DOC 56 **1631/002**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

3 juli 2026

WETSONTWERP

betreffende de verwerkingen van persoonsgegevens door de Algemene Directie Dienst Vreemdelingenzaken

Adviezen

Inhoud Blz.

Zie:

Doc 56 **1631/ (2025/2026)**:
001: Wetsontwerp.

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

3 juillet 2026

PROJET DE LOI

relatif aux traitements de données à caractère personnel par la Direction générale Office des étrangers

Avis

Sommaire Pages

Voir:

Doc 56 **1631/ (2025/2026)**:
001: Projet de loi.

N-VA	:	*Nieuw-Vlaamse Alliantie*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
PS	:	*Parti Socialiste*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Les Engagés	:	*Les Engagés*
Vooruit	:	*Vooruit*
cd&v	:	*Christen-Democratisch en Vlaams*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
Anders.	:	*Anders.*
DéFI	:	*Démocrate Fédéraliste Indépendant*
ONAFH/INDÉP	:	*Onafhankelijk-Indépendant*

Afkorting bij de nummering van de publicaties:		*Abréviations dans la numérotation des publications:*	
DOC 56 0000/000	*Parlementair document van de 56e zittingsperiode + basisnummer en volgnummer*	*DOC 56 0000/000*	*Document de la 56e législature, suivi du numéro de base et numéro de suivi*
QRVA	*Schriftelijke Vragen en Antwoorden*	*QRVA*	*Questions et Réponses écrites*
CRIV	*Voorlopige versie van het Integraal Verslag*	*CRIV*	*Version provisoire du Compte Rendu Intégral*
CRABV	*Beknopt Verslag*	*CRABV*	*Compte Rendu Analytique*
CRIV	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)*	*CRIV*	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN	*Plenum*	*PLEN*	*Séance plénière*
COM	*Commissievergadering*	*COM*	*Réunion de commission*
MOT	*Moties tot besluit van interpellaties (beigekleurig papier)*	*MOT*	*Motions déposées en conclusion d'interpellations (papier beige)*

Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 166/2022 van 19 juli 2022

Betreft: Voorontwerp van wet *betreffende de verwerkingen van persoonsgegevens door de Algemene Directie Dienst Vreemdelingenzaken van de Federale Overheidsdienst Binnenlandse Zaken* (CO-A-2022-149)

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna de "Autoriteit"), aanwezig: mevrouw Cédrine Morlière en de heren Yves-Alexandre de Montjoye en Bart Preneel;

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

Gelet op de 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 Sammy Mahdi, Staatssecretaris voor Asiel en Migratie, belast met de Nationale Loterij, toegevoegd aan de Minister van Binnenlandse Zaken, Institutionele Hervormingen en Democratische Vernieuwing (hierna "de aanvrager"), ontvangen op 09/06/2022;

Brengt op 19 juli 2022 het volgend advies uit:

I. VOORWERP VAN DE ADVIESAANVRAAG

1. De aanvrager verzoekt om het advies van de Autoriteit aangaande de integraliteit van het voorontwerp van wet *betreffende de verwerkingen van persoonsgegevens door de Algemene Directie Dienst Vreemdelingenzaken van de Federale Overheidsdienst Binnenlandse Zaken* (hierna "het voorontwerp" of "het voorontwerp van wet").

2. Het voorontwerp van wet beoogt een juridisch kader te creëren voor de verwerkingen van persoonsgegevens door de Algemene Directie Dienst Vreemdelingenzaken van de Federale Overheidsdienst Binnenlandse Zaken (hierna "de Dienst Vreemdelingenzaken") in het kader van de vervulling van zijn wettelijke opdrachten inzake migratie[1]. Deze wettelijke opdrachten worden hoofdzakelijk geregeld door de wet van 15 december 1980 *betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen* (hierna ook: "de Vreemdelingenwet"), het koninklijk besluit van 8 oktober 1981 *betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen* (hierna ook: "het koninklijk besluit van 8 oktober 1981") en het koninklijk besluit van 14 januari 2002 *houdende oprichting van de Federale Overheidsdienst Binnenlandse Zaken*.

3. Een adviesaanvraag met betrekking tot het voorontwerp werd eveneens gericht aan het Controleorgaan op de politionele informatie (COC) alsook het Vast Comité van Toezicht op de politiediensten (Comité P) en het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten (Comité I).

II. ONDERZOEK VAN DE AANVRAAG

a. Rechtsgrond

4. De Autoriteit wijst erop dat elke verwerking van persoonsgegevens een inmenging vormt in het recht op bescherming van de persoonlijke levenssfeer, dat is vastgelegd in artikel 8 EVRM en in artikel 22 van de Grondwet. Dit recht is echter niet absoluut. De artikelen 8 EVRM en 22 van de Grondwet sluiten overheidsinmenging in het recht op bescherming van het privéleven (waar ook persoonsgegevens deel van uitmaken) niet uit, maar vereisen dat zij wordt toegestaan door een voldoende precieze wettelijke bepaling; dat zij beantwoordt aan een algemeen maatschappelijk belang en dat zij evenredig is met de daarmee nagestreefde wettige doelstelling[2]. Elke norm die de verwerking

[1] Memorie van toelichting, p. 6.

[2] Vaste rechtspraak van het Grondwettelijk Hof. Zie bv. GwH, Arrest van 4 april 2019, nr. 49/2019 (*"Zij sluiten een overheidsinmenging in het recht op eerbiediging van het privéleven niet uit, maar vereisen dat zij wordt toegestaan door een voldoende precieze wettelijke bepaling, dat zij beantwoordt aan een dwingende maatschappelijke behoefte in een democratische samenleving en dat zij evenredig is met de daarmee nagestreefde wettige doelstelling").*

van persoonsgegevens regelt (en die van nature een inmenging vormt in het recht op bescherming van persoonsgegevens) moet niet alleen noodzakelijk en evenredig zijn, maar ook voldoen aan de eisen van voorspelbaarheid en nauwkeurigheid, zodat de betrokkenen, over wie gegevens worden verwerkt, een duidelijk beeld krijgen van de verwerking van hun gegevens.

5. De verwerking van persoonsgegevens die noodzakelijk is voor de vervulling van een wettelijke verplichting[3] en/of voor de uitoefening van een opdracht van algemeen belang of in het kader van de uitoefening van het openbaar gezag die aan verwerkingsverantwoordelijke is toevertrouwd[4], moet overeenkomstig artikel 6.3 AVG, gelezen in het licht van overweging 41 van de AVG, worden geregeld door duidelijke en nauwkeurige regelgeving, waarvan de toepassing voor de betrokkenen voorzienbaar moet zijn. Bovendien is het volgens artikel 22 van de Grondwet noodzakelijk dat de "wezenlijke elementen" van de gegevensverwerking door middel van een formele wettelijke norm worden vastgesteld.

6. Bepaalde verwerkingen van persoonsgegevens waartoe het voor advies voorliggende ontwerp aanleiding geeft, berusten op artikel 6.1.c) AVG aangezien deze noodzakelijk zijn voor de naleving van de Europese wetgeving inzake asiel en migratie. Andere in het ontwerp voorziene verwerkingen zijn gesteund op artikel 6.1.e) AVG. De verwerkingen hebben een belangrijke inmenging in de rechten en vrijheden van de betrokkenen tot gevolg in de mate dat het voorontwerp onder Hoofdstuk 3 ("*Categorieën van verwerkte persoonsgegevens*") onder meer voorziet in een verwerking van bijzondere categorieën van persoonsgegevens (met name gegevens met betrekking tot de gezondheid, raciale of etnische gegevens, gegevens met betrekking tot het seksuele gedrag, politieke opinies, lidmaatschap van een vakbond of soortgelijke groep en levensbeschouwelijke of religieuze overtuigingen; cf. artikel 6 voorontwerp).

7. Krachtens artikel 6.3 van de AVG, gelezen in samenhang met artikel 22 van de *Grondwet* en artikel 8 van het EVRM, moet een norm van wettelijke rangorde bepalen onder welke omstandigheden dergelijke gegevensverwerking is toegestaan. Overeenkomstig het legaliteits- en het voorzienbaarheidsprincipe moet deze wetgevingsnorm dus in ieder geval de essentiële elementen van de verwerking(en) vastleggen[5]. Wanneer de gegevensverwerking(en) een belangrijke inmenging in de rechten en vrijheden van de betrokkenen vertegenwoordig(t)(en), zoals *in casu*[6] het geval is, moeten volgende essentiële elementen door de wetgever worden vastgesteld:

---

[3] Art. 6.1.c) van de AVG

[4] Art. 6.1.e) van de AVG.

[5] Zie DEGRAVE, E., *"L'egouvernement et la protection de la vie privée – Légalité, transparance et contrôle"*, Collection du CRIDS, Larcier, Brussel, 2014, p. 161 e.v. (zie o.m.: EHRM, arrest *Rotaru c. Roumania*, 4 mei 2000); Zie ook enkele arresten van het Grondwettelijk Hof: Arrest nr. 44/2015 van 23 april 2015 (p. 63), Arrest nr. 108/2017 van 5 oktober 2017 (p. 17) en Arrest nr. 29/2018 van 15 maart 2018 (p. 26).

[6] Aangezien de verwerking in bepaalde gevallen betrekking heeft op speciale categorieën van (gevoelige) persoonsgegevens in de zin van art. 9 of 10 AVG.

- het (de) precieze en concrete doeleinde(n);
- de identiteit van de verwerkingsverantwoordelijke(n) (tenzij dit duidelijk is);
- de (categorieën van) gegevens die noodzakelijk zijn voor de verwezenlijking van (dit) (deze) doeleinde(n);
- de (categorieën van) betrokkenen wiens gegevens zullen worden verwerkt;
- de maximale bewaartermijn van de gegevens;
- de (categorieën van) ontvangers aan wie de gegevens worden meegedeeld, evenals de omstandigheden waarin en de redenen waarom de gegevens worden verstrekt;
- in voorkomend geval en voor zover noodzakelijk, de beperking van de verplichtingen en/of rechten vermeld in de artikelen 5, 12 tot 22 en 34 AVG.

8. Hoofdstuk 1 van het voorontwerp vermeldt de rechtmatigheidsgronden op basis waarvan de Dienst Vreemdelingenzaken persoonsgegevens kan verwerken. Artikel 4, §1 van het voorontwerp stelt in dit verband:

"*De Dienst Vreemdelingenzaken kan persoonsgegevens verwerken, voor zover die verwerkingen noodzakelijk zijn:*

1° voor de vervulling van zijn taken van algemeen belang of de taken in het kader van het openbaar gezag waarmee hij is belast door het koninklijk besluit van 14 januari 2002 houdende oprichting van de Federale Overheidsdienst Binnenlandse Zaken;

2° voor de wettelijke verplichtingen waaraan hij onderworpen is".

9. De Autoriteit wijst er vooreerst op dat de formulering van artikel 4, §1, 2° zeer algemeen is en dat het aangewezen is te preciseren welke verplichtingen het *in casu* betreft, met verwijzing naar de desbetreffende wetgevende normen.

10. De Autoriteit wijst er verder op dat, gelet op het feit dat *in casu* bovendien bijzondere categorieën van persoonsgegevens worden verwerkt, tevens (ten minste) één van de uitzonderingsgronden op het principiële verwerkingsverbod voor dit type van persoonsgegevens, opgesomd in artikel 9.2 AVG, toepassing dient te vinden. Een verwerking van de bijzondere categorieën van persoonsgegevens in de zin van artikel 9 AVG dient namelijk gebaseerd te zijn op artikel 9.2 AVG in samenhang gelezen met artikel 6.1 AVG. Zulks werd vastgesteld door de Europese Commissie en de EDPB[7] en wordt eveneens bevestigd in overweging 51 AVG, dat met betrekking tot de verwerking van bijzondere categorieën van persoonsgegevens stelt dat "*naast de specifieke*

[7] Cf. hieromtrent GEORGIEVA, L. en KUNER, C., "Article 9. Processing of special categories of personal data" in KUNER, C., BYGRAVE, L.A. en DOCKSEY, C., *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, Oxford, p. 37: "*The Commission has stated that the processing of sensitive data must always be supported by a legal basis under Article 6 GDPR, in addition to compliance with one of the situations covered in Article 9(2). The EDPB has also stated that 'If a video surveillance system is used in order to process special categories of data, the data controller must identify both an exception for processing special categories of data under Article 9 (i.e. and exemption from the general rule that one should not process special categories of data) and a legal basis under Article 6'.*

voorschriften voor die verwerking de algemene beginselen en andere regels van deze verordening [dienen] te worden toegepast, met name wat betreft de voorwaarden voor rechtmatige verwerking".

11. In dit verband stelt de Autoriteit vast dat artikel 4, §2 van het voorontwerp bepaalt:
"§ 2. De Dienst Vreemdelingenzaken kan persoonsgegevens bedoeld in artikel 9 van de algemene verordening gegevensbescherming verwerken, voor zover deze verwerkingen noodzakelijk zijn:
1° voor de instelling, uitoefening of onderbouwing van een rechtsvordering of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid;
2° wegens redenen van zwaarwegend algemeen belang op grond van de regelgeving die België bindt;
3° voor medische diagnosen en het verstrekken van gezondheidszorg;
4° wegens redenen van algemeen belang op het gebied van de volksgezondheid".

12. De voormelde rechtsgronden zijn een parafrasering van (enkele van de) gronden vermeld in artikel 9.2 AVG. De Autoriteit wijst er wat dit betreft evenwel op dat het eenvoudigweg hernemen of parafraseren van bepalingen van de AVG geen juridische meerwaarde biedt. De uitzonderingsgrond(en) *ex* artikel 9.2 AVG die wordt/worden gehanteerd voor de verwerking dient/dienen *in concreto* te worden toegepast en gepreciseerd. Meer specifiek dient te worden bepaald voor welke categorieën van gevoelige persoonsgegevens op welke uitzonderingsgrond(en) uit artikel 9.2 AVG zal worden gesteund.

b. <u>Doeleinde(n) van de in te voeren gegevensverwerking</u>

13. Volgens artikel 5.1.b) AVG is de verwerking van persoonsgegevens enkel toegestaan voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.

14. Artikel 10, §1 van het voorontwerp somt de doeleinden op voor dewelke de Dienst Vreemdelingenzaken persoonsgegevens kan verzamelen en verwerken:

*"**Art. 10.** De Dienst Vreemdelingenzaken kan de in artikel 6 bedoelde categorieën van persoonsgegevens verwerken voor de volgende doeleinden:*
1° identificeren van de personen bedoeld in artikel 9;
2° behandelen van de visumaanvragen die vereist zijn voor doorreis door of verblijf in België of een andere lidstaat, met het oog op over de afgifte, verlenging, intrekking of annulering ervan;
3° behandelen van de aanvragen voor reisautorisaties die vereist zijn voor doorreis door of verblijf in België of een andere lidstaat met het oog op over de afgifte, verlenging, intrekking of annulering ervan;
4° controleren van vreemdelingen aan de buitengrenzen van België of van een andere lidstaat, in het bijzonder het nagaan van de voorwaarden voor binnenkomst en verblijf, en het nemen van beslissingen betreffende hun binnenkomst of terugdrijving;
5° controleren van vreemdelingen in België, in het bijzonder het nagaan van de voorwaarden voor verblijf en het nemen van beslissingen met betrekking tot hun verblijf of hun verwijdering, met inbegrip van hun inreisverbod;

6° behandelen van de in België ingediende aanvragen tot verblijf met het oog op over de toekenning, verlenging, hernieuwing of beëindiging van het verblijf;
7° het tot een goed einde brengen van de hervestigingsprocedures van vreemdelingen in België;
8° instaan voor de uitvoering van de internationale beschermingsprocedure, in het bijzonder:
a) de registratie van verzoeken om internationale bescherming;
b) de vaststelling van de lidstaat die verantwoordelijk is voor de verwerking van het verzoek om internationale bescherming, met inbegrip van de vaststelling van vasthoudingsmaatregelen, de behandeling en de opvolging van aanvragen tot overname of terugname en de vaststelling van overdrachtsmaatregelen;
c) de overdracht aan het Commissariaat-generaal voor de Vluchtelingen en de Staatlozen van de verzoeken om internationale bescherming waarvoor België verantwoordelijk is, met het oog op het onderzoek ervan en om een beslissing te nemen over de erkenning als vluchteling of begunstigde van subsidiaire bescherming;
d) de opvolging van de verblijfssituatie van personen die internationale bescherming aanvragen in de loop van de procedure of wier verzoek is afgewezen, met inbegrip van de aanneming van verwijderings- of vasthoudingsmaatregelen;
e) de opvolging van het verblijf van personen met het vluchtelingenstatus of subsidiaire beschermingsstatus, met inbegrip van verzoeken om intrekking of opheffing die zijn gericht aan het Commissariaat-generaal voor de Vluchtelingen en de Staatlozen;
9° instaan voor de afgifte, hernieuwing, verlenging en intrekking van verblijfstitels en verblijfsdocumenten, alsmede van elk document waarvan de afgifte is voorzien door of krachtens de wet van 15 december 1980;
10° instaan voor de uitvoering en de opvolging van de procedures voor de terugdrijving, de verwijdering en de overdracht van vreemdelingen, in het bijzonder het verkrijgen van de vereiste reisdocumenten, het nemen van de vereiste dwangmaatregelen, met inbegrip van maatregelen om de betrokkene aan de grens te houden of te begeleiden, het eventuele uitstel van vertrek, de uitvoering van overnameakkoorden die België binden, de erkenning van door andere lidstaten genomen verwijderingsmaatregelen en de voorbereiding, organisatie, uitvoering en opvolging van de al dan niet vrijwillige vertrekken in samenwerking met de bevoegde autoriteiten, instanties, instellingen en organisaties;
11° instaan voor de opvolging van de inreisverboden, met inbegrip van de opheffing of schorsing ervan, en het beheer van de registratie ervan in het Schengeninformatiesysteem en in de algemene nationale gegevensbank of in een andere nationale gegevensbank;
12° opleggen van de administratieve geldboeten voorzien in de wet van 15 december 1980 en het verzekeren van de invordering ervan;
13° instaan voor het beheer en de opvolging van geschillen in verband met de toepassing van de wetgeving inzake de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen;
14° bestrijden van identiteitsfraude, misbruik van reisdocumenten en alle andere vormen van misbruik of oneigenlijk gebruik van procedures inzake migratie en internationale bescherming, zoals schijnhuwelijken, schijnwettelijke samenwoning of frauduleuze erkenningen;
15° terugvorderen van de kosten van gezondheidszorg, verblijf en verwijdering;
16° opsporen en vaststellen van de inbreuken op de wet van 15 december 1980 en andere wetgeving waarvoor de personeelsleden van de Dienst Vreemdelingenzaken bevoegd zijn;
migratie en internationale bescherming, in het bijzonder om het beleid ter zake te ontwikkelen of te motiveren, om migratiefenomenen in kaart te brengen of om te voldoen aan wettelijke verplichtingen;

18° voldoen aan de Europese en internationale verplichtingen in verband met visumbeleid, grensoverschrijding, vrij verkeer van personen, internationale bescherming en immigratiebeleid, met inbegrip van beleid inzake hervestiging, terugkeer en re-integratie."

15. De Autoriteit stelt vast dat de formulering van bepaalde van de in artikel 10 van het voorontwerp opgesomde doeleinden algemeen is en een marge laat voor een subjectieve invulling. De doeleinden moeten voldoende precies zijn zodat een rechtsonderhorige duidelijkheid heeft over de exacte redenen die aanleiding geven tot de verwerking van zijn of haar persoonsgegevens[8]. Hij moet bij de lectuur ervan kunnen opmaken welke gegevensverwerkingen nodig zijn om de doeleinden te realiseren. De Autoriteit verwijst in dit verband bij wijze van voorbeeld naar de structuur van artikel 11 van het voorontwerp, betreffende de ontvangers van persoonsgegevens, waarbij voor wat betreft bepaalde van de opgesomde (categorieën van) ontvangers in artikel 11, §1 van het voorontwerp de exacte doeleinden worden gepreciseerd voor dewelke persoonsgegevens kunnen worden doorgegeven aan de desbetreffende ontvanger (cf. "*met oog op* (…)"). In dit verband wordt onder meer verwezen naar artikel 11, §1, 2° (Belgische diplomatieke of consulaire posten), 8° (de gemeenten) en 12° (de socialezekerheidsinstanties) (cf. eveneens *infra*).

16. Een nauwkeurige omschrijving van de doeleinden van de verwerking(en) is eveneens van belang teneinde de verwerkingsverantwoordelijke in staat te stellen te bepalen welke (categorieën van) persoonsgegevens precies moeten worden verzameld en verwerkt (cf. *infra*). De verwerkte gegevens dienen immers relevant te zijn met betrekking tot de doeleinden. Indien de doeleinden te ruim of vaag worden geformuleerd, bestaat het risico op de verwerking van een te ruim scala aan persoonsgegevens[9]. Bovendien is het eveneens in functie van de doeleinde dat de relevantie van de verschillende (categorieën van) ontvangers kan worden beoordeeld.

17. Overeenkomstig het hierboven vermelde legaliteits- en voorzienbaarheidsprincipe dient elke verwerking van persoonsgegevens te worden geregeld door duidelijke en nauwkeurige regelgeving, waarvan de toepassing voor de betrokkenen voorzienbaar moet zijn. De Autoriteit stelt evenwel vast dat bepaalde van de in artikel 10 van het voorontwerp opgesomde verwerkingsdoeleinden omwille van hun ruime formulering, enerzijds, niet toelaten te begrijpen wat er precies met de verzamelde gegevens zal worden gedaan, door wie en waarom en, anderzijds, niet toelaten te bepalen welke

---

[8] Zie in dezelfde zin: advies nr. 34/2018 van 11 april 2018 van de Commissie voor de bescherming van de persoonlijke levenssfeer, rechtsvoorganger van de Autoriteit, dat stelde dat het doeleinde "*datamatching en datamining met oog op een efficiënte aanpak van sociale fraude*" te ruim was geformuleerd om een rechtsonderhorige duidelijkheid te verschaffen over de exacte toedracht van het samenbrengen van zijn of haar persoonsgegevens in een datawarehouse. Dit advies kan worden geraadpleegd via volgende link: https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/advies_34_2018.pdf.

Zie ook advies nr. 99/2019 van de Autoriteit van 3 april 2019, waarin de Autoriteit van mening was dat het doeleinde "*het verrichten van onderzoeken die nuttig zijn voor de kennis, de conceptie en het beheer van de sociale bescherming*" ook te vaag omschreven was. Dit advies kan worden geraadpleegd via volgende link: https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_99_2019.pdf.

[9] Poullet, Y., Rosier, K. en de Terwangne, C., *Le Règlement Général Sur La Protection Des Données (RGPD/GDPR) : Analyse Approfondie,* Bruxelles, Larcier, 2018, p. 95.

(categorieën van) persoonsgegevens noodzakelijkerwijs zullen dienen te worden verwerkt teneinde de beoogde doeleinde(n) te kunnen verwezenlijken. Bijgevolg kunnen deze doeleinden niet als "*welbepaald en uitdrukkelijk omschreven*" in de zin van artikel 5.1.b) AVG worden beschouwd.

18. De Autoriteit verwijst in dit verband onder meer naar de doeleinden opgenomen in artikel 10, §1, 7° ("*het tot een goed einde brengen van de hervestigingsprocedures van vreemdelingen in België*"), en 18° ("*voldoen aan de Europese en internationale verplichtingen in verband met visumbeleid* (…)").

19. De Autoriteit wijst er verder op dat bepaalde van de in artikel 10, §1 van het voorontwerp opgenomen doeleinden nader zouden kunnen worden verduidelijkt door de toevoeging van een verwijzing naar de precieze wettelijke bepaling die de desbetreffende opdracht van de Dienst Vreemdelingenzaken omkadert (bijv. de betrokken bepalingen van de Vreemdelingenwet en het KB van 8 oktober 1981) dan wel andere toepasselijke wettelijke bepalingen.

20. De Autoriteit merkt met betrekking tot artikel 10, §1 van het voorontwerp verder op dat artikel 10, §1, 17° als doeleinde vermeldt: het "*opstellen van verslagen en statistieken over migratie en internationale bescherming, in het bijzonder om het beleid ter zake te ontwikkelen of te motiveren, om migratiefenomenen in kaart te brengen of om te voldoen aan wettelijke verplichtingen*"[10].

21. De Autoriteit stelt vast dat voormelde wordt opgenomen in de lijst van doeleinden waarvoor de Dienst Vreemdelingenzaken persoonsgegevens verzamelt en verwerkt. Er dient evenwel op te worden gewezen dat *in casu* geen persoonsgegevens mogen worden verzameld met als doeleinde het opstellen van statistieken. De verwerking van persoonsgegevens voor statistische doeleinden betreft hier een verdere verwerking in de zin van artikelen 5.1.b) en 6.4 AVG.

22. Artikel 89.1 AVG vereist dat elke verwerking voor statistische doeleinden moet worden omkaderd door passende waarborgen zodat technische en organisatorische maatregelen worden getroffen om de naleving van het beginsel van de minimale gegevensverwerking te verzekeren en wanneer de statistische doeleinden kunnen worden bereikt door latere verwerkingen die geen of niet langer een identificatie van de betrokkenen toelaat, dient op deze wijze te werk te worden gegaan.

23. De verdere verwerking voor statistische doeleinden gebeurt dus bij voorkeur aan de hand van anonieme gegevens[11]. Indien het niet mogelijk is om met anonieme gegevens het beoogde

[10] De Autoriteit onderlijnt.

[11] Anonieme gegevens: informatie die niet aan een geïdentificeerde of identificeerbare natuurlijke persoon kan worden gekoppeld (art. 4.1) AVG, *a contrario*).

verwerkingsdoeleinde te bereiken, kunnen gepseudonimiseerde[12] persoonsgegevens worden gebruikt. Indien ook deze niet toelaten het beoogde doeleinde te verwezenlijken kunnen, slechts in laatste instantie, ook niet-gepseudonimiseerde persoonsgegevens worden aangewend.

24. In dit verband herhaalt de Autoriteit dat de identificatie van een persoon niet enkel slaat op de mogelijkheid om zijn naam en/of adres te achterhalen maar eveneens op de mogelijkheid om hem te identificeren via een proces van individualisering, correlatie of gevolgtrekking.

25. Voor het overige verwijst de Autoriteit naar advies 05/2014 van de Werkgroep « Artikel 29 » over gegevensbescherming, voorganger van het Europees Comité voor gegevensbescherming, over de anonimiseringstechnieken[13].

26. De Autoriteit wijst erop dat de Memorie van toelichting van het ontwerp informatie dient te bevatten betreffende de beoogde anonimiseringsstrategie. Transparantie met betrekking tot de weerhouden anonimiseringsstrategie en een analyse van de risico's verbonden aan heridentificatie zijn immers elementen die bijdragen tot een weloverwogen aanpak van het anonimiseringsproces.

27. De Autoriteit vestigt de aandacht van de aanvrager op het feit dat er een verschil bestaat tussen gepseudonimiseerde gegevens, die in artikel 4(5) van de AVG worden gedefinieerd als gegevens die *"niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt"* en geanonimiseerde gegevens, die niet langer met redelijke middelen aan een bepaalde persoon kunnen worden toegeschreven, en dat enkel deze laatste geen persoonsgegevens meer vormen en dus overeenkomstig overweging 26 zijn uitgesloten van de werkingssfeer van de AVG[14].

28. Derhalve, rekening houdend met de definitie van persoonsgegevens in artikel 4, 1), van de AVG[15], moet ervoor worden gezorgd dat aan de vereiste hoge normen voor anonimisering wordt

---

[12] *"Pseudonimisering: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld."* (zie artikel 4.5) AVG).

[13] Dit advies is beschikbaar op volgend adres: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_nl.pdf

[14] Voor meer informatie, zie de opinie 5/2014 (WP216) mbt anonimiseringstechnieken, 2.2.3, blz. 10 van de Groep 29, https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2014/wp216_en.pdf (uitsluitend beschikbaar in het Engels).

[15] Namelijk: «*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 identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon*».

voldaan[16] en dat de gegevens niet eenvoudigweg worden gepseudonimiseerd. De verwerking van dergelijke gegevens, zelfs al zijn ze gepseudonimiseerd, moet immers worden gezien als een verwerking van persoonsgegeven als bedoeld in de AVG.

