



CONTROLEORGaan OP DE POLITIEInFORMATIE

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 Controlegeorgaan op de politie informatie (hierna het 'COC' of 'het Controlegeorgaan'),

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 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 Controlegeorgaan 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 Toezichhoudende Autoriteiten op vlak van Dataprotectie (cf. www.controlegeorgaan.be) .

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

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 2016/679¹ en de Richtlijn 2016/680², 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 toezichhoudende 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 WGB⁴. 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 politieambt⁵.

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 verleend⁶.

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 gegevensbanken⁷ 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^o, 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.contreleorgaan.be/files/Activiteitenverslag_COC_2020_N.pdf, randnummer 7 en 8.

verwerken in een nationale en een internationale **politie** 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 andere derde overheid, orgaan of instelling overigens) in de mogelijkheid om deze verwerkingen in de ANG of een andere politie 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 politie 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, 2° 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 gegevensbescherming⁸ 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, 2^e lid WGB.

Voorts is helemaal niet duidelijk wat in het ontworpen artikel 10, 11^o 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^o, 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 wetwijziging, 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 meegeedeelde gegevens

16. Het ontworpen artikel 11 voorziet in zijn 1^e paragraaf de diverse ontvangers of categorieën van ontvangers aan wie de DVZ de haar verzamelde persoonsgegevens kan meedelen. Daarin wordt enerzijds een ten 6^o 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^o, 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^o 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 verordening⁹ (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 bar*' 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 geargumenteed 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 politie 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 procedure¹⁰)".*

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