegevensverwerking in het Brusselse rechtssysteem, zoals hierboven is benadrukt.
182. Dit gezegd zijnde, voorziet artikel C.V.4 van het ontwerp niettemin in verdere verwerking op een algemene manier, voor historische, statistische of wetenschappelijke doeleinden, op een dubbelzinnige manier, zonder duidelijk te definiëren wanneer de gegevens anoniem moeten worden gemaakt. In het bijzonder, moeten zij dit doen wanneer zij voor deze doeleinden worden meegedeeld aan een "*instelling*" aangewezen door de regering? De Autoriteit is van mening dat artikel C.V.4 van het ontwerp moet worden verduidelijkt en schort haar analyse in dit verband op. Terloops merkt ze op dat de memorie van toelichting hierover zwijgt.
183. De ontwerpbevestiging voorziet in de verwerking van persoonsgegevens en bijgevolg moeten de essentiële elementen van een dergelijke verwerking in het dispositief van het ontwerp worden vastgesteld overeenkomstig de beginselen van voorspelbaarheid en rechtmatigheid die zijn vastgelegd in artikel 8 EVRM en artikel 22 van de Grondwet.
184. De ontwerpbevestiging moet met name duidelijk de (categorieën van) gegevens aangeven die waarschijnlijk zullen worden onderworpen aan de beoogde verdere verwerking alsook de verwerkingsverantwoordelijken. De motivering van de noodzaak van de ontwerpbevestiging zal aanzienlijk verschillen naargelang het gaat om het uitvoeren van statistieken of onderzoek in verband met de activiteiten en de werking van het Brussels gegevensplatform (met andere woorden, statistieken en onderzoek met betrekking tot gegevens die door de werking van het platform worden gegenereerd) of in verband met de overheidsinstanties en de specifieke gegevens die door hen worden verwerkt via de diensten van het platform. Deze tweede mogelijkheid vereist in elk geval een speciale rechtvaardiging omdat hetzelfde onderzoek of dezelfde statistieken waarschijnlijk op het niveau van (vanuit) de betrokken overheidsinstantie zullen worden uitgevoerd. Wat statistieken betreft, zal de

omkadering van de verwerkingen met een norm van wettelijke rangorde variëren naargelang de geplande statistieken.¹⁷⁶

185. Bij de rechtvaardiging van de noodzaak om te voorzien in de verdere verwerking van de beoogde gegevens, moet ook rekening worden gehouden met het feit dat het ontwerp zelf de toegang tot en het hergebruik van informatie in het bezit van de Brusselse overheidsinstanties op een zeer ruime manier organiseert, waarbij deze gevallen ook wetenschappelijk onderzoek of statistiek omvatten. In het licht van deze overwegingen moet in de memorie van toelichting worden uitgelegd waarom artikel C.V.4 noodzakelijk is in een context van statistisch of wetenschappelijk onderzoek.

186. Nogmaals, gezien de aanzienlijke inmenging in rechten en vrijheden die het ontwerp met zich meebrengt, is de Autoriteit van mening dat in het ontwerp moet worden verduidelijkt dat de gegevens in elk geval moeten worden geanonimiseerd voor het beoogde doel.

II.11 AANWIJZING VAN URBIS ALS GEGEVENS BANK AFKOMSTIG VAN AUTHENTIEKE BRONNEN

187. Het ontwerp bevat een Titel III "URBIS". Deze aparte titel van het Wetboek bevat zijn eigen definities van de begrippen authentieke bronnen en gegevensbanken afgeleid van authentieke bronnen, die nochtans worden gedefinieerd in het Wetboek Gegevensbeheer dat door het ontwerp is gecreëerd. Het verwijst ook naar de ordonnantie van 8 mei 2014 *tot oprichting en organisatie van een gewestelijke dienstenintegrator*, die door het ontwerp wordt ingetrokken. En het is niet volledig in overeenstemming met de artikelen C.IV.15 en C.IV.16 van het ontwerp (betreffende de aanwijzing van authentieke bronnen)¹⁷⁷. De Autoriteit heeft daarom een voorbehoud ten aanzien van de consistentie van de aanpak in het ontwerp, dat enerzijds het gegevensbeheer regelt in een alomvattend wetboek en anderzijds al een authentieke gegevensbron vaststelt onder het gezag, onvermijdelijk, van een andere wettelijke regeling *sui generis*.

