Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 144/2023 van 29 september 2023

Betreft: Voorontwerp van wet tot wijziging van de wet van 4 mei 2016 inzake het hergebruik van overheidsinformatie (CO-A-2023-334)

Vertaling[1]

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit"),
aanwezig: de dames Cédrine Morlière, Nathalie Ragheno en Griet Verhenneman, en de heren Yves-Alexandre de Montjoye, 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 Mathieu Michel, staatssecretaris voor Digitalisering, belast met Administratieve Vereenvoudiging, Privacy, Regie der gebouwen (hierna "de staatssecretaris") ontvangen op 12 juli 2023;

[1] Voor de oorspronkelijke versie van de tekst, die collegiaal werd gevalideerd, cf. de Franse versie van de tekst, die beschikbaar is in de FR-versie van de rubriek "adviezen" van de website van de Autoriteit.

Brengt op 29 september 2023 het volgende advies uit:

I. Onderwerp en context van de adviesaanvraag

1. De staatssecretaris vroeg de Autoriteit om advies over de artikelen 2, 1° tot 5° en 14° tot 20°, 3, 6bis, 9, 10bis, 12bis tot 15bis en 17 bis van een voorontwerp van wet *tot wijziging van de wet van 4 mei 2016 inzake het hergebruik van overheidsinformatie* (hierna "de wet van 2016"), dat de omzetting is 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)*, (hierna «het ontwerp»). Deze bepalingen die de wet van 4 mei 2016 *inzake het hergebruik van overheidsinformatie* (hierna «d**e wet van 2016**») wijzigen, zijn de omzetting van de Richtlijn (EU) nr. 2019/1024 van het Europees Parlement en de Raad van 20 juni 2019 inzake open data en het hergebruik van overheidsinformatie (herschikking) (hierna **«de richtlijn** »).

II. Onderzoek

2. De Autoriteit bracht al verschillende adviezen uit over het hergebruik van overheidsinformatie en de omzetting van de richtlijn. **Ter inleiding verwijst zij naar de volgende adviezen, waarin de beginselen van gegevensbescherming worden uiteengezet zoals die worden toegepast op het hergebruik van overheidsinformatie** :

- Advies 203/2021 van 25 oktober 2021 over (geen Nederlandse vertalingbeschikbaar) *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 (ontwerpdecreet nr. 2020/279 van de Franse Gemeenschapscommissie inzake open gegevens en het hergebruik van overheidsinformatie) (*CO-A-2021-196) ;

- Advies 167/2022 van 19 juli 2022 (geen Nederlandse vertaling beschikbaar) *concernant un avant-projet de décret relatif à la diffusion et à la réutilisation des informations du secteur public, et un avant-projet de décret relatif à la diffusion et à la réutilisation des informations du secteur public pour les matières réglées à l'article 138 de la Constitution* 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);

- Advies 227/2022 van 29 oktober 2022 over (geen Nederlandse vertaling beschikbaar) *un projet de décret n° 227/2022 de la Commission communautaire française relatif aux données ouvertes et à la réutilisation des informations du secteur public (een ontwerpdecreet nr. 227/2022 van de Franse Gemeenschapscommissie over open gegevens en het hergebruik van overheidsinformatie) (*CO-A-2022-209).

3. Het ontwerp brengt onder andere wijzigingen aan in de wet van 2016 ***en sluit aan bij een recente hervorming van de wet van 11 april 1994 betreffende de openbaarheid van bestuur*** (hierna "de wet van 1994" genoemd). De Autoriteit heeft twee adviezen over deze hervorming uitgebracht en **verwijst daarom ter inleiding ook naar deze eerdere adviezen** :

- Zie 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);

- Advies 131/2023 *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-2023-316)*.

