AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

[redacted]
De Staatssecretaris van Justitie en Veiligheid
Mevrouw mr. A. Broekers-Knol
Postbus 20301
2500 EH Den Haag

Datum	Ons kenmerk	Uw brief van
19 mei 2021	[redacted]	4 januari 2021
	Contactpersoon	Uw kenmerk
	[redacted]	[redacted]

Onderwerp
Advies concept uitvoeringswet EU-verordeningen grenzen en veiligheid

Geachte mevrouw Broekers-Knol,

Bij brief van 4 januari 2021 is de Autoriteit Persoonsgegevens (AP) op grond van het bepaalde in artikel 36, vierde lid, van de Algemene verordening gegevensbescherming (AVG), artikel 35b, eerste lid, onder b, van de Wet politiegegevens (WPG) en artikel 39r, tweede lid, van de Wet justitiële en strafvorderlijke gegevens (WJSG) geraadpleegd over het concept voor de uitvoeringswet EU-verordeningen grenzen en veiligheid (hierna: concept).[1]

Het wetsvoorstel geeft voor Nederland uitvoering aan een omvangrijk pakket van EU-verordeningen die beogen Europa veiliger te maken en de reizigersmobiliteit te bevorderen.

Wat betreft het aantal beboetbare feiten en de hoogte van de boetes wordt voorgesteld aan te sluiten bij de AVG en de Richtlijn gegevensbescherming opsporing en vervolging (RGB), zoals geïmplementeerd in de Wet politiegegevens (WPG) en de Wet justitiële en strafvorderlijke gegevens (WJSG). Dat is echter voor wat betreft de RGB niet steeds toereikend omdat de RGB destijds naar het oordeel van de AP onvolledig is geïmplementeerd Zo eisen de operabiliteitsverordeningen bijvoorbeeld dat overtreding van regels over doorgifte van gegevens aan derde landen strafbaar wordt gesteld, terwijl dit in de WPG en WJSG niet het geval is.
De AP heeft op het punt van sanctionering in de WPG en WJSG bezwaar tegen het concept en adviseert de procedure niet voort te zetten, tenzij het bezwaar is weggenomen. Meer in het algemeen adviseert de AP

[1] De volledige titel luidt: Voorstel voor de wet van [datum], houdende regels ter uitvoering van EU-verordeningen op het terrein van grenzen en veiligheid (Uitvoeringswet EU-verordeningen grenzen en veiligheid).

om wat betreft het aantal van concrete beboetbare feiten en de hoogte daarvan in de WPG en WJSG meer aan te sluiten bij de AVG.

Hoofdlijn advies

- Wat betreft het aantal beboetbare feiten en de hoogte van de boetes wordt voorgesteld aan te sluiten bij de AVG en de Richtlijn gegevensbescherming opsporing en vervolging (RGB), die is geïmplementeerd in de WPG en WJSG. De operabiliteitsverordeningen eisen echter dat verwerkingen in strijd met de verordeningen strafbaar worden gesteld, zoals bijv. overtreding van de regels over doorgifte van gegevens aan derde landen. Dat is strenger dan de regeling in de WPG en WJSG waarin slechts overtreding van enkele voorschriften beboetbaar is gesteld met bovendien vaak met fors lagere boetes dan in de AVG. Dit terwijl artikel 57 RGB bepaalt dat de lidstaten op inbreuken op de RGB afschrikkende straffen stellen. Aangezien de bestaande implementatie van de RGB in de WPG en WJSG zo bezien onvolledig is, schiet ook het voorliggende voorstel tekort op het punt van bestraffing.

- De AP adviseert daarom om de implementatie van de RGB op het punt van bestraffing te repareren, alsmede te bezien welke eventuele andere concrete voorschriften uit de EU verordeningen in aanvulling op de bepalingen in met name de WPG strafbaar dienen worden gesteld, tegen de achtergrond van de regeling van de beboetbare feiten in de AVG. Tevens adviseert de AP om voor wat betreft de hoogte van de straffen in de WPG meer aan te sluiten bij de hoogte van de pendanten in de AVG. Dit omdat de AVG en RGB één Europees stelsel van gegevensbescherming betreft.

- Voorgesteld wordt om voortaan de officier van justitie aan te wijzen als centraal toegangspunt voor rechtshandhaving en de huidige taak van de rechter-commissaris te schrappen. Naar het oordeel van de AP sluit de rechter-commissaris beter aan bij de eis uit de EU-verordeningen van een van de aangewezen autoriteiten onafhankelijk toegangspunt.

- Verder wordt in de toelichting een onjuiste uitleg gegeven van het begrip "voldoende ernstig strafbaar feit", waardoor het risico bestaat dat gegevensverwerkingen plaatsvinden zonder rechtmatige grondslag.

- Naast de nationale opslag van gegevens uit het C.SIS houdt Nederland tevens een gehele kopie aan van het C.SIS omdat het C.SIS soms niet beschikbaar is door technische problemen en onderhoud. Dit is weliswaar mogelijk op grond van de verordeningen, maar gelet op het beginsel van dataminimalisatie opvallend, zeker voor een dergelijke grote opslag van vaak bijzondere persoonsgegevens. Bovendien is de vraag of na de evaluatie van SIS II inmiddels verbeteringen tot stand zijn gebracht in C.SIS waardoor de noodzaak tot een gehele kopie mogelijk is verminderd.