188. De Autoriteit is zich er echter terdege van bewust dat het in dit stadium onmogelijk zou zijn om de aanwijzing van een authentieke bron in volledige overeenstemming met het wetboek te organiseren,

¹⁷⁶ Voor een illustratie van een situatie waarin geen specifiek regelgevingskader vereist is, zie Advies nr. 110/2022 van 3 juni 2022.2022 *over een Koninklijk besluit met betrekking tot de opleiding van professionele gebruikers van biociden* (CO-A-2022-106), overweging 14. Voor een illustratie van een verwerking waarvoor een specifiek rechtskader nodig is, zie Advies nr. 211/2022 van 9 september 2022 *over een ontwerp van Koninklijk besluit houdende de wijziging van het koninklijk besluit van 22 februari 2017 houdende oprichting van de Federale Overheidsdienst Beleid en Ondersteuning* (CO-A-2022-187). Voor een illustratie op het specifieke gebied van overheidsstatistieken, zie advies nr. 35/2023 van 9 februari 2023 *concernant un projet de décret introduisant dans le Code wallon de l'Action sociale et de la santé des dispositions relatives aux programmes de médecine préventive* (CO-A-2022-295) (geen NL versie beschikbaar), overwegingen 56-59, het advies 127/2021 van 28 juli 2021 *met betrekking tot een voorontwerp van wet tot wijziging van de wet van 4 juli 1962 betreffende de openbare statistiek* (CO-A-2021-127).

¹⁷⁷ In titel III wordt bijvoorbeeld het begrip *initiator* gebruikt, dat vreemd is aan het ontwerp van wetboek, en de UrbIS-commissie kan nieuwe gegevens toevoegen aan de gedetailleerde lijst van gegevens die deel uitmaken van het Brusselse UrbIS-product, terwijl in het wetboek terecht wordt bepaald dat het de aanwijzingshandeling is die de lijst van gegevens in de authentieke bron moet bevatten.

aangezien de verschillende vereiste adviezen bijvoorbeeld niet zouden kunnen worden verkregen omdat de betrokken instellingen nog niet bestaan. Dit belet de aanvrager echter niet om enerzijds te verwijzen naar de begrippen die zijn vastgelegd in het wetboek en anderzijds nodigt de Autoriteit de aanvrager uit om te wachten tot het wetboek is geïmplementeerd alvorens verder te gaan met het aanmerken van UrbIS als een authentieke gegevensbron. Aangezien dit een belangrijke authentieke Brusselse bron is, zou het betreuenswaardig zijn als deze niet zou kunnen profiteren van het normatieve kader van het wetboek. Met andere woorden, de Autoriteit beveelt aan om de aanwijzing van UrbIS als authentieke gegevensbron te overwegen na de goedkeuring en inwerkingtreding van het wetboek.

189. Voor het overige, met betrekking tot de verwerking van persoonsgegevens, herhaalt de Autoriteit haar opmerkingen over het concept van een bank/gegevensbank die is afgeleid van authentieke bronnen, dat moet worden losgelaten¹⁷⁸. Daarom moeten in titel III van het ontwerp, in overeenstemming met de hierboven genoemde voorspelbaarheids- en rechtmatigheidsbeginselen, de essentiële elementen worden vastgesteld van de gegevensverwerking in verband met de authentieke bron die het ontwerp beoogt in te voeren.

190. Hoofdstuk 3 van Titel III van het ontwerp, getiteld « *De doelstellingen van Brussels UrbIS als gegevensbank van authentieke bronnen* » bevat een artikel 5 dat als volgt is geformuleerd:

« Brussels UrbIS is, als gegevensbank van authentieke bronnen, het cartografisch basisreferentiekader in het Brussels Hoofdstedelijk Gewest dat het mogelijk maakt om:

- Geografische informatie over elkaar heen te plaatsen;
- De geografische coördinaten van eender welke plaats te kennen, of het nu gaat om een specifiek punt of om een geografisch object dat zich op het gewestelijk grondgebied bevindt;
- Bedrijfsgegevens te digitaliseren en te lokaliseren in eenzelfde referentiekader;
- Gegevens uit te wisselen die met Brussels UrbIS gekoppeld kunnen worden;

¹⁷⁸ Zie de overwegingen 65--71..