II.1. Persoonlijke gegevens die hergebruikt kunnen worden

4. Wat de persoonsgegevens betreft die toegankelijk zijn voor hergebruik, brengt het ontwerp geen principiële wijzigingen aan in de beginselen die momenteel zijn vastgelegd in artikel 3, § 2, 4° en 5°, van de wet van 2016. Volgens deze bepalingen is de wet van 2016 niet van toepassing op « *de bestuursdocumenten die op grond van de toepasselijke publieke toegangsregels niet openbaar kunnen worden gemaakt* »[2] en op «*de bestuursdocumenten waartoe enkel toegang kan worden verkregen op grond van regels die voorzien in een recht van persoonlijke toegang of persoonlijk belang*» (onderstreept door de Autoriteit)[3]. Als gevolg hiervan **kunnen persoonlijke gegevens alleen**

[2] Het ontwerp voegt de volgende verduidelijking toe aan deze bepaling : «*zoals bijvoorbeeld wegens de bescherming van de veiligheid van de bevolking, de veiligheid of de verdediging van het land, of de openbare veiligheid en de openbare orde binnen het bestaande kader van de openbaarheidswetgevingen* ».

[3] Zie ook meer expliciet artikel 1, 2, h) (te vergelijken met f) van de Richtlijn.

De Memorie van toelichting vermeldt met name het volgende:

« *Een belangrijke uitsluiting, die reeds in de bestaande wet van 4 mei 2016 is opgenomen blijft uiteraard behouden, en geldt voor bestuursdocumenten die, op grond van de toepasselijke publieke toegangsregels (d.w.z. de openbaarheidsregelgevingen), niet openbaar kunnen worden gemaakt of waartoe enkel toegang kan worden verkregen op basis van een recht van persoonlijke toegang of persoonlijk belang.*

Deze niet-toepasbaarheid van de wet is bedoeld voor de uitsluitingen die, onder meer, worden gemotiveerd door:

[…]

- *de fundamentele rechten en vrijheden van de bestuurden;*

worden hergebruikt als ze toegankelijk zijn voor het iedereen, zonder dat het nodig is om welk belang dan ook te rechtvaardigen[4].

II.2. overheidsinstantie;

5. In overeenstemming met de bovengenoemde hervorming van de wet van 1994 vervangt de wet van 2016 het begrip «*overheid*» door het begrip « *overheidsinstantie* »[5], waarvan de definitie wordt aangevuld naar positief recht. In de memorie van toelichting bij het ontwerp staat hierover het volgende in detail beschreven :

> « *In lijn met de op korte termijn voorziene aanpassing van de wet van 11 april 1994, wordt zo het toepassingsgebied ratione personae van de wet van 4 mei 2016 ook verder uitgebreid door het niet langer te beperken tot de administratieve overheden als bedoeld in artikel 14 van de gecoördineerde wetten op de Raad van State en zoals bepaald door de rechtspraak. Voortaan zullen ook andere instanties onderhevig zijn aan de wet van 11 april 1994 en aan de wet van 4 mei 2016.*
>
> *Zo omvat het toepassingsgebied van de wet :*
> - *de provincies en de gemeenten, wanneer zij federale bevoegdheden uitoefenen;*
> - *de instellingen van openbaar nut, zijnde de organismen bedoeld in artikel 1 van de wet van 16 maart 1954 betreffende de controle op sommige instellingen van openbaar nut, wanneer zij federale bevoegdheden uitoefenen;*
> - *de meergemeentepolitiezones bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst - gestructureerd op twee niveaus en hun organen, wanneer zij federale bevoegdheden uitoefenen;*
> - *de hulpverleningszones bedoeld in de wet van 15 mei 2007 betreffende de civiele veiligheid en hun organen, wanneer zij federale bevoegdheden uitoefenen.*

[…]

- *het uit de aard van de zaak vertrouwelijk karakter van de ondernemings- en fabricagegegevens en commerciële informatie (beroepsgeheim, zakengeheim of bedrijfsgeheim) die aan de overheid zijn meegedeeld;*
- *de geheimhouding van de identiteit van de persoon die het document of de inlichting vertrouwelijk aan de administratieve overheid heeft meegedeeld ter aangifte van een strafbaar of strafbaar geacht feit;*
- *de bescherming van de persoonlijke levenssfeer;*
- *de bescherming van een bij wet ingestelde geheimhoudingsverplichting, zoals de statistische geheimhouding ;*
- […] ».

[4] Zie in dit verband de overwegingen 4-12 van het advies 203/021 van 15 oktober 2021 (geen Nederlandse vertaling) *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 (CO-A-2021-196)*.

