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

Aangetekend
De Staatssecretaris van Veiligheid en Justitie
De heer mr. dr. K.H.D.M. Dijkhoff
Directie Wetgeving en Juridische Zaken
Sector Staats- en bestuursrecht
Postbus 20301
2500 EH DEN HAAG

Datum	Ons kenmerk	Uw brief van
7 april 2017	z2017-01571	16 februari 2017
	Contactpersoon	Uw kenmerk
		2044742

Onderwerp
Verzoek om advies ten aanzien van wetsvoorstel inzake implementatie van Richtlijn (EU) 2016/680

Geachte heer Dijkhoff,

Bij brief van 16 februari 2017, ontvangen op 22 februari, heeft u de Autoriteit Persoonsgegevens (hierna: de AP) verzocht om op grond van artikel 51, tweede lid, van de Wet bescherming persoonsgegevens te adviseren over het wetsvoorstel tot wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen (hierna: de Wijzigingswet).

De AP voldoet met dit advies aan uw verzoek. Op 29 maart 2017 heeft de AP van u een gewijzigde versie van het wetsvoorstel ontvangen. De AP heeft kennisgenomen van de aangebrachte wijzigingen, maar heeft haar advies gebaseerd op de oorspronkelijke, op 22 februari 2017 ontvangen versie.

Bij brief van 20 maart 2017 heeft u de AP gevraagd eveneens te adviseren over het voorstel van wet inzake regels ter uitvoering van 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 (PbEU 2016, L 119/1) (hierna: de Uitvoeringswet). Over dat wetsvoorstel ontvangt u een separaat advies.

Datum
7 april 2017

Ons kenmerk
z2017-01571

Inhoud van het wetsvoorstel Wijzigingswet

De adviesaanvraag betreft het volgende voorstel.

Het wetsvoorstel strekt tot wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van de 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 (PbEU 2016, L 119/89) (hierna: de Richtlijn). Bij de implementatie van de Richtlijn is het algemene uitgangspunt van beleidsneutraliteit gehanteerd. Dit houdt in dat het bestaande recht wordt gehandhaafd, tenzij de Richtlijn daaraan in de weg staat. De AP adviseert over de Richtlijn met inachtneming van het vorenstaande en neemt daarbij in aanmerking dat, voor zover het wetsvoorstel voorziet in bepalingen over de oprichting, de taken en bevoegdheden van de AP, daarover, vanwege de samenhang met de Uitvoeringswet, in het advies over de Uitvoeringswet wordt geadviseerd. Deze bepalingen uit de Wijzigingswet blijven derhalve in dit advies buiten beschouwing.

Separaat zullen het Besluit politiegegevens en het Besluit justitiële gegevens worden gewijzigd. De AP verzoekt deze te zijner tijd ter advisering voorgelegd te krijgen.

Advies

I. Rechtsgrondslag en reikwijdte van de Richtlijn

1 Inleiding

Het oorspronkelijke voorstel van de Europese Commissie[1] beoogde te komen tot een richtlijn die ziet op 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. Later in het wetgevingsproces is daaraan toegevoegd dat de doelstellingen waarop de Richtlijn ziet, tevens omvat 'met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid' ('including the safeguarding against and the prevention of threats to public security').

Voor een doeltreffende justitiële samenwerking in strafzaken en een doeltreffende politiële samenwerking is het, zo wordt in de overwegingen bij de Richtlijn gesteld, van het allergrootste belang dat een consequente en hoge mate van bescherming van de persoonsgegevens van natuurlijke personen wordt gewaarborgd, én dat de uitwisseling van persoonsgegevens tussen de bevoegde autoriteiten van de lidstaten wordt vergemakkelijkt. Daartoe moet in alle lidstaten worden voorzien in een gelijkwaardige mate van bescherming van de rechten en vrijheden van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het

[1] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25.1.2012 COM(2012) 10 final.

onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid. Doeltreffende bescherming van persoonsgegevens in de gehele Unie vereist versterking van de rechten van de betrokkenen en van de verplichtingen van degenen die persoonsgegevens verwerken, alsmede gelijkwaardige bevoegdheden om de regelgeving inzake de bescherming van persoonsgegevens in de lidstaten te handhaven en toe te zien op naleving daarvan.

De implementatie van de Richtlijn beperkt zich tot aanpassing op onderdelen van de bestaande nationale wetgeving, in aanvulling op hetgeen reeds eerder naar aanleiding van het kaderbesluit dataprotectie is aangepast. Uit de memorie van toelichting leidt de AP af dat de keuze voor een minimumimplementatie een gevolg is van het destijds bij de implementatie van het kaderbesluit dataprotectie in de Wpg en Wjsg (Stb. 2011, 490) gehanteerde uitgangspunt van een zoveel mogelijk extensieve werking van de regels van het kaderbesluit voor de verwerking en verstrekking van de persoonsgegevens. Dit wil zeggen dat de regels van het kaderbesluit ook golden voor de gegevens die uitsluitend op nationaal niveau werden verwerkt, aldus de memorie van toelichting.

2 Huidige naleving van de norm in relatie tot de keuze voor een minimumimplementatie

Bij brief van 7 december 2015 [2] heeft de Minister van Veiligheid en Justitie (hierna: de minister) de Tweede Kamer geïnformeerd over de privacy-audit die de Auditdienst Rijk (hierna: ADR) heeft verricht naar de naleving van de Wpg door de politie. De minister verwijst daarbij tevens naar de onderzoeksresultaten van het (toenmalige) CBP naar de naleving door de politie in Nederland van informatiebeveiligings- en gegevensbeschermingsvoorschriften van het Schengen Informatiesysteem (N.SIS II). In deze brief merkt de minister op dat op basis van eerdere audits en de evaluatie van de Wpg uit 2013 reeds duidelijk was dat de Wpg, de politiepraktijk en de huidige ICT-ondersteuning niet goed op elkaar aansluiten. In de toenmalige evaluatie werd dit gekenmerkt als een 'worstelende praktijk'. In de auditrapportage van de ADR wordt het beeld van een worstelende praktijk volgens de minister opnieuw bevestigd. In deze rapportage wordt gesignaleerd dat de politie op vijf essentiële thema's – autoriseren, verstrekken, protocolleren, bewaartermijnen en rechten van betrokkene – nog onvoldoende aan de wet voldoet. Een van de verklarende factoren die daarbij een rol bij speelt, is de complexiteit van de Wpg, aldus de auditrapportage. Naar aanleiding daarvan heeft de minister aangekondigd om de Wpg en de eveneens geëvalueerde Wjsg in onderlinge samenhang te zullen herzien. Het doel van deze herziening was om de complexiteit van beide wetten voor de uitvoeringspraktijk terug te dringen en de toepasbaarheid ervan in de keten te vergroten.