29. Uit het voorgaande volgt dat als er sprake is van pseudonimisering (en niet anonimisering):
- er moet worden verwezen naar het verslag van het Europees Agentschap voor Cyberbeveiliging betreffende technieken en goede praktijken voor pseudonimisering[17];
- deze verwerking moet worden omkaderd met alle vereiste waarborgen en moet voldoen aan de heersende beginselen ter zake[18].

30. De Autoriteit wijst er tot slot met betrekking tot artikel 10, §1, 17° van het voorontwerp op dat de zinsnede "*opstellen van verslagen en statistieken (…) om te voldoen aan wettelijke verplichtingen*" zeer ruim geformuleerd is en stelt vast dat in de Memorie van toelichting evenmin wordt verduidelijkt om welke wettelijke verplichtingen het precies gaat. De Autoriteit is van oordeel dat het, met oog op transparantie en voorzienbaarheid, aangewezen is de wettelijke norm(en) te preciseren die deze verplichting aan de Dienst Vreemdelingenzaken oplegt of opleggen.

31. In zijn § 2 bepaalt artikel 10 van het voorontwerp met betrekking tot de in §1 opgesomde doeleinden: "*De Koning kan, bij een koninklijk besluit vastgesteld na overleg in de Ministerraad en na advies van de Gegevensbeschermingsautoriteit, de in paragraaf 1 vermelde doeleinden nader bepalen of aanvullen*"[19].

32. De Autoriteit wijst er evenwel op dat voormelde in strijd is met het legaliteitsbeginsel vervat in artikel 6.3 AVG, in samenhang gelezen met overweging 41 AVG, *j°* artikel 22 van de Grondwet, volgens hetwelk de wezenlijke elementen van de gegevensverwerking - waaronder de doeleinden van deze verwerkingen - door middel van een formele wettelijke norm (*i.e.* een wet, een decreet of een ordonnantie) dienen te worden vastgesteld. De doeleinden van de verwerking kunnen bijgevolg niet worden aangevuld of uitgebreid door middel van een reglementaire norm (zoals, *in casu*, een koninklijk besluit). Hoogstens kunnen deze doeleinden nader worden *gepreciseerd*. In artikel 10, § 2 van het voorontwerp dient bijgevolg "of aanvullen" te worden geschrapt.

---

[16] De identificatie van een persoon slaat niet enkel op de mogelijkheid om zijn naam en/of adres te achterhalen, maar eveneens op de mogelijkheid om hem te identificeren via een proces van individualisering, correlatie of gevolgtrekking.

[17] ENISA: https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases en https://www.enisa.europa.eu/news/enisa-news/enisa-proposes-best-practices-and-techniques-for-pseudonymisation;

[18] Hetzelfde geldt voor het proportionaliteitsbeginsel dat verwijst naar het specifiekere beginsel van "*minimale gegevensverwerking*" dat inhoudt dat de persoonsgegevens toereikend, ter zake dienend en beperkt moeten zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt, overeenkomstig artikel 5, § 1, c), van de AVG.

[19] De Autoriteit onderlijnt.

c. <u>Verwerkingsverantwoordelijke(n)</u>

33. Artikel 4.7) AVG bepaalt dat voor de verwerkingen waarvan de regelgeving het doel en de middelen vastlegt, de verwerkingsverantwoordelijke diegene is die daarin als dusdanig wordt aangewezen.

34. Artikel 5 van het voorontwerp stelt in dit verband: "§*1. De minister is de verantwoordelijke voor de verwerking van persoonsgegevens door de Dienst Vreemdelingenzaken. § 2. De minister kan zich bij het nakomen van zijn verplichtingen als verwerkingsverantwoordelijke laten vertegenwoordigen door de Directeur-generaal van de Dienst Vreemdelingenzaken*."

35. Wanneer het nationaal recht de doelstellingen van en de middelen voor de verwerking bepaalt, "*kan worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria van het [nationaal] recht deze wordt aangewezen*"[20]. Hoewel de lidstaten in bijzondere domeinen de toepassing van de regels van de AVG kunnen bepalen teneinde in deze domeinen de coherentie en de duidelijkheid van het wettelijk kader te bewaren dat toepasselijk is op gegevensverwerkingen, kunnen zij evenwel niet afwijken van de AVG of afzien van de daarin bepaalde definities[21]. De aanduiding van een verwerkingsverantwoordelijke in de regelgeving dient met andere woorden te stroken met de rol die deze actor in de praktijk opneemt. Het tegenovergestelde beweren zou niet alleen ingaan tegen de letter van de AVG maar zou eveneens de doelstelling ervan in gevaar kunnen brengen om een coherent en hoog beveiligingsniveau te verzekeren voor natuurlijke personen.

36. Het Europees Comité voor Gegevensbescherming stelt in dit verband in zijn Richtsnoeren *over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG* dat bedrijven of overheidsinstanties soms een specifieke natuurlijke persoon aanduiden als verantwoordelijke voor de uitvoering van de verwerkingsactiviteit, hoewel deze in wezen optreedt namens de rechtspersoon (onderneming of overheidsinstantie) die uiteindelijk verantwoordelijk is in geval van inbreuk op de regels in zijn hoedanigheid van verwerkingsverantwoordelijke"[22].

37. In het licht van voorgaande, stelt de Autoriteit zich vragen bij de aanduiding van de minister als verwerkingsverantwoordelijke. Onafgezien van de *politieke* verantwoordelijkheid die rust op de

---

[20] Artikel 4, 7), AVG. Betreffende de vaststelling van de respectieve verantwoordelijkheden van de gezamenlijke verwerkingsverantwoordelijken, lees eveneens artikel 26, 1., van de AVG

[21] Lees Artikel 6, 3., 2de lid en de overwegingen 8 en 10 van de AVG.

[22] Europees Comité voor Gegevensbescherming, Richtsnoeren 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG, 2 september 2020, p. 10, nr. 18: "*Sometimes, companies and public bodies appoint a specific person responsible for the implementation of the processing activity. Even if a specific natural person is appointed to ensure compliance with data protection rules, this person will not be the controller but will act on behalf of the legal entity (company or public body) which will be ultimately responsible in case of infringement of the rules in its capacity as controller. In the same vein, even if a particular department or unit of an organisation has operational responsibility for ensuring compliance for certain processing activity, it does not mean that this department or unit (rather than the organisation as a whole) becomes the controller".*

bevoegde minister, lijkt diens aanduiding als verwerkingsverantwoordelijke *in casu*, voor verwerkingen van persoonsgegevens uitgevoerd door de Dienst Vreemdelingenzaken, niet passend. In de praktijk lijkt het immers niet de minister te zijn die de doeleinden nastreeft waarvoor de onder zijn bevoegdheid ressorterende dienst persoonsgegevens verwerkt, doch wel de administratie zelf. Het dient bijgevolg de administratie van de Dienst Vreemdelingenzaken te zijn die de rol van verwerkingsverantwoordelijke in de zin van artikel 4.7) AVG dient waar te nemen en aldus in het voorontwerp dient te worden aangeduid[23].

d. <u>Categorieën van persoonsgegevens en betrokkenen</u>

38. Artikel 5.1.c) AVG bepaalt dat persoonsgegevens toereikend, ter zake dienend en beperkt moeten zijn tot wat noodzakelijk is voor de beoogde doeleinden ('minimale gegevensverwerking').

39. Artikel 6 van het voorontwerp somt de (categorieën van) persoonsgegevens op die door de Dienst Vreemdelingenzaken kunnen worden verwerkt:

Art. 6. *De Dienst Vreemdelingenzaken kan de volgende categorieën van persoonsgegevens verwerken:*
1° identificatiegegevens, met inbegrip van de foto's en de vingerafdrukken;
2° financiële bijzonderheden;
3° persoonlijke kenmerken;
4° leefgewoonten;
5° gegevens betreffende de persoonlijkheid, het karakter en/of het gedrag;
6° samenstelling van het gezin;
7° hobby's en interesses;
8° lidmaatschappen (andere dan professionele lidmaatschappen, politieke lidmaatschappen of vakbondslidmaatschappen);
9° gegevens met betrekking tot overtredingen en strafbare feiten;
10° consumptiegewoonten;
11° kenmerken van de woning;
12° gegevens met betrekking tot de gezondheid;
13° studies en vorming;
14° beroep en tewerkstelling;
15° raciale of etnische gegevens;
16° gegevens met betrekking tot het seksueel gedrag;
17° politieke opinies;

[23] Cf. in dit verband eveneens het advies 122/2022 van de Autoriteit d.d. 1 juli 2022 (randnrs. 8-16).

18° lidmaatschap van een vakbond of een soortgelijke groep, vervulde functies;
19° levensbeschouwelijke of religieuze overtuigingen.

40. De Autoriteit wijst erop dat, in het licht van het beginsel van minimale gegevensverwerking alsook het voorzienbaarheidsbeginsel, niet kan worden volstaan met het louter opnemen van een lijst van alle (categorieën van) persoonsgegevens die door de Dienst Vreemdelingenzaken kunnen worden verwerkt. Teneinde de betrokkenen in staat te stellen bij de lezing van de tekst te kunnen begrijpen welke gegevensverwerkingen noodzakelijk zijn, dienen de (categorieën van) persoonsgegevens in verband te worden gebracht met de verwerkingsdoeleinden (art. 10 voorontwerp) en de ontvangers (art. 11 voorontwerp). Er dient vooreerst nader te worden gepreciseerd welke (types) verwerkingen door de Dienst Vreemdelingenzaken zullen kunnen worden uitgevoerd op welke (categorieën van) persoonsgegevens (verzamelen, opslaan, consulteren, anonimiseren, wissen, etc.) en voor welke doeleinden. Niet elke van de in artikel 6 van het voorontwerp opgesomde categorieën van persoonsgegevens zal immers (dienen te) worden verwerkt voor elk van de in artikel 10 van het voorontwerp opgelijste doeleinden. Zo zal bijvoorbeeld wellicht niet worden overgegaan tot pseudonimisering van de gegevens betreffende hobby's en interesses (art. 6, 7°) met oog op de opvolging van de reisverboden en de registratie ervan in het Schengeninformatiesysteem (art. 10, 11°). Er dient aldus een duidelijkere koppeling te worden opgenomen in het voorontwerp tussen de verwerkte (categorieën van) persoonsgegevens en de verwerkingsdoeleinden. Verder dient in geval van doorgifte van bepaalde (categorieën van) persoonsgegevens eveneens te worden gepreciseerd aan welke ontvangers deze desgevallend zullen worden overgemaakt en voor welke doeleinden (cf. ook *infra* randnr. 13 e.v.).

41. Overeenkomstig het proportionaliteitsbeginsel en het beginsel van minimale gegevensverwerking mogen enkel de persoonsgegevens worden verzameld en verwerkt – en bijgevolg overgemaakt aan bepaalde (categorieën van) ontvangers – die noodzakelijk zijn voor het verwezenlijken van de doeleinden. In dit verband wijst de Autoriteit erop dat op basis van de tekst van het voorliggende voorontwerp bepaalde (categorieën van) persoonsgegevens kunnen worden doorgegeven aan bepaalde (categorieën van) ontvangers, hoewel de noodzakelijkheid hiervan geenszins aangetoond is. Bij wijze van voorbeeld wijst de Autoriteit erop dat op basis van de samenlezing van artikelen 6, 17° en 11, §1, 7° van het voorontwerp de gegevens met betrekking tot het seksueel gedrag van de betrokkenen kunnen worden doorgegeven aan vervoerders. Er dient bijgevolg nader te worden gepreciseerd voor welke van de in artikel 6 van het voorontwerp opgenomen (categorieën van) persoonsgegevens de doorgifte noodzakelijk is aan welke in artikel 11 opgesomde ontvangers en voor welke doeleinde(n).

42. Artikel 8, 1° van het voorontwerp stelt: "*De Koning kan, bij een koninklijk besluit vastgesteld na overleg in de Ministerraad en na advies van de Gegevensbeschermingsautoriteit: de in artikel 6 vermelde categorieën van persoonsgegevens specificeren of aanvullen*"[24].

43. De Autoriteit wijst er evenwel op dat voormelde in strijd is met het legaliteitsbeginsel vervat in artikel 6.3 AVG, in samenhang gelezen met overweging 41 AVG, *j°* artikel 22 van de Grondwet, volgens hetwelk de wezenlijke elementen van de gegevensverwerking door middel van een formele wettelijke norm (*i.e.* een wet, een decreet of een ordonnantie) dienen te worden vastgesteld. Wanneer de gegevensverwerking een belangrijke inmenging vormt op de rechten en vrijheden van de betrokkenen, zoals in het onderhavige geval, dienen eveneens de (categorieën van) persoonsgegevens in een formele wettelijke norm te worden vastgesteld. Deze kunnen bijgevolg niet worden aangevuld of uitgebreid door middel van een reglementaire norm (zoals, *in casu*, een koninklijk besluit). Hoogstens kunnen deze nader worden *gepreciseerd*. In artikel 8, 1° van het voorontwerp dient bijgevolg "*of aanvullen*" te worden geschrapt.

44. Artikel 9 van het voorontwerp somt de categorieën van betrokkenen op waarvan de Dienst Vreemdelingenzaken persoonsgegevens kan verwerken:

> ***"Art. 9.*** *De Dienst Vreemdelingenzaken kan de in artikel 6 bedoelde categorieën van persoonsgegevens verwerken voor de volgende personen:*
> *1° vreemdelingen die een aanvraag voor een visum of een reisautorisatie hebben ingediend om naar België of een andere lidstaat af te reizen;*
> *2° vreemdelingen die zich aanbieden aan de buitengrenzen van België of van een andere lidstaat;*
> *3° vreemdelingen die zich op Belgisch grondgebied of op het grondgebied van een andere lidstaat bevinden;*
> *4° vreemdelingen die zich buiten het Belgische grondgebied bevinden en die de toegang tot het grondgebied wordt geweigerd met toepassing van de wet van 15 december 1980;*
> *5° de vreemdelingen die het voorwerp uitmaken van een hervestigingsprocedure in België;*
> *6° de Belgen en de vreemdelingen die een familiale, professionele, economische, culturele of andere band hebben met een vreemdeling bedoeld in 1° tot 5°, die in aanmerking moet worden genomen bij de behandeling van zijn aanvraag of de beoordeling van zijn situatie".*

45. De Autoriteit wijst erop dat het aangewezen is, met oog op transparantie, de voormelde categorieën van betrokkenen - in het bijzonder deze vermeld in artikel 9, 1° t.e.m. 5° - te

[24] De Autoriteit onderlijnt.

verduidelijken door middel van verwijzing naar de desbetreffende bepalingen van de Vreemdelingenwet.

46. Verder dient erop te worden gewezen dat de formulering van de categorie van betrokkenen bedoeld onder artikel 9, 6° van het voorontwerp zeer ruim is ("*de Belgen en de vreemdelingen die een familiale, professionele, economische, culturele of andere band hebben met een vreemdeling* (…)[25]", waardoor weinig voorzienbaar is welke personen het *in casu* kan betreffen. De Memorie van toelichting[26] bevat bijkomende preciseringen ter zake en geeft een aantal voorbeelden van de personen die concreet worden geviseerd. Er wordt in dit verband onder meer verwezen naar de artsen die een standaard medisch getuigschrift hebben ondertekend in het kader van een verblijfsaanvraag om medische redenen, de familieleden die het recht op gezinshereniging openen, de politieambtenaren die een administratief rapport hebben opgesteld, de werkgevers die de aanvragen voor een gecombineerde vergunning bij de gewestelijke overheden indienen, etc. Het verdient aanbeveling deze betrokkenen op te lijsten in de tekst van het voorontwerp zelf. De Autoriteit stelt zich evenwel vragen betreffende de noodzakelijkheid en proportionaliteit van de verwerking van de persoonsgegevens van "*de Belgen en de vreemdelingen die een (…) een culturele band hebben met een vreemdeling*"[27]. Uit de Memorie van toelichting blijkt niet wat deze categorie van betrokkenen concreet inhoudt en voor welke doeleinden de persoonsgegevens van deze betrokkenen zullen worden verwerkt. Verder komt het de Autoriteit evenmin noodzakelijk en proportioneel voor om voor alle betrokkenen geviseerd door artikel 9, 6° van het voorontwerp alle (categorieën van) persoonsgegevens te verzamelen die worden opgelijst in artikel 6 van het voorontwerp. Zo lijkt het voor de hierboven opgesomde betrokkenen, die bij wijze van illustratie worden vermeld in de Memorie van toelichting (artsen, politieambtenaren en werkgevers), enkel noodzakelijk de identificatiegegevens (art. 6, 1°, met uitzondering van de in deze bepaling opgesomde biometrische gegevens) te verzamelen en verwerken. De verwerking van de overige (categorieën van persoonsgegevens) lijkt - in bepaalde gevallen - hoogstens noodzakelijk voor wat betreft de personen die een familiale band hebben met de vreemdeling en/of die afhankelijk zijn van deze vreemdeling.

e. Ontvangers of categorieën van ontvangers

47. Artikel 11, §1 van het voorontwerp somt de (categorieën van) ontvangers op aan wie de door de Dienst Vreemdelingenzaken verzamelde en verwerkte persoonsgegevens kunnen worden meegedeeld. Voormelde bepaling bevat een zeer uitgebreide lijst van 37 verschillende (categorieën van) ontvangers. Artikel 11, §1 van het voorontwerp maakt zowel melding van nationale als internationale ontvangers. Verder bepaalt Hoofdstuk 2 van het voorontwerp (artikelen 28 tot en met

[25] De Autoriteit onderlijnt.

[26] Memorie van toelichting, p. 37, 6e alinea.

[27] De Autoriteit onderlijnt.

31) welke derden gemachtigd kunnen worden om toegang te hebben tot de informatie geregistreerd door de Dienst Vreemdelingenzaken beheerde gegevensbanken.

48. De Autoriteit stelt vast dat voor wat betreft bepaalde van de opgesomde (categorieën van) ontvangers in artikel 11, §1 van het voorontwerp de exacte doeleinden worden gepreciseerd voor dewelke persoonsgegevens kunnen worden doorgegeven aan de desbetreffende ontvanger (cf. "*met oog op* (…)"). In dit verband wordt onder meer verwezen naar artikel 11, §1, 2° (Belgische diplomatieke of consulaire posten), 8° (de gemeenten) en 12° (de socialezekerheidsinstanties).

49. Evenwel is zulks *niet* het geval voor een andere van de 37 opgesomde (categorieën van) ontvangers. In dit verband wordt bijvoorbeeld verwezen naar artikel 11, §1, 4° ("*de externe dienstverleners met wie België samenwerkt in het kader van de procedure voor de afgifte van visa*"), 5° (de commerciële tussenpersonen), 23° (niet-gouvernementele organisaties) en 35° (het Nationaal Crisiscentrum). Er dient op te worden gewezen dat, bij gebrek aan precisering van de doeleinden waarvoor een uitwisseling van de persoonsgegevens tussen de Dienst Vreemdelingenzaken en elke betrokken ontvanger kan plaatsvinden, de beoogde verwerkingen in kwestie niet voorzienbaar zijn zoals vereist door artikel 6.3 AVG, gelezen in het licht van overweging 41 AVG. De Autoriteit stelt vast dat de aanvrager in de Memorie van toelichting voor bepaalde van deze (categorieën van) ontvangers bijkomende preciseringen opneemt. Het is aangewezen deze doeleinden - die een wezenlijk element van de verwerking uitmaken - in de tekst van het voorontwerp zelf op te nemen.

50. Uit het gebrek aan precisering van de doeleinde(n) van de doorgifte aan bepaalde van de in artikel 11, §1 opgesomde ontvangers vloeit voort dat bijgevolg evenmin kan worden beoordeeld welke (categorieën van) persoonsgegevens dienen te worden doorgegeven aan de desbetreffende ontvangers, hetgeen nochtans vereist is met oog op de voorzienbaarheid voor de rechtsonderhorigen en betrokkenen in de zin van de AVG. De Autoriteit verwijst in dit verband naar overwegingen 40 en 41 (*supra*).

51. Wat betreft de internationale ontvangers opgenomen in artikel 11, §1 van het voorontwerp, wijst de Autoriteit erop dat overeenkomstig artikel 44 e.v. AVG voor de doorgiften van persoonsgegevens aan derde landen of internationale organisaties een passend beschermingsniveau dient te worden gewaarborgd door:

- hetzij het voorhanden zijn van een adequaatheidsbesluit van de Europese Commissie met betrekking tot het derde land waarnaar de persoonsgegevens worden doorgegeven (artikel 45 AVG);
- hetzij door passende waarborgen te voorzien zoals voorgeschreven door artikel 46 AVG (bijvoorbeeld het sluiten van een juridische bindend instrument met de internationale organisatie of het derde land in kwestie).

52. Het voorontwerp dient voor elke voorziene doorgifte van persoonsgegevens aan een derde land of internationale organisatie te vermelden op welke basis deze plaatsvindt en dient eveneens te preciseren welke waarborgen worden voorzien (zoals het verbod op verdere doorgifte en het eventuele verbod op doorgifte naar andere landen).

53. Artikel 11, §2 van het voorontwerp stelt: "*De Koning kan, bij een koninklijk besluit vastgesteld na overleg in de Ministerraad en na advies van de Gegevensbeschermingsautoriteit, de lijst met entiteiten vermeld in paragraaf 1 nader bepalen of aanvullen*"[28].

54. De Autoriteit wijst er evenwel op dat voormelde in strijd is met het legaliteitsbeginsel vervat in artikel 6.3 AVG, in samenhang gelezen met overweging 41 AVG, *j°* artikel 22 van de Grondwet, volgens hetwelk de wezenlijke elementen van de gegevensverwerking - waaronder de (categorieën van) ontvangers van deze verwerkingen - door middel van een formele wettelijke norm (*i.e.* een wet, een decreet of een ordonnantie) dienen te worden vastgesteld. De ontvangers van de verwerking kunnen bijgevolg niet worden aangevuld of uitgebreid door middel van een reglementaire norm (zoals, *in casu*, een koninklijk besluit). Hoogstens kunnen deze nader worden *gepreciseerd*. In artikel 11, § 2 van het voorontwerp dient bijgevolg "of aanvullen" te worden geschrapt.

f. Bewaartermijn van de gegevens

55. Krachtens artikel 5.1.e) AVG mogen persoonsgegevens niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren dan noodzakelijk voor de verwezenlijking van de doeleinden waarvoor zij worden verwerkt.

56. Artikelen 12 tot en met 18 van het voorontwerp hebben betrekking op de bewaartermijn van de door de Dienst Vreemdelingenzaken verzamelde en verwerkte persoonsgegevens.

57. Meer bepaald voorziet artikel 13, §1 van het voorontwerp een bewaartermijn van vijf jaar van de door de Dienst Vreemdelingenzaken verzamelde en verwerkte persoonsgegevens die betrekking hebben op de betrokkenen opgesomd in artikel 9, 1° tot 5° van het voorontwerp. Artikel 14 van het voorontwerp bepaalt het aanvangspunt van de bewaartermijn voor elk van de categorieën van betrokkenen. Artikel 15 van het voorontwerp bepaalt dat de persoonsgegevens van de Belgen en vreemdelingen die een familiale, professionele, economische, culturele of andere band hebben met een vreemdeling, bedoeld in artikel 9, 6°, beschikbaar en raadpleegbaar zijn tijdens dezelfde duur als die van toepassing op de persoonsgegevens van die vreemdeling.

[28] De Autoriteit onderlijnt.

58. In de Memorie van toelichting licht de aanvrager toe dat voor een bewaartermijn van vijf jaar werd geopteerd met oog op afstemming met het bepaalde in Verordening (EG) nr. 767/2008 van het Europees Parlement en de Raad van 9 juli 2008 *betreffende het Visuminformatiesysteem (VIS) en de uitwisseling tussen de lidstaten van gegevens op het gebied van visa voor kort verblijf*, die in dit verband bepaalt: "*De in het VIS opgeslagen persoonsgegevens mogen niet langer worden bewaard dan voor de doelstellingen van het VIS noodzakelijk is. Het is aangewezen de gegevens gedurende een periode van ten hoogste vijf jaar te bewaren, zodat bij de beoordeling van visumaanvragen rekening kan worden gehouden met in eerdere aanvragen verstrekte gegevens, inclusief de goede trouw van de aanvragers, en met het oog op de registratie van illegale immigranten die wellicht ooit een visum hebben aangevraagd. Een kortere periode zou voor deze doelstellingen niet toereikend zijn*[29]*.*" De Autoriteit neemt hier akte van.

59. De Autoriteit wijst er vooreerst evenwel op dat de in artikel 13, §1 van het voorontwerp voorziene bewaartermijn van vijf jaar, in het licht van de hierboven hernomen motivering, niet noodzakelijk lijkt voor alle geviseerde (categorieën van) betrokkenen en persoonsgegevens. In dit verband dient er bij wijze van voorbeeld op te worden gewezen dat de noodzakelijkheid niet is aangetoond van het bewaren gedurende vijf jaar van het verblijfsadres van onderdanen van derde landen die naar België komen voor een verblijf van ten hoogste drie maanden (cf. artikel 5 Vreemdelingenwet). Het bewaren van voormelde gegevens lijkt niet langer noodzakelijk op het ogenblik dat de betrokkene het Belgisch grondgebied heeft verlaten en niet langer op het aangegeven adres verblijft[30].

60. Artikel 18 van het voorontwerp stelt: "*De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van de Gegevensbeschermingsautoriteit, de in dit hoofdstuk voorziene bepalingen betreffende de duur voor de bewaring van de persoonsgegevens nader bepalen <u>of aanvullen</u>*"[31]*.*

61. De Autoriteit wijst er evenwel op dat voormelde in strijd is met het legaliteitsbeginsel vervat in artikel 6.3 AVG, in samenhang gelezen met overweging 41 AVG, *j°* artikel 22 van de Grondwet, volgens hetwelk de wezenlijke elementen van de gegevensverwerking door middel van een formele wettelijke norm (*i.e.* een wet, een decreet of een ordonnantie) dienen te worden vastgesteld. Wanneer de gegevensverwerking een belangrijke inmenging vormt op de rechten en vrijheden van de betrokkenen, zoals in het onderhavige geval, dienen eveneens de bewaartermijnen door middel van een formele wettelijke norm (*i.e.* een wet, een decreet of een ordonnantie) te worden vastgesteld. Deze kunnen bijgevolg niet worden aangevuld of uitgebreid door middel van een reglementaire norm

[29] Overweging 14 Verordening.

[30] Cf. in dit verband eveneens het advies 122/2022 van de Autoriteit d.d. 1 juli 2022 (randnrs. 37-40)

[31] De Autoriteit onderlijnt.

(zoals, *in casu*, een koninklijk besluit). In artikel 18 van het voorontwerp dient bijgevolg "of aanvullen" te worden geschrapt.

g. <u>Beperkingen van de rechten van betrokkenen</u>

62. Artikelen 19 tot en met 24 van het voorontwerp van wet voorzien beperkingen op de rechten van de betrokkenen in de zin van artikel 23 AVG.

63. Meer bepaald voorziet artikel 20 van het voorontwerp in een beperking van de toepassing van de rechten vervat in artikelen 16 tot 22 AVG (recht op rectificatie, recht op gegevenswissing, recht op beperking van de verwerking, de kennisgevingsplicht inzake rectificatie of gegevenswissing, recht op overdraagbaarheid van gegevens, recht van bezwaar en geautomatiseerde individuele besluitvorming) alsook van het transparantiebeginsel vervat in artikel 5 AVG en dit voor zover de uitoefening van voormelde rechten en beginselen schade kan toebrengen aan één van de volgende belangen:
"1° de vrijwaring van de openbare orde en van de nationale veiligheid;
2° het voorkomen, opsporen, onderzoeken en vervolgen van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
3° de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;
4° de bescherming van de betrokkenen of van de rechten en vrijheden van anderen;
5° de naleving van de verplichting tot beroepsgeheim".

64. Overeenkomstig artikel 23 AVG, zoals uitgelegd in overweging 73 AVG, kunnen de rechten van betrokkenen evenwel enkel worden ingeperkt onder de voorwaarden en binnen de grenzen vastgelegd in deze bepaling, die gebaseerd is op artikel 52 van het Handvest van de Grondrechten van de Europese Unie en dient te worden gelezen in het licht van de rechtspraak van het Hof van Justitie en artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM).