[5] Zoals het er op het ogenblik van de voorlegging door de Autoriteit uitzag, bevatte het toen voor advies voorgelegde ontwerp voortaan het begrip "*administratieve instanties*", dat met name administratieve instanties omvat in de zin van artikel 14 van de Geconsolideerde wetten op de Raad van State, zie de overwegingen 4-6 van advies nr. 42/2023 van 9 februari 2023 *betreffende een voorontwerp van wet tot wijziging van de wet van 11 april 1994 betreffende de openbaarheid van bestuur* (CO-A-2022-311).

Samenvattend omvat de nieuwe definitie van "overheidsinstantie" dus de in artikel 2, 1° in a) tot en met d) opgesomde entiteiten die krachtens het Europees recht al binnen het toepassingsgebied van de wet van 4 mei 2016 vielen. Daarnaast worden nu dus ook de administratieve overheidsinstanties die nog niet onder het actuele toepassingsgebied van deze wet vielen, zoals hierboven beschreven, maar die wel degelijk onderworpen zijn aan de openbaarheidsregels van de wet van 11 april 1994, ook binnen het toepassingsgebied van deze wet gebracht door invoeging van een nieuwe bepaling onder artikel 2, 1° e) en f).

Tenslotte, in lijn met de op korte termijn voorziene aanpassing van de wet van 11 april 1994 inzake openbaarheid van bestuur, wordt artikel 2, 1° nog aangevuld met een nieuwe bepaling onder g) die verduidelijkt dat voor de toepassing van deze wet tevens onder "Overheidsinstantie" wordt verstaan : de beleidsorganen van de federale regering bedoeld in het koninklijk besluit van 19 juli 2001 betreffende de invulling van de beleidsorganen van de federale overheidsdiensten en betreffende de personeelsleden van de federale overheidsdiensten aangewezen om deel uit te maken van een kabinet van een lid van een Regering of van een College van een Gemeenschap of een Gewest.

Hiermee worden dus voornamelijk de zogeheten ministeriële kabinetten en de kabinetten van de staatssecretarissen (met dien verstande dat de officiële benaming van kabinet "beleidsorgaan" is) bedoeld. Uit de memorie van toelichting bij de op korte termijn voorziene aanpassing van de wet van 11 april 1994 inzake openbaarheid van bestuur, blijkt dat er minstens twijfel bestaat over de mate waarin die instanties onderworpen zijn aan de verplichtingen van openbaarheid van bestuur, zoals opgenomen op federaal niveau in de wet van 11 april 1994.

Daarom wordt ook in de wet van 4 mei 2016, naar analogie met de wetgeving inzake openbaarheid van bestuur, de bestuursdocumenten van de beleidsorganen expliciet onder het toepassingsgebied van de wetgeving gebracht ».

6. Deze uitbreiding van het toepassingsgebied ratione personae van de wet van 2016 behoeft van de Autoriteit niet meer commentaar dan de hervorming van de wet van 1994.

II.3. Toepasselijke regels inzake gegevensbescherming

7. Het ontwerp voor artikel 3, §3 van de wet van 2016 voorziet in de toepassing van gegevensbeschermingsregels in deze bewoordingen:

« *Deze wet doet geen afbreuk aan het Unierecht of het nationale recht betreffende de bescherming van persoonsgegevens, met name 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; Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en de overeenkomstige bepalingen van het Belgisch recht; de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens; de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid en de uitvoeringsbesluiten van deze wetten.*

Persoonsgegevens zijn uitsluitend herbruikbaar voor zover dit hergebruik in overeenstemming is met de wetgeving betreffende de bescherming van persoonsgegevens en met de bescherming van de rechten en vrijheden van de betrokken personen.

De persoonsgegevens worden, in voorkomend geval, geanonimiseerd of gepseudonimiseerd De persoonsgegevens worden, in voorkomend geval, geanonimiseerd of gepseudonimiseerd door de overheidsinstantie of door een vertrouwde derde partij voor rekening en op instructie van de overheidsinstantie, voorafgaandelijk aan de overdracht met het oog op het hergebruik ervan» (onderstreept door de Autoriteit).