- Voorts adviseert de AP om een evaluatiebepaling op te nemen, mede gelet op de verschillende nationale keuzes in het voorstel tegen de achtergrond van de grootschalige verwerkingen van bijzondere persoonsgegevens die de EU-verordeningen tot gevolg hebben.

- Tenslotte adviseert de AP om in de toelichting in te gaan op de door de AP opgestelde uitvoeringstoets. De EU-verordeningen schrijven voor dat de nationale toezichthouders over voldoende middelen beschikken. Zonder adequaat toezicht komt het mensenrecht op daadwerkelijke bescherming van persoonsgegevens in gevaar.

Strekking van het concept

Het wetsvoorstel geeft nationale uitvoering aan een groot pakket EU-verordeningen die beogen Europa veiliger te maken en de reizigersmobiliteit te bevorderen.

Het gaat om onder meer twee nieuwe Europese informatiesystemen (EES, ETIAS), de wijziging van het bestaande Schengen Informatie Systemen (SIS) en de introductie van "Interoperabiliteit" tussen deze Europese informatiesystemen. Dit houdt in dat de informatiesystemen onderling kunnen communiceren en samenwerken. Daarbij gaat het niet alleen om bestaande systemen, maar ook om nieuwe systemen en verwerkingen.

Het gaat in alle gevallen om centrale EU-informatiesystemen, kortom systemen die worden beheerd door de Europese Unie, meer specifiek het Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht, eu-LISA. In deze systemen voeren de lidstaten van de Europese Unie en andere Schengenlanden informatie in over (meestal) derdelanders (personen die geen Unieburger zijn). Deze informatie wordt vervolgens geraadpleegd voor diverse doeleinden, afhankelijk van de onderliggende verordeningen.

In de EU-informatiesystemen van het wetsvoorstel is sprake van verwerking van persoonsgegevens van meestal derdelanders (personen die geen Unieburger zijn), maar in sommige gevallen ook Unieburgers (op grond van de SIS-verordening politiële en justitiële samenwerking in strafzaken). In de meeste EU-informatiesystemen worden niet alleen 'gewone' persoonsgegevens verwerkt, maar tevens bijzondere, zoals biometrie. Hier komt bij dat niet alleen persoonsgegevens van volwassenen maar ook van minderjarigen in de EU-informatiesystemen worden opgenomen, die op grond van de AVG extra bescherming behoeven.

In de praktijk worden persoonsgegevens van miljoenen personen in deze databases ingevoerd, verwerkt en gedeeld. Concreet kan het dan bijvoorbeeld gaan om gegevens van reizigers die het Schengengebied in- of uitreizen, om gegevens van gezochte personen of gegevens van ongewenst verklaarde personen.

Gegevens worden op centraal niveau in deze systemen verwerkt waarbij publieke autoriteiten in de lidstaten gegevens kunnen invoeren, raadplegen, wijzigen of wissen.[2] Het toezicht op het centrale systeem is belegd bij de European Data Protection Supervisor (EDPS), terwijl het toezicht op - kort gezegd - de

[2] Toelichting, blz. 26.

nationale communicatie met het centrale Europese systeem is belegd bij de nationale privacytoezichthouders (in Nederland: de AP).

Het voorliggende concept ziet op het uitvoering geven aan de verordeningen en betreft onder meer het aanwijzen van de bevoegde instanties.

Advies

0. Opmerking vooraf

Vooropgesteld merkt de AP op dat het pakket aan EU verordeningen omvangrijk en complex is. Alle EU verordeningen bevatten bepalingen over persoonsgegevens en verklaren tegelijkertijd de AVG en de RGB van toepassing. In sommige gevallen liepen de onderhandelingen over de verordeningen en die over de AVG en RGB parallel en in andere was het nieuwe algemene EU-kader voor gegevensbeschermingsrecht reeds tot stand gekomen. Dit roept de vraag op hoe deze kaders zich tot elkaar verhouden. In paragraaf 5 van de toelichting wordt hierop uitgebreid ingegaan. Dat neemt niet weg dat voor de uitvoerende diensten en de betrokkenen waarop het gaat (veelal derdelanders) zelf duidelijk dient te zijn wat de rechten en plichten zijn waarvoor het raadplegen van het complex van EU-verordeningen, de uitvoeringswet en de toelichting niet snel uitkomst bieden.

Gelet hierop adviseert de AP te voorzien in een beknopte en praktische handreiking of een helpdesk.

1. Straffen

Alle verordeningen van het wetsvoorstel bevatten bepalingen over sanctionering. De EES-verordening (artikel 48), de SIS-verordeningen (artikelen 41, 45 en 49 van de SIS-verordening grenscontroles en 60 en 73 van de SIS-verordening politiële en justitiële samenwerking) en de verordeningen over interoperabiliteit (artikel 45) schrijven voor dat de lidstaten ervoor zorgen dat – kort samengevat – gegevensverwerking die niet volgens de regels verloopt strafbaar wordt gesteld volgens het nationaal recht, waarbij de sancties doeltreffend, evenredig en afschrikkend dienen zijn. De ETIAS-verordening bepaalt dat de lidstaten regels vaststellen en alle maatregelen nemen die nodig zijn om ervoor te zorgen dat de regels worden uitgevoerd, waarbij eveneens is aangegeven dat de sancties doeltreffend, evenredig en afschrikkend dienen te zijn.