65. Artikel 23 AVG biedt de lidstaten de mogelijkheid de reikwijdte van de rechten van de betrokkenen te beperken, mits een dergelijke beperking de essentie van de fundamentele rechten en vrijheden eerbiedigt en in een democratische samenleving een noodzakelijke en evenredige maatregel is om een van de in artikel 23.1 AVG genoemde gerechtvaardigde doeleinden te verwezenlijken, zoals de nationale veiligheid, de openbare veiligheid of andere belangrijke doelstellingen van algemeen openbaar belang van de Unie of van een lidstaat, in het bijzonder een belangrijk economisch of financieel belang van de Unie of van een lidstaat, met

inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid, in het bijzonder een controle-, inspectie- of regelgevingsopdracht die verband houdt met de uitoefening van het openbaar gezag, ook al is dat slechts incidenteel het geval.

66. Iedere wettelijk maatregel die voorziet in beperkingen op de rechten van de betrokkene moet ten minste specifieke bepalingen bevatten betreffende de elementen opgesomd in artikel 23.2 AVG zoals:
    - de doeleinden van de verwerking,
    - de (categorieën van) persoonsgegevens,
    - het toepassingsgebied van de beperkingen,
    - waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte,
    - specificatie van de (categorieën van) verwerkingsverantwoordelijke(n),
    - de opslagperiodes,
    - de risico's voor de rechten en vrijheden van de betrokkenen en het recht van de betrokkene op kennisgeving inzake de beperking.

67. Om de draagwijdte van de beoordelingsmarge die de wetgever hierbij geniet in kaart te brengen, is het van belang om te herinneren aan de rechtspraak van het Hof van Justitie over artikel 13 van Richtlijn 95/46/EG dat voorzag in een gelijkaardige mogelijkheid om uitzonderingen te voorzien op de rechten van de betrokkenen. In het arrest *Smaranda Bara* bevestigde het Hof dat deze uitzonderingen alleen door "*wetgevende maatregelen*" kunnen ingevoerd worden[32]. Later preciseerde het Hof dat de Lidstaten deze uitzonderingen slechts kunnen aannemen voor zover deze "*noodzakelijk*" zijn[33]. Gelet op het onveranderde streven van de Europese wetgever naar een hoog beschermingsniveau[34] van persoonsgegevens moeten de beperkingen op de rechten van de betrokkenen absoluut noodzakelijk[35] zijn om het nagestreefde doeleinde te realiseren. De noodzaak en de evenredigheid van deze beperkingen moeten dus strikt geïnterpreteerd worden[36].

68. Vooreerst wijst de Autoriteit erop dat artikel 19 van het voorontwerp, enerzijds, een opsomming van de beperkte rechten bevat en, anderzijds, een verwijzing naar de bepalingen van de AVG die voormelde rechten waarborgen. In dit verband stelt de Autoriteit evenwel vast dat beide

---

[32] Hof van Justitie 1 oktober 2015 (C-201/14), *Smaranda Bara e.a.*, §39; Hof van Justitie 27 september 2017 (C-73/16), *Puškár*, §96.

[33] Hof van Justitie 7 november 2013 (C-473/12), *BIV v. Englebert*, §32.

[34] Overweging 10 AVG; Overweging 10 Richtlijn 95/46/EG.

[35] Ibid., §39.

[36] Advies nr. 34/2018 van 11 april 2018 inzake een voorontwerp van wet *tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van Verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad 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* en meer in het bijzonder de punten 36 tot 38.

zinsneden van artikel 19 van het voorontwerp niet overeenstemmen. In het eerste gedeelte van artikel 19 van het ontwerp wordt immers geen melding gemaakt van de kennisgevingsplicht inzake rectificatie of gegevenswissing, het recht op overdraagbaarheid van gegevens, het recht van bezwaar en geautomatiseerde individuele besluitvorming, hoewel deze rechten wel vervat zitten in de verderop in deze bepaling geciteerde "artikelen 16 tot 22" AVG. Omgekeerd wordt in het tweede gedeelte van artikel 19 enkel verwezen naar de artikelen 16 tot en met 22 AVG (cf. de zinsnede "(…) *en die hem worden toegekend door de artikelen 16 tot 22 van de algemene verordening gegevensbescherming* (…)"), daar waar eerder in dezelfde bepaling alsook in het gedeelte van de Memorie van toelichting betreffende artikel 20 van het voorontwerp eveneens gewag wordt gemaakt van een beperking op het recht op informatie (artikelen 12-14 AVG) alsook het recht van inzage (artikel 15 AVG)[37]. Dit dient te worden rechtgezet.

69. Verder merkt de Autoriteit, meer fundamenteel, op dat niet alle in artikel 23.2 AVG vermelde elementen betreffende de beperking van de rechten van betrokkenen terug te vinden zijn in het voorontwerp van wet. Zo dient erop te worden gewezen dat uit de huidige tekst van het voorontwerp en de Memorie van toelichting de noodzaak en de doeleinden alsook het toepassingsgebied van de voorziene beperkingen niet voldoende concreet blijken. Artikel 20 van het voorontwerp bevat ter rechtvaardiging van de voorziene beperkingen op de rechten van betrokkenen in het kader van de verwerking van persoonsgegevens door de Dienst Vreemdelingenzaken een letterlijke herneming van (bepaalde van de) gronden vervat in artikel 23.1 AVG (cf. *supra* randnr. 61). In de Memorie van toelichting worden weliswaar enkele illustraties opgenomen van situaties die welbepaalde beperkingen zouden rechtvaardigen, zoals de beperking van het recht van inzage van tussenkomende advocaten of artsen in het geval van een hangende klacht ingediend door de Dienst Vreemdelingenzaken bij respectievelijk de stafhouder van de balie of de Orde van Artsen, teneinde te voorkomen dat het goed verloop van de tuchtprocedure in het gedrang zou worden gebracht. Het volstaat evenwel niet in de Memorie van toelichting enkele voorbeelden op te nemen van omstandigheden waarop artikel 20 van het voorontwerp betrekking heeft. De gevallen waarin en de motieven op basis waarvan de rechten worden beperkt, dienen vooreerst nauwkeuriger en *in concreto* in het voorontwerp te worden bepaald. Ten tweede rijst de vraag of in de in de Memorie van toelichting aangegeven gevallen de beperking van *alle* in artikel 19 van het voorontwerp opgesomde rechten van betrokkenen kan rechtvaardigen. Zulks dit eveneens geval per geval te worden gepreciseerd, conform artikel 23.2.c) AVG.

70. Verder dient erop te worden gewezen dat het voorontwerp niet preciseert op welke (categorieën van) persoonsgegevens de beperkingen betrekking hebben. Artikel 21 van het voorontwerp stelt

[37] Memorie van toelichting, p. 82.

in dit verband op zeer algemene wijze: "*De beperking van de rechten bedoeld in artikel 20 beoogt uitsluitend de persoonsgegevens die verband houden met de redenen die haar rechtvaardigen*". Voormelde formulering is evenwel te algemeen en biedt onvoldoende voorzienbaarheid voor de betrokkenen. Er dient nader te worden gepreciseerd welke (categorieën van) persoonsgegevens in welke gevallen het voorwerp kunnen uitmaken van beperkingen.

71. Verder stelt de Autoriteit vast dat artikel 22 van het voorontwerp bepaalt dat "*de beperking van de rechten bedoeld in artikel 20 van toepassing [blijft] totdat* (sic) *de redenen die haar rechtvaardigen, geldig blijven*". Hoewel artikel 23 AVG zulks niet uitdrukkelijk bepaalt, dienen overeenkomstig het proportionaliteitsbeginsel de beperkingen op de rechten van betrokkenen beperkt te zijn in de tijd.[38] Dit werd bevestigd door het Grondwettelijk Hof, dat bij arrest 51/2014 artikel 11 van de wet van 3 augustus *2012 houdende bepalingen betreffende de verwerking van persoonsgegevens door de Federale Overheidsdienst Financiën in het kader van zijn opdrachten* vernietigde wegens schending van het beginsel van gelijkheid en niet-discriminatie "(…) *in zoverre het niet voorziet in een beperking in de tijd van de mogelijkheid om een uitzondering te maken op de toepassing van die rechten die verantwoord is door de uitvoering van werkzaamheden ter voorbereiding van een controle of van een onderzoek*"[39]. Ook de afdeling Wetgeving van de Raad van State wees op het problematisch karakter van de afwezigheid van een tijdsbeperking in dit verband[40].

72. De Autoriteit merkt in het licht van bovenstaande op dat artikel 21 van het voorontwerp geen criteria bevat ter bepaling van de (maximale) duur van de opschorting van de rechten van betrokkenen vermeld in artikel 19 van het voorontwerp, hetgeen kan leiden tot een disproportioneel lange opschorting van de rechten van betrokkenen. De (criteria ter bepaling van de) duur van de beperking van de rechten dient bijgevolg nader te worden gepreciseerd.

h. Varia

73. De Autoriteit merkt op dat in de Nederlandse versie van de ter advies voorgelegde tekst Titel 1 ("*Titre 1er. Disposition générale"* in de Franse versie) ontbreekt.

[38] K. HUYSMANS, "De implementatie van artikel 23 AVG: na de hervorming de contrareformatie?", Tijdschrift Privacy & Persoonsgegevens (TPP), 2019/2, p. 10.

[39] De Geschillenkamer onderlijnt.

[40] RvS, advies nr. 51.291/2 van 21 mei 2012, https://www.dekamer.be/FLWB/pdf/53/2343/53K2343001.pdf, 23, nr. 3.2.

74. Artikel 33 van het voorontwerp bevat een opsomming van de gegevens die worden geregistreerd in het kader van de registratie ("*logging*") van de toegangen tot de gegevensbanken van de Dienst Vreemdelingenzaken. Deze bepaling luidt als volgt:

> *"**Art. 33.** De in artikel 32 bedoelde registratie van de verwerking bevat de volgende informatie:*
> *1° het uniek identificatiekenmerk van de uitvoerder van de bewerking;*
> *2° de datum en het uur van de bewerking;*
> *3° de aard van de bewerking;*
> *4° het unieke nummer van de verwerking;*
> *5° het uniek identificatiekenmerk van de betrokkene[41];*
> *6° ingeval van mededeling van persoonsgegevens, de identiteit van de ontvanger aan wie de gegevens zijn bekendgemaakt;*
> *7° in voorkomend geval, de reden van de uitgevoerde bewerking[42]".*

De Autoriteit stelt vast dat artikel 33, 5° van het voorontwerp in het kader van deze registratie voorziet dat in het logboek het "*uniek identificatiekenmerk van de betrokkene*" wordt geregistreerd, hetgeen een persoonsgegeven uitmaakt in de zin van de AVG. Dit dient te worden onderscheiden van het uniek identificatienummer van het personeelslid dat de uitvoerder is van de betrokken bewerking (geviseerd in art. 33, 1°). De Autoriteit wijst erop dat de logging van de toegang tot de gegevensbank evenwel niet mag toelaten om bepaalde verzamelde persoonsgegevens van betrokkenen langer op te slaan dan wat strikt noodzakelijk is voor de nagestreefde doeleinden. In dit verband dient erop te worden gewezen dat overeenkomstig artikel 13, §1 van het voorontwerp de bewaartermijn van de persoonsgegevens van de betrokkenen in beginsel maximum vijf jaar bedraagt, daar waar de bewaartermijn van de gegevens opgenomen in het logboek door artikel 35 van het voorontwerp wordt vastgesteld op tien jaar, te rekenen vanaf de registratie van de informatie. Er dient op te worden gewezen dat het uniek identificatienummer van de betrokkene kan toelaten bepaalde informatie met betrekking tot de betrokkene te achterhalen (bijvoorbeeld waar deze zich bevond of wat deze deed op het ogenblik dat zijn of haar gegevens werden gelogd) en dit in bepaalde gevallen (lange tijd) na het verstrijken van de bewaartermijn van vijf jaar voorzien in artikel 13 van het voorontwerp. De Autoriteit begrijpt dat het, in het licht van het doel van het logboek (*i.e.* de controle betreffende eventuele fraude of foutief gebruik van de gegevensbanken van de Dienst Vreemdelingenzaken), noodzakelijk is het uniek identificatienummer van de betrokkene te bewaren teneinde de in het logboek vermelde bewerkingen in verband te kunnen brengen met het betrokken dossier. Het is evenwel aangewezen de in artikelen 13 en 33 voorziene

[41] De Autoriteit onderlijnt.

[42] De Autoriteit onderlijnt.

bewaartermijnen op elkaar af te stemmen en alle noodzakelijke informatie oftewel vijf jaar oftewel tien jaar te bewaren. Indien wordt geopteerd voor een bewaartermijn van tien jaar, dient deze (lange) bewaartermijn evenwel te kunnen worden verantwoord op basis van één of meer objectieve criteria (bijv. afstemming op de (verjarings)termijn voor het instellen van een vordering). In de Memorie van toelichting citeert de aanvrager relevante rechtspraak van het Hof van Justitie in dit verband, doch preciseert deze vervolgens niet *in concreto* waarom in dit geval voor een bewaartermijn van tien jaar wordt gekozen. Dit dient desgevallend te worden verduidelijkt.

75. Verder merkt de Autoriteit op dat artikel 33, 7° van het voorontwerp vermeldt dat "*in voorkomend geval*" de reden van de uitgevoerde bewerking wordt vermeld. De Autoriteit wijst erop dat deze reden evenwel steeds dient te worden opgenomen.

OM DEZE REDENEN
de Autoriteit,

is van oordeel dat volgende aanpassingen zich opdringen in het voorontwerp van wet:

- nauwkeuriger omschrijven van de doeleinden van de verwerking van persoonsgegevens (overwegingen 13-30);

- preciseren dat de *Dienst Vreemdelingenzaken* als verwerkingsverantwoordelijke dient te worden beschouwd in de zin van artikel 4.7) AVG voor de verwerkingen van persoonsgegevens waarop het voorontwerp van wet betrekking heeft (en niet de Minister) (overwegingen 33-37);

- nauwkeuriger preciseren van de (categorieën van) verwerkte persoonsgegevens en betrokkenen, in het licht van het proportionaliteitsbeginsel en het beginsel van minimale gegevensverwerking (overwegingen 38-46);

- nader preciseren van de (categorieën van) ontvangers alsook de (categorieën van) persoonsgegevens waartoe elk van deze ontvangers toegang heeft en voor welke doeleinden (overwegingen 47-54);

- schrapping van de zinsnede in artikel 8, 1°, artikel 10, §2, artikel 11, §2 en artikel 18 van het voorontwerp volgens dewelke de wezenlijke elementen van de verwerking bij koninklijk besluit kunnen worden *aangevuld* (overwegingen 32, 43, 54 en 61); en

- precisering in de artikelen 19 tot en met 22 van het voorontwerp van de elementen opgesomd in 23.2 AVG teneinde de voorziene beperkingen op de rechten van de betrokkenen in overeenstemming te brengen met voormelde bepaling (overwegingen 62-72).

Voor het Kenniscentrum,
Cédrine Morlière, Directeur

Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 166/2022 du 19 juillet 2022

Objet : Avant-projet de loi *relatif aux traitements de données à caractère personnel par la Direction générale Office des étrangers du Service public fédéral Intérieur* (CO-A-2022-149)

Le Centre de Connaissances de l'Autorité de protection des données (ci-après "l'Autorité"), en présence de Madame Cédrine Morlière et de Messieurs Yves-Alexandre de Montjoye et Bart Preneel ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après "la LCA") ;

Vu le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE* (Règlement général sur la protection des données, ci-après le "RGPD") ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après "la LTD") ;

Vu la demande d'avis de Monsieur Sammy Mahdi, Secrétaire d'État à l'Asile et la Migration, chargé de la Loterie nationale, adjoint à la Ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique (ci-après "le demandeur"), reçue le 09/06/2022 ;

Émet, le 19 juillet 2022, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1. Le demandeur sollicite l'avis de l'Autorité concernant l'intégralité de l'avant-projet de loi *relatif aux traitements de données à caractère personnel par la Direction générale Office des étrangers du Service public fédéral Intérieur* (ci-après "l'avant-projet" ou "l'avant-projet de loi").

2. L'avant-projet de loi vise à créer un cadre juridique pour les traitements de données à caractère personnel réalisés par la Direction générale Office des étrangers du Service public fédéral Intérieur (ci-après "l'Office des étrangers") dans le cadre de l'accomplissement de ses missions légales en matière migratoire[1]. Ces missions légales sont régies principalement par la loi du 15 décembre 1980 *sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers* (ci-après également : "la Loi étrangers"), l'arrêté royal du 8 octobre 1981 *sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers* (ci-après également : "l'arrêté royal du 8 octobre 1981") et l'arrêté royal du 14 janvier 2002 *portant création du service public fédéral Intérieur*.

3. Une demande d'avis au sujet de l'avant-projet a également été adressée à l'Organe de contrôle de l'information policière (COC) ainsi qu'au Comité permanent de contrôle des services de police (Comité P) et au Comité permanent de contrôle des services de renseignement et de sécurité (Comité R).

II. EXAMEN DE LA DEMANDE

a. Base juridique

4. L'Autorité souligne que tout traitement de données à caractère personnel constitue une ingérence dans le droit à la protection de la vie privée, consacré à l'article 8 de la CEDH et à l'article 22 de la *Constitution*. Ce droit n'est toutefois pas absolu. Les articles 8 de la CEDH et 22 de la Constitution n'excluent pas toute ingérence d'une autorité publique dans le droit à la protection de la vie privée (comprenant également les données à caractère personnel), mais exigent que cette ingérence soit prévue par une disposition législative suffisamment précise, qu'elle réponde à un intérêt social général et qu'elle soit proportionnée à l'objectif légitime qu'elle poursuit[2]. En plus de devoir être nécessaire et proportionnée, toute norme régissant le traitement de données à caractère personnel (et constituant par nature une ingérence dans le droit à la protection des données à caractère personnel) doit

[1] Exposé des motifs, page 6.

[2] Jurisprudence constante de la Cour constitutionnelle. Voir par exemple Cour Constitutionnelle, Arrêt du 4 avril 2019, n° 49/2019 (*"Ils n'excluent pas toute ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée mais exigent que cette ingérence soit prévue par une disposition législative suffisamment précise, qu'elle réponde à un besoin social impérieux dans une société démocratique et qu'elle soit proportionnée à l'objectif légitime qu'elle poursuit.*").

répondre aux exigences de prévisibilité et de précision afin que les personnes concernées au sujet desquelles des données sont traitées aient une idée claire du traitement de leurs données.

5. Conformément à l'article 6.3 du RGPD, lu à la lumière du considérant 41 du RGPD, le traitement de données à caractère personnel qui est nécessaire au respect d'une obligation légale[3] et/ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement[4] doit être régi par une réglementation claire et précise dont l'application doit être prévisible pour les personnes concernées. En outre, selon l'article 22 de la *Constitution*, il est nécessaire que les "éléments essentiels" du traitement de données soient définis au moyen d'une norme légale formelle.

6. Certains traitements de données à caractère personnel auxquels donne lieu le présent projet soumis pour avis se fondent sur l'article 6.1.c) du RGPD étant donné que ceux-ci sont nécessaires au respect de la législation européenne en matière d'asile et de migration. D'autres traitements prévus dans le projet reposent sur l'article 6.1.e) du RGPD. Les traitements entraînent une ingérence importante dans les droits et libertés des personnes concernées dans la mesure où le Chapitre 3 de l'avant-projet ("*Catégories de données à caractère personnel traitées*") prévoit notamment un traitement de catégories particulières de données à caractère personnel (à savoir des données relatives à la santé, des données raciales ou ethniques, des données relatives au comportement sexuel, aux opinions politiques, à l'appartenance syndicale ou à un groupement assimilé et les convictions philosophiques ou religieuses ; cf. l'article 6 de l'avant-projet).

7. En vertu de l'article 6.3 du RGPD, lu conjointement avec l'article 22 de la *Constitution* et l'article 8 de la CEDH, une telle norme de rang législatif doit déterminer les circonstances dans lesquelles un tel traitement de données est autorisé. Conformément aux principes de légalité et de prévisibilité, cette norme législative doit ainsi, en tout cas, définir les éléments essentiels du (des) traitement(s)[5]. Lorsque le(s) traitement(s) de données représente(nt) une ingérence importante dans les droits et libertés des personnes concernées, comme dans le cas présent [6], les éléments essentiels suivants doivent être définis par le législateur :

- la (les) finalité(s) précise(s) et concrète(s) ;
- l'identité du (des) responsable(s) du traitement (à moins que cela ne soit clair) ;

[3] Article 6.1.c) du RGPD.

[4] Article 6.1.e) du RGPD.

[5] Voir DEGRAVE, E., "*L'e-gouvernement et la protection de la vie privée – Légalité, transparence et contrôle*", Collection du CRIDS, Larcier, Bruxelles, 2014, p. 161 e.s. (voir e.a. : CEDH, Arrêt *Rotaru c. Roumanie*, 4 mai 2000) ; Voir également quelques arrêts de la Cour constitutionnelle : l'Arrêt n° 44/2015 du 23 avril 2015 (p. 63), l'Arrêt n° 108/2017 du 5 octobre 2017 (p. 17) et l'Arrêt n° 29/2018 du 15 mars 2018 (p. 26).

[6] Étant donné que le traitement concerne dans certains cas des catégories particulières de données à caractère personnel (sensibles) au sens de l'article 9 ou de l'article 10 du RGPD.

- les (catégories de) données qui sont nécessaires à la réalisation de cette (ces) finalité(s) ;
- les (catégories de) personnes concernées dont les données seront traitées ;
- le délai de conservation maximal des données ;
- les (catégories de) destinataires auxquels les données seront communiquées et les circonstances dans lesquelles elles le seront, ainsi que les motifs y afférents ;
- le cas échéant et dans la mesure où cela est nécessaire, la limitation des obligations et/ou droits mentionné(e)s aux articles 5, 12 à 22 et 34 du RGPD.

8. Le Chapitre 1er de l'avant-projet mentionne les bases de licéité en fonction desquelles l'Office des étrangers peut traiter données à caractère personnel. L'article 4, § 1er de l'avant-projet dispose ce qui suit à cet égard :
"*L'Office des étrangers peut traiter des données à caractère personnel dans la mesure où ces traitements sont nécessaires :*
1° à l'exécution des missions d'intérêt public qui sont les siennes ou relevant de l'autorité publique dont il est investi telles que déterminées par l'arrêté royal du 14 janvier 2002 portant création du Service public fédéral Intérieur ;
2° au respect des obligations légales auxquelles il est soumis."

9. L'Autorité souligne avant tout que la formulation de l'article 4, § 1er, 2° est très générale et qu'il est recommandé de préciser de quelles obligations il s'agit en l'espèce, en renvoyant aux normes législatives correspondantes.

10. L'Autorité souligne par ailleurs que, vu qu'en l'espèce des catégories particulières de données à caractère personnel sont en outre traitées, (au moins) un des motifs d'exception au principe d'interdiction du traitement pour ce type de données à caractère personnel, énoncés à l'article 9.2 du RGPD, doit s'appliquer. Un traitement de catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD doit en effet se fonder sur l'article 9.2 du RGPD, lu conjointement avec l'article 6.1 du RGPD. Ceci a été établi par la Commission européenne et l'EDPB[7] et est également confirmé par le considérant 51 du RGPD, qui dispose ce qui suit au sujet du traitement de catégories particulières de données à caractère personnel : "*Outre les exigences spécifiques applicables à ce traitement, les principes généraux et les autres règles du présent règlement devraient s'appliquer, en particulier en ce qui concerne les conditions de licéité du traitement.*"

[7] Voir à ce sujet GEORGIEVA, L. et KUNER, C., "Article 9. Processing of special categories of personal data" in KUNER, C., BYGRAVE, L.A. et DOCKSEY, C., *The EU General Data Protection Regulation (GDPR). A commentary*, Oxford University Press, Oxford, p. 37 : "*The Commission has stated that the processing of sensitive data must always be supported by a legal basis under Article 6 GDPR, in addition to compliance with one of the situations covered in Article 9(2). The EDPB has also stated that 'If a video surveillance system is used in order to process special categories of data, the data controller must identify both an exception for processing special categories of data under Article 9 (i.e. and exemption from the general rule that one should not process special categories of data) and a legal basis under Article 6'.*

11. À cet égard, l'Autorité constate que l'article 4, § 2 de l'avant-projet dispose ce qui suit :
"§ 2. L'Office des étrangers peut traiter des données à caractère personnel visées à l'article 9, du règlement général sur la protection des données dans la mesure où ces traitements sont nécessaires :
1° à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ;
2° pour des motifs d'intérêt public important sur base de la législation liant la Belgique ;
3° aux fins de diagnostics médicaux et de la prise en charge sanitaire ;
4° pour des motifs d'intérêt public dans le domaine de la santé publique."

12. Les fondements juridiques précités sont une paraphrase (de quelques-uns) des fondements mentionnés à l'article 9.2 du RGPD. À cet égard, l'Autorité souligne toutefois que la simple reprise ou paraphrase de dispositions du RGPD n'offre aucune plus-value juridique. Le(s) motif(s) d'exception de l'article 9.2 du RGPD qui est/sont utilisé(s) pour le traitement doit/doivent être appliqués et précisés concrètement. Plus spécifiquement, il convient de déterminer le ou les motifs d'exception de l'article 9.2 du RGPD sur lesquels repose chaque catégorie de données à caractère personnel sensibles.

b. <u>Finalité(s) du traitement de données qui sera instauré</u>

13. En vertu de l'article 5.1.b) du RGPD, le traitement de données à caractère personnel n'est autorisé que pour des finalités déterminées, explicites et légitimes.

14. L'article 10, § 1er de l'avant-projet énonce les finalités pour lesquelles l'Office des étrangers peut collecter et traiter des données à caractère personnel :

*"**Art. 10.** L'Office des étrangers peut traiter les catégories de données à caractère personnel visées à l'article 6 pour les finalités suivantes :*
1° identifier les personnes visées à l'article 9 ;
2° traiter les demandes de visa requis pour transiter par la Belgique ou un autre État membre ou pour y séjourner et décider de leur délivrance, de leur prolongation, de leur abrogation ou de leur annulation ;
3° traiter les demandes d'autorisation de voyage requise pour transiter par la Belgique ou un autre État membre ou pour y séjourner et décider de leur délivrance, de leur prolongation, de leur abrogation ou de leur annulation ;
4° contrôler les étrangers aux frontières extérieures de la Belgique ou d'un autre État membre, en particulier la vérification des conditions d'entrée et de séjour et prendre les décisions relatives à leur entrée ou leur refoulement ;
5° contrôler les étrangers se trouvant en Belgique, en particulier la vérification des conditions de séjour et prendre les décisions relatives à leur séjour ou à leur éloignement, en ce compris leur interdiction d'entrée ;
6° traiter les demandes de séjour introduites en Belgique et décider de l'octroi, de la prolongation, du renouvellement ou de la fin du séjour ;
7° mener à bien les procédures de réinstallation des étrangers en Belgique ;

8° assurer la mise en œuvre de la procédure de protection internationale, en particulier :
a) l'enregistrement des demandes de protection internationale ;
b) la détermination de l'État membre responsable du traitement de la demande de protection internationale, en ce compris l'adoption des mesures de maintien, le traitement et le suivi des demandes de prise en charge ou de reprise en charge et l'adoption des mesures de transfert ;
c) la transmission au Commissariat général aux réfugiés et aux apatrides des demandes de protection internationale dont le traitement incombe à la Belgique en vue de leur examen et de décider de la reconnaissance de la qualité de réfugié ou de bénéficiaire de la protection subsidiaire ;
d) le suivi de la situation de séjour des demandeurs de protection internationale en cours de procédure ou déboutés, en ce compris l'adoption de mesures d'éloignement ou de maintien ;
e) le suivi du séjour des bénéficiaires de la qualité de réfugié ou de la protection subsidiaire, en ce compris les demandes de retrait ou d'abrogation adressées au Commissariat général aux réfugiés et aux apatrides ;
9° assurer la délivrance, le renouvellement, la prolongation et le retrait des titres et des documents de séjour ainsi que de tout document dont la délivrance est prévue par ou vertu de la loi du 15 décembre 1980 ;
10° assurer la mise en œuvre et le suivi des procédures de refoulement, d'éloignement et de transfert des étrangers, notamment, l'obtention des documents de voyage requis, l'adoption des mesures coercitives requises, en ce compris les mesures de maintien ou de reconduite à la frontière, le report éventuel du départ, l'exécution des accords de réadmission liant la Belgique, la reconnaissance des mesures d'éloignement prises par les autres États membres ainsi que la préparation, l'organisation, l'exécution et le suivi des départs volontaires ou non en coopération avec les autorités, les instances, les organismes et organisations compétentes ;
11° assurer le suivi des interdictions d'entrée, en ce compris leur levée ou leur suspension ainsi que la gestion de leur enregistrement dans le Système d'Information Schengen et dans la Banque de données nationale générale ou dans toute autre banque de données nationale ;
12° infliger les amendes administratives prévues par la loi du 15 décembre 1980 et en assurer la récupération ;
13° assurer la gestion et le suivi du contentieux liés à l'application de la législation relative à l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers ;
14° lutter contre la fraude à l'identité, l'utilisation abusive des documents de voyage et toutes autres formes d'abus ou de détournement de procédure en matière de migration et de protection internationale tels que les mariages de complaisance, les cohabitations légales de complaisance ou les reconnaissances frauduleuses ;
15° récupérer les frais de soins de santé, de séjour et d'éloignement ;
16° rechercher et constater les infractions à loi du 15 décembre 1980 et aux autres législations pour lesquelles les membres du personnel de l'Office des étrangers sont compétents ;
17° établir des rapports et des statistiques en matière de migration et de protection internationale, en particulier pour élaborer ou justifier la politique en cette matière, pour identifier les phénomènes migratoires ou pour satisfaire à des obligations légales ;
18° remplir les obligations européennes et internationales liées aux politiques en matière de visas, de franchissement des frontières, de libre circulation des personnes, de protection internationale et d'immigration, en ce compris les politiques en matière de réinstallation, de retour et de réintégration."