In overweging 9 van haar advies 001/2019 van 12 april 2019 *betreffende een voorontwerp van ordonnantie van het Brussels Hoofdstedelijk Gewest tot uitvoering van de ordonnantie van 8 mei 2014 betreffende de oprichting en de organisatie van een gewestelijke dienstenintegrator en tot aanwijzing van de grootschalige kaartendatabank Brussel Urbis als authentieke gewestelijke bron, "plaatst de Brusselse Controlecommissie niettemin vraagtekens bij het feit dat UrbIS een databank blijkt te zijn die is afgeleid van authentieke bronnen en niet een loutere authentieke bron", zonder evenwel verdere details te verstrekken. De Autoriteit merkt op dat het verzoek om een advies van de Controlecommissie aanvankelijk gericht was op de implementatie van een authentieke gegevensbron.*

De Autoriteit merkt op dat de Raad van State geen advies heeft uitgebracht over het ontwerpbesluit dat vervolgens werd voorgelegd aan de Brusselse Controlecommissie, zie <http://www.raadvst-consetat.be/dbx/avis/65845.pdf#search=URBIS>, laatst geraadpleegd op 06/10/2023.

- *De administratieve lasten in het kader van deze ordonnantie te beperken (onderstreept door de Autoriteit*¹⁷⁹.

191. De Autoriteit merkt op dat deze bepaling gegevensverwerkingen identificeert en niet de doeleinden waarvoor ze worden uitgevoerd¹⁸⁰. Met betrekking tot de invoering van een authentieke gegevensbron moet in de wettekst die deze authentieke bron regelt, in de eerste plaats worden bepaald voor welk(e) doel(en) de betrokken (categorieën) persoonsgegevens worden verzameld, waarbij deze doelen onlosmakelijk verbonden moeten zijn met de taak van algemeen belang waarvoor de gegevens aanvankelijk door de verwerkingsverantwoordelijke van de authentieke gegevensbron worden verzameld¹⁸¹.

192. Voor het overige herhaalt de Autoriteit dat de gezamenlijke ordonnantie en het gezamenlijk decreet alle essentiële elementen van de verwerkingen in verband met de authentieke gegevensbron moeten vaststellen, overeenkomstig de beginselen van voorspelbaarheid en rechtmatigheid die zijn vastgelegd in artikel 8 EVRM en artikel 22 van de Grondwet, zoals ook in het ontwerp van wetboek wordt vermeld. De Autoriteit wijst er overigens op dat een instantie zoals het Comité Brussels UrbIS waarnaar wordt verwezen in artikel 11 van Titel III van het ontwerp geen normatieve bevoegdheden heeft en niet bevoegd kan zijn om de essentiële elementen van de gegevensverwerking te bepalen die wordt uitgevoerd op basis van de authentieke gegevensbron.

193. In deze omstandigheden is de Autoriteit niet in staat om haar analyse (die zij opschort) met betrekking tot de erkenning van UrbIS als authentieke gegevensbron voort te zetten.

¹⁷⁹ De toelichting herhaalt alleen het volgende « deze bepaling geeft aan welke doeleinden de databank Brussels UrbIS nastreeft bij het verzamelen van de gegevens die ze verwerkt ».

¹⁸⁰ In de overwegingen 11-12 van haar advies, aangehaald in voetnoot 178178, overwoog de Brusselse Controlecommissie echter het volgende :

« L'article 5 de l'avant-projet d[arrêt] décrit les finalités poursuivies par Brussels UrbIS en tant que source authentique.

Ainsi, « Brussels UrbIS en tant que source authentique, a pour vocation d'être le référentiel cartographique de base en Région de Bruxelles-Capitale, permettant de :

-superposer des informations géographiques de n'importe quel point du territoire de la Région ;

-échanger des données entre partenaires ».

Au vu et dans les limites de ce qui précède, la Commission estime que ces finalités sont déterminées, explicites et légitimes au sens de l'article 5, §1, b) du RGPD ».

Artikel 4 van de AVG bepaalt het begrip verwerking al volgt « een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens ».