8. Met betrekking tot deze bepaling wordt in de memorie van toelichting met name het volgende uiteengezet :

« *De verantwoordelijke overheidsinstantie dient telkens en concreet te evalueren of aan de voorwaarden van artikel 6.4 van de AVG (verenigbaarheidsanalyse) wordt voldaan. Het proportionele hergebruik dient gepaard te gaan met voorwaarden voor wat betreft de naleving van de regels inzake de bescherming van persoonsgegevens.*

In principe kunnen persoonsgegevens enkel worden hergebruikt nadat ze geanonimiseerd of gepseudonimiseerd zijn. Anonimisering of pseudonimisering van informatie is een manier om het belang om overheidsinformatie zo herbruikbaar mogelijk te maken te verzoenen met de verplichtingen die voortvloeien uit de regelgeving inzake gegevensbescherming. […]

Anonimisering of pseudonimisering dient te gebeuren door de verantwoordelijke overheidsinstanties of het verantwoordelijke overheidsbedrijf vooraleer de gegevens worden doorgegeven met het oog op hergebruik. Hierbij is de tussenkomst mogelijk van een

gecertificeerde 'trusted third party' die de anonimisering of pseudonimisering van de gegevensset uitvoert en waarborgt, voor rekening van en ten laste van de overheidsinstanties of het overheidsbedrijf. Anonimisering en pseudonimisering dienen te gebeuren door de overheidinstantie of het overheidsbedrijf voorafgaand aan de doorgifte van de gegevens voor hun hergebruik.

De tekst creëert de mogelijkheid om documenten met persoonsgegevens te kunnen hergebruiken, ofwel geanonimiseerd ofwel gepseudonimiseerd

De keuze voor ofwel anonimisering ofwel pseudonimisering dient weloverwogen te worden gemaakt op basis van een analyse van de concrete omstandighedenvan het geval, de aard van de betrokken persoonsgegevens en de betrokken categorieën van personen, de initiële doeleinden waarvoor deze gegevens werden verwerkt, de omvang, de context en de doeleinden van het hergebruik en of dit al dan niet een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

In verband met de keuze voor anonimisering ofwel pseudonimisering en in verband met de te gebruiken anonimiserings- of pseudonimiseringstechnieken en -strategieën kan onder andere verwezen worden naar het Advies nr. 5/2014 over anonimiseringstechnieken van 10 april 2014, WP216 van de "Artikel 29 Gegevensbeschermingswerkgroep", de (toekomstige) werkzaamheden van het Europees Comité voor gegevensbescherming (European Data Protection Board – EDPB) en het Enisa, het Agentschap van de Europese Unie voor cyberbeveiliging ("ENISA Report on Data Pseudonymisation: Advanced Techniques and Use Cases, Published January 28, 2021 and ENISA Report on Best Practices and Techniques for Pseudonymisation" gepubliceerd op 3 december 2019") op dit vlak.

Bij anonimisering of pseudonimisering dient men rekening te houden met mogelijke risico's op heridentificatie van geanonimiseerde of gepseudonimiseerde gegevens en kan het noodzakelijk zijn om bijkomende maatregelen aan te bevelen om de persoonlijke levenssfeer optimaal te beschermen.

Een bijkomende waarborg voor de betrokkenen bestaat in het bekomen van een advies van de Gegevensbeschermingsautoriteit inzake de geschiktheid van de maatregel in dit concrete geval. De Gegevensbeschermingsautoriteit, die beschikt over de nodige expertise ter zake, kan advies geven over het type en de sterkte van pseudonimisering en/of de gekozen gecertifieerde trusted third party, of een aanbeveling tot anonimisering doen in verband met bepaalde categorieën van gegevens.

Deze bepalingen gelden onverminderd de specifieke regels voor verdere verwerking van persoonsgegevens voor historische, statistische of wetenschappelijke doeleinden die in de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens zijn bepaald» (onderstreept door de Autoriteit).