15. L'Autorité constate que la formulation de certaines finalités énoncées à l'article 10 de l'avant-projet est générale et laisse une marge pour une interprétation subjective. Les finalités doivent être suffisamment précises pour qu'un justiciable connaisse clairement les raisons exactes qui ont

conduit au traitement de ses données à caractère personnel[8]. À la lecture de ces finalités, il doit pouvoir déduire quels traitements de données sont nécessaires pour les atteindre. À titre d'exemple, l'Autorité renvoie à la structure de l'article 11 de l'avant-projet portant sur les destinataires de données à caractère personnel, où, en ce qui concerne certain(e)s (catégories de) destinataires énoncé(e)s à l'article 11, § 1er de l'avant-projet, on précise les finalités exactes pour lesquelles des données à caractère personnel peuvent être transmises au destinataire en question (cf. "*aux fins* (…)"). À cet égard, on renvoie notamment à l'article 11, § 1, 2° (les postes diplomatiques ou consulaires belges), 8° (les communes) et 12° (les instances de la sécurité sociale) (cf. également le point 47 ci-après).

16. Une description précise des finalités du ou des traitements est également importante afin de permettre au responsable du traitement de déterminer quelles (catégories de) données à caractère personnel doivent précisément être collectées et traitées (cf. ci-après). Les données traitées doivent en effet être pertinentes par rapport aux finalités. Des finalités formulées de manière trop large ou trop vague engendrent le risque d'un traitement d'un trop grand éventail de données à caractère personnel[9]. En outre, c'est également en fonction de la finalité que la pertinence des différent(e)s (catégories de) destinataires peut être évaluée.

17. Conformément au principe précité de légalité et de prévisibilité, tout traitement de données à caractère personnel doit être régi par une réglementation claire et précise, dont l'application doit être prévisible pour les personnes concernées. L'Autorité constate toutefois qu'en raison de leur formulation large, certaines finalités de traitement énoncées à l'article 10 de l'avant-projet d'une part ne permettent pas de comprendre ce qui sera fait précisément des données collectées, par qui et pourquoi, et d'autre part ne permettent pas de déterminer quelles (catégories de) données à caractère personnel devront nécessairement être traitées afin de pouvoir réaliser la ou les finalités visées. Ces finalités ne peuvent dès lors pas être considérées comme "*déterminées, explicites et légitimes*" au sens de l'article 5.1.b) du RGPD.

18. L'Autorité renvoie à cet égard notamment aux finalités reprises à l'article 10, § 1er, 7° ("*mener à bien les procédures de réinstallation des étrangers en Belgique*"), et 18° ("*remplir les obligations européennes et internationales liées aux politiques en matière de visas* (…)").

---

[8] Voir dans le même sens l'avis n° 34/2018 du 11 avril 2018 de la Commission de la protection de la vie privée, prédécesseur en droit de l'Autorité, qui affirmait que la finalité "*de datamatching et de datamining en vue d'une lutte efficace contre la fraude sociale*" était formulée de manière trop large pour fournir au justiciable suffisamment de précision quant aux circonstances exactes du regroupement de ses données à caractère personnel dans un datawarehouse. Cet avis peut être consulté via le lien suivant : https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/avis_34_2018.pdf.

Voir également l'avis n° 99/2019 de l'Autorité du 3 avril 2019, dans lequel l'Autorité estimait que la finalité "*la réalisation de recherches pouvant être utiles à la connaissance, à la conception et à la gestion de la protection sociale*" était aussi définie de manière trop vague. Cet avis peut être consulté via le lien suivant : https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/avis_99_2019.pdf.

[9] Poullet, Y., Rosier, K. et de Terwangne, C., *Le Règlement Général Sur La Protection Des Données (RGPD/GDPR) : Analyse Approfondie,* Bruxelles, Larcier, 2018, p. 95.

19. L'Autorité souligne par ailleurs que certaines finalités reprises à l'article 10, § 1er de l'avant-projet devraient être précisées davantage en ajoutant un renvoi vers la disposition légale précise qui encadre la mission en question de l'Office des étrangers (par exemple les dispositions pertinentes de la Loi étrangers et de l'arrêté royal du 8 octobre 1981) ou vers d'autres dispositions légales applicables.

20. L'Autorité fait également remarquer que l'article 10, § 1er, 17° mentionne comme finalité : "*établir des rapports et des statistiques en matière de migration et de protection internationale, en particulier pour élaborer ou justifier la politique en cette matière, pour identifier les phénomènes migratoires ou pour satisfaire à des obligations légales*"[10].

21. L'Autorité constate que cette disposition est reprise dans la liste des finalités pour lesquelles l'Office des étrangers collecte et traite des données à caractère personnel. Il convient toutefois de remarquer qu'en l'espèce, des données à caractère personnel ne peuvent pas être collectées dans le but d'établir des statistiques. Le traitement de données à caractère personnel à des fins statistiques constitue ici un traitement ultérieur au sens des articles 5.1.b) et 6.4 du RGPD.

22. L'article 89.1 du RGPD requiert que tout traitement de données à caractère personnel à des fins statistiques soit encadré de garanties appropriées assurant que des mesures techniques et organisationnelles soient mises en place pour assurer le respect du principe de minimisation des données et que, lorsque les finalités statistiques peuvent être atteintes par un traitement ultérieur ne permettant pas ou plus l'identification des personnes concernées, il convient de procéder de cette manière.

23. Le traitement ultérieur à des fins statistiques se fait donc de préférence à l'aide de données anonymes[11]. S'il n'est pas possible d'atteindre la finalité de traitement visée à l'aide de données anonymes, des données à caractère personnel pseudonymisées[12] peuvent être utilisées. Si ces données ne permettent pas non plus d'atteindre la finalité visée, des données à caractère personnel non pseudonymisées peuvent aussi être utilisées, uniquement en dernière instance.

---

[10] Soulignement par l'Autorité.

[11] Données anonymes : informations qui ne peuvent pas être reliées à une personne physique identifiée ou identifiable (art. 4.1) du RGPD, *a contrario*).

[12] "*Pseudonymisation : le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.*" (voir l'article 4.5) du RGPD).

24. L'Autorité rappelle à cet égard que l'identification d'une personne ne concerne pas uniquement la possibilité de retrouver son nom et/ou son adresse mais également la possibilité de l'identifier par un processus d'individualisation, de corrélation ou d'inférence.

25. Pour le surplus, l'Autorité renvoie à l'avis 05/2014 du Groupe de travail "Article 29" sur la protection des données (prédécesseur du Comité européen de la protection des données) sur les techniques d'anonymisation[13].

26. L'Autorité souligne que l'Exposé des motifs du projet doit contenir des informations concernant la stratégie d'anonymisation envisagée. En effet, la transparence quant à la stratégie d'anonymisation retenue ainsi qu'une analyse des risques liés à la réidentification constituent des éléments qui contribuent à une approche réfléchie du processus d'anonymisation.

27. L'Autorité attire l'attention du demandeur sur le fait qu'il existe une différence entre des données pseudonymisées définies par l'article 4(5) du RGPD comme des données *"qui ne peuvent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires"* et des données anonymisées qui ne peuvent plus, par aucun moyen raisonnable, être attribuées à une personne précise et que seules ces dernières ne constituent plus des données à caractère personnel et sont donc exclues du champ d'application du RGPD, conformément à son considérant 26[14].

28. Dès lors, eu égard à la définition de donnée à caractère personnel telle que figurant à l'article 4.1) du RGPD[15], il convient de s'assurer que le standard élevé requis pour l'anonymisation est bien atteint[16] et que les données ne sont pas simplement pseudonymisées. Le traitement de telles données, même pseudonymisées, doit effectivement être considéré comme un traitement de données à caractère personnel au sens du RGPD.

29. Il résulte de ce qui précède que lorsqu'il sera question de pseudonymisation (et non d'anonymisation) :

---

[13] Cet avis est disponible à l'adresse suivante : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf.

[14] Pour plus d'informations, voir l'avis 5/2014 (WP216) relatif aux techniques d'anonymisation, 2.2.3, p. 10 du Groupe 29, https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2014/wp216_fr.pdf.

[15] À savoir : "*toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale*".

[16] L'identification d'une personne ne vise pas uniquement la possibilité de retrouver son nom et/ou son adresse mais également la possibilité de l'identifier par un processus d'individualisation, de corrélation ou d'inférence.

- il convient de se référer aux rapports de l'Agence de l'Union européenne pour la cybersécurité relatifs aux techniques et meilleures pratiques de pseudonymisation[17] ;
- ce traitement doit être encadré par toutes les garanties requises et répondre aux principes prévalant en la matière[18].

30. L'Autorité indique enfin, en ce qui concerne l'article 10, § 1er, 17° de l'avant-projet, que les termes "*établir des rapports et des statistiques (…) pour satisfaire à des obligations légales*" sont formulés de manière très vague et constate que l'Exposé des motifs ne précise pas non plus les obligations légales dont il s'agit précisément. L'Autorité estime qu'en vue de la transparence et de la prévisibilité, il est recommandé de préciser la ou les normes légales qui imposent cette obligation à l'Office des étrangers.

31. Dans son § 2, l'article 10 de l'avant-projet dispose ce qui suit au sujet des finalités énoncées au § 1er : "*Le Roi peut, par arrêté royal délibéré en Conseil des Ministres et après avis de l'Autorité de protection des données, préciser ou compléter les finalités mentionnées au paragraphe 1er*" [19].

32. L'Autorité souligne toutefois que cette disposition est contraire au principe de légalité repris à l'article 6.3 du RGPD, lu conjointement avec le considérant 41 du RGPD, *j°* l'article 22 de la Constitution, en vertu duquel les éléments essentiels du traitement de données – dont les finalités de ces traitements – doivent être définis au moyen d'une norme légale formelle (à savoir une loi, un décret ou une ordonnance). Les finalités du traitement ne peuvent dès lors pas être complétées ou étendues au moyen d'une norme réglementaire (comme en l'occurrence un arrêté royal). Tout au plus, celles-ci peuvent être *précisées*. À l'article 10, § 2 de l'avant-projet, il convient par conséquent de supprimer les termes "ou compléter".

c. Responsable(s) du traitement

33. L'article 4.7) du RGPD dispose que pour les traitements dont les finalités et les moyens sont déterminés par la réglementation, le responsable du traitement est celui qui est désigné en tant que tel dans cette réglementation.

34. L'article 5 de l'avant-projet dispose ce qui suit à cet égard : "§ 1er. *Le Ministre est le responsable du traitement des traitements de données à caractère personnel effectués par l'Office des*

[17] ENISA : https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases et https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices_fr;

[18] Il en va ainsi du principe de proportionnalité renvoyant à celui, plus spécifique, de "*minimisation des données*" impliquant que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées, conformément à l'article 5, § 1, c) du RGPD.

[19] Soulignement par l'Autorité.

étrangers. § 2. Le Ministre peut se faire représenter par le Directeur général de l'Office des étrangers pour l'accomplissement des obligations qui lui incombent en sa qualité de responsable du traitement."

35. Certes, lorsque les finalités et les moyens de traitement sont déterminés par le droit national, "*le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit [national]*"[20]". Si les États membres peuvent préciser l'application des règles du RGPD dans des domaines particuliers où ils légifèrent afin de garantir en ces domaines la cohérence et la clarté du cadre normatif applicable au traitement de données, ils ne peuvent, à ce titre, déroger au RGPD ou se départir des définitions qu'il consacre[21]. En d'autres termes, la désignation d'un responsable du traitement dans la réglementation doit concorder avec le rôle que cet acteur joue dans la pratique. En juger autrement serait non seulement contraire à la lettre du RGPD, mais pourrait également mettre en péril l'objectif qu'il poursuit d'assurer un niveau cohérent et élevé de protection des personnes physiques.

36. Le Comité européen de la protection des données dispose à cet égard dans ses Lignes directrices *concernant les notions de responsable du traitement et de sous-traitant dans le RGPD* que les entreprises ou les organismes publics désignent parfois une personne physique spécifique comme responsable de l'exécution de l'activité de traitement, bien que celle-ci agisse en soi au nom de la personne morale (entreprise ou organisme public) qui est au final responsable en cas de violation des règles en sa qualité de responsable du traitement"[22].

37. À la lumière de ce qui précède, l'Autorité s'interroge quant à la désignation du ministre en tant que responsable du traitement. Indépendamment de la responsabilité *politique* qui repose sur le ministre compétent, sa désignation en l'espèce en tant que responsable du traitement pour des traitements de données à caractère personnel réalisés par l'Office des étrangers ne semble pas appropriée. Dans la pratique, il ne semble en effet pas que ce soit le ministre qui vise les finalités pour lesquelles le service qui relève de sa compétence traite des données à caractère personnel, mais bien l'administration elle-même. C'est donc l'administration de l'Office des étrangers qui doit assurer le rôle

[20] Article 4, 7), du RGPD. Concernant la détermination des obligations respectives des responsables conjoints du traitement, lire également l'article 26, 1. du RGPD.

[21] Lire l'article 6.3, alinéa 2 et les considérants 8 et 10 du RGPD.

[22] Comité européen de la protection des données, Lignes directrices 07/2020 *concernant les notions de responsable du traitement et de sous-traitant dans le RGPD*, 2 septembre 2020 (version 1.0), p. 11, n° 18: "*Parfois, des entreprises et des organismes publics chargent une personne particulière de la mise en œuvre du traitement. Même si une personne physique particulière est désignée pour veiller au respect des règles en matière de protection des données, cette personne ne sera pas le responsable du traitement mais agira pour le compte de l'entité juridique (entreprise ou organisme public) qui, en sa qualité de responsable du traitement, sera responsable en dernier ressort en cas de violation des règles. Dans le même ordre d'idées, même si un service particulier ou une unité particulière d'une organisation assume la responsabilité opérationnelle de veiller à la conformité de certaines activités de traitement, cela ne signifie pas pour autant que ce service ou cette unité (plutôt que l'organisation dans son ensemble) devient le responsable du traitement*".

de responsable du traitement au sens de l'article 4.7) du RGPD et qui doit donc être désignée dans l'avant-projet.[23]

d. <u>Catégories de données à caractère personnel et personnes concernées</u>

38. L'article 5.1.c) du RGPD prévoit que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités visées (minimisation des données).

39. L'article 6 de l'avant-projet énumère les (catégories de) données à caractère personnel qui peuvent être traitées par l'Office des étrangers :

Art. 6. *L'Office des étrangers peut traiter les catégories de données à caractère personnel suivantes :*
1° les données d'identification en ce compris les images faciales et les empreintes digitales ;
2° les particularités financières ;
3° les caractéristiques personnelles ;
4° les habitudes de vie ;
5° les données relatives à la personnalité, au caractère et/ou au comportement ;
6° la composition du ménage ;
7° les loisirs et les intérêts ;
8° les affiliations (autres que professionnelles, politiques ou syndicales) ;
9° les données relatives aux infractions et aux condamnations ;
10° les habitudes de consommation ;
11° les caractéristiques du logement ;
12° les données concernant la santé ;
13° les études et la formation ;
14° la profession et l'emploi ;
15° les données raciales ou ethniques ;
16° les données relatives au comportement sexuel ;
17° les opinions politiques ;
18° l'affiliation à un syndicat ou à un groupement assimilé, les fonctions occupées ;
19° les convictions philosophiques ou religieuses.

40. L'Autorité souligne qu'à la lumière du principe de minimisation des données ainsi que du principe de prévisibilité, on en peut se contenter de reprendre simplement une liste de toutes les (catégories de) données à caractère personnel qui peuvent être traitées par l'Office des étrangers.

[23] Cf. également à cet égard l'avis 122/2022 de l'Autorité du 1er juillet 2022 (points 8-16).

Afin de permettre aux personnes concernées de comprendre, à la lecture du texte, quels traitements de données sont nécessaires, les (catégories de) données à caractère personnel doivent être mises en relation avec les finalités de traitement (art. 10 de l'avant-projet) et les destinataires (art. 11 de l'avant-projet). Il convient avant tout de préciser davantage quels (types de) traitements pourront être réalisés par l'Office des étrangers sur quelles (catégories de) données à caractère personnel (collecte, enregistrement, consultation, anonymisation, effacement, etc.) et pour quelles finalités. En effet, toutes les catégories de données à caractère personnel énoncées à l'article 6 de l'avant-projet ne seront pas (devront pas être) traitées pour chacune des finalités énoncées à l'article 10 de l'avant-projet. Par exemple, on ne procèdera peut-être pas à la pseudonymisation des données concernant les hobbies et les intérêts (art. 6, 7°) en vue d'assurer le suivi des interdictions d'entrées et leur enregistrement dans le Système d'information Schengen (art. 10, 11°). Il convient donc de reprendre dans l'avant-projet un lien plus clair entre les (catégories de) données à caractère personnel traitées et les finalités de traitement. Par ailleurs, il convient également de préciser, en cas de transfert de certaines (catégories de) données à caractère personnel, à quels destinataires celles-ci seront éventuellement transmises et pour quelles finalités (cf. également ci-après aux points 13 e.s.).

41. Conformément au principe de proportionnalité et au principe de minimisation des données, seules les données à caractère personnel nécessaires à la réalisation des finalités peuvent être collectées et traitées (et par conséquent transmises à certain(e)s (catégories de) destinataires). À cet égard, l'Autorité souligne que sur la base du texte du présent avant-projet, certaines (catégories de) données à caractère personnel peuvent être transmises à certain(e)s (catégories de) destinataires, bien que la nécessité de cette transmission ne soit nullement démontrée. À titre d'exemple, l'Autorité souligne que sur la base de la lecture conjointe des articles 6, 17° et 11, § 1, 7° de l'avant-projet, les données relatives au comportement sexuel des personnes concernées peuvent être transmises à des transporteurs. Il convient dès lors de préciser pour quelles (catégories de) données à caractère personnel reprises à l'article 6 de l'avant-projet la transmission est nécessaire, pour quels destinataires énoncés à l'article 11 et pour quelle(s) finalité(s).

42. L'article 8, 1° de l'avant-projet dispose ce qui suit : "*Le Roi peut, par arrêté royal délibéré en Conseil des Ministres et après avis de l'Autorité de protection des données :* (…) *préciser ou compléter les catégories de données à caractère personnel mentionnées à l'article 6*" [24].

43. L'Autorité souligne toutefois que cette disposition est contraire au principe de légalité repris à l'article 6.3 du RGPD, lu conjointement avec le considérant 41 du RGPD, *j°* l'article 22 de la Constitution, en vertu duquel les éléments essentiels du traitement de données doivent être définis au moyen d'une norme légale formelle (à savoir une loi, un décret ou une ordonnance). Lorsque le

[24] Soulignement par l'Autorité.

traitement de données constitue une ingérence importante dans les droits et libertés des personnes concernées, comme en l'occurrence, les (catégories de) données à caractère personnel doivent également être définies dans une norme légale formelle. Celles-ci ne peuvent dès lors pas être complétées ou étendues par le biais d'une norme réglementaire (comme en l'occurrence un arrêté royal). Tout au plus celles-ci peuvent être *précisées*. À l'article 8, 1° de l'avant-projet, il convient par conséquent de supprimer les termes "*ou compléter*".

44. L'article 9 de l'avant-projet énumère les catégories de personnes concernées dont l'Office des étrangers peut traiter des données à caractère personnel :

> ***"Art. 9.*** *L'Office des étrangers peut traiter les catégories de données à caractère personnel visées à l'article 6 des personnes suivantes :*
> *1° les étrangers ayant introduit une demande de visa ou d'autorisation de voyage pour se rendre en Belgique ou dans un autre État membre ;*
> *2° les étrangers se présentant aux frontières extérieures de la Belgique ou d'un autre État membre ;*
> *3° les étrangers se trouvant sur le territoire belge ou sur celui d'un autre État membre ;*
> *4° les étrangers se trouvant en dehors du territoire belge et interdit d'entrée en application de la loi du 15 décembre 1980 ;*
> *5° les étrangers faisant l'objet d'une procédure de réinstallation en Belgique ;*
> *6° les Belges et les étrangers ayant un lien familial, professionnel, économique, culturel ou autre avec un étranger visé aux 1° à 5°, devant être pris en compte dans le cadre du traitement de sa demande ou de l'appréciation de sa situation."*

45. L'Autorité souligne qu'il est recommandé, en vue de la transparence, de préciser les catégories précitées de personnes concernées – en particulier celles mentionnées à l'article 9, 1° à 5° inclus – au moyen d'un renvoi vers les dispositions correspondantes de la Loi étrangers.

46. Par ailleurs, il convient de noter que la formulation de la catégorie de personnes concernées visée à l'article 9, 6° de l'avant-projet est très large ("*les Belges et les étrangers ayant un lien familial, professionnel, économique, culturel ou autre avec un étranger* (…)[25]", ce qui ne permet pas véritablement de prévoir de quelles personnes il s'agit en l'espèce. L'Exposé des motifs[26] contient des précisions supplémentaires en la matière et donne plusieurs exemples de personnes qui sont visées concrètement. On se réfère notamment aux médecins ayant signé un certificat médical type dans le cadre d'une demande de séjour pour raisons médicales, les membres de la famille ouvrant le droit au regroupement familial, les fonctionnaires de police ayant rédigé un rapport administratif, les

[25] Soulignement par l'Autorité.

[26] Exposé des motifs, p. 37, 6e alinéa.

employeurs introduisant les demandes de permis unique auprès des autorités régionales, etc. Il est recommandé de lister ces personnes concernées dans le texte de l'avant-projet proprement dit. L'Autorité s'interroge toutefois quant à la nécessité et à la proportionnalité du traitement des données à caractère personnel des "*Belges et* [des] *étrangers ayant un lien* (…) *culturel* (…) *avec un étranger*"[27]. Il ne ressort pas de l'Exposé des motifs ce que cette catégorie de personnes concernées implique concrètement ni pour quelles finalités les données à caractère personnel de ces personnes concernées seront traitées. Par ailleurs, l'Autorité n'estime pas non plus nécessaire et proportionnel de collecter toutes les (catégories de) données à caractère personnel énumérées à l'article 6 de l'avant-projet pour toutes les personnes concernées visées à l'article 9, 6° de l'avant-projet. Ainsi, pour les personnes concernées énumérées ci-dessus qui sont mentionnées en exemple dans l'Exposé des motifs (médecins, fonctionnaires de police et employeurs), il semble uniquement nécessaire de collecter et de traiter les données d'identification (art. 6, 1°, à l'exception des données biométriques énoncées dans cette disposition). Le traitement des autres (catégories de) données à caractère personnel semble – dans certains cas – tout au plus nécessaire en ce qui concerne les personnes qui ont un lien familial avec l'étranger et/ou qui sont dépendants de cet étranger.

e. Destinataires ou catégories de destinataires

47. L'article 11, § 1er de l'avant-projet énumère les (catégories de) destinataires auxquels les données à caractère personnel collectées et traitées par l'Office des étrangers peuvent être communiquées. La disposition précitée comporte une liste très étendue de 37 (catégories de) destinataires différent(e)s. L'article 11, § 1er de l'avant-projet mentionne des destinataires tant nationaux qu'internationaux. Par ailleurs, le Chapitre 2 de l'avant-projet (articles 28 à 31 inclus) définit quels tiers peuvent être habilités à accéder aux informations enregistrées dans les banques de données gérées par l'Office des étrangers.

48. L'Autorité constate qu'en ce qui concerne certain(e)s (catégories de) destinataires énoncés à l'article 11, § 1er de l'avant-projet, on précise les finalités exactes pour lesquelles des données à caractère personnel peuvent être communiquées au destinataire en question (cf. "*aux fins* (…)"). À cet égard, on renvoie notamment à l'article 11, § 1, 2° (les postes diplomatiques ou consulaires belges), 8° (les communes) et 12° (les instances de la sécurité sociale).

49. Ce n'est toutefois *pas* le cas pour une d'autres (catégories de) destinataires parmi les 37 énoncé(e)s. On revoie par exemple à l'article 11, § 1er, 4° ("*les prestataires de services extérieurs avec lesquels la Belgique coopère aux fins de la procédure de délivrance des visas*"), 5° (les intermédiaires commerciaux), 23° (les organisations non gouvernementales) et 35° (le Centre de

[27] Soulignement par l'Autorité.

crise national). Il est à noter qu'en l'absence de précision des finalités pour lesquelles un échange des données à caractère personnel peut avoir lieu entre l'Office des étrangers et tout destinataire en question, les traitements visés ne sont pas prévisibles comme le requiert l'article 6.3 du RGPD, lu à la lumière du considérant 41 du RGPD. L'Autorité constate que dans l'Exposé des motifs, le demandeur reprend des précisions supplémentaires pour certain(e)s de ces (catégories de) destinataires. Il est recommandé de reprendre ces finalités (qui constituent un élément essentiel du traitement) dans le texte de l'avant-projet proprement dit.

50. Étant donné le manque de précision de la ou des finalités de la communication à certains destinataires énoncés à l'article 11, § 1er, on ne peut pas non plus déterminer quelles (catégories de) données à caractère personnel doivent être communiquées aux destinataires en question, ce qui est pourtant requis en vue de la prévisibilité pour les justiciables et les personnes concernées au sens du RGPD. À cet égard, l'Autorité renvoie aux points 40 et 41 (*supra*).

51. En ce qui concerne les destinataires internationaux repris à l'article 11, § 1er de l'avant-projet, l'Autorité souligne que conformément aux articles 44 e.s. du RGPD, pour les transferts de données à caractère personnel vers des pays tiers ou des organisations internationales, un niveau de protection adéquat doit être garanti :

- soit par une décision d'adéquation de la Commission européenne concernant le pays tiers vers lequel les données à caractère personnel sont transférées (article 45 du RGPD) ;
- soit en prévoyant des garanties appropriées telles que prescrites par l'article 46 du RGPD (par exemple la conclusion d'un instrument juridiquement contraignant avec l'organisation internationale ou le pays tiers en question).

52. L'avant-projet doit mentionner, pour chaque transfert de données à caractère personnel envisagé vers un pays tiers ou vers une organisation internationale, la base sur laquelle ce transfert a lieu et doit également préciser quelles garanties sont prévues (comme l'interdiction de transfert ultérieur et l'éventuelle interdiction de transfert vers d'autres pays).

53. L'article 11, § 2 de l'avant-projet dispose ce qui suit : "*Le Roi peut, par arrêté royal délibéré en Conseil des Ministres et après avis de l'Autorité de protection des données, préciser ou compléter la liste des entités mentionnées au paragraphe 1er*"[28].