Wat gesanctioneerd dient te worden is uiteenlopend geformuleerd. De gemene deler is dat sprake dient te zijn van schending van de regels over het gegevensbeschermingsrecht (of deze nu voortvloeien uit de verordeningen zelf of de algemene kaders van de AVG en de RGB). Hier wordt aangesloten bij de bestaande bepalingen in de (U)AVG en RGB.

Hoewel in de EES-verordening, de SIS-verordeningen en de verordeningen over interoperabiliteit gesproken wordt van het nationaal "strafbaar" ("punishable") maken van schendingen, is er in de toelichting van uit gegaan dat niet bedoeld is strafrechtelijke handhaving van de desbetreffende verordeningen dwingend voor te schrijven. Het in de relevante artikelen van de verordeningen gebruikte

begrip "sancties" ("penalties") wordt in EU-wetgeving over het algemeen opgevat als zowel omvattend strafrechtelijk van aard als bestuursrechtelijk, waarbij het vervolgens aan de nationale wetgever wordt gelaten hier een keuze in te maken, aldus de toelichting. "Alleen daar waar in EU-wetgeving de term "criminal penalties" wordt gebezigd is sanctionering via het strafrecht wel uitdrukkelijk verplicht. Dat is hier niet aan de orde."[3]

Volgens de toelichting is in en ter uitvoering van de AVG en ter uitvoering van de RGB reeds in sancties op dit soort schendingen voorzien. Artikel 83 van de AVG bevat de voorwaarden waaronder nationale toezichthouders administratieve boetes kunnen opleggen. Artikel 84 van de AVG bepaalt dat de lidstaten regels vaststellen over andere sancties die van toepassing zijn op inbreuken op de verordening, in het bijzonder op inbreuken die niet aan administratieve geldboeten onderworpen zijn overeenkomstig artikel 83 van de AVG, en dat zij alle nodige maatregelen treffen om ervoor te zorgen dat sancties worden toegepast. Ook schrijft de AVG voor dat de sancties doeltreffend, evenredig en afschrikkend dienen te zijn. "De RGB bevat een vergelijkbare implementatieplicht in artikel 57," aldus de toelichting.[4]

De AP onderschrijft dat het begrip "straffen" in de EU-verordeningen en de RGB niet alleen ziet op straffen via het klassieke strafrecht, maar ook via het bestuursrecht door bestuurlijke boetes. Immers, een belangrijk onderdeel van de sanctionering in de AVG is artikel 83, dat juist betrekking heeft op administratieve boetes die worden opgelegd door de aangewezen toezichthouder, dus buiten de klassieke strafrechtelijke handhaving om.

Met betrekking tot "de vergelijkbare implementatieplicht in artikel 57" wijst de AP evenwel op belangrijke discrepanties tussen enerzijds de (U)AVG en anderzijds de WPG en WJSG ter implementatie van de RGB. Het aantal beboetbare feiten en de hoogte van de boetes zijn in de AVG aanzienlijk groter dan onder de WPG en WJSG.
De AP en de Afdeling advisering van de Raad van State hebben hierop gewezen in 2017 in het kader van de implementatie van de RGB in de WPG en WJSG en hebben geadviseerd om aan te sluiten bij de AVG.[5] In reactie daarop stelde de minister:

> "Anders dan de verordening, verplicht de richtlijn de lidstaten niet om bepaalde bevoegdheden tot handhaving toe te delen aan de toezichthoudende instantie. De richtlijn volstaat met een verplichting voor de lidstaten om te voorzien in effectieve bevoegdheden terzake waarbij rekening gehouden kan worden met de specifieke nationale situatie. Voor de implementatie van dit onderdeel van de richtlijn is aangesloten bij

[3] Toelichting, blz. 41.
[4] Toelichting, blz. 41.
[5] Advies AP van 7 april 2017 (z2017-01571) en Kamerstukken II 2017/18, 34 889, nr. 4. De AP merkte op dat in het toenmalige wetsvoorstel slechts een bevoegdheid was gegeven om een boete op te leggen vanwege een overtreding van de documentatieplicht (artikel 32 Wpg). Het boetemaximum bedraagt ten hoogste het bedrag van de vierde boetecategorie van artikel 23, vierde lid, Sr (€ 20.500). De maximum boetebedragen in de Verordening variëren van 10 tot 20 miljoen euro. De AP wees op de samenhang met de Verordening en de verplichting voor de lidstaten om inbreuken op de Richtlijn te bestraffen met doeltreffende, evenredige en afschrikkende sancties (artikel 57 RGB) en stelt voor om voor de administratieve geldboeten aan te sluiten bij de regeling van artikel 83 van de Verordening. Om die reden adviseert de AP de bepalingen waarvoor een administratieve boete kan worden opgelegd aan te vullen en de boetemaxima te heroverwegen en in dat verband aansluiting te zoeken bij de Verordening. Daarbij was een lijst van overtredingen voorgesteld, waarvoor een bestuurlijke boete kan worden opgelegd.

> de huidige regeling op basis van de Wpg en de Wjsg. De huidige regeling voorziet in vergaande bevoegdheden voor de AP ter handhaving, zoals het opleggen van een last onder bestuursdwang."[6]

De AP wijst erop dat bestuursdwang een effectieve bestuurlijke sanctie kan zijn, maar geen "afschrikkende straf" in de zin van artikel 57 RGB. Het heeft geen punitief oogmerk en beoogt niet om af te afschrikken of leed toe te voegen, maar 'slechts' om de verwerkingen in overeenstemming te brengen met de RGB. Het betreft zodoende een "corrigerende maatregel" in de zin van artikel 47 RGB.