9. Ten eerste is de Autoriteit van mening dat, gezien de logica die in de memorie van toelichting is uiteengezet maar niet is overgenomen in het dispositief van het ontwerp - dit laatste, gezien het brede scala aan beoogde verwerkingen, in overeenstemming met het beginsel van minimale gegevensverwerking zoals vastgelegd in artikel 5,1. c), van de AVG - **moet van de overheidsinstantie worden geëist dat zij de gegevens anonimiseert voordat zij toestemming geeft om ze opnieuw te gebruiken of, indien anonimisering niet volstaat om het beoogde doel te bereiken (**namelijk het doeleinde van het geplande hergebruik) **en op voorwaarde dat het in dit geval evenredig is, de pseudonimisering van persoonsgegevens (wetende dat gepseudonimiseerde gegevens persoonsgegevens blijven, wat het gebruik ervan beperkt).**

10. Dit gezegd zijnde, vestigt de Autoriteit ook de aandacht van de aanvrager op de **overwegingen 17-19 van haar advies nr. 203/2021 v**an 25 oktober 2021 (Nederlandse vertaling niet beschikbaar) c*oncernant 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 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.). die vervolgens als zodanig worden meegedeeld 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 diensten*[6]», (in plaats van alleen maar ongeïdentificeerde gegevens mee te delen) (onderstreept door de Autoriteit in dit advies).

11. **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[7]) aan 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.

12. 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**

---

[6] « *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.

[7] Zie de overwegingen13 e.v. betreffende het begrip "third trusted party" dat in het ontwerp wordt gebruikt. De betrokken dienstverlener kan worden beschouwd als een vertrouwde derde partij en moet voldoen aan de vereisten die gelden voor dit type entiteit. Dit gezegd hebbende, staat het ontwerp in zijn huidige vorm alleen de tussenkomst van een dergelijke vertrouwde derde partij toe om over te gaan tot het anonimiseren of pseudonimiseren van gegevens. Met betrekking tot de in voetnoot 5 aangehaalde CASD merkt de Autoriteit niettemin op dat deze niet alle situaties bestrijkt die vallen onder het hergebruik van gegevens in de zin van de richtlijn en de wet van 2016 voor zover (de Autoriteit vertaalt): *«het voornaamste doel van de CASD is het organiseren en implementeren van beveiligde toegangsdiensten voor vertrouwelijke gegevens met het oog op onderzoek, studie, evaluatie of innovatie zonder winstoogmerk. Zijn opdracht is ook om de technologie te promoten die is ontwikkeld om de toegang tot gegevens in de publieke en private sector te beveiligen* » (https://www.casd.eu/le-centre-dacces-securise-aux-donnees-casd/gouvernance-et-missions/, laatst geraadpleegd op 21/09/2023) (onderstreept door de Autoriteit).

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.

13. Ten tweede definieert het ontwerp het begrip "***gecertificeerde third trusted party***" niet, noch verwijst het naar een normatief kader met betrekking tot de certificering in kwestie. Met betrekking tot het gebruik van een begrip als "*trusted third parties*" verklaarde de Autoriteit in overweging 53 van haar advies nr. 37/2022 *van 16 februari 2022 betreffende een voorontwerp van decreet tot invoering van het gecentraliseerde platform voor geautomatiseerde gegevensuitwisseling "E-Paysage" (CO-A-2022-003)*[8] het volgende:

> « *In deze context is de Autoriteit niet gekant tegen het gebruik van een " trusted third party " om de pseudonimisering of anonimisering van gegevens uit te voeren. Aangezien dit concept niet bestaat in de* [AVG]*, zal het ontwerp toch moeten definiëren wat een "trusted third party" is in de context van dit ontwerp, en vooral welke verantwoordelijkheden en kwaliteiten van deze derde worden verwacht in vergelijking met bijvoorbeeld een verwerker. Artikel 2, 3°, a), van het samenwerkingsakkoord kent bijvoorbeeld een mogelijk vergelijkbare rol toe aan de BCED*[9]*: «een vertrouwde onafhankelijke entiteit die diensten aanbiedt die de betrouwbaarheid vergroten van elektronische gegevensuitwisseling en gegevensregistratie en die zelf geen opdracht of belang heeft bij de feitelijke verwerking van persoonsgegevens» (onderstreept door de Autoriteit). In het licht van deze definitie zou het doel van het ontwerp van artikel 106/20 bijvoorbeeld kunnen zijn om de inschakeling te eisen van een onafhankelijke/neutrale entiteit ten aanzien van de beoogde verwerkingen en de betrokken verwerkingsverantwoordelijken, die er geen belang bij heeft de verwerkte persoonsgegevens of het resultaat van de verwerking ervan te kennen, en die, in overeenstemming met de stand van de techniek, bewezen deskundigheid heeft op het gebied van de verwerking van persoonsgegevens en met name de pseudonimisering en anonimisering van persoonsgegevens. Aangezien de toelichting hierover zwijgt en het ontwerpartikel 106/20 zelf zeer beknopt is, kan de Autoriteit geen gedetailleerder advies over het voorstel geven en*