54. L'Autorité souligne toutefois que cette disposition est contraire au principe de légalité repris à l'article 6.3 du RGPD, lu conjointement avec le considérant 41 du RGPD, *j°* l'article 22 de la

[28] Soulignement par l'Autorité.

Constitution, en vertu duquel les éléments essentiels du traitement de données – dont les (catégories de) destinataires de ces traitements – doivent être définis au moyen d'une norme légale formelle (à savoir une loi, un décret ou une ordonnance). Les destinataires du traitement ne peuvent dès lors pas être complétés ou étendus par le biais d'une norme réglementaire (comme en l'occurrence un arrêté royal). Tout au plus ceux-ci peuvent être *précisés*. À l'article 11, § 2 de l'avant-projet, il convient par conséquent de supprimer les termes "ou compléter".

f. <u>Délai de conservation des données</u>

55. En vertu de l'article 5.1.e) du RGPD, les données à caractère personnel ne peuvent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées.

56. Les articles 12 à 18 inclus de l'avant-projet concernent le délai de conservation des données à caractère personnel collectées et traitées par l'Office des étrangers.

57. Plus précisément, l'article 13, § 1er de l'avant-projet prévoit un délai de conservation de cinq ans pour les données à caractère personnel collectées et traitées par l'Office des étrangers qui concernent les personnes concernées énoncées à l'article 9, 1° à 5° de l'avant-projet. L'article 14 de l'avant-projet définit le point de commencement du délai de conservation pour chacune des catégories de personnes concernées. L'article 15 de l'avant-projet dispose que les données à caractère personnel des Belges et des étrangers ayant un lien familial, professionnel, économique, culturel ou autre avec un étranger, visés à l'article 9, 6°, sont disponibles et consultables pendant la même durée que celle applicable aux données à caractère personnel de cet étranger.

58. Dans l'Exposé des motifs, le demandeur explique que l'on a opté pour un délai de conservation de cinq ans en vue de s'aligner sur le prescrit du Règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 *concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS)*, qui dispose ce qui suit à cet égard : "*Les données à caractère personnel enregistrées dans le VIS ne devraient pas être conservées plus longtemps que ce qui est nécessaire pour les besoins du VIS. Il est approprié de conserver les données pendant une période maximale de cinq ans, afin que les données relatives à des demandes précédentes puissent être prises en considération pour évaluer des demandes de visas, y compris la bonne foi des demandeurs, et pour établir des dossiers sur les personnes en situation irrégulière qui peuvent avoir déposé une demande de visa à un moment donné. Une période plus courte ne serait pas suffisante à ces fins.*[29]" L'Autorité en prend acte.

[29] Considérant 14 du Règlement.

59. Avant tout, l'Autorité souligne toutefois qu'à la lumière de la motivation reprise ci-dessus, le délai de conservation de cinq ans prévu à l'article 13, § 1er de l'avant-projet ne semble pas nécessaire pour toutes les (catégories de) personnes concernées et données à caractère personnel visées. À cet égard, on peut citer par exemple le fait que l'on n'a pas démontré la nécessité de la conservation pendant cinq ans de l'adresse de résidence de ressortissants de pays tiers qui viennent en Belgique pour un séjour de maximum trois mois (cf. l'article 5 de la Loi étrangers). La conservation des données précitées ne semble plus nécessaire au moment où la personne concernée a quitté le territoire belge et ne réside plus à l'adresse indiquée[30].

60. L'article 18 de l'avant-projet dispose ce qui suit : "*Le Roi peut, par arrêté délibéré en Conseil des Ministres et après avis de l'Autorité de protection des données, préciser ou compléter les dispositions relatives aux durées de conservation des données à caractère personnel prévues dans le présent chapitre.*"[31]

61. L'Autorité fait toutefois remarquer que cette disposition est contraire au principe de légalité repris à l'article 6.3 du RGPD, lu conjointement avec le considérant 41 du RGPD, *j°* l'article 22 de la Constitution, en vertu duquel les éléments essentiels du traitement de données doivent être définis au moyen d'une norme légale formelle (à savoir une loi, un décret ou une ordonnance). Lorsque le traitement de données constitue une ingérence importante dans les droits et libertés des personnes concernées, comme en l'occurrence, les délais de conservation doivent également être définis au moyen d'une norme légale formelle (à savoir une loi, un décret ou une ordonnance). Ceux-ci ne peuvent dès lors pas être complétés ou étendus par le biais d'une norme réglementaire (comme en l'occurrence un arrêté royal). À l'article 18 de l'avant-projet, il convient par conséquent de supprimer les termes "ou compléter".

g. Limitations des droits des personnes concernées

62. Les articles 19 à 24 inclus de l'avant-projet de loi prévoient des limitations des droits des personnes concernées au sens de l'article 23 du RGPD.

63. Plus précisément, l'article 20 de l'avant-projet prévoit une limitation de l'application des droits repris aux articles 16 à 22 du RGPD (droit de rectification, droit à l'effacement, droit à la limitation du traitement, obligation de notification en ce qui concerne la rectification ou l'effacement de données, droit à la portabilité des données, droit d'opposition et prise de décision individuelle

[30] Cf. à cet égard aussi l'avis n° 122/2022 de l'Autorité du 1er juillet 2022 (points 37-40).

[31] Soulignement par l'Autorité.

automatisée) ainsi que du principe de transparence repris à l'article 5 du RGPD, et ce pour autant que l'exercice des droits et principes précités puisse porter atteinte à un des intérêts suivants :
"1° la préservation de l'ordre public et de la sécurité nationale ;
2° la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;
3° la prévention et la détection de manquements à la déontologie des professions réglementées, ainsi que les enquêtes et les poursuites en la matière ;
4° la protection des personnes concernées ou des droits et libertés d'autrui ;
5° le respect de l'obligation de secret professionnel".

64. Conformément à l'article 23 précité du RGPD, et comme expliqué au considérant 73 du RGPD, les droits des personnes concernées peuvent toutefois être limités aux conditions et dans les limites fixées dans cette disposition, qui est basée sur l'article 52 de la Charte des droits fondamentaux de l'Union et qui doit être lue à la lumière de la jurisprudence de la Cour de justice de l'Union européenne ainsi que de l'article 8 de la Convention européenne des droits de l'homme (CEDH).

65. L'article 23 du RGPD offre aux États membres la possibilité de limiter la portée des droits des personnes concernées, à condition qu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour réaliser une des finalités légitimes énumérées à l'article 23.1 du RGPD, telles que la sécurité nationale, la sécurité publique ou d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale, en particulier une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique.

66. Toute mesure législative prévoyant des limitations des droits de la personne concernée doit au moins contenir des dispositions spécifiques relatives aux éléments énumérés à l'article 23.2 du RGPD, comme :
- les finalités du traitement,
- les (catégories de) données à caractère personnel,
- l'étendue des limitations,
- les garanties destinées à prévenir les abus ou l'accès ou le transfert illicites,
- la détermination du (des) responsable(s) du traitement (ou des catégories de responsables du traitement),

- les durées de conservation,
- les risques pour les droits et libertés des personnes concernées et le droit de la personne concernée à la communication de la limitation.

67. Afin de déterminer la portée de la marge d'évaluation dont le législateur bénéficie dans ce cadre, il importe de rappeler la jurisprudence de la Cour de justice concernant l'article 13 de la Directive 95/46/CE qui prévoyait une possibilité similaire d'instaurer des exceptions aux droits des personnes concernées. Dans l'arrêt *Smaranda Bara*, la Cour a confirmé que ces exceptions ne pouvaient être instaurées que par "*des mesures législatives*"[32]. Ultérieurement, la Cour a précisé que les États membres ne pouvaient adopter ces exceptions que pour autant qu'elles soient "*nécessaires*"[33]. Vu les efforts constants du législateur européen de veiller à un niveau de protection élevé[34] des données à caractère personnel, les limitations des droits des personnes concernées doivent être absolument nécessaires[35] pour réaliser la finalité poursuivie. La nécessité et la proportionnalité de ces limitations doivent donc être interprétées de manière stricte[36].

68. Tout d'abord, l'Autorité souligne que l'article 19 de l'avant-projet contient d'une part une énumération des droits limités et d'autre part un renvoi vers les dispositions du RGPD qui garantissent les droits précités. À cet égard, l'Autorité constate toutefois que les deux segments de phrase de l'article 19 de l'avant-projet ne correspondent pas. Dans la première partie de l'article 19 du projet, on ne mentionne en effet pas l'obligation de notification en ce qui concerne la rectification ou l'effacement de données, le droit à la portabilité des données, le droit d'opposition et la prise de décision individuelle automatisée, bien que ces droits soient repris dans les "articles 16 à 22" du RGPD cités ensuite dans cette disposition. À l'inverse, dans la deuxième partie de l'article 19, on ne se réfère qu'aux articles 16 à 22 inclus du RGPD (cf. les termes "(…) *et qui lui sont reconnus par les articles 16 à 22, du règlement général sur la protection des données* (…)"), alors que plus haut dans la même disposition ainsi que dans la partie de l'Exposé des motifs concernant l'article 20 de l'avant-projet, on mentionne également une limitation du droit à l'information (articles 12-14 du RGPD) ainsi que du droit d'accès (article 15 du RGPD)[37]. Cela doit être rectifié.

---

[32] Cour de justice, 1er octobre 2015 (C-201/14), *Smaranda Bara e.a.*, § 39 ; Cour de justice, 27 septembre 2017 (C-73/16), *Puškár*, § 96.

[33] Cour de justice, 7 novembre 2013 (C-473/12), *IPI c. Englebert*, § 32.

[34] Considérant 10 du RGPD ; Considérant 10 de la Directive 95/46/CE.

[35] Ibid., § 39.

[36] Avis n° 34/2018 du 11 avril 2018 concernant un avant-projet de loi *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* et plus particulièrement les points 36 à 38.

[37] Exposé des motifs, p. 82.

69. Par ailleurs, l'Autorité remarque de manière plus fondamentale que dans l'avant-projet de loi, on ne retrouve pas tous les éléments mentionnés à l'article 23.2 du RGPD concernant la limitation des droits des personnes concernées. Il convient ainsi de souligner que le texte actuel de l'avant-projet et de l'Exposé des motifs ne laisse pas transparaître suffisamment concrètement la nécessité et les finalités ainsi que le champ d'application des limitations prévues. Pour justifier les limitations prévues des droits des personnes concernées dans le cadre du traitement de données à caractère personnel par l'Office des étrangers, l'article 20 de l'avant-projet prévoit une reprise littérale (de certains) des fondements repris à l'article 23.1 du RGPD (cf. *supra* point 61). L'Exposé des motifs reprend certes quelques illustrations de situations qui justifieraient certaines limitations, comme la limitation du droit d'accès d'avocats ou de médecins qui interviennent en cas de plainte introduite par l'Office des étrangers respectivement auprès du bâtonnier du barreau ou de l'Ordre des médecins, afin d'éviter de compromettre le bon déroulement de la procédure disciplinaire. Il ne suffit toutefois pas de reprendre dans l'Exposé des motifs quelques exemples de circonstances auxquelles l'article 20 de l'avant-projet se rapporte. Premièrement, les cas dans lesquels les droits sont limités et les motifs sur la base desquels ils le sont doivent être définis plus précisément et concrètement dans l'avant-projet. Deuxièmement, il se pose la question de savoir si les cas repris dans l'Exposé des motifs peuvent justifier la limitation de *tous* les droits des personnes concernées énoncés à l'article 19 de l'avant-projet. Il convient également de le préciser au cas par cas, conformément à l'article 23.2.c) du RGPD.

70. Ensuite, il faut noter que l'avant-projet ne précise pas les (catégories de) données à caractère personnel auxquelles les limitations se rapportent. L'article 21 de l'avant-projet dispose à cet égard de manière très générale que : "*La limitation des droits prévue à l'article 20 vise uniquement les données à caractère personnel qui sont en lien avec les motifs qui la justifient*". La formulation précitée est toutefois trop générale et n'offre pas suffisamment de prévisibilité pour les personnes concernées. Il convient de préciser davantage quelles (catégories de) données à caractère personnel peuvent faire l'objet de limitations et dans quels cas.

71. Par ailleurs, l'Autorité constate que l'article 22 de l'avant-projet dispose que "*La limitation des droits prévue à l'article 20 continue de s'appliquer aussi longtemps que les motifs qui la justifient restent valables*". Bien que l'article 23 du RGPD ne le prévoit pas expressément, les limitations des droits des personnes concernées doivent être limitées dans le temps, conformément au principe de proportionnalité.[38]

[38] K. HUYSMANS, "De implementatie van artikel 23 AVG: na de hervorming de contrareformatie?", Tijdschrift Privacy & Persoonsgegevens (TPP), 2019/2, p. 10.

Cela a été confirmé par la Cour constitutionnelle qui, dans son arrêt 51/2014, a annulé l'article 11 de la loi du 3 août 2012 *portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions* en raison de la violation du principe d'égalité et de non-discrimination "(…) *en ce qu'il ne prévoit pas de limitation dans le temps de la possibilité de faire exception à l'application de ces droits justifiée par l'accomplissement d'actes préparatoires à un contrôle ou à une enquête*"[39]. La section de législation du Conseil d'État a également relevé le caractère problématique de l'absence de limitation dans le temps à cet égard[40].

72. À la lumière de ce qui précède, l'Autorité fait remarquer que l'article 21 de l'avant-projet ne comporte aucun critère permettant de déterminer la durée (maximale) de la suspension des droits des personnes concernées mentionnée à l'article 19 de l'avant-projet, ce qui peut donner lieu à une suspension disproportionnellement longue de ces droits. La durée (ou les critères déterminant la durée) de la limitation des droits doit dès lors être davantage précisée.

h. Divers

73. L'Autorité remarque que dans la version néerlandaise du texte soumis pour avis, le Titre 1er ("*Titre 1er. Disposition générale*" dans la version française) est absent.

74. L'article 33 de l'avant-projet contient une énumération des données enregistrées dans le cadre l'enregistrement ("*logging*") des accès aux banques de données de l'Office des étrangers. Cette disposition est énoncée comme suit :

> "***Art. 33.*** *L'enregistrement du traitement prévu à l'article 32 comprend les informations suivantes :*
> *1° l'identifiant unique de l'auteur du traitement ;*
> *2° la date et l'heure précise du traitement ;*
> *3° la nature du traitement ;*
> *4° le numéro unique du traitement ;*
> *5° l'identifiant unique de la personne concernée*[41] *;*
> *6° en cas de communication de données à caractère personnel, l'identité du destinataire auquel les données sont communiquées ;*
> *7° le cas échéant, la motivation du traitement réalisé*[42]*".*

[39] Soulignement par la Chambre Contentieuse.
[40] Conseil d'État, avis n° 51.291/2 du 21 mai 2012, https://www.dekamer.be/FLWB/pdf/53/2343/53K2343001.pdf, 23, n° 3.2.
[41] Soulignement par l'Autorité.
[42] Soulignement par l'Autorité.

L'Autorité constate que l'article 33, 5° de l'avant-projet prévoit l'enregistrement dans la journalisation de "*l'identifiant unique de la personne concernée*", ce qui constitue une donnée à caractère personnel au sens du RGPD. Il convient de le distinguer du numéro d'identification unique du membre du personnel qui est l'auteur du traitement en question (visé à l'art. 33, 1°). L'Autorité souligne que le logging de l'accès à la banque de données ne peut toutefois pas permettre d'enregistrer certaines données à caractère personnel collectées des personnes concernées plus longtemps que ce qui est nécessaire en vue des finalités poursuivies. À cet égard, il convient de noter que conformément à l'article 13, § 1er de l'avant-projet, le délai de conservation des données à caractère personnel des personnes concernées s'élève en principe à maximum cinq ans, alors que le délai de conservation des données reprises dans la journalisation est fixé par l'article 35 de l'avant-projet à dix ans, à compter de l'enregistrement de l'information. Il convient de souligner que le numéro d'identification unique de la personne concernée peut permettre de retrouver certaines informations au sujet de la personne concernée (par exemple l'endroit où elle se trouvait ou ce qu'elle faisait au moment où ses données ont été journalisées), et ce dans certains cas (un long moment) après l'échéance du délai de conservation de cinq ans prévu à l'article 13 de l'avant-projet. L'Autorité comprend qu'à la lumière de la finalité de la journalisation (à savoir le contrôle quant à une éventuelle fraude ou à un usage impropre des banques de données de l'Office des étrangers), il est nécessaire de conserver le numéro d'identification unique de la personne concernée afin de mettre en relation les traitements mentionnés dans la journalisation avec le dossier concerné. Il est toutefois recommandé d'harmoniser les délais de conservation prévus aux articles 13 et 33 et de conserver toutes les informations soit cinq ans, soit dix ans. Si l'on opte pour un délai de conservation de dix ans, ce (long) délai de conservation doit toutefois pouvoir être justifié sur la base d'un ou plusieurs critères objectifs (par exemple l'harmonisation avec le délai (de prescription) pour introduire une action). Dans l'Exposé des motifs, le demandeur cite la jurisprudence pertinente de la Cour de justice à cet égard, mais il ne précise ensuite pas concrètement pourquoi dans ce cas on opte pour un délai de conservation de dix ans. Il convient de le préciser le cas échéant.

75. Enfin, l'Autorité fait remarquer que l'article 33, 7° de l'avant-projet mentionne que "*le cas échéant*" la motivation du traitement réalisé est mentionnée. L'Autorité indique que cette motivation doit cependant toujours être reprise.

PAR CES MOTIFS,

l'Autorité,

estime que les adaptations suivantes s'imposent dans l'avant-projet de loi :

- décrire plus précisément les finalités du traitement de données à caractère personnel (points 13-30) ;

- préciser que l'Office des étrangers doit être considéré comme le responsable du traitement au sens de l'article 4.7) du RGPD pour les traitements de données à caractère personnel auxquels l'avant-projet de loi se rapporte (et non le ministre) (points 33-37) ;

- préciser davantage les (catégories de) données à caractère personnel traitées et les personnes concernées, à la lumière du principe de proportionnalité et du principe de minimisation des données (points 38-46) ;

- préciser davantage les (catégories de) destinataires ainsi que les (catégories de) données à caractère personnel auxquelles chacun de ces destinataires a accès et pour quelles finalités (points 47-54) ;

- supprimer les termes de l'article 8, 1°, de l'article 10, § 2, de l'article 11, § 2 et de l'article 18 de l'avant-projet en vertu desquels les éléments essentiels du traitement peuvent être *complétés* par arrêté royal (points 32, 43, 54 et 61) ; et

- préciser, aux articles 19 à 22 inclus de l'avant-projet, les éléments énoncés à l'article 23.2 du RGPD afin d'harmoniser les limitations prévues des droits des personnes concernées avec la disposition précitée (points 62-72).

Pour le Centre de Connaissances,
Cédrine Morlière, Directrice

CONTROLEORGAAN OP DE POLITIONELE INFORMATIE

Uw kenmerk	Ons kenmerk	Bijlage(n)	Datum
/	DA220021		14.7.2022

Betreft: Advies betreffende een voorontwerp van wet betreffende de verwerkingen van persoonsgegevens door de Algemene Directie Dienst Vreemdelingenzaken van de Federale Overheidsdienst Binnenlandse Zaken

Het Controleorgaan op de politionele informatie (hierna het 'COC' of 'het Controleorgaan'),

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (*B.S.*, 5 september 2018, hierna afgekort als 'WGB'), inzonderheid het artikel 59 §1, 2de lid, artikel 71 en Titel VII, inzonderheid artikel 236;

Gelet op de wet van 3 december 2017 *tot oprichting van een Gegevensbeschermingsautoriteit* (hierna afgekort 'WOG');

Gelet op de wet van 5 augustus 1992 *op het politieambt* (hierna 'WPA');

Gelet op de *Law Enforcement Directive* 2016/680 van 27 april 2016 (hierna *LED*);

Gelet op het verzoek van de Staatssecretaris voor Asiel en Migratie aan de Gegevensbeschermingsautoriteit (hierna: 'GBA') op 9 juni 2022 om advies uit te brengen op een voorontwerp van wet betreffende de verwerking van betreffende de verwerkingen van persoonsgegevens door de Algemene Directie Dienst Vreemdelingenzaken van de Federale Overheidsdienst Binnenlandse Zaken (hierna 'het voorontwerp');

Gelet op de overmaking van voormeld verzoek door de GBA aan het Controleorgaan op 9 juni 2022 in het kader van de één loket functie van de GBA (art. 54/1 WOG) en conform de bepalingen van het samenwerkingsprotocol tussen de Belgische Federale Toezichthoudende Autoriteiten op vlak van Dataprotectie (cf. www.controleorgaan.be) .

Gelet op het verslag van de heer Frank Schuermans, lid-raadsheer in het Controleorgaan;

Brengt op 14 juli 2022 het volgend advies uit.

...

I. Voorafgaande opmerking nopens de bevoegdheid van het Controleorgaan

1. In het licht van, respectievelijk, de toepassing en de omzetting van de Verordening 2016/679[1] en de Richtlijn 2016/680[2], heeft de wetgever de taken en opdrachten van het Controleorgaan grondig gewijzigd. Artikel 4 § 2, vierde lid van de organieke wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit (hierna 'WOG') bepaalt dat de competenties, taken en bevoegdheden als toezichthoudende autoriteit bedoeld door de Verordening 2016/679 voor de politiediensten in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie, gestructureerd op twee niveaus, worden uitgeoefend door het Controleorgaan. Dat betekent met name dat het Controleorgaan ook bevoegd is wanneer politiediensten persoonsgegevens verwerken die niet onder de opdrachten van bestuurlijke en gerechtelijke politie vallen, bijvoorbeeld in het kader van sociaaleconomische doeleinden of HR-verwerkingen. Het Controleorgaan moet worden geraadpleegd in het kader van de voorbereiding van wetgeving of een regelgevende maatregel betreffende de verwerking van persoonsgegevens door de politiediensten van de geïntegreerde politie (zie artikelen 59 §1, 2de lid en 236 § 2 van de WGB, artikel 36.4 van de AVG en artikel 28.2 van de Richtlijn Politie-Justitie). In dit kader heeft het Controleorgaan als opdracht om na te gaan of de door de politiediensten beoogde verwerkingsactiviteit in overeenstemming is met de bepalingen van Titel 1 (voor de niet-operationele verwerkingen)[3] en van Titel 2 (voor de operationele verwerkingen) van de WGB[4]. Bovendien heeft het COC ook een opdracht van advies uit eigen beweging, zoals bepaald in artikel 236, § 2, van de WGB, en een opdracht van algemene informatieverstrekking aan het grote publiek, de betrokkenen, de verwerkingsverantwoordelijken en de verwerkers op het gebied van het recht op bescherming van de persoonlijke levenssfeer en gegevensbescherming, zoals bepaald in artikel 240 van de WGB.

2. Met betrekking tot in het bijzonder de verwerkingsactiviteiten in het kader van de opdrachten van bestuurlijke en/of gerechtelijke politie brengt het Controleorgaan uit eigen

[1] 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 de 'Algemene Verordening Gegevensbescherming' of 'AVG' genoemd).
[2] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (hierna de 'Richtlijn Politie en Justitie' of *LED* (*Law Enforcement Directive*) genoemd).
[3] Artikel 4 §2, 4de lid WGB.
[4] Artikel 71 §1, 3de lid WGB.

beweging of op verzoek van de regering of de Kamer van Volksvertegenwoordigers, een bestuurlijke of gerechtelijke autoriteit of een politiedienst advies uit over elke aangelegenheid die verband houdt met het beheer van politionele informatie, zoals bepaald in afdeling 12 van hoofdstuk 4 van de wet op het politieambt[5].

3. Het Controleorgaan is, ten aanzien van de politiediensten, de Algemene Inspectie van de federale politie en lokale politie (afgekort 'AIG') zoals bedoeld in de wet van 15 mei 2007 op de Algemene Inspectie en de Passagiersinformatie-eenheid (hierna afgekort 'BEL-PIU') bedoeld in Hoofdstuk 7 van de wet van 25 december 2016 tevens belast met het toezicht op de toepassing van Titel 2 van de WGB en/of de verwerking van persoonsgegevens zoals bedoeld in de artikelen 44/1 tot 44/11/13 van de wet op het politieambt en/of elke andere opdracht die krachtens of door andere wetten aan het Controleorgaan wordt verleend[6].

4. Het Controleorgaan is tot slot ingevolge artikel 281, § 4, van de algemene wet van 18 juli 1977 inzake douane en accijnzen, zoals gewijzigd door de wet van 2 mei 2019 tot wijziging van diverse bepalingen met betrekking tot de verwerking van passagiersgegevens ten aanzien van de Dienst Geschillen van de Algemene Administratie van Douane en Accijnzen bevoegd in het kader van de vorderingen gericht aan de BELPIU in fiscale materies.

II. Voorwerp van de aanvraag

5. De adviesaanvraag heeft betrekking op een voorontwerp van wet betreffende de verwerkingen van persoonsgegevens door de Algemene Directie Dienst Vreemdelingenzaken van de Federale Overheidsdienst Binnenlandse Zaken.

6. De overheden, evenals de verwerkingen van persoonsgegevens en informatie waarvoor het COC exclusief bevoegd is, worden strikt door de wet gedefinieerd. Bijgevolg beperkt het Controleorgaan zijn adviezen tot de verwerkingen die tot zijn bevoegdheid behoren, i.e. in het huidige geval die welke door de politiediensten worden verricht of die een effect hebben op de werking van de politiediensten. *In casu* werd door de verzoekende Staatsecretaris bovendien ook het vakje 'politiediensten' aangevinkt op de vraag of "*het ontwerp betrekking* (heeft) *op of impliceert de verwerking(en) van persoonsgegevens door een of meer van de volgende autoriteiten*".

[5] Artikelen 59 §1, 2de lid en 236, §2 van de WGB.
[6] Artikel 71, §1, derde lid *juncto* artikel 236, §3 van de WGB.

Hoe dan ook blijven de adviezen van het COC niet noodzakelijk beperkt tot het (de) (eventuele) artikel(en) zoals vermeld in een adviesaanvraag. Het COC houdt immers altijd rekening met alle elementen en bepalingen die tot zijn bevoegdheid behoren krachtens bovenvermelde regelgeving. Het Controleorgaan is daarenboven niet alleen een dataprotectie autoriteit, maar is tevens belast met de controle en het toezicht op de politionele gegevensbanken[7] en op alle politionele verwerkingen, ook in termen van legaliteit, efficiëntie en effectiviteit. Ook deze elementen (van bijvoorbeeld operationele haalbaarheid en capaciteit) worden steeds mee in ogenschouw genomen bij elke adviesverlening.

III. Analyse van de aanvraag

7. Het COC beperkt zich in deze tot die artikelen die een weerslag hebben op de werking van de politiediensten van de geïntegreerde politie (hierna' GPI') of op de werking van het Controleorgaan.

1. De verwerkingen in de Algemene Nationale Gegevensbank en in het Schengeninformatiesysteem

8. Het ontworpen artikel 10 voorziet de doeleinden waarvoor de persoonsgegevens kunnen worden verwerkt door de Dienst Vreemdelingenzaken (hierna 'DVZ'). De in artikel 6 bedoelde categorieën van persoonsgegevens kunnen verwerkt worden voor onder meer het doeleinde voorzien in het ten 11°, met name het "*instaan voor de opvolging van de inreisverboden, met inbegrip van de opheffing of schorsing ervan, en het beheer van de registratie ervan in het Schengeninformatiesysteem en in de algemene nationale gegevensbank of in een andere nationale gegevensbank*". In de toelichting staat bij het ontworpen artikel 9 te lezen dat "*De Dienst Vreemdelingenzaken … de persoonsgegevens van deze categorie van betrokken personen* (moet) *kunnen verwerken om de besluiten tot weigering van toegang op te kunnen volgen, de registratie van deze inreisverboden in het SIS en/of de ANG te kunnen beheren (eigen onderlijning) en de aanvragen tot schorsing of opheffing van deze aanvragen te kunnen behandelen*". Een gelijkaardige alinea staat vermeld bij de commentaar op artikel 10 ("*instaan voor de reisverboden*")

Het voorontwerp brengt met zich dus mee dat **voor het eerst, zij het impliciet,** in een wettelijke bepaling een 'niet-politiedienst', met name de DVZ, rechtstreeks gegevens kan

[7] Zie ook Activiteitenverslag 2020 van het COC, https://www.controleorgaan.be/files/Activiteitenverslag_COC_2020_N.pdf, randnummer 7 en 8.

verwerken in een nationale en een internationale **politionele** gegevensbank. Onder "verwerking" wordt *in casu* dan ook begrepen het daadwerkelijke vatten van gegevens en alle aanverwante handelingen, zoals wijzigen, rectificeren, wissen, enz. … en dus niet het enkele 'raadplegen'. Personeelsleden van de DVZ zou dus worden toegestaan meerdere keren verwerkingen te doen in de ANG m.b.t. eenzelfde persoon (vb. naar gelang zijn verblijfsstatus).