In de brief van de minister van 7 december 2015 stelt hij dat die herziening nog niet kan plaatsvinden vanwege de lopende onderhandelingen in Brussel over de verordening en de richtlijn en dat de herziening zal moeten aansluiten bij deze ontwikkelingen in EU-verband. Daarbij geeft de minister aan een tussentijdse wetswijziging onwenselijk te vinden, omdat daarmee de uitvoeringspraktijk in korte tijd twee keer zou worden belast met wijzigingen in deze complexe wetgeving. De thans gehanteerde minimumimplementatie leidt er echter toe dat de uitvoeringspraktijk op termijn tweemaal zal worden geconfronteerd met wijzigingen in het van toepassing zijnde wettelijk kader van gegevensbescherming:

[2] https://zoek.officielebekendmakingen.nl/kst-33842-3.html

eenmaal door de onderhavige Wijzigingswet en eenmaal door de voorgenomen algehele herziening van het stelsel van de Wpg en de Wjsg.
In haar rol als toezichthouder herkent de AP dat de naleving van de geldende normen nog steeds op problemen stuit. Hetgeen ertoe heeft geleid dat de AP de laatste jaren meerdere handhavingstrajecten heeft doorlopen. De AP acht het van groot belang dat de politie, gelet op de belangrijke rol die zij in de rechtsstaat heeft en de grote schaal waarop in dat verband - veelal gevoelige - persoonsgegevens worden verwerkt, daadwerkelijk voldoet aan de bij die verwerkingen te stellen wettelijke eisen en dat de politie komt tot het realiseren van het verbeterplan inzake de informatiebeveiliging.[3] De AP acht de gemaakte keuze voor een minimumimplementatie daarom niet bevorderlijk voor de tussentijdse naleving van de geldende normen.

3 Implementatie van EU-richtlijnen in de nationale wetgeving

Een EU-Verordening heeft rechtstreekse werking in de lidstaten en hoeft als zodanig niet te worden omgezet naar nationaal recht. Een EU-Richtlijn daarentegen behoeft omzetting in de nationale wet- en regelgeving door middel van implementatie in nieuwe regelgeving dan wel aanpassing van bestaande regelgeving. De wetgever is gehouden zorg te dragen voor de objectieve rechtmatigheid van onze rechtsorde en is daarmee verantwoordelijk voor een tijdige, volledige en correctie implementatie van richtlijnen. Waar de bestaande constructie van nationale wetgeving onvoldoende aansluit bij de nieuwe voorschriften waarvan implementatie wordt verlangd, kan dit evenwel tot gevolg hebben dat meer fundamentele en mogelijk ingrijpende aanpassingen van de bedoelde wetgeving noodzakelijk zijn.

Ieder bestuursorgaan is daarentegen verplicht om in zijn handelen of nalaten Unierecht niet te schenden, ook in een situatie waarin nationale regelgeving niet met het Unierecht in overeenstemming is. Daaruit volgt dat bestuursorganen zich niet exclusief kunnen verlaten op het nationale recht en zelfstandig dienen na te gaan of de nationale regelgeving conform het Unierecht is. Zo nodig moeten bestuursorganen zelfstandig nationale wetgeving terzijde stellen, wanneer de toepassing daarvan hen in strijd brengt met direct werkende bepalingen van het Unierecht, zijnde bepalingen die 'onvoorwaardelijk en voldoende nauwkeurig zijn' (zie zaak C-103/88 van het Hof van Justitie van de Europese Unie). Een dergelijke verplichting geldt voor bestuursorganen ook om tot richtlijnconforme interpretatie over te gaan (zie zaken C-462/99 en C-198/01).

Op grond van het in het nationale recht verankerde legaliteitsbeginsel behoeft de bevoegdheid van bestuursorganen een wettelijke grondslag. Bestuursorganen kunnen hun bevoegdheid daarbij in beginsel rechtstreeks baseren op het Unierecht.[4] Dit betekent naar vaste rechtspraak van het Hof van Justitie echter niet dat in het geval van een onvolledige of onjuiste implementatie van een richtlijn deze uit zichzelf aan particulieren verplichtingen kan opleggen en een bepaling van een richtlijn als zodanig tegenover een particulier kan worden ingeroepen (zie bijvoorbeeld zaak C-201/02 van het Hof van Justitie; ECLI:EU:C:2004:12). De Afdeling Bestuursrechtspraak van de Raad van State is evenmin ruimhartig wat betreft het kunnen handhaven van nationale regelgeving die niet richtlijnconform geïnterpreteerd is.[5]

[3] https://www.rijksoverheid.nl/documenten/rapporten/2016/05/27/tk-bijlage-verbeterplan-wet-politiegegevens-en-informatiebeveiliging
[4] Uitspraak van de ABRvS van 24 december 2008; LJN BG8291
[5] Zie de uitspraken van 8 juni 2016, ECLI:NL:RVS: 2016:1613; 4 maart 2009, ECLI:NL:RVS:2009:BH4621; 1juni 2011, ECLI:NL:RVS: 2011:BQ6832; 28 februari 2007: AZ9494 en 28 januari 2009, ECLI:NL:RVS:2009:BH1137.

Dit zou concreet voor de AP betekenen dat zij niet handhavend kan optreden op grond van onvolledige of onjuiste geïmplementeerde rechtstreeks werkende bepalingen uit de Richtlijn.

De hierna beschreven onderdelen van de te implementeren Richtlijn leiden de AP tot de conclusie dat de voorstellen zoals vervat in de Wijzigingswet ter implementatie van de Richtlijn dermate problematisch zijn dat een meer fundamentele benadering nodig is om te komen tot een toereikende omzetting van de Richtlijn in nationale regelgeving. In het bijzonder maar niet uitsluitend gaat het hierbij om de uitleg van het autonoom Unierechtelijke begrip 'strafbaar feit', de omzetting van het begrip 'verwerkingsverantwoordelijke' in relatie tot het begrip 'bevoegde autoriteit' en de in de Wijzigingswet opgenomen begrippen 'beheer' en 'gezag'.

4 Rechtsgrondslag voor de Richtlijn

De Richtlijn maakt, zoals hiervoor vermeld samen met de Verordening, deel uit van het gehele pakket tot herziening van EU-regelgeving ten aanzien van de bescherming van persoonsgegevens. Krachtens artikel 8, eerste lid, van het Handvest van de grondrechten van de EU (Handvest) en artikel 16, eerste lid, van het Verdrag betreffende de werking van de Europese Unie (VWEU) heeft eenieder recht op bescherming van de hem betreffende persoonsgegevens.