[8] Het volgende standpunt wordt ook verwoord in de overwegingen 46-48 van advies nr. 143/2023 van de Autoriteit 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 dienst integratoren van het Waals Gewest en de Franse Gemeenschap en een ontwerp van samenwerkingsakkoord betreffende de oprichting van de gemeenschappelijke dienst van het Waals Gewest en de Franse Gemeenschap, genaamd Banque Carrefour d'échange de données (niet voor instemming voorgelegd) (CO-A-2023-375), en betreffende een voorontwerp van decreet houdende instemming met het samenwerkingsakkoord tussen het Waals Gewest en de Franse Gemeenschap tot aanwijzing van de dienstenintegrator van het Waals Gewest en de Franse Gemeenschap en een ontwerp van samenwerkingsakkoord betreffende de oprichting van de gemeenschappelijke dienst van de Waalse Regering en de Franse Gemeenschap, genaamd Banque Carrefour d'échange de données (niet voor instemming voorgelegd) (CO-A-2023-376).

[9] Ofwel de " Banque-Carrefour d'échanges de données " in de zin van het samenwerkingsakkoord van 23 mei 2013 tussen het Waals Gewest en de Franse Gemeenschap *over het oçpstarten van een gemeenschappelijk initiatief gegevens te delen en over het gemeenschappelijk beheer van dat initiatief*..

verzoekt zij de aanvrager het dispositief en het daarmee nagestreefde doel te verduidelijken» (onderstreept door de Autoriteit in de oorspronkelijke tekst).

14. De Autoriteit heeft onlangs opnieuw een standpunt ingenomen dat vergelijkbaar is met het standpunt dat zojuist in herinnering werd gebracht in de overwegingen 39-41 van haar advies nr. 115/2023 van 18 juli 2023 *over het ontwerp van Koninklijk Besluit tot wijziging van het Koninklijk Besluit van 13 juni 2014 tot vaststelling van, enerzijds, de specifieke regelgevende, administratieve, technische en organisatorische maatregelen om de naleving van de vereisten inzake de bescherming van persoonsgegevens of van gegevens over individuele entiteiten en inzake statistische vertrouwelijkheid te verzekeren en anderzijds de voorwaarden vast te leggen waaronder het Nationaal Instituut voor de Statistiek (NSI) kan optreden als intermediaire organisatie met het oog op verdere verwerking voor statistische doeleinden (CO-A-2023-213)*. Artikel 203 van de WVG, dat ook verwijst naar het concept van een vertrouwde derde partij in de context van verwerking voor archiefdoeleinden, wetenschappelijk of historisch onderzoek, of voor statistische doeleinden, bepaalt dat de vertrouwde derde partij onderworpen moet zijn aan het beroepsgeheim en onafhankelijk moet zijn van de oorspronkelijke verwerkingsverantwoordelijke.

15. Op een ander gebied dan anonimisering en pseudonimisering reguleert de Europese wetgeving ook specifiek het aanbieden van bepaalde vertrouwensdiensten (waaronder elektronische handtekeningen en tijdstempels[10]). Dit normatieve kader kan, mutatis mutandis, ook een bron van inspiratie zijn voor de aanvrager.