Naar aanleiding van deze adviezen is de minister zowel wat betreft het aantal beboetbare feiten en de hoogte daarvan in de WPG en de WJSG iets opgeschoven richting de AVG.[7]

Toch zijn er - zeker in verband met de voorliggende EU verordeningen – nog relevante discrepanties tussen de sancties in de AVG en de implementatie van de RGB in de WPG en WJSG. Zo kan bijv. volgens artikel 83, vijfde lid, onderdeel c, van de AVG overtreding van de regels over doorgifte aan derde landen worden bestraft met een boete van maximaal 20 miljoen euro, terwijl overtreding van de vergelijkbare bepalingen in de RGB (artikel 17a WPG) helemaal niet kan worden beboet (artikel 35c, eerste lid, onderdeel c, WPG), maar kan worden gehandhaafd door een last onder bestuursdwang. Dit terwijl artikel 57 van de RGB bepaalt dat de lidstaten doeltreffende, evenredige en afschrikkende *straffen* ("penalties") vaststellen *op inbreuken op de richtlijn*. Het niet voorzien in de WPG en WJSG van afschrikkende straffen op een aantal inbreuken op de RGB is naar het oordeel van de AP een onvolledige implementatie van de RGB.[8] Dit klemt temeer nu de hier voorliggende EU verordeningen over operabiliteitbepalen dat gegevens, niet aan derde landen worden doorgegeven (vgl. artikel 50 van verordening 2019/818) en dat uitwisseling van gegevens in strijd met de verordening strafbaar wordt gesteld volgens het nationale recht (artikel 45 van verordening 2019/818). Dit betekent dat de bestaande regeling in de WPG tekort schiet.

In de toelichting bij het toenmalige implementatievoorstel is ter rechtvaardiging van de discrepanties gewezen op de omstandigheid dat een serieuze boete ten koste kan gaan van de dienstverlening ("vestzak-broekzak"), de omstandigheid dat de overheid doorgaans geen winstoogmerk heeft en de omstandigheid dat de politie nog in een ontwikkeltraject zit.[9]

> "In afwachting van de herziening van de Wpg en de Wjsg verdient het de voorkeur een voorlopige balans te vinden waarbij enerzijds wordt voorzien in afschrikwekkende en effectieve sancties en anderzijds rekening

[6] Vgl. overweging 152: Waar deze verordening niet voorziet in een harmonisering van de administratieve straffen of indien nodig in andere gevallen, bijvoorbeeld bij ernstige inbreuken op deze verordening, dienen de lidstaten een systeem toe te passen dat zorgt voor doeltreffende, evenredige en afschrikkende straffen. De aard van die straffen, strafrechtelijk of administratief, dient te worden bepaald in het lidstatelijke recht.

[7] Kamerstukken II 2017/18, 34 889, nr. 3, blz. 90 e.v.

[8] Artikel 83, eerste lid, AVG geeft aan dat op overtreding van welke bepalingen van de AVG door de toezichthoudende autoriteit administratieve geldboeten worden opgelegd alsmede de maximale hoogte daarvan. Volgens het tweede lid worden administratieve geldboeten, naargelang de omstandigheden van het geval, opgelegd *naast of in plaats* van de in artikel 58, tweede lid, bedoelde corrigerende maatregelen. Omdat de AVG en RGB uiteindelijk één Europees stelsel van bescherming van persoonsgegevens betreft, ligt het in de rede om voor de uitleg van artikel 57 RGB aan te sluiten bij de pendant in artikel 83 AVG.

[9] Kamerstukken II 2017/2018, 34 889, nr. 3, blz. 91.

wordt gehouden met de draagkracht van de betreffende organen en de mogelijkheid om op korte termijn te voldoen aan de soms tamelijk complexe normen van de richtlijn".

Afgezien van de genoemde eis van de EU verordeningen over operabiliteit vallen de forse discrepanties tussen de AVG en RGB niet te rijmen met het feit dat het gaat om één Europees stelsel van gegevensbescherming en evenmin met het standpunt van de regering dat de mogelijkheid van bestuurlijke boetes het belangrijke signaal afgeeft dat de overheid zichzelf heeft te houden aan de verplichtingen van het gegevensbeschermingsrecht en hierin niet anders wordt behandeld dan het bedrijfsleven.[10]

Bovendien kan in voorkomend geval bij de vaststelling van de hoogte van een sanctie zo nodig rekening worden gehouden met de bijzondere omstandigheden van het geval. Dit doet geenszins af aan het uitgangspunt dat de *wettelijke* punitieve sanctionering wat betreft voldoende concrete voorschriften in de WPG in beginsel moet aansluiten bij de AVG.

Gelet op het voorgaande adviseert de AP om de implementatie van de RGB op het punt van straffen op de inbreuken op de RGB te repareren, alsmede te bezien welke eventuele andere concrete voorschriften uit de verordeningen in aanvulling op de bepalingen in met name de WPG strafbaar dienen worden gesteld. Tevens adviseert de AP om voor wat betreft de hoogte van de straffen in de WPG meer aan te sluiten bij de hoogte van de pendanten in de AVG.