¹⁸¹ De memorie van toelichting bij het wetboek zelf erkent deze logica correct:

« Wanneer een Overheidsinstantie een databank creëert en/of beheert, doet zij dat op basis van een rechtsgrondslag die haar deze taak toekent en met inachtneming van de toepasselijke beginselen, met name deze betreffende de persoonlijke levenssfeer. Het hier gecreëerde mechanisme treedt in een tweede fase in werking: zodra binnen een Overheidsinstantie een databank bestaat, kan deze worden aangewezen om te dienen als referentiedatabank, als authentieke bron voor alle of een deel van de erin opgenomen gegevens, voor andere Overheidsinstanties. ».

II.12. BESLUIT

Om deze redenen,
is de Autoriteit de volgende mening toegedaan:

- 1.** Hoewel het ontwerp in sommige opzichten gedurfd en innovatief is, leidt het tot een aanzienlijke inbreuk op de rechten en vrijheden van de betrokkenen en tot een algemeen en belangrijk probleem op het gebied van gegevensbescherming, en wel om de volgende drie redenen: de bepalingen van het ontwerp hebben de neiging om de verwerking van gegevens door de Brusselse overheidsinstanties en in het bijzonder het verkeer van gegevens tussen deze instanties aanzienlijk te vergemakkelijken, in het bijzonder door het nastreven van een concentratiedynamiek op het gebied van gegevensverwerking ; het plaatst een essentiële overheidsinstantie in het hart van de gegevensverwerking in het Brussels Hoofdstedelijk Gewest ; conceptueel lijkt het een bepaalde patrimoniale opvatting van gegevens (al dan niet persoonlijk) in zich te dragen waarvan de concrete gevolgen vaag zijn (**overwegingen 4-22**) ;
- 2.** De noodzaak en evenredigheid van het vergemakkelijken van de verwerking van persoonsgegevens door de Brusselse overheidsinstanties moet worden aangetoond, en de waarborgen tegen de risico's voor de rechten en vrijheden van de betrokkenen moeten worden vastgesteld en in een effectbeoordeling worden belicht (**overwegingen 15 en 27**) ;
- 3.** De noodzaak en evenredigheid van de toewijzing van alle bevoegdheden aan uitsluitend het CIBG (PARADIGM) moet worden aangetoond en de waarborgen tegen de risico's voor de rechten en vrijheden van de betrokkenen moeten worden vastgesteld en in een effectbeoordeling worden aangegeven (**overwegingen 19-17**) ;
- 4.** Het valoriseren van gegevens vormt op zichzelf geen specifiek doel voor het verwerken van persoonsgegevens. De impact van de doelstelling voor gegevensvalorisatie op de verwerking van persoonsgegevens moet duidelijk worden vastgesteld, door in het kader van een effectbeoordeling de inbreng op juridisch vlak, de risico's voor de rechten en vrijheden van de betrokkenen en de geïmplementeerde maatregelen om deze risico's te beperken-, te benoemen (**overwegingen 21-22 en 27**) ;
- 5.** Een algemene bepaling moet specificeren dat het ontwerp geen afbreuk doet aan de AVG en niet kan worden gelezen als een beperking van de rechten van betrokkenen of de verplichtingen van verwerkingsverantwoordelijke (**overweging 26**) ;

6. Artikel B.I.16, § 3, van het ontwerp moet worden aangepast om te garanderen dat - onverminderd een norm van wettelijke rangorde die voorziet in vrije en onvoorwaardelijke toegang van het grote publiek tot de betrokken documenten, om toegang te krijgen tot een administratief document dat persoonsgegevens bevat - de aanvrager het doel moet rechtvaardigen (legitiem, specifiek, enz.) van het beoogde gebruik (verwerking) van de gegevens, wat in sommige gevallen gelijk kan staan aan de eis dat de verwerkingsverantwoordelijke een gerechtvaardigd belang aantoont (**overwegingen 28-32**) ;

7. In de context van passieve openbaarmaking door de administratie moet de verwerkingsverantwoordelijke voldoende speelruimte hebben om de methode voor het meedelen van persoonsgegevens te bepalen, rekening houdend met de technische en organisatorische maatregelen die moeten worden geïmplementeerd in overeenstemming met de AVG (**overwegingen 33-35**) ;