16. **De Autoriteit is van mening dat, <u>in het licht van bovenstaande overwegingen, het dispositief het begrip "gecertifieerde third trusted party" moet definiëren door de verantwoordelijkheden, de kwaliteiten en de waarborgen te specificeren waarvan de aanbieder, de diensten en de certificering</u> die verand houden met de verwerking van persoonsgegevens, vergezeld moeten gaan. Dergelijke bepalingen hebben namelijk een directe impact op de bepaling van de essentiële elementen van de gegevensverwerking in kwestie:** ze zijn betrokken bij het bepalen van het doel van de geplande verwerking (dit houdt in dat een specifieke entiteit wordt gebruikt, omwille van zijn kenmerken, om ervoor te zorgen dat de verwerking correct wordt uitgevoerd) en zorgen ervoor dat deze evenredig is, in het bijzonder door passende waarborgen voor de rechten en vrijheden van de betrokkenen vast te stellen, en ze bepalen ook de verantwoordelijkheden met betrekking tot de verwerking van persoonsgegevens.

[10] Zie de Verordening (EU) Nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 *betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG*.

17. 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 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 externe audits[11]. 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.

18. Ten derde benadrukt de memorie van toelichting dat het verkrijgen van «*een **advies van de Gegevensbeschermingsautoriteit** inzake de geschiktheid van de maatregel*» in dit concrete geval in kwestie een «*bijkomende waarborg*» vormt (vet toegevoegd door de Autoriteit). 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 vande WOG (wat het geval is bij voorliggend advies).

19. 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 Gegevensbeschermingsautoriteit[12], wanneer de betrokken verwerking ondanks de door de verwerkingsverantwoordelijke geplande risicobeheersmaatregelen nog steeds een hoog restrisico inhoudt[13].

20. Tot besluit kan worden gesteld dat **het bestuursorgaan bij wie een aanvraag voor hergebruik is ingediend, op grond van de WOG in de regel geen adviesaanvraag bij de Autoriteit mag indienen over de vraag of de voorgestelde maatregel al dan niet passend is**. Het is aan de verwerkingsverantwoordelijke (het bestuursorgaan dat haar wettelijke verplichting uitvoert) om, in overeenstemming met het *accountabilitybeginsel*, de beoogde maatregelen vast te stellen en uit te

[11] 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)*.

[12] Artikel 20, §1, 3° van de WOG.

[13] 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.

voeren, en te kunnen verantwoorden dat de uitgevoerde gegevensverwerking in overeenstemming is met de AVG en de wet van 2016 zoals gewijzigd door het ontwerp.

21. Ten vierde wijst de Autoriteit erop dat **de wet van 2016 in het algemeen geen afbreuk doet aan de verdere verwerking van gegevens die kan worden uitgevoerd door een verwerkingsverantwoordelijke die toegang heeft kunnen krijgen tot persoonsgegevens in overeenstemming met de toegangsregels en binnen de grenzen die zijn vastgelegd in die toegangsregels en in artikel 6. 4. van de AVG.** Met andere woorden, het is aan de aanvrager (verwerkingsverantwoordelijke) om te bepalen wat de meest geschikte juridische manier is om toegang te krijgen tot de betreffende gegevens, afhankelijk van zijn geplande persoonsgegevensverwerking : een eenvoudig verzoek om toegang tot of raadpleging van de gegevens in overeenstemming met de wet van 1994 (of andere wetgeving); of een verzoek om toegang met het oog op hergebruik van de gegevens in overeenstemming met de wet van 2016.

22. Ten vijfde, wat betreft **de definitie van anonimisering** in artikel 3, 16°, van het ontwerp, stelt de memorie van toelichting: «*deze definitie is afgestemd op de betekenis die aan anonimisering wordt gegeven in de Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens), die rechtstreeks van toepassing is in België* ». De Autoriteit merkt op dat deze definitie een letterlijke weergave is (met uitzondering van het begrip "document", dat is vervangen door "bestuursdocument") van de definitie in artikel 2, 7) van de richtlijn zelf. De AVG definieert het anonimiseringsproces immers niet. De memorie van toelichting kan worden aangepast door te specificeren dat het ontwerp de definitie van het anonimiseringsproces overneemt die in de richtlijn is vastgelegd, maar dat, dit gezegd hebbende, de richtlijn geen afbreuk doet aan de AVG, waarnaar de richtlijn ook verwijst met betrekking tot de definitie van het begrip persoonsgegevens, en dat **de verwerking van anoniem gemaakte gegevens moet worden begrepen en geïnterpreteerd in overeenstemming met de AVG**.