Overeenkomstig artikel 52, eerste lid, van het Handvest moeten beperkingen op de uitoefening van de in het Handvest erkende rechten en vrijheden bij wet worden gesteld en de wezenlijke inhoud van die rechten en vrijheden worden geëerbiedigd. Met inachtneming van het evenredigheidsbeginsel kunnen slechts beperkingen worden gesteld, indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen. Het derde lid van dit artikel bepaalt dat, voor zover het Handvest rechten bevat die corresponderen met rechten die zijn gegarandeerd door het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), de inhoud en reikwijdte ervan dezelfde zijn als die er door dat verdrag aan worden toegekend. Deze bepaling verhindert echter niet dat het recht van de Unie een ruimere bescherming biedt. Dat brengt tevens mee dat de diverse kernbegrippen uit deze Europese regelgeving worden gebezigd overeenkomstig de autonome betekenis en uitleg die daaraan volgens Unierecht en de daarmee verband houdende jurisprudentie van het Hof van Justitie en van het Europese Hof voor de rechten van de mens (EHRM) wordt gegeven.

Op grond van artikel 16, tweede lid, van het VWEU stelt de Europese wetgever volgens de gewone wetgevingsprocedure de voorschriften vast betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie, alsook door de lidstaten, bij de uitoefening van activiteiten die binnen het toepassingsgebied van het recht van de Unie vallen, alsmede de voorschriften betreffende het vrij verkeer van die gegevens.

Uit overweging 10 bij de Richtlijn blijkt het uitgangspunt dat op grond van Verklaring nr. 21 betreffende de bescherming van persoonsgegevens op het gebied van justitiële samenwerking in strafzaken en politiële samenwerking, gehecht aan de slotakte van het Verdrag van Lissabon is aangenomen dat, vanwege de specifieke aard van de justitiële samenwerking in strafzaken en de politiële samenwerking, op die gebieden specifieke voorschriften inzake de bescherming van persoonsgegevens en het vrije verkeer van persoonsgegevens op basis van artikel 16 van het VWEU nodig zouden kunnen blijken. Om die reden – zo is overwogen onder overweging 11 – zijn in de Richtlijn specifieke regels vastgesteld voor 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 of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, daarbij rekening houdend met de specifieke aard van die activiteiten. Verwerking door die autoriteiten voor andere doeleinden dan in de Richtlijn omschreven, valt binnen het toepassingsgebied van de Verordening.

5 Betekenis van het autonoom Unierechtelijk begrip 'strafbaar feit' voor de reikwijdte van de Richtlijn
In overweging 13 bij de Richtlijn staat vermeld dat een strafbaar feit (in het Engels: criminal offence) in de zin van de Richtlijn een autonoom Unierechtelijk begrip moet zijn zoals uitgelegd door het Hof van Justitie. De uitleg van dit begrip is van fundamenteel belang voor de reikwijdte en daarmee de doorwerking van deze richtlijn in de Nederlandse rechtsorde.

Het begrip 'strafbaar feit' kan op twee manieren worden uitgelegd. In de eerste plaats is een formele benadering mogelijk, waarbij doorslaggevend is dat het nationale recht van de lidstaten een overtreding als strafbaar feit aanmerkt. In de tweede plaats kan het begrip – in lijn met de jurisprudentie van het EHRM in onder meer het arrest van 8 juni 1976 in de zaak Engel e.a. tegen Nederland (CE:ECHR:1976:1123JUD000510071) – functioneel benaderd worden. Hierbij is met name van belang of sancties een repressief doel hebben. De kwalificatie van een overtreding naar nationaal recht als strafrechtelijk is bij deze benadering op zichzelf niet doorslaggevend. Zie in dezelfde lijn zaak C-60/12, waarin werd benadrukt dat het begrip 'met name in strafzaken bevoegde rechter' een autonoom Unierechtelijk begrip is, waarbij de kwalificatie van strafbare feiten door de lidstaten niet doorslaggevend is. Bepalend voor de vraag van welke uitleg van het begrip 'strafbaar feit' moet worden uitgegaan, is de rechtsgrondslag van de Richtlijn.

Uit de jurisprudentie van het Hof van Justitie (zaak C-43/12; ECLI:EU:C:2014:298) volgt dat een formele benadering van het begrip 'strafbaar feit' specifiek geldt voor besluitvorming die als rechtsgrondslag artikel 87 van het VWEU (politiële samenwerking) heeft. In alle andere gevallen dient te worden uitgegaan van een functionele benadering van het desbetreffende begrip.

De rechtsgrondslag van de onderhavige richtlijn betreft artikel 16, tweede lid, van het VWEU, zodat het begrip 'strafbaar feit' functioneel dient te worden benaderd in lijn met het arrest van het Hof van Justitie van 5 juni 2012, zaak C-489/10, waarin het Hof van Justitie aansluit bij de zogeheten Engel-criteria zoals geformuleerd door het EHRM. Ook de Europese Commissie houdt deze uitleg van het begrip 'strafbaar feit' aan in het licht van de Richtlijn.[6] Deze functionele benadering houdt in dat het doel waarvoor de verwerking van persoonsgegevens plaatsvindt, bepalend is voor de vraag of de Richtlijn daarop van toepassing is en niet het/de verwerkende orgaan/entiteit en/of de kwalificatie van de overtreding naar Nederlands recht. Het onderhavige wetsvoorstel miskent dit, waardoor de reikwijdte van de Richtlijn te nauw is opgevat. De verwerking van persoonsgegevens die plaatsvindt door alle daartoe bevoegde autoriteiten – publiek en privaat - met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten ('criminal offences') – dat wil zeggen feiten waarop met een bestraffende bestuurlijke sanctie (waaronder in ieder geval een bestuurlijke boete) of zwaarder kan worden gereageerd

[6] Minutes of the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 van 7 November 2016 (http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=27802&no=2)

– of de tenuitvoerlegging daarvan, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, geheel onder de reikwijdte van de Richtlijn valt en daarmee dus niet onder de reikwijdte van de Verordening.

Naar thans het inzicht van de AP leidt de bovenstaande benadering voor de praktijk tot een grotere mate van rechtszekerheid en een eenduidige beantwoording van de vraag of de Richtlijn op de gegevenswerking van toepassing is. De verwerking van persoonsgegevens door bijvoorbeeld het CJIB valt daarmee – ook indien voor een bestuurlijke punitieve sanctie wordt gekozen – in zijn geheel onder de bescherming van de Richtlijn. Dit geldt ook voor de gegevensverwerking door andere toezichthouders en bestuursorganen die bevoegd zijn om in ieder geval bestraffende bestuurlijke sancties op te leggen.