2. Officier van justitie als centraal toegangspunt rechtshandhaving

Wat betreft de procedure voor raadpleging schrijven alle verordeningen voor dat de lidstaten een centraal toegangspunt voor rechtshandhaving aanwijzen. Het centrale toegangspunt heeft als taak toegang te geven aan de aangewezen autoriteiten tot de gegevens in het EU-informatiesysteem, nadat is geverifieerd of aan alle inhoudelijke (zie daarover nader, punt 3) en procedurele voorwaarden voor toegang is voldaan.

De EU-verordeningen bevatten geen definitie van het begrip centraal toegangspunt, maar bepalen – samengevat- wel het volgende over het centrale toegangspunt:
a. Het dient onafhankelijk te zijn van de aangewezen autoriteiten in een lidstaat, in die zin dat het toegangspunt wel onderdeel kan uitmaken van dezelfde organisatie als de aangewezen autoriteiten, maar losstaat van de aangewezen autoriteiten en van deze geen instructies ontvangt in het kader van de toets op de voorwaarden voor toegang respectievelijk de resultaten van de verificatie, die het onafhankelijk verricht;
b. Het behoeft niet bij één overheidsdienst te worden belegd.[11]

In de huidige praktijk gaat het voorgaande via een vordering op grond van artikel 126nd van het Wetboek van Strafvordering en in geval van EURODAC dient dit bevel vergezeld te zijn van een machtiging van de rechter-commissaris. Er is hiermee aangesloten bij de regeling en praktijk in strafvordering.[12]

[10] Kamerstukken II 2017/18, 34 851, nr. 3, blz. 100–101.
[11] Toelichting, blz. 24.
[12] Vgl. artikel 126nf Sv en Kamerstukken II 2012/13, 33 192, nr. 17.

In het concept is voorgesteld om de officier van justitie aan te wijzen als centraal toegangspunt ten aanzien van de toetsing op de materiële voorwaarden voor toegang voor alle vier de systemen (artikel 5). Dit betekent ten aanzien van EURODAC een verandering, omdat de procedure van een vordering van de officier van justitie en een machtiging van de rechter-commissaris, wordt omgevormd tot alleen een toets door de officier van justitie.

Deze verandering is ingegeven door de wens om een uniforme werkwijze voor alle systemen te hanteren.[13] Daarnaast stelt de toelichting dat de verordeningen al uitgebreide waarborgen bevatten voor toegang: "Vanuit dit perspectief is het onnodig zwaar en kostbaar om de rechter-commissaris te betrekken". Bovendien blijven EURODAC verzoeken zeldzaam, aldus de toelichting. Om bij de toetsing van de toegang tot de systemen ten behoeve van de opsporing en vervolging conform de wens van de Tweede Kamer bij de invoering van de EURODAC-verordening, te borgen dat er extra toetsing plaatsvindt, heeft het College van procureurs-generaal besloten om een interne instructie op te stellen waarin een toegangsverzoek wordt getoetst door een officier van justitie die niet aan de zaak is verbonden in het kader van tegenspraak en zorgvuldigheid. Dit is in aanvulling op toetsing door de zaaksofficier, indien een zaaksofficier (reeds) betrokken is.[14]

De AP wijst erop dat, niettegenstaande de diverse andere waarborgen in de verordening, de lidstaten een centraal toegangspunt voor rechtshandhaving dienen aanwijzen. Een rechter komt naar het oordeel van de AP beter tegemoet aan de eis van de verordeningen dan een officier van justitie omdat een rechter per definitie onafhankelijk is van de aangewezen autoriteit. Dit is anders voor de officier van justitie die immers op grond van de aanwijzingsbevoegdheid van de minister van Justitie en Veiligheid bijzondere aanwijzingen kan ontvangen over het al dan niet opsporen of vervolgen in individuele zaken.[15]

In dit verband wijst de AP erop dat het Hof van Justitie van de Europese Unie op 24 november 2020 oordeelde dat het Nederlandse openbaar ministerie niet als 'uitvoerende rechterlijke autoriteit' kan gelden in het kader van de overleveringsprocedure.[16] Dit omdat de minister van Justitie en Veiligheid bevoegd is tot het geven van individuele instructies en aanwijzingen aan het openbaar ministerie.

Weliswaar hoeft het bij het centraal toegangspunt niet te gaan om een rechterlijke autoriteit, maar het centraal toegangspunt dient op grond van de verordeningen ook onafhankelijk te zijn van de aangewezen autoriteiten in een lidstaat, in die zin dat het toegangspunt geen instructies ontvangt in het kader van de toets op de voorwaarden voor toegang respectievelijk de resultaten van de verificatie, die het onafhankelijk verricht. Via de wettelijke mogelijkheid van de minister tot het geven van een bijzondere aanwijzing is dit echter niet geheel uitgesloten.

[13] Toelichting, blz. 25.
[14] Toelichting, blz. 25.
[15] Artikel 127 en artikel 128 van de Wet op de rechterlijke organisatie.
[16] Arrest in zaak C-510/19, ECLI:EU:C:2020:953 (België).