23. En tot slot bepaalt artikel 9, §1 van de wet van 2016 als gewijzigd door artikel 14 van het ontwerp het volgende «d*e overheidsinstanties de bestuursdocumenten waarover zij beschikken, in een reeds bestaande vorm en taal beschikbaar moeten stellen, op voorwaarde dat dit geen onevenredig grote inspanningen of kosten met zich meebrengt die verder gaan dan een eenvoudige handeling*» (onderstreept door de Autoriteit). Zoals aangegeven in de memorie van toelichting gaat deze bepaling over de vormen waarin bestuursdocumenten beschikbaar moeten worden gesteld.

24. Aangezien de anonimisering of pseudonimisering van gegevens in beginsel een gegevensverwerking vereist die verder gaat dan «een eenvoudige handeling», i**s 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 eeunvoudige handeling. De Autoriteit lijkt uit de logica van het dispositief van het ontwerp te begrijpen dat artikel 9, §1, van de wet van 2016 geen afbreuk doet aan de verplichting van de instantie om de betrokken documenten te pseudonimiseren of anonimiseren, op voorwaarde dat een dergelijke verwerking kan worden gecompenseerd door de kosten door te rekenen aan de aanvragers. Met andere woorden, het feit dat de inspanningen die van de instantie op dit gebied worden gevraagd, verder gaan dan een eenvoudige handeling, kan geen rechtvaardiging zijn voor een weigering van de betrokken instantie om gepseudonimiseerde of geanonimiseerde administratieve documenten beschikbaar te stellen.

Om deze redenen,
oordeelt de Autoriteit als volgt :

1. Op grond van de wet van 2016 mogen persoonsgegevens alleen worden hergebruikt als de toegang ertoe openstaat voor eenieder, zonder dat een belang hoeft te worden gerechtvaardigd **(overweging 3**) ;

2. In overeenstemming met het beginsel van minimale gegevensverwerking moeten de bepalingen van het ontwerp de overheidsinstantie verplichten om de gegevens te anonimiseren voordat ze opnieuw mogen worden gebruikt of, indien anonimisering niet volstaat om het doel van het beoogde hergebruik te bereiken en mits dit in het betreffende geval proportioneel is, om de persoonsgegevens te pseudonimiseren voordat ze opnieuw mogen worden gebruikt **(overwegingen 7-9**) ;

3. Vanuit een meer algemeen perspectief op het gebied van hergebruik van gegevens moet de aanvrager prioriteit geven aan andere technische methoden die hergebruik van gegevens mogelijk maken zonder dat gepseudonimiseerde (of geanonimiseerde) gegevens aan aanvragers worden doorgegeven, via de beschikbaarstelling van beveiligde diensten voor gegevenstoegang, op zodanige wijze dat een betere controle over de beoogde gegevensverwerking wordt gewaarborgd **(overwegingen 10-11**) ;

4. Het dispositief moet het concept van een gecertificeerde vertrouwde derde partij definiëren en de verantwoordelijkheden, kwaliteiten en garanties specificeren die de aanbieder van de dienst, de diensten en de certificering in kwestie moeten bieden die verband houden met de verwerking van persoonsgegevens **(overwegingen 13-17**) ;

5. Over het algemeen staat de WOG niet toe dat een overheidsinstantie de Autoriteit om advies vraagt over de maatregel die zij van plan is te nemen om het hergebruik van gegevens mogelijk te maken **(overwegingen 18-20**) ;

6. De wet van 2016 geldt onverminderd voor elke verdere verwerking van gegevens die kan worden uitgevoerd door een verwerkingsverantwoordelijke die toegang heeft kunnen krijgen tot persoonsgegevens in overeenstemming met de toegangsregels en binnen de grenzen die in die regels en artikel 6, 4 van de AVG zijn vastgesteld **(overweging 21**) ;

7. De memorie van toelichting bij het ontwerp kan in zoverre worden verduidelijkt dat het begrip anonimiseringsproces uit de richtlijn zelf afkomstig is **(overweging 20**) ;

8. Het ontwerp moet de impact verduidelijken van artikel 9, § 1, van de wet van 2016, zoals gewijzigd bij artikel 14 van het ontwerp, met betrekking tot de verplichting om gegevens beschikbaar te stellen na anonimisering of pseudonimisering **(overwegingen 23-24**).

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