8. Het ontwerp moet duidelijk de rechtsregels bepalen die van toepassing zijn op de toestemming van de betrokkenen wanneer het voorziet in de mogelijkheid om deze te gebruiken (**overwegingen 36-37** - toegang tot milieu-informatie; **overwegingen 120-121** - bekendmaking van de beslissingen van CTBG; - artikel C.III.14, § 3 van het ontwerp

9. Het verwijderen van gegevens uit een gegevensset leidt niet altijd tot het anonimiseren van gegevens (**overwegingen 38-39**) ;

10. Artikel B.I.4 van het ontwerp moet worden gerechtvaardigd en aangepast in overeenstemming met de beginselen van rechtmatigheid en voorspelbaarheid (**overwegingen 40-45**) ;

11. De beginselen voor het delen van administratieve gegevens die zijn vastgelegd in de artikelen C.IV.4 en C.II.3, § 1 van het ontwerp moeten worden herzien in het licht van de beginselen die van toepassing zijn op de uitwisseling van gegevens tussen overheidsinstantie (**overwegingen 46-50**) ;

12. Wat betreft het gebruik van authentieke gegevensbronnen moet artikel C.II.3, § 2, lid 1 van het ontwerp worden aangepast in overeenstemming met het beginsel van minimale gegevensverwerking. Dit is niet alleen om ervoor te zorgen dat de overheid niet zelf het verzamelen van gegevens (van de betrokkene) organiseert. Het beginsel van eenmalige inzameling ontslaat de wetgever niet van de verplichting om een verenigbaarheidsanalyse uit te voeren overeenkomstig artikel 6.4 van de AVG. De reikwijdte van artikel C.IV.13 van het

ontwerp moet worden verhelderd en de Autoriteit schort haar analyse daarvan op. Een authentieke gegevensbron is onderworpen aan de beginselen van voorspelbaarheid en rechtmatigheid die zijn vastgelegd in artikel 8 EVRM en artikel 22 van de Grondwet wanneer deze wordt gebruikt in het kader van de verwerking van persoonsgegevens. Tot slot moet het ontwerp criteria bevatten voor het aanwijzen van authentieke gegevensbronnen **(overwegingen 51-64)**;

13. Het concept van een gegevensbank afgeleid uit authentieke bronnen moet worden losgelaten **(overwegingen 65-71)** ;

14. Aangezien het ontwerp standaard voorziet in het hergebruik van administratieve documenten, zal de wetgever in de toekomst in het kader van zijn verwerkingsprojecten moeten nagaan of het nodig is om het hergebruik van administratieve documenten te verbieden **(overwegingen 74-75)** ;

15. Het ontwerp moet het rechtstelsel verduidelijken en waar nodig uitwerken dat van toepassing is op het hergebruik van persoonsgegevens, bij het omzetten van de richtlijn inzake hergebruik en bij de tenuitvoerlegging van de verordening data governance **(overwegingen 82-86 - hergebruik in het kader van de richtlijn- hergebruik, overwegingen 87-99 - betreffende de verordening data governance:**

16. Artikel C.V.10, § 3, van het ontwerp, betreffende de openbaarmaking van gevallen van hergebruik van gegevens, moet worden verduidelijkt **(overwegingen 100-106)** ;

17. Zoals het ontwerp nu is, kan data-altruïsme niet worden geïmplementeerd **(overwegingen 105-106)** ;

18. Het ontwerp is niet bedoeld om van de CTBG een gegevensbeschermingsautoriteit te maken **(overwegingen 107--108)** ;

19. De systematische verstrekking van gegevens als bedoeld in de artikelen B.II.19 en B.II.20 van het ontwerp is onevenredig **(overwegingen 109-111)** ;

20. Het advies van de Autoriteit kan alleen worden gevraagd onder de voorwaarden die in de WOG zijn vastgesteld **(overwegingen 114-119)** ;

21. De aanvrager moet overwegen of de adviezen en voorstellen van de CTBG vóór de openbaarmaking anoniem moeten worden gemaakt **(overweging 122)** ;

22. De juridische reikwijdte van de regels inzake gegevensbeheer moet worden verduidelijkt en artikel C.III.1 van het ontwerp, betreffende de reikwijdte van de verplichtingen op dit gebied, is onvolledig (**overwegingen 123-125**) ;