Tot op heden voorziet geen enkele wettelijke bepaling voor de DVZ (of eender welke ander derde overheid, orgaan of instelling overigens) in de mogelijkheid om deze verwerkingen in de ANG of een andere politionele gegevensbank te doen. Tot op heden kan de DVZ enkel een mededeling krijgen van informatie en persoonsgegevens uit de ANG (cf. art. 44/11/4 e.v. en meer bepaald de art. 44/11/9 §1, 2° en 44/11/12 §1, 2° WPA). Deze verwerkingen ten behoeve van de DVZ gebeuren op heden ook niet zelf door DVZ, maar nog steeds door de GPI (op vraag van DVZ, zie ook randnummer 15). Dit alles wijzigen waarbij een derde overheid, orgaan of instelling zelf rechtstreeks de hier bedoelde verregaande verwerkingen in al zijn facetten zou kunnen doen is dan ook een belangrijk precedent waarvan het vooral niet de bedoeling kan zijn dat dit navolging krijgt, behoudens specifiek en afdoende motivering.

Nog belangrijker is bovendien om een heldere wettelijke basis te creëren – met een afdoende motivering waarom dat noodzakelijk is of zou zijn - om de DVZ toe te laten zelfstandig deze verwerkingen in politionele gegevensbanken zoals de ANG te doen. Dit betekent alleszins dat de Wet op het Politieambt in die zin dient te moeten worden geamendeerd en meer bepaald afdeling 12 ("*Het informatiebeheer*") van Hoofdstuk IV "*De algemene vorm en voorwaarden van uitvoering van de opdrachten*") waarin, bij voorkeur in een apart artikel, de wettelijke grondslag wordt gecreëerd voor de DVZ om de in het ontworpen artikel 10, 11° van huidig voorontwerp bedoelde verwerkingen ("…*de opvolging van de inreisverboden, met inbegrip van de opheffing of schorsing ervan, en* ***het beheer van de registratie ervan*** *in het Schengeninformatiesysteem en in de algemene nationale gegevensbank of in een andere nationale gegevensbank"*) te kunnen doen. Deze noodzakelijke wetswijziging van de WPA zal bovendien voorafgaandelijk dienen te worden voorgelegd voor advies aan het Controleorgaan op grond van art. 59 §1, 2e lid WGB.

9. Voor wat de ANG betreft zijn de verwerkingsverantwoordelijken de Minister van Binnenlandse Zaken en Justitie en de operationeel verantwoordelijken zijn de politiediensten. Het is het Controleorgaan niet duidelijk of de Minister van Justitie, als medeverwerkingsverantwoordelijke, op de hoogte is van de hier gecreëerde mogelijkheid

voor de DVZ om rechtstreeks de meest verregaande verwerkingen in de ANG te laten uitvoeren; naast de evidente noodzaak van deze betrokkenheid van de Minister van Justitie als mede verwerkingsverantwoordelijke, lijkt het er op dat ook formeel de Minister van Justitie het voorontwerp mede dient te ondertekenen, vermits er rechtstreeks wordt geraakt aan wetgeving die tot zijn bevoegdheid behoort.

10. Het is evident niet zonder gevaar en risico een administratie zoals de DVZ toe te laten zelf rechtstreeks in de ANG verwerkingen te laten uitvoeren waarbij die verwerkingen veel verder gaan dan het louter raadplegen. Het voorontwerp gaat op dit wezenlijk aspect op geen enkele wijze in noch motiveert het überhaupt de noodzaak voor de DVZ om deze bevoegdheid en mogelijkheden te krijgen, wellicht ook opdat één en ander slechts impliciet en onrechtstreeks – en dus niet afdoende - wettelijk wordt verankerd. Hoe zal één en ander praktisch georganiseerd worden? Welke controlemechanismen worden er voorzien; wie binnen de DVZ zal toegang krijgen tot de ANG? Tot welke applicaties binnen de ANG zal er toegang worden voorzien? Welke opleiding zal er voorzien worden voor de personeelsleden van de DVZ? Enz. …

M.a.w. de concrete modaliteiten zullen in een regelgevende tekst moeten opgenomen worden. Een mogelijkheid kan erin bestaan één en ander nader uit te werken in het bestaande KB van 28 april 2016 betreffende de rechtstreekse bevraging van de Algemene Nationale Gegevensbank bedoeld in artikel 44/7 van de wet op het politieambt door de aangewezen personeelsleden van de Dienst Vreemdelingenzaken (*BS* van 12 mei 2016), dat overigens sowieso al langer in lijn had of zou moeten worden gebracht met het nieuwe juridisch kader inzake gegevensbescherming[8] dat sedert 2018 van toepassing is. Op grond van dit KB hebben bepaalde personeelsleden van de DVZ actueel enkel de mogelijkheid een 'rechtstreekse bevraging' te doen van de ANG, wat dus veel minder ver gaat dan het daadwerkelijk vatten van gegevens, signaleringen op te stellen en te vatten, verbeteringen en wijzigingen door te voeren, enz. … Het KB zal dus grondig moeten herschreven worden in het licht van dit voorontwerp en de noodzakelijk in de WPA te creëren rechtsgrondslag (cf. randnummer 8). Ook dit gewijzigde KB zal bovendien voorafgaandelijk dienen te worden voorgelegd voor advies aan het Controleorgaan op grond van art. 59 §1, 2e lid WGB.

Voorts is helemaal niet duidelijk wat in het ontworpen artikel 10, 11° juist wordt bedoeld met "*of in een andere nationale gegevensbank"* (in het Frans luidt het overigens niet helemaal

[8] Zo bijvoorbeeld verwijst het KB nog naar de oude Commissie voor de Bescherming van de Persoonlijke Levenssfeer (art. 1, 8°, art. 5), naar een "*een consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer*" (art. 5), het COC was op dat moment nog geen gegevensbeschermingsautoriteit wat het nu t.a.v. de GPI uiteraard wel is geworden, enz. …

hetzelfde, met name "*ou dans **toute** autre banque de données nationale*"). De toelichting verstrekt op dat vlak evenmin enige duiding. Het COC ziet niet in over welke andere nationale gegevensbank het potentieel zou kunnen gaan zodat er geen enkele reden is om deze zinssnede te houden, vermits het in enkel over de ANG kan gaan die reeds vermeld werd.

11. Verder maakt het KB ook gewag van een protocol tussen de DVZ en "*de directie die de toegangen tot de A.N.G. beheert*" (in de feiten DRI, de Directie van de politionele informatie en de ICT-middelen van de federale politie (een directie binnen het Commissariaat Generaal). Ook dit protocol van 29 september 2016 zal dienen herschreven te worden om dezelfde hogervermelde redenen van aanpassing aan het nieuwe gegevensbeschermingskader en gelet op de verregaande verwerkingsmogelijkheden die men zinnens is toe te kennen aan de DVZ en zal evenzeer voorafgaandelijk niet enkel aan de Gegevensbeschermingsautoriteit dienen te worden voorgelegd, maar ook aan het Controleorgaan (cf. art. 6 van het KB van 28 april 2016). Vragen die daarbij aan de orde dienen te zijn, zijn, niet limitatief:

- de draagwijdte van het antecedenten – en omgevingsonderzoek (zie ook punt 2 van het protocolakkoord DVZ-DRI) dat de personeelsleden van de DVZ thans moeten ondergaan vooraleer zou kunnen toegelaten worden tot een rechtstreekse bevraging van de ANG; thans wordt volstaan met een veiligheidsadvies in de zin van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (art. 22quinquies). Volstaat nog enkel een éénmalige positief veiligheidsadvies?

- het juiste profiel van de DVZ medewerker? Moeten die profielen niet herbekeken worden door het feit dat de DVZ medewerker bevoegdheden zal krijgen die veel verder gaan dan actueel enkel maar de mededeling van informatie en persoonsgegevens via de rechtstreekse bevraging (*hit/no hit* systeem) en waarbij bv. op heden geen zachte informatie zichtbaar mag zijn voor de DVZ medewerkers (zie ook art. 4, b): enkel informatie opgenomen in processen-verbaal)? hoe kan men vermijden dat de DVZ medewerker kennis krijgt van alle voorhanden zijn zachte informatie als men het profiel van "vatter" krijgt?

- *quid* met het *teleworking* door de personeelsleden DVZ (cf. punt 4.1 protocolakkoord)?

- is een werkingsaudit om de twee jaar wel afdoende (cf. punt 5 protocolakkoord)?

- welke concrete opleiding zal er voorzien moeten worden voor de DVZ medewerker? Dit moet uiteraard veel verder gaan en intensiever zijn dan wat actueel voorzien wordt (cf. punt 6 protocolakkoord) voor de rechtstreekse bevraging.

- enz. …

12. In het protocol is ook nog sprake van "*een afzonderlijk ad hoc document*" waarin de technische aspecten van de rechtstreekse bevraging worden opgenomen. Het COC heeft van dit document vooralsnog geen kennis maar zal dit alleszins bij DRI opvragen wanneer dit voorontwerp tot wet zal evolueren. Het protocolakkoord voorziet trouwens zelf in zijn nummer 10 een herziening ervan, "*minstens naar aanleiding van:*

- *de wijziging van het wettelijk of reglementair kader:*
- *…;*
- *het ontstaan van bijkomende behoeften;*
- *…"*

Dit protocolakkoord had dus eigenlijk al moeten herzien geweest zijn gezien het gewijzigd wettelijk gegevensbeschermingskader in 2018; dit is des te meer het geval indien dit voorontwerp wet zou worden.

13. De verwerkingsverantwoordelijke voor het nationaal gedeelte van de SIS II databank is van zijn kant nooit bij wet of uitvoeringsbesluit vastgelegd, wat overigens tot op heden een juridisch probleem is. In dit verband moet verwezen worden naar een toezichtonderzoek dat het COC samen met de GBA heeft verricht in 2019 en waarvan een rapport werd opgemaakt op 2 februari 2020, met name het "*Rapport final de la visite de contrôle du bureau SIRENE (Système d'Information Schengen) par l'Organe de contrôle de l'information policière et par l'Autorité de protection des données*". In dit aan de commissaris-generaal van de federale politie en de directeur CGI overgemaakt rapport werd onder meer het volgende vastgesteld:

> 6.1.1.1. Première observation générale : Les instances responsables pour le bureau SIRENE et l'Office N.SIS II n'ont pas été désignées dans le droit belge
> **56.** En 2019, aucune réglementation n'a encore transposé la Décision SIS II en droit belge.
> De même, aucun texte légal belge ne complète les règles Schengen (*Ci-après la remarque de CGI suite à la remise du rapport intermédiaire de visite : « Pt. 56 pag. 16/60 : (idem vaststelling A1 pag 50) dient genuanceerd te worden; het SISII Besluit heeft rechtstreekse uitwerking in de interne rechtsorde, wat een omzetting op zich van het gehele besluit in het Belgische recht niet noodzaakt (cfr analyse FOD Binnenlandse Zaken bij de inwerkingtreding SISII). De operationele werkprincipes werden wel omgezet in de fiche C22 van de Ministeriële richtlijn MFO3. Indien een wetswijziging zich opdringt naar aanleiding van de Europese Richtlijn 680/2016, omgezet door de nationale wet van 30/07/2018, dienden de noodzakelijke aanpassingen via de wet van 22/07/2019 te zijn gebeurd geweest, wat niet het geval is. In tussentijd werd vastgesteld dat een wijziging van art.26, 8° van de wet van 30/07/2018 moet plaats vinden om toe te laten de bevoegde Ministers aan te duiden als verantwoordelijke van de behandeling en uitvoering van de Europese richtlijn. De politieke overheden werden hiervan reeds eerder in kennis gesteld.*») qui laissent aux législateurs nationaux le soin de régler certaines questions. C'est le cas par exemple dans la Décision SIS II et dans le Règlement SIS II pour les délais de conservation concernant les signalements et les informations traitées par le bureau SIRENE : rien n'est explicitement prévu sur ces questions au niveau belge.
> Les autorités de contrôle ont constaté que la Décision SIS II et le Règlement SIS II, malgré qu'ils soient d'application directe en droit belge et ne demandent par conséquent pas de transposition en tant que telle, renvoient pour certains points au droit national. Ces renvois doivent trouver une réponse en droit belge, ce qui n'est pas le cas au jour de la rédaction du présent rapport puisque certaines questions, comme les délais de conservation à appliquer à certains types de signalement ou encore la désignation du bureau SIRENE et de l'Office N.SIS II, ne

sont pas réglées en droit belge. Cette remarque de CGI ne modifie donc pas la constatation des autorités de contrôle.

57. Ce constat est le même pour la désignation des instances responsables pour le bureau SIRENE et l'Office N.SIS II (Décision SIS II et Règlement SIS II, articles 6 et 7 communs). En effet, la Belgique doit désigner un Office N.SIS II qui assume la responsabilité centrale du N.SIS II. Cette instance est responsable du bon fonctionnement et de la sécurité du N.SIS II, elle doit faire en sorte que les autorités compétentes aient accès au SIS II mais aussi prendre les mesures nécessaires pour assurer le respect des dispositions de la Décision SIS II et du Règlement SIS II.

58. La Belgique doit également désigner une instance – le bureau SIRENE - chargée de l'échange de toutes les informations supplémentaires et de vérifier la qualité des informations introduites dans le SIS II. Pour cela, le bureau SIRENE doit avoir accès aux données traitées dans le SIS II.

59. Ces instances ne sont pas identifiées dans le droit belge. En effet, l'arrêté royal du 14 novembre 2006 (*Arrêté royal du 14 novembre 2006 relatif à l'organisation et aux compétences de la police fédérale, articles 2, 1°, e) et 6, 3°*) qui attribue la détermination des normes et d'une approche standardisée en matière de sécurité de l'information et de protection de la vie privée au Commissariat général, et qui confie entre autres la préparation de la politique et des règles relatives au traitement de l'information policière à la Direction générale de la gestion des ressources de l'information («DGR») de la police fédérale, le tout en concertation avec la Commission permanente de la police locale, ne constitue pas une base suffisamment claire et précise d'identification des instances responsables pour le bureau SIRENE et l'Office N.SIS II.

60. Cela oblige les autorités de contrôle à constater que dès lors l'exercice concret, correct et efficace des missions qui incombent à ces instances responsables peut difficilement être mis en oeuvre.

61. *De facto*, le bureau SIRENE est installé sous CGI et s'occupe de la gestion des signalements ainsi que de l'échange des informations supplémentaires. DRI met pour sa part à disposition du bureau SIRENE les outils nécessaires au traitement des signalements Schengen: DRI gère le fonctionnement et la sécurité de la copie nationale du N.SIS II dont a besoin le bureau SIRENE pour travailler avec le SIS II.

62. La note de politique générale de sécurité de l'information SIS II approuvée par les Ministres de l'Intérieur et de la Justice le 18 octobre 2016 a pour objectif de «*définir un cadre pour la mise en oeuvre d'un ensemble approprié de mesures pour assurer la sécurité de la copie nationale du N.SIS II et des systèmes d'information des services de police nécessaires au fonctionnement du SIS II*». L'objectif de cette note est de garantir la confidentialité, l'intégrité et la disponibilité des informations traitées dans ces systèmes d'information.

En matière de sécurité, la note partage les responsabilités fonctionnelles et techniques: CGI détermine les objectifs du plan de sécurité pour le SIS II et est donc responsable pour le N.SIS II et le bureau SIRENE, quant à DRI, elle détermine les objectifs de sécurité et met en place les mesures techniques de sécurité pour les différents systèmes d'informations.

63. De leurs rencontres avec les *DPO* de CGI et de DRI, les autorités de contrôle ont constaté que si les deux Directions de la police fédérale s'accordent pour considérer que les Ministres de la Justice et de l'Intérieur sont responsables du traitement pour la copie nationale du N.SIS II, le *DPO* de DRI indique que DRI n'est pas responsable pour l'Office N.SIS II tandis que le *DPO* de CGI estime que CGI est l'instance responsable pour le bureau SIRENE et qu'elle partage une responsabilité avec DRI (Selon CGI, DRI s'occuperait des aspects techniques et logistiques tandis que CGI assumerait les tâches opérationnelles) en ce qui concerne le N.SIS II.

64. La vision du *DPO* de CGI va dans le même sens que ce qui est indiqué dans la note de politique générale de sécurité de l'information SIS II approuvée le 18 octobre 2016.

65. Cependant, la Belgique doit communiquer chaque année (*Ces Directions sont ainsi désignées depuis 2015 au Journal Officiel de l'Union européenne. Avant cela, les anciennes Direction de la télématique pour le SIS II et Direction de l'information policière opérationnelle pour le bureau SIRENE étaient désignées*) au gestionnaire fonctionnel du SIS II, conformément à la Décision SIS II et au Règlement SIS II *(Règlement SIS II et Décision SIS II, article 7 §3 commun)*, les coordonnées de son Office N.SIS II ainsi que de son bureau SIRENE. Elle s'y est dernièrement conformée en indiquant que pour le N.SIS II, l'autorité responsable est « le Bureau N.SIS II de la police fédérale – DRI » et que pour le bureau SIRENE, il s'agit de la « Commission SIRENE de la police fédérale – CGI (*Liste des offices N.SIS II et des bureaux SIRENE nationaux » consolidée au 15 mars 2019, J.L.O., C222, 2 juillet 2019, p. 173.*) ».

66. Ainsi, tandis que la Décision SIS II et le Règlement SIS II nécessitent, pour la bonne alimentation du SIS II, une coopération soutenue et une communication fluide entre deux instances désignées responsables au niveau national, cela est difficilement possible au niveau belge sans désignation claire puisque cette coopération et cette communication se jouent *de facto* entre deux Directions différentes qui ne se situent pas au même niveau hiérarchique (*Ci-après la remarque de CGI suite à la remise du rapport intermédiaire de visite : "Pt 66 CGI maakt geen deel uit van het commissariaat-generaal maar is een specifieke directie (zie KB 14 november 2006)." L'Organe de contrôle se réfère à l'article 3, 1° de l'arrêté royal du 14 novembre 2006 relatif à l'organisation et aux compétences de la police fédérale qui indique que le Commissariat général se compose de la Direction de la coopération policière internationale. Cette remarque de CGI ne modifie donc pas la constatation des autorités de contrôle)* de la police intégrée et structurée à deux niveaux telle qu'elle est instituée en Belgique. En effet, d'une part le bureau SIRENE est installé au sein du Single Point of Operational Contact de CGI qui fait partie du Commissariat général de la police fédérale et d'autre part, DRI fait partie de la DGR.

67. Vu l'absence de désignation claire des deux instances responsables dans le droit belge et eu égard aux positions contradictoires de CGI et DRI, les autorités de contrôle considèrent que la communication officielle de

> la Belgique au gestionnaire fonctionnel du SIS II, telle qu'elle a encore été récemment inscrite au Journal Officiel de l'Union européenne du 2 juillet 2019, constitue une désignation de CGI et de DRI comme autorités responsables, respectivement pour le bureau SIRENE et pour le N.SIS II.
> **68**. D'emblée, les autorités de contrôle insistent sur le fait que la répartition des tâches de mise à jour, de gestion des signalements et des responsabilités telle qu'elle est prévue dans le Règlement SIS II et la Décision SIS II invitent l'Office N.SIS II – DRI et le bureau SIRENE – CGI à travailler étroitement ensemble pour que l'alimentation du SIS II fonctionne plus efficacement.

14. Het spreekt voor zich dat één en ander nog nijpender wordt wanneer nu ook de DVZ een (gedeelde) verantwoordelijkheid zou krijgen met betrekking tot de in het ontworpen artikel 10, 11° van het voorontwerp bedoelde *"opvolging van de inreisverboden, met inbegrip van de opheffing of schorsing ervan, en het beheer van de registratie ervan in het Schengeninformatiesysteem en in de algemene nationale gegevensbank of in een andere nationale gegevensbank".*

Het lijkt dan ook noodzakelijk ook dit euvel van gebrek aan duidelijke rechtsgrondslag en aanduiding van verwerkingsverantwoordelijken en operationeel verantwoordelijken van het Schengeninformatiesysteem in de WPA aan te pakken en helder te regelen.

15. De problematiek van de seiningen op grond van artikel 24 SIS II verordening heeft evenzeer het voorwerp uitgemaakt van het hogervermelde onderzoek door de GBA en het COC. Hieromtrent werd het volgende vastgesteld:

> **138**. Certains autres partenaires externes comme l'ODE, le Ministère des affaires étrangères et la Direction de l'Immatriculation des véhicules («*Liste des autorités compétentes autorisées à consulter directement les données introduites dans le système d'information Schengen de deuxième génération », J.O.L. C222, 2 juillet 2019, p. 1*.) ont également accès via l'application Portal ou un webservice. Le service des Douanes n'a pour l'instant aucun accès.
> **139**. Les protocoles avec l'ODE sont en cours d'élaboration. Il existe cependant une procédure tacite applicable depuis un certain nombre d'années: les signalements visés à l'article 24 du Règlement SIS II sont introduits dans le SIS II sur base d'un formulaire standard communiqué par l'ODE et sans pièces justificatives c'est-à-dire que la décision ayant motivé le signalement n'est pas jointe. De même, les signalements sont automatiquement renouvelés jusqu'à l'échéance de la décision de l'ODE. Par ailleurs, le *Legal Office* déclare que la révision de la Directive «retour» (Directive 2008/115/CE du Parlement européen et du Conseil du 16 décembre 2008 relative aux normes et procédures communes applicables dans les États membres au retour des ressortissants de pays tiers en séjour irrégulier) devrait accroître exponentiellement le nombre de signalements. Dès lors, le protocole en projet vise à fournir à l'ODE une possibilité d'alimentation directe du N.SIS II (Ci-après la remarque de CGI suite à la remise du rapport intermédiaire de visite *(« Pt. 139 pag 32/60 : er is slechts één protocol met betrekking tot het SIS II met DVZ in uitwerking. De laatste zin is niet correct; het protocol actueel in uitwerking beoogt de huidige samenwerking tussen de politie en DVZ te officialiseren. Indien de rechtstreekse voeding van het NSIS II (bv wat betreft de terugkeerbesluiten) bevestigd en ontwikkeld wordt (of enige andere werkmethode wordt gewijzigd) zal dit protocol hier vervolgens worden voor aangepast.» Dans la mesure où cet accès est envisagé, les autorités de contrôle invitent les autorités concernées à d'ores et déjà prévoir toutes les modalités dans le protocole et à procéder à une analyse complète du respect des règles en matière de protection des données. Cette remarque de CGI ne modifie donc pas la constatation des autorités de contrôle*).

Ook deze in de praktijk kennelijk stilzwijgend gegroeide procedure waarbij de politie (meer bepaald het bureau SIRENE binnen CGI/SPOC van de federale politie) de DVZ de (zgn. art. 24 SIS II Verordening) signaleringen invoert zal dus moeten herbekeken worden in het licht

van huidige voorontwerp en dit advies van het Controleorgaan. Reeds toen werd kennelijk gespeeld met de idee om de DVZ zelf zijn signaleringen te laten doen in het Schengeninformatiesysteem en was er sprake van een ontwerp van protocol. Het COC heeft geen kennis van een definitief protocol ter zake wat overigens ook moeilijk zou kunnen zonder voorafgaande wetswijziging, zoals ook CGI terecht heeft aangegeven in zijn repliek op het ontwerp rapport van het COC en de GBA.

2. De ontvangers van de door de DVZ meegedeelde gegevens

16. Het ontworpen artikel 11 voorziet in zijn 1e paragraaf de diverse ontvangers of categorieën van ontvangers aan wie de DVZ de haar verzamelde persoonsgegevens kan meedelen. Daarin wordt enerzijds een ten 6° voorzien – met name de "*autoriteiten die belast zijn met de controle aan de buitengrenzen van België of van een andere lidstaat met het oog op*" de in de nummers a) tot d) vermelden doeleinden – maar anderzijds ook een ten 14°, met name de federale en lokale politiediensten "*om op het grondgebied van het Koninkrijk toe te zien op de naleving van de wettelijke bepalingen betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen en om de vereiste maatregelen te nemen ter uitvoering van die bepalingen*". Onder de overheden "*die belast zijn met de controle aan de buitengrenzen van België of van een andere lidstaat"* behoren, volgens de toelichting, de luchtvaartpolitie, de scheepvaartpolitie en de spoorwegpolitie van de federale politie, terwijl diezelfde toelichting bij de diensten van de federale en lokale politie nogmaals de drie voormelde gespecialiseerde eenheden van de federale politie vermeldt. Deze twee bepalingen lijken aldus (minstens gedeeltelijk) dubbel gebruik uit te maken.

17. Bij de potentiële ontvangers worden in het ten 22° ook de federale ombudsmannen voorzien. In de toelichting staat hieromtrent te lezen dat deze met name "*als opdracht* (hebben) *om de klachten van de burgers met betrekking tot de handelingen en de werking van de federale administratieve overheden te onderzoeken en om, op verzoek van de Kamer van Volksvertegenwoordigers, elk onderzoek in verband met de werking van de federale administratieve overheden uit te voeren. De Dienst Vreemdelingenzaken maakt deel uit van die "federale administratieve diensten" [Wet van 22 maart 1995 tot instelling van federale ombudsmannen]*.

Het Controleorgaan stelt daarentegen vast dat het zelf niet werd opgenomen bij de instellingen die persoonsgegevens van de DVZ kunnen ontvangen of beter aan wie de DVZ

persoonsgegevens kan meedelen. Het Controleorgaan kan als onafhankelijke toezichthouder ook niet beschouwd worden als een "*Belgische politionele of gerechtelijke overheid*" in de zin van het ten 36° van het ontworpen artikel 11 §1. Nochtans gebeurt er in de praktijk heel wat communicatie van persoonsgegevens over en weer tussen het Controleorgaan en de DVZ in het kader van de verzoeken tot rechtstreekse (bij de DVZ) of onrechtstreekse toegang (bij het Controleorgaan). Wanneer het voorwerp van het verzoek een zgn. artikel 24 van de SIS II verordening[9] (zie hoger) is, worden dergelijke verzoeken zeer regelmatig ook bij het COC ingediend die ze dan overmaakt aan DVZ; ook omgekeerd gebeurt het dat het COC een verzoek ontvangt dat initieel is binnengekomen bij de DVZ, maar dat na onderzoek betrekking heeft op een signalering om een andere reden dan een inreisverbod. De onderlinge samenwerking tussen de DVZ, de GBA en het COC werd overigens ook overeen gekomen en op punt gesteld op en tijdens een overleg tussen de DVZ, het COC en de GBA op een vergadering van 27 juni 2019 bij het Controleorgaan. Wanneer het voorwerp van het verzoek een zgn. 'artikel 24 *Entry ban*" verzoek is maakt het COC die voor verdere behandeling over aan de DVZ conform voormelde afspraken.

18. Die communicatie moet evident mogelijk blijven zodat het aangewezen is ook het Controleorgaan op de politionele informatie, die, net zoals de federale ombudsmannen, een dotatie gerechtigde instelling van het federale parlement is en de dataprotectie autoriteit en toezichthouder van onder meer de GPI, ook op te nemen bij de gerechtigde ontvangers van persoonsgegevens van de DVZ. Ook wanneer zou geargumenteerd worden dat het COC zou vallen onder de toepassing van het ontworpen artikel 28 e.v. lijkt dit geen oplossing te bieden nu het daar lijkt te gaan om een werkelijk toegang (na machtiging door de bevoegde Minister) tot de gegevensbanken van de DVZ, wat voor het COC niet aan de orde is en ook niet wordt gevraagd.