Ook in het recente arrest Prokuratuur ging het om de wettelijke bevoegdheid van het openbaar ministerie om toegang te verlenen tot om een overheidsinstantie toegang te verlenen tot verkeers- en locatiegegevens om een strafrechtelijk onderzoek te verrichten.[17] Het Hof van Justitie EU oordeelt dat wanneer een dergelijke toetsing niet door een rechterlijke instantie, maar door een onafhankelijke bestuurlijke entiteit wordt uitgeoefend, deze laatste een zodanige status moet hebben dat zij bij de uitoefening van haar taken objectief en onpartijdig kan handelen, en daartoe vrij moet zijn van elke invloed van buitenaf:

> "In het bijzonder impliceert het vereiste van onafhankelijkheid op strafrechtelijk gebied dat de instantie die belast is met die voorafgaande toetsing, enerzijds niet betrokken mag zijn bij de uitvoering van het betrokken strafrechtelijk onderzoek en, anderzijds, neutraal moet zijn ten opzichte van de partijen in de strafprocedure. Dat is niet het geval bij een openbaar ministerie, zoals het Estse parket, dat de onderzoeksprocedure leidt en, in voorkomend geval, optreedt als openbaar aanklager. Hieruit volgt dat het openbaar ministerie niet in een positie is om de bovengenoemde voorafgaande toetsing te verrichten."

Het gaat hier bovendien om biometrische gegevens, dus bijzondere persoonsgegevens die een bijzondere bescherming verdienen. In de huidige regeling is voor het vorderen van dergelijke gegevens, nog los van andere voorwaarden, steeds een machtiging van de rechter-commissaris vereist op vordering van de officier van justitie.[18]

Uitgangspunt in strafvordering is dat naarmate de privacy-inbreuken groter zijn, de voorwaarden navenant strenger zijn. De lat kan natuurlijk niet worden verlaagd, enkel omwille van de wens om te komen tot uniformiteit. Bovendien stelt de toelichting dat deze verzoeken zeldzaam zijn, zodat de gewenste uniformiteit en de kosten ook daarom geen valide argumenten zijn om de toets door de rechter-commissaris af te schaffen.

Ten slotte blijkt uit evaluatie van de Wet biometrie vreemdelingenketen dat sinds 2016 ook gezichtsopnames worden verstrekt op grond van dezelfde voorwaarden als die gelden voor de verstrekking van vingerafdrukken, terwijl voor dergelijke verstrekkingen geen nadere regeling getroffen.[19] Een dergelijke praktijk geeft niet direct aanleiding tot de voorgestelde uitholling van de rechtsbescherming voor EURODAC.

Gelet op het voorgaande adviseert de AP om de huidige eis van een machtiging van de rechter-commissaris op vordering van de officier van justitie voor EURODAC te handhaven en uit te breiden tot de andere systemen.

---

[17] Arrest in zaak C-746/18 H. K. / Prokuratuur (Estland).
[18] Artikel 107, zesde lid, van de Vreemdelingenwet 2000.
[19] Vgl. het advies van de AP van 24 juni 2020 over het voorstel tot Wijziging van de Vreemdelingenwet 2000 ter bestendiging van verwerking biometrie, blz. 4 en de reactie van de Staatssecretaris in de brief aan de Vice-President van de Afdeling advisering van de Raad van State van 16 juli 2020 (Appreciatie advies AP).

3. Een voldoende ernstig strafbaar feit

De materiële voorwaarden in de verschillende verordeningen komen grotendeels overeen en daarbij dient onder meer sprake te zijn van een "voldoende ernstig strafbaar feit of een terroristische dreiging".

In de EU verordeningen wordt aangesloten bij ernstige strafbare feiten als bedoeld in Kaderbesluit 2002/584/JBZ van de Raad. Het gaat dan, kort samengevat, bij de EURODAC-verordening om de vormen van criminaliteit die volgens het nationale recht strafbaar zijn gesteld met een vrijheidsstraf of een tot vrijheidsbeneming strekkende maatregel met een maximumduur van ten minste drie jaar.[20]

In de toelichting is opgemerkt dat de kwalificatie 'voldoende ernstig strafbaar feit' snel wordt bereikt en dat het daarbij gaat om misdrijven waarbij voorlopige hechtenis mogelijk is, zoals diefstal.[21]

De AP wijst erop dat voorlopige hechtenis inderdaad mogelijk is bij misdrijven waarop een gevangenisstraf van vier jaar of meer is gesteld (artikel 67, eerste lid, onderdeel a, Sv). Daarnaast bevat artikel 67, eerste lid, onder b en c, Sv echter een reeks van misdrijven waarop een maximumgevangenisstraf van minder dan drie jaar is gesteld, zoals bijv. eenvoudige mishandeling (artikel 300, eerste lid, Sr). Dit betekent dat niet alle misdrijven die een geval voor voorlopige hechtenis betreffen ook een voldoende ernstig strafbaar feit in de zin van de EU-verordeningen opleveren. Hierdoor bestaat het risico dat toegang wordt verleend tot de systemen terwijl niet aan de voorwaarde in de EU-verordeningen is voldaan en zodoende geen sprake is van een rechtmatige verwerking.[22]

De AP adviseert de toelichting aan te passen in die zin dat voor wat betreft voorlopige hechtenis in beginsel alleen sprake is van voldoende ernstige feiten als het gaat om de hoofdregel van misdrijven waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaar of meer is gesteld als bedoeld in artikel 67, eerste lid onderdeel a, Sv.