Gelet hierop is voor de in de Wijzigingswet gekozen beperkte, functionele benadering van het begrip 'bevoegde autoriteit' uit de Richtlijn geen plaats, nu daarmee geen recht wordt gedaan aan de bevoegde autoriteiten – publiek en privaat – die bevoegd zijn om in ieder geval een bestuurlijke sanctie op te leggen. Een meer materiële benadering van het begrip 'bevoegde autoriteit' zou hier meer voor de hand hebben gelegen, zodat recht wordt gedaan aan de reikwijdte van de Richtlijn, die breder is dan slechts de uitoefening van de politietaak.

Conclusie begrip 'strafbaar feit'
De rechtsgrondslag van de onderhavige Richtlijn is artikel 16, tweede lid, van het VWEU, zodat het begrip 'strafbaar feit' in lijn met het arrest van het Hof van Justitie van 5 juni 2012, zaak C-489/10, waarin het Hof van Justitie aansluit bij de zogeheten Engel-criteria zoals geformuleerd door het EHRM, functioneel benaderd dient te worden. Dit betekent dat het doel waarvoor de verwerking van persoonsgegevens plaatsvindt, bepalend is voor de vraag of de Richtlijn daarop van toepassing is en niet het verwerkende orgaan/de entiteit en/of de kwalificatie van het strafbaar feit naar Nederlands recht. Dit heeft tot gevolg dat de reikwijdte van de Richtlijn breder is. Doordat dit in het wetsvoorstel is miskend, is een heroverweging van de in het wetsvoorstel gemaakte keuzes ter implementatie van de Richtlijn op zijn plaats. De AP wijst er in dat kader op dat een verbreding en versteviging van de boetebevoegdheid in dat geval zeker is vereist. Volledigheidshalve wordt hierbij verwezen naar het besprokene bij II onder 2.

Hieronder wordt over de Wijzigingswet verder geadviseerd, waarbij de door de wetgever aangehouden reikwijdte van de Richtlijn tot uitgangspunt wordt genomen.

6 Implementatie begrip 'verwerkingsverantwoordelijke'

De verwerkingsverantwoordelijke is in artikel 3, achtste lid, van de Richtlijn gedefinieerd als de bevoegde autoriteit die, alleen of samen met andere, de doeleinden van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doeleinden van en de middelen voor die verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

In Advies 1/2010 van de Artikel 29 Werkgroep[7] wordt ten aanzien van het begrip 'voor de verwerking verantwoordelijke' vooropgesteld dat dit begrip autonoom is in die zin dat het met name dient te worden

[7] Advies 1/2010 van de Werkgroep gegevensbescherming Artikel 29 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", vastgesteld te Brussel op 16 februari 2010.

geïnterpreteerd volgens de communautaire wetgeving voor gegevensbescherming. Daarnaast is het functioneel in die zin dat het bedoeld is om de verantwoordelijkheden te leggen op de plaats waar ook de feitelijke invloed ligt. Allereerst is bepalend wie verantwoordelijk is voor de naleving van de regelgeving voor gegevensbescherming en de manier waarop betrokkenen de rechten in de praktijk kunnen uitoefenen. Het doel van 'bescherming van personen in verband met de verwerking van persoonsgegevens' kan alleen worden bereikt en in de praktijk gestalte krijgen wanneer de voor de verwerking van gegevens verantwoordelijken met wettelijke en andere middelen voldoende kunnen worden gestimuleerd om alle maatregelen te nemen die noodzakelijk zijn om deze bescherming in de praktijk tot stand te brengen. Wie het doel van de verwerking vaststelt, wordt in ieder geval als voor de verwerking verantwoordelijk aangemerkt, terwijl bij het vaststellen van de middelen alleen van verantwoordelijkheid sprake is wanneer die vaststelling betrekking heeft op de wezenlijke aspecten van de middelen, aldus het Advies.

Hieronder wordt ingegaan op de wijze waarop het begrip 'verwerkingsverantwoordelijke' is geïmplementeerd in de Wijzigingswet en hoe dit zich verhoudt tot de systematiek van de Richtlijn.

a) Onderscheid tussen verwerkingsverantwoordelijke en de bevoegde autoriteit
De Richtlijn stelt het begrip bevoegde autoriteit centraal. Omdat dit begrip bepalend is voor het toepassingsbereik van zowel de Richtlijn als de Wpg en de Wjsg en samenhangt met het begrip verwerkingsverantwoordelijke, volgt hierna eerst een korte uiteenzetting van het relevante juridisch kader.

Omschrijving in Richtlijn
De Richtlijn heeft in artikel 2, eerste lid, opgenomen dat deze van toepassing is op de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de doeleinden van artikel 1, eerste lid.

Een bevoegde autoriteit is in artikel 3, aanhef en onder het zevende lid van de Richtlijn omschreven als:
a) iedere overheidsinstantie die bevoegd is voor de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid; of
b) ieder ander orgaan dat of iedere andere entiteit die krachtens het lidstatelijke recht is gemachtigd openbaar gezag en openbare bevoegdheden uit te oefenen met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

Omschrijving in Wpg
In artikel 2 van de Wpg wordt na implementatie van de Richtlijn de volgende toevoeging opgenomen (onderstreping): Deze wet is van toepassing op de verwerking van politiegegevens door een bevoegde autoriteit die in een bestand zijn opgenomen of die bestemd zijn daarin te worden opgenomen.

Artikel 1, aanhef en onder l, van de Wpg komt als volgt te luiden:
Een bevoegde autoriteit is iedere overheidsinstantie die bevoegd is voor de taken, bedoeld in onderdeel a, of ieder ander orgaan dat of iedere andere entiteit die is gemachtigd openbaar gezag en openbare bevoegdheden uit te oefenen met het oog op de taken, bedoeld in onderdeel a.
Onderdeel a van ditzelfde artikel 1 geeft de volgende definitie van de bedoelde taken:
Een politiegegeven is elk persoonsgegeven dat wordt verwerkt in het kader van de uitoefening van de

politietaak, bedoeld in de artikelen 3 en 4, met uitzondering van de uitvoering van de bij of krachtens de Vreemdelingenwet 2000 gestelde voorschriften en opgedragen taken, bedoeld in de artikelen 1, eerste lid, onderdeel i, onder 1° en 4, onderdeel f, van de Politiewet 2012.

Volgens artikel 3 van de Politiewet heeft de politie tot taak in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven. Artikel 4 van de Politiewet is gekoppeld aan de politietaken van de Koninklijke Marechaussee.