23. Overheidsinstanties moeten voldoen aan de wettelijke regelingen die van toepassing zijn op gegevens (**overwegingen 126-127**) ;

24. Het ontwerp moet verduidelijken wat de "*omkeerbaarheid*" van gegevens inhoudt. Volgens de Autoriteit zou dit niet langer mogelijk zijn als de betrokken overheidsinstantie de betrokken persoonsgegevens niet langer zou kunnen verwerken. Bovendien vormt met name het bewaren van gegevens in de vorige staat of staten of het terugbrengen naar een vorige staat, een verwerking van persoonsgegevens die moet worden gerechtvaardigd in overeenstemming met de AVG (en het toepasselijke Brusselse of andere regelgevingskader) (**overwegingen 128-131**) ;

25. De categorieën van gegevens bedoeld in artikel C.III.10, § 1, van het ontwerp sluiten elkaar niet uit (**overwegingen 132-134**) ;

26. De Autoriteit schort haar standpunt over gegevensvalorisatie op, aangezien de ontwerpbevestiging grondiger moet worden onderzocht (**overwegingen 135-140**) ;

27. Artikel C.III.14, § 3, van het ontwerp moet worden verduidelijkt en gespecificeerd (**overwegingen 141-152**) ;

28. Artikel C.III.14, § 4, van het ontwerp moet specificeren dat het niet van toepassing is op klachten over de verwerking van persoonsgegevens, in overeenstemming met de memorie van toelichting van het ontwerp. Bovendien moet het worden aangepast in het licht van de beginselen van voorspelbaarheid en rechtmatigheid die zijn neergelegd in artikel 8 EVRM en artikel 22 van de Grondwet en, in voorkomend geval, in overeenstemming met het standpunt dat de Raad van State ter zake zal innemen (**overwegingen 153-158**) ;

29. Artikel C.III.16, leden 3 en 4, kunnen op zichzelf niet worden gebruikt als grondslag voor het verzamelen van persoonsgegevens en moeten worden toegepast binnen de grenzen die worden toegestaan door de regels die gelden voor de taak van algemeen belang of de wettelijke verplichting waarop de gegevensverwerking in kwestie is gebaseerd (**overwegingen 159-161**) ;

30. De Autoriteit schort haar analyse op over de verdeling van de in artikel C.III.17 bedoelde referentiegegevens. De verwerkingsverantwoordelijke moet worden opgenomen in de metagegevens (**overwegingen 162-163**) ;

31. Artikel C.III.18 van het ontwerp mag niet worden gebruikt als rechtsgrondslag voor geautomatiseerde besluiten met betrekking tot betrokkenen. Deze bepaling draagt ook bij aan de uitvoering van maatregelen ter bescherming van de rechten en vrijheden van betrokkenen, die nog specifiek moeten worden opgenomen in de wetgevingsteksten die afwijken van artikel 2.1 van de AVG (**overwegingen 164-166**) ;

32. Het ontwerp moet de verantwoordelijkheden met betrekking tot de persoonsgegevens beter in kaart brengen (**overwegingen 167-172**) ;

33. Zoals het ontwerp er nu uitziet, staat artikel C.V.11 niet toe dat persoonsgegevens worden verwerkt via het centrum voor gegevensanalyse en gegevensverwerking. De Autoriteit schort haar analyse van dit punt dan ook op (**overwegingen 173-174**) ;

34. Artikel C.V.4 van het ontwerp en de memorie van toelichting daarbij moeten nader worden uitgewerkt, zowel wat betreft de verdere verwerking van gegevens als de bewaartermijn ervan. De Autoriteit schort haar analyse hierover op (**overwegingen 174-186**). In de context van het ontwerp is de garantie dat gegevens na een bepaalde periode vernietigd moeten worden belangrijk (**overweging 181**) ;

35. De Autoriteit schort haar oordeel op over de vraag of UrbIS moet worden aangewezen als authentieke gegevensbron, met name binnen een ander kader dan dat waarin het wetboek voorziet en dat in het ontwerp is vastgelegd (**overwegingen 187-193**).

Voor het Kenniscentrum,
(get.) Cédrine Morlière, Directeur