4. Noodzaak van nationale opslag C.SIS

Het Centrale Schengen Informatie Systeem (C.SIS) is een grootschalig EU-informatiesysteem dat grenscontroles en samenwerking in de rechtshandhaving ondersteunt in en tussen de Schengenlidstaten.[23]

Elk Schengenland heeft volgens afgesproken specificaties een nationaal informatiesysteem (hierna: N.SIS) ontwikkeld dat via het centrale Schengeninformatiesysteem (hierna: C.SIS) is gekoppeld aan de N.SIS-

[20] Vgl. de toelichting op de artikelen 4 en 5 en Artikel 2, onderdeel k, van de Eurodac-verordening.
[21] Toelichting, blz. 24, noot 44.
[22] Politiegegevens worden slechts verwerkt voor zover dit behoorlijk en rechtmatig is, de gegevens rechtmatig zijn verkregen en de gegevens, gelet op de doeleinden waarvoor zij worden verwerkt, toereikend, terzake dienend en niet bovenmatig zijn (artikel 3 eerste lid, WPG).
[23] Het C.SIS is een 'hit/no-hit' systeem. Dit houdt in dat nationale autoriteiten het systeem niet integraal kunnen doorzoeken maar dat alleen bij een aanleiding, bijvoorbeeld een (grens)controle op een persoon die gesignaleerd staat, informatie over die persoon voor de eindgebruiker zichtbaar wordt.

systemen van andere Schengenlanden. Wijzigingen worden in het eigen N.SIS ingevoerd en de N.SIS-systemen worden vrijwel continu met elkaar gesynchroniseerd via het C.SIS.

Thans bevat het Nederlandse N.SIS minder en tegelijkertijd ook meer gegevens dan de welke naar het C.SIS worden doorgestuurd.[24] Het Nederlandse N.SIS is een nationale kopie van het Nederlandse deel van C.SIS, maar dan zonder zogeheten binaire data. Dit houdt in dat Nederland er voor gekozen heeft de biometrische gegevens van door Nederland gesignaleerde personen niet nationaal op te slaan in het N.SIS.

De wettelijke grondslag voor het N.SIS is te vinden in de SIS-verordeningen zelf. Deze schrijven dwingend voor dat elke lidstaat een N.SIS heeft, maar laten het tegelijkertijd aan de lidstaten zelf te bepalen of het N.SIS een volledige of gedeeltelijke kopie bevatten van de CSIS-databank (en dus ook van signaleringen van andere lidstaten). De verordeningen gaan er daarbij vanuit dat het C.SIS vrijwel gelijk is aan de Europese signaleringen van de nationale N.SIS systemen. In beeldspraak is het C.SIS dus een huis bestaande uit diverse lid statelijke kamers. Het N.SIS is met andere woorden niet enkel een toegangsportaal.

Naast de nationale opslag van gegevens uit het C.SIS houdt Nederland tevens een gehele kopie aan van het C.SIS. Volgens de toelichting was en is de ratio hiervan nog steeds de beschikbaarheid en performance van signaleringen en follow up acties in eigen hand te houden in verband met de nationale veiligheid en beschikbaarheid 24 uur per dag. De in incidentele gevallen niet beschikbaarheid van het C.SIS door technische problemen en onderhoud hebben aangetoond dat dit de juiste keuze is en blijft.

De AP wijst erop dat uit een oogpunt van het in de AVG opgenomen beginsel van dataminimalisatie het opvallend is dat enkel vanwege de incidentele niet beschikbaarheid een gehele kopie van C.SIS wordt aangehouden. In de evaluatie van SIS II door de Europese Commissie uit 2016 is gesteld dat de bedrijfscontinuïteit op centraal niveau moet worden gewaarborgd en storing van het centrale SIS II moet worden vermeden:

> "Er worden technische oplossingen onderzocht om de omschakeltijd tussen het centrale SIS II en de back-upsite te verkorten, omdat de huidige technische mogelijkheden en procedures niet aan de verwachte normen voor systeembeschikbaarheid voldoen.[25]

Gelet hierop adviseert de AP de noodzaak voor het aanhouden een gehele kopie van C.SIS nader te motiveren.

[24] Toelichting, blz. 29.
[25] VERSLAG VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD over de evaluatie van het Schengeninformatiesysteem van de tweede generatie (SIS II) overeenkomstig artikel 24, lid 5, artikel 43, lid 3, en artikel 50, lid 5, van Verordening (EG) nr. 1987/2006, en artikel 59, lid 3, en artikel 66, lid 5, van Besluit 2007/533/JBZ. 21 december 2016.

5. Grensoverschrijdende verwerkingen

In het kader van de verordeningen is regelmatig sprake van grensoverschrijdende verwerkingen in de zin dat verschillende lidstaten aan eenzelfde set van gegevens werken.

De AVG kent een één-loketmechanisme. Dit houdt in dat organisaties die grensoverschrijdende verwerkingen uitvoeren, maar met één privacytoezichthouder te maken hebben. Op basis van artikel 55, tweede lid, AVG vallen, kort samengevat, overheidsinstanties die persoonsgegevens verwerken omdat dit noodzakelijk is op grond van wettelijke verplichting of ter uitvoering van een wettelijke taak, buiten het één-loketmechanisme.[26]

In de toelichting wordt echter de suggestie gewekt dat het een-loketmechanisme wél van toepassing is, al dan niet als "restcategorie".[27]

Gelet op het voorgaande adviseert de AP om de passage in de toelichting aan te passen.