In artikel 1, aanhef en onder f, van de *huidige* Wpg zijn de verantwoordelijken specifiek aangewezen:
1. de politie: de korpschef, bedoeld in artikel 27 van de Politiewet 2012;
2. de rijksrecherche: het College van procureurs-generaal;
3. de Koninklijke marechaussee: Onze Minister van Defensie;
4. een gemeenschappelijke verwerking van politiegegevens met het oog op een gemeenschappelijk doel door twee of meer organisaties als bedoeld in dit onderdeel: de verantwoordelijke die door de betrokken verantwoordelijken is belast met de feitelijke zorg voor de verwerking en het treffen van de maatregelen, bedoeld in artikel 4.

De aanwijzing van deze functionele verwerkingsverantwoordelijken blijft in de Wijzigingswet ongewijzigd.

Implementatie begrippen bevoegde autoriteit en verwerkingsverantwoordelijke in Wpg
Zowel de Richtlijn als de Wpg verklaren deze van toepassing indien sprake is van bepaalde gegevensverwerkingen door een bevoegde autoriteit, waarbij een bevoegde autoriteit niet tevens verwerkingsverantwoordelijke hoeft te zijn. De Richtlijn koppelt het zijn van verwerkingsverantwoordelijke aan het begrip bevoegde autoriteit.

In tegenstelling tot de Richtlijn wordt het begrip verwerkingsverantwoordelijke in de Wpg niet materieel gedefinieerd als diegene die doel en middelen vaststelt. Op nationaal niveau zijn – waartoe de Richtlijn op zichzelf ruimte laat – de verwerkingsverantwoordelijken uit hoofde van hun functie als zodanig aangewezen in de Wpg, dan wel in bijzondere wetgeving zoals het Besluit politiegegevens bijzondere opsporingsdiensten. Ondanks dat in de memorie van toelichting van de Wijzigingswet bij artikel 1, onder f, van de Wpg de koppeling tussen degene die het doel en de middelen bepaalt en het bevoegde gezag expliciet wordt benoemd, is echter de vraag of de gekozen wijze van omzetting in de Wijzigingswet, gelet op de systematiek van de Richtlijn, daaraan ook daadwerkelijk een juiste invulling geeft.

Wellicht moet worden aangenomen dat de als verwerkingsverantwoordelijke benoemde functies, in samenhang gelezen met de Richtlijn, het begrip bevoegde autoriteit impliceren. Indien naar de definitie van bevoegde autoriteit wordt gekeken geldt dat in ieder geval voor een aantal functies, zoals bijvoorbeeld die van de Korpschef; die is zowel verwerkingsverantwoordelijke als bevoegde autoriteit. Indien echter naar een aantal andere als verwerkingsverantwoordelijken aangemerkte functies wordt gekeken, dan moet geconcludeerd worden dat een aantal daarvan niet tevens ook bevoegde autoriteit zijn.
De Minister van Economische Zaken bijvoorbeeld heeft geen bevoegdheden ten aanzien van de uitoefening van politietaken. Zijn verwerkingsverantwoordelijkheid vloeit voort uit het feit dat de Wpg in het Besluit politiegegevens bijzondere opsporingsdiensten grotendeels van overeenkomstige toepassing

wordt verklaard op een aantal opsporingsdiensten en onder andere hij als verwerkingsverantwoordelijke daarbij wordt aangewezen.

Het begrip verwerkingsverantwoordelijke heeft daarmee op nationaal niveau een andere invulling gekregen dan in de Richtlijn: de koppeling met het begrip bevoegde autoriteit wordt in de Wijzigingswet daarmee niet gemaakt. Voor zover al moet worden aangenomen dat de verwerkingsverantwoordelijken tevens bevoegde autoriteit zijn, kan dat niet in alle gevallen worden volgehouden.

Bevoegde autoriteit in relatie tot de Buitengewoon Opsporingsambtenaar (BOA)
Daarnaast roept de implementatie van het begrip bevoegde autoriteit in de Wijzigingswet ook vragen van meer praktische aard op. Omdat het begrip bevoegde autoriteit niet tevens het zijn van verwerkingsverantwoordelijke impliceert, betekent dit dat ook hiërarchisch lager (dan de verwerkingsverantwoordelijke) geplaatsten onder dit begrip vallen. Als voorbeeld wordt de BOA genoemd. De BOA valt onder het begrip bevoegde autoriteit en zijn werkgever (bijvoorbeeld een gemeente) is de verwerkingsverantwoordelijke. Indien echter de verwerkingsverantwoordelijke in bepaalde gevallen niet tevens ook bevoegde autoriteit is - die de betreffende gegevens om die reden zelf ook mag verwerken - (bijvoorbeeld de gemeente als werkgever van een BOA), dan leidt dat tot de situatie dat de verwerkingsverantwoordelijke de gegevens waarvoor hij verantwoordelijk is niet zelf mag verwerken. In een aantal gevallen lijkt dat, juist vanwege de gezagsrelatie tussen verwerkingsverantwoordelijke en de hiërarchisch ondergeschikte bevoegde autoriteit niet wenselijk en ook praktisch gezien niet uitvoerbaar.

Implementatie begrippen bevoegde autoriteit en verwerkingsverantwoordelijke in Wjsg
Het begrip bevoegde autoriteit uit de Richtlijn is ook in de Wjsg geïmplementeerd.
Artikel 1, onder v, merkt de bevoegde autoriteit aan als de overheidsinstantie die bevoegd is voor of ieder ander orgaan of iedere andere entiteit belast met openbaar gezag of openbare bevoegdheden ter voorkoming van, het onderzoek naar, de opsporing van of de vervolging van strafbare feiten, of voor de tenuitvoerlegging van straffen.

Onderdeel k van artikel 1 benoemt de verwerkingsverantwoordelijken:
1. justitiële gegevens en rapporten in een persoonsdossier: Onze Minister;
2. strafvorderlijke gegevens: het College van procureurs-generaal;
3. tenuitvoerleggingsgegevens: Onze Minister dan wel het College van procureurs-generaal;
4. gerechtelijke strafgegevens: de gerechten, bedoeld in artikel 2 van de Wet op de rechterlijke organisatie.

Omdat ook de Wjsg een implementatie is van dezelfde hiervoor genoemde begrippen uit de Richtlijn geldt ook hier dat de vraag aan de orde is of de verwerkingsverantwoordelijken tevens als bevoegde autoriteit kunnen worden aangemerkt. Dat is ook hier niet steeds het geval omdat bijvoorbeeld de Minister van Veiligheid en Justitie geen eigen zelfstandige bevoegdheden heeft ter voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen. Wat daarnaast opvalt is dat, in tegenstelling tot de Wpg waarin het van toepassing zijn van die wet wordt gekoppeld aan de verwerking door een bevoegde autoriteit, dit bij de Wjsg niet het geval is. De implementatie heeft op dit punt niet juist plaatsgevonden.