[9] Verordening (EG) nr. 1987/2006 van het Europees Parlement en de Raad van 20 december 2006 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II). Deze Verordening en ook het Besluit 2007/533/JBZ van de Raad van 12 juni 2007 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) zullen worden vervangen door de Verordening (EU) 2018/1860 van het Europees Parlement en de Raad van 28 november 2018 betreffende het gebruik van het Schengeninformatiesysteem voor de terugkeer van illegaal verblijvende onderdanen van derde landen, de Verordening (EU) 2018/1861 van het Europees Parlement en de Raad van 28 november 2018 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van grenscontroles, tot wijziging van de Overeenkomst ter uitvoering van het Akkoord van Schengen en tot wijziging en intrekking van Verordening (EG) nr. 1987/2006 en de Verordening (EU) 2018/1862 van het Europees Parlement en de Raad van 28 november 2018 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van politiële en justitiële samenwerking in strafzaken, tot wijziging en intrekking van Besluit 2007/533/JBZ van de Raad en tot intrekking van Verordening (EG) nr. 1986/2006 van het Europees Parlement en de Raad en Besluit 2010/261/EU van de Commissie.

De vraag stelt zich tot slot of ook voor het Vast Comité van Toezicht op de Inlichtingendiensten (Comité I) en de Gegevensbeschermingsautoriteit (GBA) niet dezelfde opmerking moet gemaakt worden.

3. De toegang tot de loggings

19. Het ontworpen artikel 36 voorziet in een beperkte toegang tot de in artikel 32 en 33 bedoelde loggings (of registraties van een aantal metadata). Het lijkt niet de bedoeling te zijn de toegang tot de loggings onmogelijk te maken voor de politiediensten en de gerechtelijke overheden, wat ook blijkt uit de toelichting waar wordt gesteld dat "*Volgens de aanbevelingen van het Agence nationale de la sécurité des systèmes d'information het gemachtigd personeel, enerzijds,* (moet) *onderworpen worden aan bijzondere vertrouwelijkheidsverplichtingen en mag het deze informatie enkel in beperkte gevallen in verband met de technische werking of de veiligheid van de systemen onthullen, en mag het, anderzijds, aan geen enkele dwang worden onderworpen met betrekking tot de onthulling van informatie, tenzij de wet iets anders voorziet (bijvoorbeeld in het geval van een gerechtelijke procedure[10])*".

Het spreekt inderdaad voor zich dat de loggings toegankelijk moeten zijn voor politie en justitie in het kader van hun wettelijke opdrachten. Het verdient dan ook aanbeveling het artikel 36 te beginnen met de zinssnede "*Behoudens wettelijke uitzonderingen mogen, met het oog op de doeleinden …*". Op die manier is helder dat dit ontworpen artikel 36 geen afbreuk doet aan de wettelijke bepalingen van bijvoorbeeld het Wetboek van Strafvordering of de bijzondere strafwetten en de onderzoeksbevoegdheden van de politie.

De bedoeling moet hoe dan ook zijn dat er loggings worden bijgehouden zowel op het niveau van de DVZ als op het niveau van het N.SIS II die toegankelijk zijn voor politie en justitie. Zo niet zou de politie wel kunnen achterhalen dat de DVZ een consultatie of verwerking heeft gedaan in de N.SIS.II maar niet wie binnen de DVZ de verwerking heeft gedaan; dat moet evident vermeden worden.

OM DEZE REDENEN,

[10] Eigen onderlijning.

Het Controleorgaan op de politionele informatie

verzoekt de aanvrager gevolg te geven aan de hogervermelde opmerkingen en aanbevelingen.

Advies goedgekeurd door het Controleorgaan op de Politionele Informatie op 14 juli 2022.

Voor het Controleorgaan,
De voorzitter,
(get.) Philippe ARNOULD

1

ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
/	DA220021		14.7.2022

Objet : Avis relatif à un avant-projet de loi relatif aux traitements de données à caractère personnel par la Direction générale Office des étrangers du Service public fédéral Intérieur

L'Organe de contrôle de l'information policière (ci-après le 'COC' ou 'l'Organe de contrôle').

Vu la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (M.B. du 5 septembre 2018, ci-après 'la LPD'), en particulier l'article 59 §1er, 2e alinéa, l'article 71 et le Titre VII, en particulier l'article 236.

Vu la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après 'la LAPD').

Vu la loi du 5 août 1992 sur la fonction de police (ci-après 'la LFP').

Vu la *Law Enforcement Directive* 2016/680 du 27 avril 2016 (ci-après 'la *LED*').

Vu la demande adressée le 9 juin 2022 par le Secrétaire d'État à l'Asile et à la Migration à l'Autorité de protection des données (ci-après : 'APD') en vue d'émettre un avis sur l'avant-projet de loi relatif aux traitements de données à caractère personnel par la Direction générale Office des étrangers du Service public fédéral Intérieur (ci-après 'l'avant-projet') ;

Vu la transmission de la demande susmentionnée, en date du 9 juin 2022, par l'APD à l'Organe de contrôle dans le cadre de la fonction de guichet unique de l'APD (article 54/1 de la LAPD) et conformément aux dispositions du protocole de coopération entre les autorités de contrôle fédérales belges en matière de protection des données (cf. www.organedecontrole.be).

Vu le rapport de Monsieur Frank Schuermans, membre-conseiller de l'Organe de contrôle.

Émet, le 14 juillet 2022, l'avis suivant.

...

I. Remarque préalable concernant la compétence de l'Organe de contrôle

1. À la lumière respectivement de l'application et de la transposition du Règlement 2016/679[1] et de la Directive 2016/680[2], le législateur a remanié en profondeur les tâches et missions de l'Organe de contrôle. L'article 4 §2, quatrième alinéa de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après 'la LAPD') dispose qu'à l'égard des services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle. Cela signifie notamment que l'Organe de contrôle est compétent également lorsque des services de police traitent des données à caractère personnel qui ne relèvent pas des missions de police administrative et judiciaire, par exemple dans le cadre de finalités socioéconomiques ou de traitements relevant de la gestion des ressources humaines. L'Organe de contrôle doit être consulté lors de la préparation de la législation ou d'une mesure réglementaire ayant trait au traitement de données à caractère personnel par les services de police de la police intégrée (voir les articles 59 §1er, 2e alinéa et 236 §2 de la LPD, l'article 36.4 du RGPD et l'article 28.2 de la directive Police-Justice ou *LED*). L'Organe de contrôle a dans ce contexte pour mission d'examiner si l'activité de traitement projetée par les services de police est conforme aux dispositions du Titre 1er (pour les traitements non opérationnels)[3] et du Titre 2 (pour les traitements opérationnels) de la LPD[4]. De plus, le COC est aussi chargé d'émettre des avis d'initiative, comme prévu à l'article 236 §2 de la LPD, et est investi conformément à l'article 240 de la LPD d'une mission générale d'information à l'égard du grand public, des personnes concernées, des responsables du traitement et des sous-traitants dans le domaine du droit à la protection des données et à la protection de la vie privée.

2. En ce qui concerne en particulier les activités de traitement dans le cadre des missions de police administrative et/ou judiciaire, l'Organe de contrôle émet dès lors des avis soit

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données ou « RGPD »).
[2] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après dénommée « directive Police-Justice » ou *Law Enforcement Directive* (*LED*)).
[3] Article 4 §2, 4e alinéa de la LPD.
[4] Article 71 §1er, 3e alinéa de la LPD.

d'initiative, soit à la demande du Gouvernement ou de la Chambre des Représentants, d'une autorité administrative ou judiciaire ou d'un service de police, concernant toute matière ayant trait à la gestion de l'information policière telle que régie par la Section 12 du Chapitre 4 de la loi sur la fonction de police[5].

3. Par ailleurs, l'Organe de contrôle est également chargé, à l'égard des services de police, de l'inspection générale de la police fédérale et de la police locale (en abrégé 'AIG'), telle que visée dans la loi du 15 mai 2007 sur l'Inspection générale, et de l'Unité d'information des passagers (ci-après dénommée en abrégé 'BELPIU') visée au Chapitre 7 de la loi du 25 décembre 2016, de la surveillance de l'application du Titre 2 de la LPD et/ou du traitement de données à caractère personnel tel que visé aux articles 44/1 à 44/11/13 de la loi sur la fonction de police, et/ou de toute autre mission qui lui est confiée en vertu ou par d'autres lois[6].

4. Enfin, l'Organe de contrôle est compétent à l'égard du Service Contentieux de l'Administration générale des Douanes et Accises en ce qui concerne les réquisitions adressées par ce service à la BELPIU dans des matières fiscales, et ce en vertu de l'article 281 §4 de la loi générale sur les douanes et accises du 18 juillet 1977, telle que modifiée par la loi du 2 mai 2019 modifiant diverses dispositions relatives au traitement des données des passagers.

II. Objet de la demande

5. La demande d'avis a trait à un avant-projet de loi relatif aux traitements de données à caractère personnel par la Direction générale Office des étrangers du Service public fédéral Intérieur.

6. Les autorités et les traitements de données à caractère personnel et d'informations pour lesquels le COC est exclusivement compétent sont strictement définis par la loi. En conséquence, l'Organe de contrôle limite ses avis aux traitements relevant de sa compétence, en l'occurrence dans le cas présent ceux qui sont effectués par les services de police ou qui ont un impact sur le fonctionnement des services de police. En l'occurrence, le Secrétaire d'État qui a formulé la demande a également coché les services de police en réponse à la

[5] Articles 59 §1er, 2e alinéa et 236 §2 de la LPD.
[6] Article 71 §1er, troisième alinéa juncto article 236 §3 de la LPD.

question de savoir si *« le projet a trait à ou implique un (des) traitement(s) de données à caractère personnel par une ou plusieurs des autorités suivantes »*.

Quoi qu'il en soit, les avis du COC ne se limitent pas nécessairement à l'éventuel article ou aux éventuels articles mentionnés dans une demande d'avis. Le COC tient en effet toujours compte de tous les éléments et dispositions relevant de sa compétence en vertu de la réglementation susmentionnée. De plus, l'Organe de contrôle n'est pas seulement une autorité de protection des données, mais est aussi chargé du contrôle et de la surveillance des banques de données policières[7] et de tous les traitements policiers, également en termes de légalité, d'efficacité et d'effectivité. Ces éléments (par exemple la faisabilité opérationnelle et la capacité) sont toujours pris en compte lors de la formulation d'un avis.

III. Analyse de la demande

7. Le COC se limite dans le présent avis aux articles qui ont un impact sur le fonctionnement des services de la police intégrée (ci-après 'la GPI') ou sur le fonctionnement de l'Organe de contrôle.

1. Les traitements dans la Banque de données Nationale Générale et dans le Système d'Information Schengen

8. Le projet d'article 10 prévoit les finalités pour lesquelles les données à caractère personnel peuvent être traitées par l'Office des étrangers (ci-après 'l'OE'). Les catégories de données à caractère personnel visées à l'article 6 peuvent être traitées notamment pour la finalité prévue au point 11°, à savoir pour *« assurer le suivi des interdictions d'entrée, en ce compris leur levée ou leur suspension ainsi que la gestion de leur enregistrement dans le Système d'Information Schengen et dans la Banque de données Nationale Générale ou dans toute autre banque de données nationale »*. L'exposé des motifs stipule pour le projet d'article 9 que *« … l'Office des étrangers doit pouvoir traiter les données à caractère personnel de cette catégorie de personnes concernées afin de pouvoir assurer le suivi des décisions d'interdiction d'entrée, la gestion de l'enregistrement de ces interdictions d'entrée dans le SIS et/ou dans la BNG* (soulignement propre) *ainsi que traiter les demandes de suspension ou de levée de*

[7] Voir aussi le rapport d'activité 2020 du COC, https://www.organedecontrole.be/files/Rapport-dactivit%C3%A9_COC_2020_F.pdf, points 7 et 8.

ces décisions ». Un alinéa similaire est mentionné dans le commentaire relatif à l'article 10 (*« assurer le suivi des interdictions d'entrée »*).

L'avant-projet fait donc en sorte que **pour la première fois, ne serait-ce qu'implicitement**, une disposition légale prévoit qu'un 'service non policier', à savoir l'OE, puisse traiter des données dans une banque de données **policière** nationale et dans une banque de données **policière** internationale. On entend donc en l'occurrence par « traitement » la saisie effective de données et tous les actes apparentés, comme la modification, la rectification, l'effacement, etc., et donc pas uniquement la 'consultation'. Les membres du personnel de l'OE seraient donc autorisés à effectuer plusieurs fois des traitements dans la BNG concernant une même personne (par exemple en fonction de son statut de séjour).

À ce jour, aucune disposition légale ne prévoit pour l'OE (ni d'ailleurs pour quelque autre administration, organe ou institution tierce) la possibilité d'effectuer ces traitements dans la BNG ou dans une autre banque de données policière. Jusqu'ici, l'OE pouvait uniquement obtenir communication d'informations et données à caractère personnel de la BNG (cf. articles 44/11/4 et suivants et plus précisément l'article 44/11/9 §1er, 2° et l'article 44/11/12 §1er, 2° de la LFP). Ces traitements au bénéfice de l'OE ne sont d'ailleurs actuellement pas effectués par l'OE lui-même, mais toujours par la GPI (à la demande de l'OE, voir aussi le point 15). Modifier cette situation en permettant à une administration, un organe ou une institution tierce d'effectuer soi-même les traitements intrusifs visés ici sous toutes leurs facettes constitue dès lors un précédent important dont l'objectif ne saurait être qu'il ouvre la voie à d'autres modifications similaires, à moins qu'une motivation spécifique ne le justifie.

Il est en outre encore plus important de créer une base légale claire – en en motivant suffisamment la nécessité – pour permettre à l'OE d'effectuer de manière autonome ces traitements dans des banques de données policières comme la BNG. Cela signifie en tout cas que la loi sur la fonction de police doit être amendée en ce sens, et plus particulièrement la section 12 (*« De la gestion des informations »*) du Chapitre IV (*« De la forme et des conditions générales d'exercice des missions »*) en y créant, de préférence dans un article distinct, la base légale permettant à l'OE d'effectuer les traitements visés dans le projet d'article 10, 11° de l'avant-projet de loi (*« … le suivi des interdictions d'entrée, en ce compris leur levée ou leur suspension ainsi que **la gestion de leur enregistrement** dans le Système d'Information Schengen et dans la Banque de données nationale générale ou dans toute autre banque de données nationale »*). De plus, cette modification indispensable de la LFP

devra au préalable être soumise pour avis à l'Organe de contrôle en vertu de l'article 59 §1er, 2e alinéa de la LPD.

9. En ce qui concerne la BNG, les responsables du traitement sont les ministres de l'Intérieur et de la Justice et les responsables opérationnels sont les services de police. L'Organe de contrôle n'a pas été en mesure d'établir si le ministre de la Justice, en sa qualité de coresponsable du traitement, est au courant de la possibilité qui est ici créée de permettre à l'OE d'effectuer directement les traitements les plus intrusifs dans la BNG ; en marge de l'évidente nécessité d'impliquer le ministre de la Justice en sa qualité de coresponsable du traitement, il semble que d'un point de vue formel, le ministre de la Justice doive également cosigner l'avant-projet étant donné qu'il touche directement à une législation relevant de ses attributions.

10. Il n'est évidemment pas sans danger ni sans risque d'autoriser une administration comme l'OE à effectuer directement dans la BNG des traitements qui vont beaucoup plus loin que la seule consultation. L'avant-projet n'approfondit nullement cet aspect essentiel et ne motive pas non plus la nécessité pour l'OE d'obtenir cette compétence et ces possibilités, peut-être aussi pour que l'ancrage légal ne soit qu'implicite et indirect, et donc insuffisant. Comment ces possibilités seront-elles organisées dans la pratique ? Quels mécanismes de contrôle sont prévus ? Qui au sein de l'OE aura accès à la BNG ? À quelles applications de la BNG l'OE pourra-t-il accéder ? Quelle formation sera prévue pour le personnel de l'OE ? Etc.

Autrement dit, les modalités concrètes devront être reprises dans une réglementation. Une possibilité serait de mettre ce système en œuvre dans l'arrêté royal existant du 28 avril 2016 relatif à l'interrogation directe de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police par les membres du personnel désignés de l'Office des étrangers (M.B. 12 mai 2016), qui aurait d'ailleurs de toute façon dû depuis longtemps ou devrait être adapté en fonction du nouveau cadre juridique de la protection des données[8] qui est d'application depuis 2018. En vertu de cet arrêté royal, certains membres du personnel de l'OE disposent actuellement uniquement d'une possibilité 'd'interrogation directe' de la BNG, ce qui va donc beaucoup moins loin que la possibilité d'effectuer effectivement des saisies de données, d'établir et de saisir des signalements, d'apporter des corrections et des modifications, etc. L'arrêté royal devra donc être remanié en profondeur à la lumière de cet avant-projet de loi et du fondement juridique qui devra nécessairement être créé dans la LFP

[8] L'arrêté royal fait notamment encore référence à l'ancienne Commission de la protection de la vie privée (art. 1, 8°, art. 5) et à un *« conseiller en sécurité et en protection de la vie privée »* (art. 5), le COC n'était à l'époque pas encore une autorité de protection des données, ce qu'il est dans l'intervalle évidemment devenu à l'égard de la GPI, etc.

(voir le point 8). De plus, cette modification de l'arrêté royal devra elle aussi être soumise pour avis à l'Organe de contrôle en vertu de l'article 59 §1er, 2e alinéa de la LPD.

Par ailleurs, l'Organe de contrôle ne voit pas clairement ce que le projet d'article 10, 11° entend par *« ou dans toute autre banque de données nationale »* (la version néerlandaise ne dit d'ailleurs pas tout à fait la même chose puisque l'on y trouve la formulation *« of in **een** andere nationale gegevensbank »*). L'exposé des motifs ne fournit lui non plus aucune précision à ce sujet. Le COC ne voit pas de quelle autre banque de données nationale il pourrait potentiellement s'agir, de sorte qu'il n'y a aucune raison de maintenir cette partie de la phrase vu qu'il ne peut s'agir que de la BNG qui est déjà citée.

11. En outre, l'arrêté royal fait également mention d'un protocole entre l'OE et *« la direction qui gère les accès à la B.N.G. »* (dans les faits, il s'agit de la DRI, la Direction de l'information policière et des moyens ICT de la police fédérale (une direction faisant partie du Commissariat général). Ce protocole du 29 septembre 2016 devra lui aussi être remanié pour la même raison que celle que nous évoquions plus haut, à savoir la nécessité de l'adapter en fonction du nouveau cadre de la protection des données, et compte tenu des possibilités de traitement étendues que l'avant-projet a l'intention d'offrir à l'OE. Cette modification du protocole devra elle aussi être soumise au préalable non seulement à l'Autorité de protection des données, mais aussi à l'Organe de contrôle (cf. article 6 de l'arrêté royal du 28 avril 2016). Les questions qu'il faudra dans ce contexte se poser porteront notamment, mais sans s'y limiter, sur les aspects suivants :

- la portée de l'enquête de milieu et des antécédents (voir aussi le point 2 du protocole d'accord entre l'OE et la DRI) dont les membres du personnel de l'OE doivent actuellement faire l'objet avant d'être autorisés à interroger directement la BNG ; à l'heure actuelle, seul un avis de sécurité au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (art. 22quinquies) est requis. Un avis de sécurité positif ponctuel suffira-t-il encore à l'avenir ?

- le profil exact du collaborateur de l'OE. Ces profils ne doivent-ils pas être réexaminés à présent que le collaborateur de l'OE se verra attribuer des compétences qui vont beaucoup plus loin qu'aujourd'hui, où il peut seulement obtenir communication d'informations et de données à caractère personnel à travers l'interrogation directe (système *hit/no hit*) et n'a par exemple pas accès aux informations douces (voir aussi l'article 4, b) : uniquement les informations consignées dans des procès-verbaux) ? Comment peut-on éviter que le

collaborateur de l'OE prenne connaissance de toutes les informations douces disponibles à partir du moment où il obtient un profil lui permettant de saisir des données ?

- *quid* du télétravail prévu pour les membres du personnel de l'OE (voir le point 4.1 du protocole d'accord) ?

- un audit de fonctionnement tous les deux ans est-il suffisant (voir le point 5 du protocole d'accord) ?

- quelle formation concrète va-t-on devoir prévoir pour le collaborateur de l'OE ? Il va de soi que cette formation devra être beaucoup plus poussée et plus intensive que celle qui est prévue actuellement (voir le point 6 du protocole d'accord) pour l'interrogation directe.

- etc.

12. Le protocole parle encore aussi d'un *« document ad hoc distinct »* reprenant les aspects techniques de l'interrogation directe. Le COC n'a pas encore connaissance de ce document mais le demandera en tout état de cause à la DRI lorsque cet avant-projet sera en passe de devenir une loi. Le protocole d'accord prévoit d'ailleurs lui-même sa révision en son point 10, *« à tout le moins, dans les cas suivants :*

- *modification du cadre légal ou réglementaire :*
- *… ;*
- *émergence de besoins supplémentaire ;*
- *… »*

Ce protocole d'accord aurait donc en réalité déjà dû être revu à la lumière de la modification du cadre juridique de la protection des données en 2018, et ce sera encore davantage le cas si cet avant-projet devient une loi.

13. D'un autre côté, le responsable du traitement de la partie nationale de la banque de données SIS II n'a jamais été identifié dans une loi ou dans un arrêté d'exécution, ce qui pose d'ailleurs toujours un problème juridique à ce jour. À cet égard, il convient de faire référence à une enquête de contrôle que le COC a menée en 2019 en collaboration avec l'APD et qui a conduit à l'établissement le 2 février 2020 d'un rapport intitulé *« Rapport final de la visite de contrôle du bureau SIRENE (Système d'Information Schengen) par l'Organe de contrôle de l'information policière et par l'Autorité de protection des données »*. Ce rapport transmis au commissaire général de la police fédérale et au directeur de CGI contient notamment les constatations suivantes :

6.1.1.1. Première observation générale : Les instances responsables pour le bureau SIRENE et l'Office N.SIS II n'ont pas été désignées dans le droit belge

56. En 2019, aucune réglementation n'a encore transposé la Décision SIS II en droit belge.

De même, aucun texte légal belge ne complète les règles Schengen (*ci-après la remarque de CGI suite à la remise du rapport intermédiaire de visite : « Point 56 de la page 16/60 : (idem constatation A1 à la page 50) à nuancer ; la Décision SIS II produit ses effets directement sur l'ordre juridique interne, de sorte qu'une transposition en tant que telle de l'intégralité de la décision en droit belge n'est pas nécessaire (voir aussi l'analyse du SPF Intérieur lors de l'entrée en vigueur de la Décision SIS II). Les principes opérationnels ont toutefois été transposés dans la fiche C22 de la directive ministérielle MFO-3. Si une modification légale s'impose dans le sillage de la directive européenne 680/2016 qui a été transposée par la loi nationale du 30/07/2018, les adaptations requises auraient dû être apportées par la loi du 22/07/2019, ce qui n'est pas le cas. Dans l'intervalle, il a été constaté que l'article 26, 8° de la loi 30/07/2018 doit être modifié pour permettre de désigner les ministres compétents en tant que responsables du traitement et de l'exécution de la directive européenne. Les autorités politiques en ont été informées au préalable. »*) qui laissent aux législateurs nationaux le soin de régler certaines questions. C'est le cas par exemple dans la Décision SIS II et dans le Règlement SIS II pour les délais de conservation concernant les signalements et les informations traitées par le bureau SIRENE : rien n'est explicitement prévu sur ces questions au niveau belge.

Les autorités de contrôle ont constaté que la Décision SIS II et le Règlement SIS II, malgré qu'ils soient d'application directe en droit belge et ne demandent par conséquent pas de transposition en tant que telle, renvoient pour certains points au droit national. Ces renvois doivent trouver une réponse en droit belge, ce qui n'est pas le cas au jour de la rédaction du présent rapport puisque certaines questions, comme les délais de conservation à appliquer à certains types de signalements ou encore la désignation du bureau SIRENE et de l'Office N.SIS II, ne sont pas réglées en droit belge. Cette remarque de CGI ne modifie donc pas la constatation des autorités de contrôle.

57. Ce constat est le même pour la désignation des instances responsables pour le bureau SIRENE et l'Office N.SIS II (Décision SIS II et Règlement SIS II, articles 6 et 7 communs). En effet, la Belgique doit désigner un Office N.SIS II qui assume la responsabilité centrale du N.SIS II. Cette instance est responsable du bon fonctionnement et de la sécurité du N.SIS II, elle doit faire en sorte que les autorités compétentes aient accès au SIS II mais aussi prendre les mesures nécessaires pour assurer le respect des dispositions de la Décision SIS II et du Règlement SIS II.

58. La Belgique doit également désigner une instance – le bureau SIRENE – chargée de l'échange de toutes les informations supplémentaires et de vérifier la qualité des informations introduites dans le SIS II. Pour cela, le bureau SIRENE doit avoir accès aux données traitées dans le SIS II.

59. Ces instances ne sont pas identifiées dans le droit belge. En effet, l'arrêté royal du 14 novembre 2006 (*Arrêté royal du 14 novembre 2006 relatif à l'organisation et aux compétences de la police fédérale, articles 2, 1°, e) et 6, 3°*) qui attribue la détermination des normes et d'une approche standardisée en matière de sécurité de l'information et de protection de la vie privée au Commissariat général, et qui confie entre autres la préparation de la politique et des règles relatives au traitement de l'information policière à la Direction générale de la gestion des ressources de l'information (« DGR ») de la police fédérale, le tout en concertation avec la Commission permanente de la police locale, ne constitue pas une base suffisamment claire et précise d'identification des instances responsables pour le bureau SIRENE et l'Office N.SIS II.

60. Cela oblige les autorités de contrôle à constater que dès lors l'exercice concret, correct et efficace des missions qui incombent à ces instances responsables peut difficilement être mis en œuvre.

61. *De facto*, le bureau SIRENE est installé sous CGI et s'occupe de la gestion des signalements ainsi que de l'échange des informations supplémentaires. DRI met pour sa part à disposition du bureau SIRENE les outils nécessaires au traitement des signalements Schengen : DRI gère le fonctionnement et la sécurité de la copie nationale du N.SIS II dont a besoin le bureau SIRENE pour travailler avec le SIS II.

62. La note de politique générale de sécurité de l'information SIS II approuvée par les Ministres de l'Intérieur et de la Justice le 18 octobre 2016 a pour objectif de *« définir un cadre pour la mise en œuvre d'un ensemble approprié de mesures pour assurer la sécurité de la copie nationale du N.SIS II et des systèmes d'information des services de police nécessaires au fonctionnement du SIS II »*. L'objectif de cette note est de garantir la confidentialité, l'intégrité et la disponibilité des informations traitées dans ces systèmes d'information.

En matière de sécurité, la note partage les responsabilités fonctionnelles et techniques : CGI détermine les objectifs du plan de sécurité pour le SIS II et est donc responsable pour le N.SIS II et le bureau SIRENE, quant à DRI, elle détermine les objectifs de sécurité et met en place les mesures techniques de sécurité pour les différents systèmes d'information.

63. De leurs rencontres avec les *DPO* de CGI et de DRI, les autorités de contrôle ont constaté que si les deux Directions de la police fédérale s'accordent pour considérer que les Ministres de la Justice et de l'Intérieur sont responsables du traitement pour la copie nationale du N.SIS II, le *DPO* de DRI indique que DRI n'est pas responsable pour l'Office N.SIS II tandis que le *DPO* de CGI estime que CGI est l'instance responsable pour le bureau SIRENE et qu'elle partage une responsabilité avec DRI (selon CGI, DRI s'occuperait des aspects techniques et logistiques tandis que CGI assumerait les tâches opérationnelles) en ce qui concerne le N.SIS II.

64. La vision du *DPO* de CGI va dans le même sens que ce qui est indiqué dans la note de politique générale de sécurité de l'information SIS II approuvée le 18 octobre 2016.