6. Doorzoeking

De artikelen 2 en 3 van het voorstel regelen de "toegang" van bepaalde aangewezen autoriteiten tot genoemde systemen. Volgens de memorie van toelichting omvang het begrip "toegang tot een systeem" tevens "doorzoeking" ervan.[28]

De AP wijst erop dat deze uitleg niet in lijn is met de verordeningen zelf waarin nadrukkelijk onderscheid wordt gemaakt tussen "toegang" en "doorzoeking" en evenmin met artikel 9 van het concept dat juist specifiek betrekking heeft op doorzoeking van een register.

Gelet op de tekst van de verordeningen en gelet op de eis van heldere en voorzienbare wetgeving voor het verwerken van persoonsgegevens in artikel 6, derde lid, van de AVG, adviseert de AP om de term doorzoeking expliciet op te nemen in de artikelen 2 en 3.

7. Uitvoeringstoets

De AP wordt aangewezen als toezichthouder op het gebruik van de nieuwe informatiesystemen door Nederlandse publieke autoriteiten.

Zoals de AP heeft onderstreept in de uitvoeringstoets op de EU verordeningen is het toezichtveld bijzonder complex en omvangrijk, onder meer vanwege de noodzakelijke afstemming van het toezicht met de EDPS

[26] Artikel 55, tweede lid, AVG luidt: 2. In het geval van verwerking door overheidsinstanties of door particuliere organen die handelen op grond van artikel 6 lid 1, onder c) of e), is de toezichthoudende autoriteit van de lidstaat in kwestie competent. In dergelijke gevallen is artikel 56 niet van toepassing.
[27] Toelichting, blz. 39-40.
[28] Toelichting, blz. 98.

en de andere Europese privacytoezichthouders. Bovendien is sprake van een complex wettelijk kader, zoals ook in de toelichting wordt erkend.[29] Niet alleen geldt dat de verschillende verordeningen ieder (deels) eigen regels voor de verwerking van persoonsgegevens introduceren, ook geldt dat deze nieuwe verordeningen (deels) teruggrijpen op de bestaande algemene regels uit de AVG en de RGB. En ten slotte gaat het om een veelheid aan instanties die gebruik maken van de nieuwe informatiesystemen, zoals de Douane, Nationale Politie (NP), Koninklijke Marechaussee (Kmar), Immigratie- en naturalisatiedienst (IND)en het Ministerie van Buitenlandse Zaken.

In de uitvoeringstoets wijst de AP tegen de achtergrond van de al bestaande werklast op de extra taken van onder meer verplichte periodieke audits, klachten in behandeling nemen en deelnemen aan verplichte Europese samenwerkingscomités die het voorstel tot gevolg heeft, hetgeen leidt tot een benodigd aantal van 11,06 fte.

De lidstaten zorgen ervoor dat hun toezichthoudende autoriteit over voldoende middelen beschikt om haar taken uit hoofde van deze verordening te kunnen vervullen, en toegang heeft tot advies van personen met voldoende kennis van biometrische gegevens. Zonder een adequaat toezicht van de nationale toezichthouder komt het grondrecht op gegevensbescherming in de sfeer van de EU-verordeningen onder druk.

De AP adviseert in de toelichting in te gaan op de uitvoeringstoets van de AP in het licht van een adequate borging van uitvoering van het toezicht op het grondrecht van verwerking van persoonsgegevens.

8. Evaluatie

De EU-verordeningen voorzien in evaluatiebepalingen. Dit neemt niet weg dat het uitvoeringsvoorstel nationale keuzes bevat, zoals de keuze voor de officier van justitie als centraal toetsingspunt rechtshandhaving en om voor wat betreft de bewaartermijn voor gegevens uit het SIS in een nationaal informatiesysteem (artikel 7) aan te sluiten bij de langere termijnen in de WPG en WJSG. Het gaat zodoende om nationale keuzes binnen het Europese kader van grootschalige verwerkingen van vaak bijzondere categorieën van persoonsgegevens of gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten. Bovendien is in het regeerakkoord uit 2017 opgenomen dat *alle* nieuwe wetgeving waarin gegevensbewaring wordt geregeld ten behoeve van de opsporing van ernstige strafbare feiten na vijf jaar zal worden geëvalueerd, waarbij in ieder geval aandacht zal worden besteed aan de effectiviteit en de impact van die wetgeving.[30]

Gelet op het voorgaande adviseert de AP om in het voorstel een evaluatiebepaling op te nemen over onder meer de effectiviteit en impact van de uitvoeringswet op de bescherming van persoonsgegevens.

[29] Opmerking verdient dat de uitvoeringstoets ook betrekking op het voorstel voor de uitvoeringswet ECRIS-TCN. Maar de voorliggende verordeningen vormen de hoofdmoot wat betreft belasting.
[30] Regeerakkoord VVD, CDA D66 en ChristenUnie, Vertrouwen in de toekomst, 10 oktober 2017, blz. 6.

AUTORITEIT
PERSOONSGEGEVENS

Datum
19 mei 2021

Ons kenmerk
[redacted]

Openbaarmaking van het advies

De AP is voornemens dit advies na vier weken openbaar te maken op de website www.autoriteitpersoonsgegevens.nl. Behoudens tegenbericht gaat zij ervan uit dat hiertegen geen bezwaar bestaat.

Hoogachtend,
Autoriteit Persoonsgegevens

[redacted]

Bestuurslid