Conclusie onderscheid tussen verwerkingsverantwoordelijke en de bevoegde autoriteit
Gelet op het vorenstaande is de AP van oordeel dat, ondanks dat de koppeling tussen verwerkingsverantwoordelijke en bevoegde autoriteit als zodanig in de memorie van toelichting wordt benoemd, de implementatie van de begrippen bevoegde autoriteit en verwerkingsverantwoordelijke in de Wijzigingswet niet in overeenstemming is met hetgeen de Richtlijn hierover bepaalt. De AP adviseert de Richtlijn alsnog als zodanig te implementeren.

b) De verwerkingsverantwoordelijke en het onderscheid tussen beheer en gezag
Op verschillende plaatsen in de huidige Wpg en Wjsg en in de Wijzigingswet dan wel in aanverwante wetgeving zoals de Politiewet komt het onderscheid tussen de begrippen beheer en gezag voor. Soms wordt dit expliciet benoemd in bepaalde artikelen en soms speelt het begrip beheer - impliciet - een rol bij de vraag wie als verwerkingsverantwoordelijke moet worden aangemerkt voor bepaalde taken. Het onderscheid tussen beheer en gezag is niet nieuw, maar is in de Wijzigingswet wel bepalend voor de vraag wie als verwerkingsverantwoordelijke moet worden aangemerkt en is in zoverre derhalve relevant.

Een dergelijk onderscheid tussen beheer en gezag kent de Richtlijn niet. Een vraag die in dit verband beantwoording behoeft is of het nationale onderscheid tussen beheer en gezag een juiste implementatie van het begrip 'verwerkingsverantwoordelijke' behelst.

Beheer
Het begrip beheer lijkt in de huidige Wpg en Wjsg en in de Wijzigingswet verweven te zijn met het begrip verwerkingsverantwoordelijke: diegenen die het beheer voeren zijn aangemerkt als verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke voor verwerking van politiegegevens door de politie bijvoorbeeld is ingevolge de Wpg de Korpschef. De Korpschef is echter niet diegene die ook het gezag over de politie en de zeggenschap over de uitoefening van hun taken uitoefent. Het beheercriterium als criterium voor het aanwijzen van verwerkingsverantwoordelijken wijkt daarmee af van de in de Richtlijn opgenomen definitie ter bepaling van de vraag wie als verwerkingsverantwoordelijke moet worden aangemerkt: diegene die doel en middelen bepaalt. Het begrip 'beheer' relateert namelijk enkel aan het vaststellen van middelen.

Gezag
Het begrip gezag is bezien vanuit de relevante artikelen in de huidige Wpg en de Politiewet 2012, gerelateerd aan de vraag wie vanuit zijn functie aan de politie opdrachten geeft wat betreft de uitoefening van hun feitelijke werkzaamheden. Wat betreft de handhaving van de openbare orde en de uitvoering van de hulpverleningstaak volgt uit artikel 11 van de Politiewet dat dat gezag aan de burgemeester is. Wat betreft de strafrechtelijke handhaving is dat blijkens artikel 12 van de Politiewet de Officier van Justitie. Het gezagscriterium in de Wijzigingswet kan, gezien de definitie van het begrip 'verwerkingsverantwoordelijke' (in de Richtlijn tevens bevoegde autoriteit) in de Richtlijn (mede)bepalend zijn voor de vraag wie als zodanig moet worden aangemerkt, aangezien vanuit deze gezagsverhouding in concrete gevallen in ieder geval de doelen van de verwerking zullen worden bepaald. Daarmee relateert het begrip 'gezag' aan het bepalen van het doel van de verwerking.

Beheer en gezag bij en over BOA's
Zoals hiervoor al opgemerkt vallen BOA's - en de politiegegevens die zij verwerken - na de implementatie van de Richtlijn onder het begrip bevoegde autoriteit en daarmee onder de werking van de Wpg.

In de memorie van toelichting is hierover opgenomen "dat in het 'Besluit politiegegevens bijzondere opsporingsdiensten' de verantwoordelijke is aangewezen voor de verwerking van politiegegevens door een bijzondere opsporingsdienst. In dit besluit zal ook de overeenkomstige toepassing van onderdelen van de Wet politiegegevens op de verwerking van politiegegevens door een buitengewoon opsporingsambtenaar, als bedoeld in artikel 142, eerste lid, van het Wetboek van Strafvordering, worden uitgewerkt. Als verwerkingsverantwoordelijke zal worden aangewezen de werkgever, bedoeld in artikel 1, onderdeel h, van het Besluit buitengewoon opsporingsambtenaar".

In geval van een BOA in dienst van een gemeente, is derhalve de gemeente de werkgever en daarmee de verwerkingsverantwoordelijke voor de verwerking van politiegegevens. De vraag is vervolgens waar het gezag met betrekking tot de taakuitoefening van de BOA berust. Wordt dit bepaald door zijn akte van opsporingsbevoegdheid (vgl. artikel 5 Besluit buitengewoon opsporingsambtenaar en art. 142 Wetboek van Strafvordering), waarvoor de verantwoordelijkheid bij de Minister van Justitie rust? Of ligt het gezag bij de werkgever omdat hij de werknemer concrete aanwijzingen kan geven wat betreft zijn taakuitoefening? In dat laatste geval zou de werkgever dan zowel het beheer als het gezag uitoefenen over de BOA en in zoverre vanuit beide 'rollen' als verwerkingsverantwoordelijke kunnen worden aangemerkt. Omdat de gemeente verantwoordelijke is voor de politiegegevens die de BOA in verband met zijn taakuitoefening verwerkt, en die gemeente niet ook tevens zelf bevoegde autoriteit is, kan / mag de gemeente de gegevens waarvoor hij verantwoordelijk is niet zelf verwerken. Zoals reeds eerder aangegeven, is het de vraag of dit in de praktijk wenselijk en/of mogelijk is. Daarnaast is het vanuit een praktisch oogpunt bezien de vraag in hoeverre de diverse werkgevers waarbij BOA's in dienst kunnen zijn, zoals bijvoorbeeld Staatsbosbeheer of de NS, zich afdoende bewust zijn van het feit dat op de verwerking van politiegegevens een ander regime van toepassing is dan voorheen (de Wbp). De memorie van toelichting zou op dit punt aangevuld moeten worden en gebruikt moeten worden als een uitleg- en communicatiemiddel naar de praktijk.