> **65**. Cependant, la Belgique doit communiquer chaque année (*ces Directions sont ainsi désignées depuis 2015 au Journal Officiel de l'Union européenne. Avant cela, les anciennes Direction de la télématique pour le SIS II et Direction de l'information policière opérationnelle pour le bureau SIRENE étaient désignées*) au gestionnaire fonctionnel du SIS II, conformément à la Décision SIS II et au Règlement SIS II *(Règlement SIS II et Décision SIS II, article 7 §3 commun)*, les coordonnées de son Office N.SIS II ainsi que de son bureau SIRENE. Elle s'y est dernièrement conformée en indiquant que pour le N.SIS II, l'autorité responsable est « le Bureau N.SIS II de la police fédérale – DRI » et que pour le bureau SIRENE, il s'agit de la « Commission SIRENE de la police fédérale – CGI (*Liste des offices N.SIS II et des bureaux SIRENE nationaux » consolidée au 15 mars 2019, J.L.O., C222, 2 juillet 2019, p. 173.*) ».
> **66**. Ainsi, tandis que la Décision SIS II et le Règlement SIS II nécessitent, pour la bonne alimentation du SIS II, une coopération soutenue et une communication fluide entre deux instances désignées responsables au niveau national, cela est difficilement possible au niveau belge sans désignation claire puisque cette coopération et cette communication se jouent *de facto* entre deux Directions différentes qui ne se situent pas au même niveau hiérarchique (*ci-après la remarque de CGI suite à la remise du rapport intermédiaire de visite : « Point 66. CGI ne fait pas partie du commissariat général mais est une direction spécifique (voir l'arrêté royal du 14 novembre 2006). » L'Organe de contrôle se réfère à l'article 3, 1° de l'arrêté royal du 14 novembre 2006 relatif à l'organisation et aux compétences de la police fédérale qui indique que le Commissariat général se compose de la Direction de la coopération policière internationale. Cette remarque de CGI ne modifie donc pas la constatation des autorités de contrôle)* de la police intégrée et structurée à deux niveaux telle qu'elle est instituée en Belgique. En effet, d'une part le bureau SIRENE est installé au sein du Single Point of Operational Contact de CGI qui fait partie du Commissariat général de la police fédérale et d'autre part, DRI fait partie de la DGR.
> **67**. Vu l'absence de désignation claire des deux instances responsables dans le droit belge et eu égard aux positions contradictoires de CGI et DRI, les autorités de contrôle considèrent que la communication officielle de la Belgique au gestionnaire fonctionnel du SIS II, telle qu'elle a encore été récemment inscrite au Journal Officiel de l'Union européenne du 2 juillet 2019, constitue une désignation de CGI et de DRI comme autorités responsables, respectivement pour le bureau SIRENE et pour le N.SIS II.
> **68**. D'emblée, les autorités de contrôle insistent sur le fait que la répartition des tâches de mise à jour, de gestion des signalements et des responsabilités telle qu'elle est prévue dans le Règlement SIS II et la Décision SIS II invite l'Office N.SIS II – DRI et le bureau SIRENE – CGI à travailler étroitement ensemble pour que l'alimentation du SIS II fonctionne plus efficacement.

14. Il va de soi que le problème se fait encore plus cuisant à partir du moment où l'OE est à présent investi d'une responsabilité (partagée) à l'égard des aspects visés par le projet d'article 10, 11° de l'avant-projet, à savoir *« le suivi des interdictions d'entrée, en ce compris leur levée ou leur suspension ainsi que la gestion de leur enregistrement dans le Système d'Information Schengen et dans la Banque de données nationale générale ou dans toute autre banque de données nationale ».*

Il semble donc indispensable de remédier à ce problème posé par l'absence, dans la LFP, d'un fondement juridique clair et d'une désignation des responsables du traitement et des responsables opérationnels du Système d'Information Schengen, et de faire la clarté sur ce point.

15. La problématique des signalements reposant sur l'article 24 du Règlement SIS II a également été abordée dans le cadre de l'enquête susmentionnée de l'APD et du COC. La constatation suivante a été formulée à ce sujet :

> **138**. Certains autres partenaires externes comme l'ODE, le Ministère des affaires étrangères et la Direction de l'Immatriculation des véhicules (*« Liste des autorités compétentes autorisées à consulter directement les données introduites dans le système d'information Schengen de deuxième génération », J.O.L. C222, 2 juillet 2019, p. 1*.) ont également accès via l'application Portal ou un webservice. Le service des Douanes n'a pour l'instant aucun accès.

139. Les protocoles avec l'ODE sont en cours d'élaboration. Il existe cependant une procédure tacite applicable depuis un certain nombre d'années : les signalements visés à l'article 24 du Règlement SIS II sont introduits dans le SIS II sur base d'un formulaire standard communiqué par l'ODE et sans pièces justificatives c'est-à-dire que la décision ayant motivé le signalement n'est pas jointe. De même, les signalements sont automatiquement renouvelés jusqu'à l'échéance de la décision de l'ODE. Par ailleurs, le *Legal Office* déclare que la révision de la Directive « retour » (Directive 2008/115/CE du Parlement européen et du Conseil du 16 décembre 2008 relative aux normes et procédures communes applicables dans les États membres au retour des ressortissants de pays tiers en séjour irrégulier) devrait accroître exponentiellement le nombre de signalements. Dès lors, le protocole en projet vise à fournir à l'ODE une possibilité d'alimentation directe du N.SIS II (ci-après la remarque de CGI suite à la remise du rapport intermédiaire de visite *(« Point 139 de la page 32/60 : il n'y a qu'un seul protocole en vigueur avec l'OE concernant la décision SIS II. La dernière phrase n'est pas correcte ; le protocole actuellement en vigueur vise à officialiser la collaboration actuelle entre la police et l'OE. Si l'alimentation directe du N.SIS II (par ex. en ce qui concerne les décisions de retour) est confirmée et déployée (ou en cas de modification de quelque autre méthode de travail), ce protocole devra être adapté en conséquence. » Dans la mesure où cet accès est envisagé, les autorités de contrôle invitent les autorités concernées à d'ores et déjà prévoir toutes les modalités dans le protocole et à procéder à une analyse complète du respect des règles en matière de protection des données. Cette remarque de CGI ne modifie donc pas la constatation des autorités de contrôle*).

Cette procédure qui s'est manifestement imposée tacitement dans la pratique et qui consiste à ce que la police (et plus précisément le bureau SIRENE de CGI/SPOC de la police fédérale) introduise les signalements pour l'OE (art. 24 du Règlement SIS II) devra donc être réexaminée à la lumière de l'avant-projet et du présent avis de l'Organe de contrôle. Déjà à l'époque, on envisageait manifestement déjà la possibilité de laisser l'OE introduire lui-même ses signalements dans le Système d'Information Schengen et il était question d'un projet de protocole. Le COC n'a pas connaissance d'un protocole définitif en la matière et il serait d'ailleurs difficile d'en conclure un sans une modification légale préalable, comme l'a à juste titre indiqué CGI dans sa réplique au projet de rapport du COC et de l'APD.

2. <u>Les destinataires des données communiquées par l'OE</u>

16. Le projet d'article 11 énumère en son paragraphe 1er les différents destinataires ou catégories de destinataires auxquels l'OE peut communiquer les données à caractère personnel qu'il collecte. Ce paragraphe prévoit d'une part un point 6° – à savoir les *« autorités chargées du contrôle aux frontières extérieures de la Belgique ou d'un autre État membre aux fins d'assurer »* les finalités visées aux points a) à d) – mais d'autre part aussi un point 14°, à savoir les services de police fédérale et de police locale *« pour veiller au respect sur le territoire du Royaume des dispositions légales relatives à l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et prendre les mesures requises en exécution de celles-ci »*. Parmi les autorités *« chargées du contrôle aux frontières extérieures de la Belgique ou d'un autre État membre »* figurent, selon l'exposé des motifs, la police aéronautique, la police de la navigation et la police des chemins de fer de la police fédérale, alors que ce même exposé des motifs mentionne encore une fois parmi les services de police

fédérale et de police locale ces trois unités spécialisées de la police fédérale. Ces deux dispositions semblent donc (du moins pour une part) faire double emploi.

17. Parmi les destinataires potentiels figurent également, au point 22°, les médiateurs fédéraux. L'exposé des motifs stipule à ce sujet que ceux-ci ont notamment *« pour missions d'examiner les réclamations des citoyens relatives aux actes et au fonctionnement des autorités administratives fédérales ainsi que de mener, à la demande de la Chambre des représentants, toute investigation sur le fonctionnement des services administratifs fédéraux. L'Office des étrangers fait partie de ces « services administratifs fédéraux » [Loi du 22 mars 1995 instaurant des médiateurs fédéraux]. »*.

L'Organe de contrôle constate par contre qu'il ne figure pour sa part pas parmi les institutions qui peuvent recevoir des données à caractère personnel de l'OE ou, mieux, auxquelles l'OE peut communiquer des données à caractère personnel. En sa qualité d'autorité de contrôle indépendante, l'Organe de contrôle ne peut pas non plus être considéré comme une *« autorité policière ou judiciaire belge »* au sens du point 36° du projet d'article 11, §1er. Dans la pratique, cependant, la communication de données à caractère personnel entre l'Organe de contrôle et l'OE est fréquente dans le cadre des demandes d'accès direct (auprès de l'OE) ou indirect (auprès de l'Organe de contrôle). Lorsque l'objet d'une demande est un article 24 du Règlement SIS II[9] (voir plus haut), de telles demandes sont aussi très régulièrement introduites auprès du COC, qui les transmet alors à l'OE ; à l'inverse, il arrive aussi que le COC reçoive une demande qui a initialement été introduite auprès de l'OE, mais qui s'avère après examen avoir trait à un signalement pour un autre motif qu'une interdiction d'entrée. La collaboration mutuelle entre l'OE, l'APD et le COC a d'ailleurs également été convenue et mise au point lors d'une concertation entre l'OE, le COC et l'APD organisée dans le cadre d'une réunion qui a eu lieu le 27 juin 2019 auprès de l'Organe de contrôle. Si l'objet

[9] Règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II). Ce Règlement et la Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) seront remplacés par le Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier, le Règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) n° 1987/2006 et le Règlement (EU) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) n° 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission.

d'une demande est un *« article 24 Entry ban »*, le COC transmet cette demande pour traitement à l'OE conformément aux conventions susmentionnées.

18. Cette communication doit évidemment rester possible, de sorte qu'il est indiqué de reprendre également l'Organe de contrôle de l'information policière parmi les destinataires légitimes des données à caractère personnel collectées par l'OE vu qu'il est, tout comme les médiateurs fédéraux, une institution ayant droit à une dotation du Parlement fédéral et l'autorité de protection des données et de contrôle notamment de la GPI. Même si l'on argumentait que le COC relèverait de l'application des articles 28 et suivants de l'avant-projet, cela ne semble pas apporter de solution étant donné qu'il semble s'agir là d'un accès effectif (après autorisation du ministre compétent) aux banques de données de l'OE, ce qui n'est pas à l'ordre du jour pour le COC et n'est d'ailleurs pas demandé.
Pour terminer, on peut se demander s'il ne faut pas formuler la même remarque pour le Comité permanent de contrôle des services de renseigenements (Comité R) et l'Autorité de protection des données (APD).

3. L'accès aux fichiers de journalisation

19. Le projet d'article 36 prévoit un accès limité aux fichiers de journalisation visés aux articles 32 et 33 (ou enregistrements d'un certain nombre de métadonnées). L'intention ne semble pas être de rendre l'accès aux fichiers de journalisation impossible pour les services de police et les autorités judiciaires, et l'exposé des motifs le confirme en précisant que *« selon les recommandations de l'Agence nationale de la sécurité des systèmes d'information, le personnel habilité doit, d'une part, être soumis à des obligations de confidentialité particulières et ne peut divulguer ces informations que dans des cas limités liés au fonctionnement technique ou à la sécurité des systèmes et, d'autre part, ne doit subir aucune contrainte quant au dévoilement des informations sauf si la loi en dispose autrement (par exemple, dans le cadre d'une procédure judiciaire[10]) »*.

Il va en effet de soi que les fichiers de journalisation doivent être accessibles pour la police et la justice dans le cadre de leurs missions légales. Il est donc indiqué de faire commencer l'article 36 par la formulation *« Sous réserve des exceptions légales, en vue des finalités … »*. De cette manière, il sera clair que ce projet d'article 36 ne porte pas préjudice aux dispositions

[10] Soulignement propre.

légales notamment du Code d'instruction criminelle ou des lois pénales spéciales, ni aux compétences d'investigation de la police.

Quoi qu'il en soit, l'objectif doit être de conserver tant au niveau de l'OE qu'au niveau du N.SIS II des fichiers de journalisation accessibles pour la police et la justice. Sans cela, la police pourrait savoir que l'OE a procédé à une consultation ou à un traitement dans le N.SIS II, mais sans pouvoir déterminer par qui au sein de l'OE ce traitement a été effectué, ce qui est bien sûr à éviter.

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

prie le demandeur de donner suite aux remarques et recommandations qui précèdent.

Avis approuvé par l'Organe de contrôle de l'information policière le 14 juillet 2022

Pour l'Organe de contrôle,
Le Président,
(s) Philippe ARNOULD

Comité Permanent de Contrôle
des services de renseignements et de sécurité
Vast Comité van Toezicht
op de inlichtingen- en veiligheidsdiensten

ADVIES nr. 003/VCI/2022 VAN 29 JUNI 2022

GEGEVENSBESCHERMING M.B.T. DE DIENST VREEMDELINGENZAKEN EN DOORGIFTE VAN PERSOONSGEGEVENS AAN VSSE EN ADIV

Gelet op het schrijven d.d. 9 juni 2022 van de Gegevensbeschermingsautoriteit (GBA) waarbij aan het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten een verzoek tot advies werd overgemaakt van de Staatssecretaris voor Asiel en Migratie met betrekking tot het voorontwerp van wet betreffende de verwerkingen van persoonsgegevens door de Algemene Dienst Vreemdelingenzaken van de Federale Overheidsdienst Binnenlandse Zaken (hierna: het wetsontwerp).

Bevoegdheid Vast Comité I

Gelet op artikel 33, achtste lid van de Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op. het Coördinatieorgaan voor de dreigingsanalyse;

Gelet op de artikelen 73, 95, 107, 128 van de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens;

Gelet op het Samenwerkingsprotocol van 24 november 2020 tussen de Belgische federale toezichthoudende autoriteiten op het vlak van dataprotectie.

AVIS n° 003/CPR/2022 DU 29 JUIN 2022

PROTECTION DES DONNÉES EN MATIÈRE DE TRANSFERT DE DONNÉES À CARACTÈRE PERSONNEL DE L'OFFICE DES ÉTRANGERS À LA VSSE ET AU SGRS

Vu le courrier du 9 juin 2022 de l'Autorité de protection des données (APD) par lequel a été transmise au Comité permanent de Contrôle des services de renseignement et de sécurité une demande d'avis du Secrétaire d'État à l'Asile et à la Migration concernant l'avant-projet de loi relatif aux traitements de données à caractère personnel par la Direction générale Office des étrangers du Service public fédéral Intérieur (ci-après le projet de loi).

Compétence du Comité permanent R

Vu l'article 33, alinéa 8 de la Loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace ;

Vu les articles 73, 95, 107 et 128 de la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;

Vu le Protocole de coopération du 24 novembre 2020 entre les autorités de contrôle fédérales belges en matière de protection des données.

Advies van het Vast Comité I

DOORGIFTE VAN PERSOONSGEGEVENS VAN DE DVZ AAN DE VSSE EN/OF DE ADIV

1. Het ontworpen artikel 6 bevat een ruime opsomming van de categorieën van persoonsgegevens die door de Dienst Vreemdelingenzaken (DVZ) verwerkt kunnen worden. De memorie van toelichting (pag. 10) bij deze bepaling stelt:

"Dit artikel bepaalt de categorieën van persoonsgegevens die kunnen worden verzameld en verwerkt door de Dienst Vreemdelingenzaken.
Overeenkomstig het minimisatiebeginsel moeten de verwerkte persoonsgegevens toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt [artikel 5, lid 1, c), van de algemene verordening gegevensbescherming].
De lijst van de door de Dienst Vreemdelingenzaken verzamelde en verwerkte categorieën van persoonsgegevens die in dit artikel is opgenomen, is gebaseerd op het overzicht van de gegevens dat de voormalige Commissie voor de bescherming van de persoonlijke levenssfeer heeft bepaald in haar aanbeveling nr. 06/2017 van 14 juni 2017 betreffende het Register van de verwerkingsactiviteiten (artikel 30 van de AVG) (CO-AR-2017-011).".

2. Krachtens het ontworpen artikel 11, §1, 32° en 33° mag de Dienst Vreemdelingenzaken bedoelde persoonsgegevens overmaken aan de VSSE respectievelijk de ADIV. Een dergelijke doorgifte van persoonsgegevens dient te geschieden, *dixit* betrokken bepalingen, *"met het oog op a) de uitvoering van zijn wettelijke opdrachten"* – m.b.t. de opdrachten van de VSSE of de ADIV – en/of *"b) de evaluatie door de Dienst Vreemdelingenzaken van de dreiging voor de openbare orde en de nationale veiligheid"*. De memorie van toelichting (pag. 66 en 67) bij deze bepalingen verduidelijkt:

Avis du Comité permanent R

TRANSFERT DE DONNÉES À CARACTÈRE PERSONNEL DE L'OE À LA VSSE ET/OU AU SGRS

1. Le projet d'article 6 contient une large énumération des catégories de données à caractère personnel qui peuvent être traitées par l'Office des étrangers (OE). L'exposé des motifs (p. 10) de cette disposition précise que :

« Cet article détermine les catégories de données à caractère personnel qui peuvent être collectées et traitées par l'Office des étrangers.
Conformément au principe de minimisation, les données à caractère personnel traitées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées [article 5, paragraphe 1, c), du règlement général sur la protection des données].
La liste des catégories de données à caractère personnel collectées et traitées par l'Office des étrangers reprise dans cet article est basée sur la cartographie des données arrêtée par l'ancienne Commission de la protection de la vie privée dans sa recommandation n°06/2017 du 14 juin 2017 relative au Registre des activités de traitements (article 30 du RGPD (CO-AR-2017-011). ».

2. En vertu du projet d'article 11, § 1er, 32° et 33°, l'Office des étrangers peut transférer les données à caractère personnel visées respectivement à la VSSE et au SGRS. Un tel transfert de données à caractère personnel doit avoir lieu, selon les dispositions concernées, « *aux fins de a) l'accomplissement de ses missions légales* » – c'est-à-dire les missions de la VSSE ou du SGRS - et/ou « *b) l'évaluation par l'Office des étrangers de la menace pour l'ordre public et la sécurité nationale* ». L'exposé des motifs (p. 66 et 67) de ces dispositions précise que :

"Overeenkomstig de bepalingen van de organieke wet houdende regeling van de inlichtingendiensten moet de Dienst Vreemdelingenzaken de informatie die nuttig is voor de uitvoering van zijn opdrachten aan de Staatsveiligheid meedelen [Artikel 14 van de organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten].
De uitwisseling van persoonsgegevens met de Staatsveiligheid stelt de Dienst Vreemdelingenzaken ook in staat om na te gaan of een vreemdeling mogelijk een gevaar vormt voor de openbare orde en/of de nationale veiligheid.".

MEDEDELING DOOR DE VSSE EN/OF DE ADIV AAN BUITENLANDSE INLICHTINGENDIENSTEN VAN DE PERSOONSGEGEVENS AFKOMSTIG VAN DE DVZ

3. Het Comité brengt in herinnering dat **de bij de VSSE en de ADIV beschikbare persoonsgegevens slechts onder beperkte voorwaarden mogen doorgegeven worden aan landen die geen lid zijn van de Europese Unie** of aan internationale organisaties (cf. artikelen 126 en 127 Gegevensbeschermingswet[1]). Ook de persoonsgegevens verkregen van de Dienst Vreemdelingenzaken kunnen niet zonder meer worden doorgegeven aan derde landen en zijn onderhevig aan een restrictief regime.

4. Het wettelijk kader voor (inter)nationale samenwerking en uitwisseling van informatie wordt, daarnaast, eveneens gevormd door de artikelen 19, eerste lid en 20 §3 W.I&V.[3] Artikel 19, eerste lid W.I&V regelt de algemene bevoegdheid tot mededeling en doorgifte van inlichtingen aan derde instanties.[4] De

Conformément aux dispositions de la loi organique des services de renseignement, l'Office des étrangers est tenu de communiquer à la Sûreté de l'État les informations utiles à l'exécution de ses missions [Article 14 la loi organique du 30 novembre 1998 des services de renseignement et de sécurité].

Les communications de données à caractère personnel avec la Sûreté de l'État permettent de vérifier si un étranger est susceptible de porter atteinte à l'ordre public et/ou à la sécurité nationale. ».

COMMUNICATION PAR LA VSSE ET/OU LE SGRS AUX SERVICES DE RENSEIGNEMENT ÉTRANGERS DE DONNÉES À CARACTÈRE PERSONNEL ÉMANANT DE L'OE

3. Le Comité rappelle que **les données à caractère personnel disponibles à la VSSE et au SGRS ne peuvent être transférées à des pays non membres de l'Union européenne** ou à des organisations internationales **que dans des conditions limitées** (cf. articles 126 et 127 de la Loi relative à la protection des données[2]). De même, les données à caractère personnel obtenues auprès de l'Office des étrangers ne peuvent pas être transférées vers des pays tiers et sont soumises à un régime restrictif.

4. En outre, les articles 19, alinéa 1er et 20 § 3 L.R&S[7] constituent le cadre juridique de la coopération (inter)nationale et de l'échange d'informations. L'article 19, alinéa 1er, L.R&S règle la compétence générale de communication et de transfert de renseignement à des instances tierces.[8]

---

1 Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (hierna: Gegevensbeschermingswet of GBW).
2 Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (ci-après : Loi Protection des données ou LPD).
3 Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (hierna: Inlichtingenwet of W.I&V).
4 Artikel 19, eerste lid W.I&V: *"De inlichtingen- en veiligheidsdiensten delen de inlichtingen bedoeld in artikel 13, tweede lid, slechts mee aan de betrokken ministers en de betrokken gerechtelijke en administratieve overheden, aan de politiediensten en aan alle bevoegde instanties en personen overeenkomstig de doelstellingen van hun opdrachten alsook aan de instanties en personen die het voorwerp zijn van een dreiging bedoeld in de artikelen 7 en 11.".*
7 Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (ci-après Loi Renseignement ou L.R&S).
8 Article 19, alinéa 1er L.R&S : « *Les services de renseignement et de sécurité ne communiquent les renseignements visés à*

wetgever was in 1998 echter zelf de mening toebedeeld dat deze bepaling onvoldoende is. Daarom schrijft artikel 20 §3 W.I&V voor dat de Nationale Veiligheidsraad (NVR), onder meer, de internationale samenwerking en informatie-uitwisseling verder moet uitwerken. Via de Richtlijn van 30 september 2016 heeft de Nationale Veiligheidsraad aan deze wettelijke plicht (deels) voldaan.[5] Van belang voor voorliggend problematiek is dat deze NVR-richtlijn de modaliteiten regelt van de internationale doorgifte van persoonsgegevens door de VSSE en de ADIV.[6]

5. In het licht van de door voorliggend wetsontwerp geregelde doorgifte van persoonsgegevens door de Dienst Vreemdelingenzaken aan de VSSE en de ADIV, is het Comité van oordeel dat, in het licht van de naleving van artikel 8.2 EVRM inzake het recht op eerbiediging voor de persoonlijke levenssfeer, de basisprincipes van de Richtlijn van de Nationale Veiligheidsraad moeten vastgelegd worden in een wet. **Het Comité adviseert bijgevolg om de installatie van artikel 11, §1, 32° en 33° van het wetsontwerp te koppelen aan een dergelijke uitwerking.**

Vanuit zijn hoedanigheid van gegevensbeschermingsautoriteit binnen het nationale veiligheidsdomein heeft het Comité als opdracht (corrigerend) te controleren of alle verwerkingen van persoonsgegevens – inbegrepen de informatieverstrekking door de inlichtingendiensten aan het buitenland –

Toutefois, en 1998, le législateur lui-même a estimé que cette disposition était insuffisante. Par conséquent, l'article 20 § 3 L.R&S prescrit que le Conseil national de sécurité (CNS), entre autres, doit approfondir la coopération internationale et l'échange d'informations. Par la Directive du 30 septembre 2016, le Conseil national de sécurité a (partiellement) rempli cette obligation légale.[9] Ce qui présente un intérêt pour la présente problématique est que la Directive du CNS règle les modalités du transfert international de données à caractère personnel par la VSSE et le SGRS.[10]

5. Compte tenu du transfert de données à caractère personnel par l'Office des étrangers à la VSSE et au SGRS qui est réglé par le présent projet de loi, le Comité est d'avis qu'au regard du respect de l'article 8.2 CEDH concernant le droit au respect de la vie privée, les principes de base de la Directive du Conseil national de sécurité doivent être inscrits dans une loi. **Le Comité conseille dès lors d'associer l'installation de l'article 11, § 1er, 32° et 33° du projet de loi à une telle élaboration.**

En sa qualité d'autorité de protection des données dans le domaine de la sécurité nationale, le Comité a pour mission de vérifier (aux fins de correction) si tous les traitements de données à caractère personnel – y compris la transmission d'informations par les services de renseignement à des pays étrangers – sont

---

l'article 13, deuxième alinéa, qu'aux ministres et autorités administratives et judiciaires concernés, aux services de police et à toutes les instances et personnes compétentes conformément aux finalités de leurs missions ainsi qu'aux instances et personnes qui font l'objet d'une menace visée aux articles 7 et 11. ».

5 De Richtlijn van 30 september 2016 van de Nationale Veiligheidsraad 'aangaande de relaties van de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichtingen en Veiligheid (ADIV) met buitenlandse inlichtingendiensten'.

6 Er werd geopteerd om deze (kwaliteitsvolle) NVR-richtlijn te classificeren (niveau Vertrouwelijk). Het Comité begrijpt niet waarom dit document dient geclassificeerd te worden. Het betrokken document bevat geen operationele gegevens, noch operationele methodologieën, noch andersoortige gevoelige gegevens. Te meer omdat de NVR-richtlijn een onderdeel vormt van het juridisch toetsingskader voor het internationaal handelen van de inlichtingen- en veiligheidsdiensten, zijn er volgens het Comité geen redenen om een dergelijk document blijvend te classificeren.

9 La Directive du 30 septembre 2016 du Conseil national de sécurité relative aux relations de la Sûreté de l'État (VSSE) et du Service Général du Renseignement et de Sécurité (SGRS) avec les services de renseignement étrangers.

10 Il a été décidé de classifier (au niveau 'Confidentiel') cette directive (de qualité) du CNS. Le Comité ne comprend pas pourquoi ce document doit être classifié. En effet, il ne contient ni des données et méthodologies opérationnelles ni d'autres types de données sensibles. En outre, vu que la directive du CNS fait partie du cadre juridique d'évaluation de l'action internationale des services de renseignement et de sécurité, le Comité estime qu'il n'y a aucune raison de classifier un tel document de manière permanente.

overeenkomen met de wettelijke en verdragsrechtelijke voorschriften.

Het Comité nodigt de regering en de beide inlichtingendiensten uit om werk te maken van het opstellen van een wetsontwerp om de huidige situatie te remediëren opdat de internationale informatie-uitwisseling door de inlichtingendiensten terug op een verdragsconforme wijze kan plaatsvinden.

Het Comité bracht op 28 september 2020 over deze aangelegenheid eerder al een advies uit, meer bepaald over het Wetsvoorstel 'tot wijziging van de wet van 30 november 1998 houdende regeling van inlichtingen- en veiligheidsdiensten met het oog op het invoeren van wegingsnotities voor de samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten' (DOC 55 0956/001). Dit advies wordt als bijlage toegevoegd.

Brussel, 1 juli 2022

conformes aux dispositions légales et conventionnelles.

Le Comité invite le gouvernement et les deux services de renseignement à œuvrer à l'élaboration d'un projet de loi visant à remédier à la situation actuelle, afin que les échanges d'informations au niveau international par les services de renseignement puissent à nouveau se dérouler conformément aux traités.

Le Comité a déjà rendu un avis sur cette question le 28 septembre 2020, plus précisément sur la Proposition de loi 'modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité en vue d'instaurer des notes d'évaluation pour la collaboration avec les services de renseignement et de sécurité étrangers' (DOC 55 0956/001). Cet avis figure en annexe.

Bruxelles, le 1 juillet 2022

VOOR HET VAST COMITÉ I

Serge LIPSZYC

Voorzitter

POUR LE COMITÉ PERMANENT R

Président

Frédéric GIVRON

Griffier

Greffier

Centrale drukkerij - Imprimerie centrale