Conclusie verwerkingsverantwoordelijke en het onderscheid tussen beheer en gezag
Het vorenstaande betekent dat het begrip beheer in de huidige Wpg en Wjsg en in de Wijzigingswet als criterium voor de vraag wie als verwerkingsverantwoordelijke moet worden aangemerkt, niet overeenkomt met hetgeen de Richtlijn voorschrijft en derhalve in de feitelijke situatie bepalend is en zou moeten zijn. Het begrip gezag zou (mede)bepalend moeten zijn voor de vraag wie als verwerkingsverantwoordelijke (en in de Richtlijn tevens als bevoegde autoriteit) moet worden aangemerkt.

c) De positie van de burgemeester in relatie tot het begrip 'verwerkingsverantwoordelijke'
In het verlengde van de hiervoor weergegeven opmerkingen naar aanleiding van de implementatie van het begrip 'verwerkingsverantwoordelijke', merkt de AP op dat in lijn daarmee ook de burgemeester onder de definitie van bevoegde autoriteit ingevolge artikel 3, aanhef en onder 7, van de Richtlijn valt. Dit doet ook opgeld, indien naar de definitie van dit begrip in de Wpg en meer in het bijzonder naar de zinsnede "ieder ander orgaan dat of iedere andere entiteit die is gemachtigd openbaar gezag en openbare bevoegdheden uit te oefenen met het oog op de taken, bedoeld in onderdeel a", wordt gekeken. Dit vanwege de positie van de burgemeester op het gebied van openbare orde en/of openbare veiligheid en het gezag dat hij in zoverre ingevolge de Politiewet uitoefent over de politie. In dat verband zij opgemerkt dat, indien de feitelijke gezagsverhouding over de politie tot uitgangspunt wordt genomen, de burgemeester tevens verwerkingsverantwoordelijke is.

Datum
7 april 2017

Ons kenmerk
z2017-01571

Eindconclusie implementatie begrip 'verwerkingsverantwoordelijke'
Door het uitgangspunt te kiezen dat de Richtlijn zo veel mogelijk beleidsneutraal moet worden geïmplementeerd, is naar het oordeel van de AP bij de Wijzigingswet ook in zoverre ten onrechte voorbij gegaan aan een juiste implementatie van de Richtlijn. Dit leidt tot de constatering dat de implementatie van het begrip verwerkingsverantwoordelijke op twee niveaus niet klopt:
1. De koppeling met het zijn van bevoegde autoriteit is niet gemaakt.
2. Ten onrechte zijn niet doel en middelen bepalend geweest bij het aanwijzen van de verwerkingsverantwoordelijken maar het criterium beheer.

Conclusie rechtsgrondslag en reikwijdte Richtlijn

De AP is van oordeel dat de implementatie van de Richtlijn zoals deze thans is vormgegeven in het voorstel voor de Wijzigingswet, is gebaseerd op een onjuiste opvatting over de grondslag en reikwijdte van de Richtlijn. Hierdoor beantwoordt het voorstel niet aan de fundamentele uitgangspunten van de Richtlijn en voldoet de uitwerking die daaraan is gegeven niet aan de vereiste nauwgezette omzetting van de Richtlijn in nationaal recht.

De AP heeft dan ook reeds om die reden bezwaar tegen het in deze vorm indienen van de Wijzigingswet. Na aanpassing van de Wijzigingswet is de AP wederom bereid om hierover te adviseren. Ten behoeve van het vervolgtraject geeft de AP ook het volgende nog in overweging.

II Uitvoeringstoets per onderwerp

1 Afbakening Verordening/ Uitvoeringswet en Wijzigingswet: uitvoerbaarheid voor de praktijk

In artikel 2, eerste lid, onder d, van de Verordening is bepaald dat de Verordening niet van toepassing is op de verwerking van persoonsgegevens door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.
In artikel 1 en 2 van de Richtlijn staan de spiegelbeeldige bepalingen opgenomen. De Verordening en de Richtlijn sluiten elkaar derhalve wat betreft toepassingsbereik uit.

a) De Richtlijn heeft ingevolge artikel 1, eerste lid, betrekking op regels 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 of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.
Volgens de memorie van toelichting bij de Wijzigingswet kan bij het begrip openbare veiligheid *"worden gedacht aan activiteiten van de politie of andere rechtshandhavingsautoriteiten die niet hoofdzakelijk zijn gericht op de voorkoming, het onderzoek of de opsporing van strafbare feiten, maar die betrekking hebben op politieactiviteiten bij demonstraties, sportevenementen en rellen of de rechts- en ordehandhaving door deze bevoegde autoriteiten ter bescherming tegen en voorkoming van gevaren voor de openbare veiligheid en bij wet beschermde fundamentele belangen van de samenleving, die tot strafbare feiten kunnen leiden (overweging 12). Hieronder valt de handhaving van de openbare orde, als onderdeel van de politietaak. De toevoeging verduidelijkt dat als persoonsgegevens door de politie of de Koninklijke marechaussee worden verwerkt met het oog op de uitvoering van de politietaak, als bedoeld in de artikelen 3 of 4 van de Politiewet 2012, de richtlijn van toepassing is op de verwerking van persoonsgegevens voor dit doel."*

Gelet op deze passage uit de memorie van toelichting vraagt de AP zich af of hieruit moet worden afgeleid dat de doeleinden voorkoming, onderzoek, opsporing of vervolging van strafbare feiten die zien op de strafrechtelijke handhaving berusten bij het Openbaar Ministerie (hierna: OM) en de bescherming tegen en de voorkoming van gevaren voor openbare veiligheid berust bij de burgemeester? De AP merkt daarbij op dat het voorkomen van of het onderzoek naar strafbare feiten een grote overlap kan hebben met maatregelen die worden genomen ten behoeve van de openbare veiligheid. In die zin is de taakafbakening en het gezag tussen enerzijds OM en anderzijds de burgemeester dan ook niet scherp te maken.

b) Zoals hiervoor is weergeven, heeft de implementatie van de Richtlijn in de Wpg zijn beslag gekregen door onder andere het criterium bevoegde autoriteit, welk criterium is gekoppeld aan het begrip politiegegevens en de uitoefening van de politietaak. Deze koppeling heeft tot gevolg dat indien een van deze begrippen niet van toepassing is, de Verordening / Uitvoeringswet vervolgens van toepassing is. Indien bijvoorbeeld sprake is van de verwerking van politiegegevens maar niet door een bevoegde autoriteit, dan is de Verordening / Uitvoeringswet van toepassing. Indien sprake is van verwerking van gegevens door de politie, maar voor een ander doel dan de uitoefening van de politietaak, dan is de Verordening / Uitvoeringswet van toepassing. En indien sprake is van de verwerking van politiegegevens (verstrekking) aan andere dan bevoegde autoriteiten, dan is de Verordening / Uitvoeringswet op de verdere verwerking van toepassing.

Hulpverleningstaken van de politie
Artikel 3 van de Politiewet 2012 en de daarin opgenomen hulpverleningstaken van de politie zijn door de gekozen invulling van het begrip bevoegde autoriteit binnen het bereik van de Wpg gebracht. De vraag is in hoeverre met de Richtlijn is beoogd deze hulpverleningstaken van de politie binnen het toepassingsbereik daarvan te laten vallen.
In overweging 12 van de Richtlijn is het volgende opgenomen:
"De lidstaten kunnen de bevoegde autoriteiten belasten met andere taken die niet noodzakelijkerwijs worden verricht met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, zodat de verwerking van persoonsgegevens voor die andere doeleinden, voor zover zij binnen het toepassingsgebied van het Unierecht valt, binnen het toepassingsgebied van Verordening (EU) 2016/679 valt."

In de huidige Politiewet 2012 is met de omschrijving van de politietaak, blijkens de memorie van toelichting bij die wet, aangesloten bij de reeds bestaande invulling daarvan. De politie is in die wet gepositioneerd als een eerstelijnsorganisatie die tijdelijk de eerste opvang verzorgt, indien dit dringend is totdat de hulpverlening het overneemt. De memorie van antwoord overweegt in dat verband dat de binnen de politietaak te onderscheiden deeltaken niet los van elkaar staan maar onlosmakelijk aan elkaar verbonden zijn en dat handhaving van de openbare orde en strafrechtelijke handhaving in toenemende mate zijn verweven.

De AP acht de keuze in de Wijzigingswet verdedigbaar dat de hulpverleningstaak van de politie, als onlosmakelijk onderdeel van de handhaving van de openbare orde en ook van de strafrechtelijke handhaving, daarmee een taak is die noodzakelijkerwijs wordt verricht met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, en aldus binnen het toepassingsbereik van de Richtlijn valt.

c) Wat betreft de uitvoering van de politietaak zijn er met de implementatie van de Richtlijn enkele beperkingen opgetreden in de reikwijdte van die taak, waarvan de belangrijkste wijzigingen inhouden dat met het wetsvoorstel de vreemdelingentaken en de taken ten dienste van justitie niet meer onder de Wpg zullen vallen, maar onder de Verordening / Uitvoeringswet.

Deze nieuwe taakafbakening heeft gevolgen voor de uitvoering van de taken door de Koninklijke Marechaussee (KMar), nu de vreemdelingentaken van de politietaak worden uitgezonderd. In artikel 4 Politiewet 2012 zijn de onderscheiden taken van de KMar omschreven, die ook taken op het gebied van de grensbewaking omvatten. Aangezien de uitvoering van de grensbewakingstaken (die nog wel onder het bereik van de politietaak volgens de gewijzigde Wpg zullen vallen) en de vreemdelingentaken (die niet meer onder de politietaak zullen vallen) door de KMar in de praktijk veelal zodanig vervlochten zullen zijn dat de vraag is of de te verwerken persoonsgegevens in het kader van deze taken in de praktijk op toereikende wijze onder de verschillende regimes gescheiden kunnen worden.

Een daarmee samenhangend punt vormt het toepasselijke regime voor de vreemdelingen-signaleringen in het Schengen Informatiesysteem van de tweede generatie, SIS II. Het nationale informatiesysteem N.SIS II valt thans onder de Wpg, waardoor niet alleen alle politiesignaleringen

(op basis van het Europese SIS II-Besluit) maar ook de vreemdelingensignaleringen (op basis van de Europese SIS II-Verordening) onder de werking van de Wpg vallen. Echter, materieel is op de vreemdelingensignalering in N.SIS II de vreemdelingenwetgeving van toepassing, wat thans valt onder de werking van de Wbp en straks dus onder de Verordening/ Uitvoeringswet. Dit vormt nu al een hybride situatie voor het toepasselijke regime, die soms lastig te volgen is in de praktijk. Maar als gevolg van het gewijzigde toepassingsbereik van de Richtlijn, waardoor de vreemdelingentaken niet meer onder de Wpg zullen vallen, zal hier een bijzonder ondoorzichtige, en mogelijk ook onwerkbare situatie ontstaan met betrekking tot het toepasselijke regime, nu dit tot gevolg zal hebben dat de inhoud van de vreemdelingensignaleringen onder het Verordeningsregime zal vallen, terwijl de overige signaleringen alsmede het informatiesysteem zelf onder het regime van de Wpg valt.

d) Wat voorts niet geheel duidelijk geregeld lijkt is de toepasselijkheid van de Wpg dan wel van de Verordening/ Uitvoeringswet bij de Wet administratieve handhaving verkeersvoorschriften (Wahv). De memorie van toelichting beschrijft op p. 8 dat deze taak valt onder de taken ten dienste van justitie, als bedoeld in artikel 1, onderdeel i, onder 2[e] van de Politiewet 2012. In de Wijzigingswet in artikel 1, onder a) wordt dit taakonderdeel uitgezonderd van de politietaak.

Echter, op p.9 van de memorie van toelichting wordt omschreven dat voor de Wahv *"geldt dat deze in de praktijk relevante samenhang vertoont met de opsporing en vervolging van strafbare feiten, omdat op het moment van waarneming van een overtreding van die wet nog geen keuze is gemaakt omtrent de wijze van afdoening. Afhankelijk van de aard en ernst van de overtreding kan dit een administratiefrechtelijk traject zijn ofwel een strafrechtelijke traject. Gelet op de verwevenheid met de andere onderdelen van de politietaak ligt het daarom voor de hand om voor de verwerking van persoonsgegevens door de ambtenaren van de politie aan te sluiten bij het toepassingsgebied van de richtlijn, zodat de gegevensverwerking onder de reikwijdte van de Wpg blijft vallen. De richtlijn biedt hiervoor de ruimte, [..]"*.
Of deze omschrijving nu tot de conclusie moet leiden dat de gegevensverwerking in het kader van de Wahv daarmee uitgezonderd wordt op de uitzonderingsbepaling bij de politietaak en daardoor weer 'terugvalt' onder de politietaak, blijkt uit de onderscheiden onderdelen van de memorie van toelichting onvoldoende.

Overigens wijst de AP nog op het feit dat, uitgaande van het hiervoor bij I onder 5 uiteengezette standpunt van de AP ten aanzien van het begrip 'strafbaar feit', de Wahv vanuit dat perspectief in zijn geheel onder de reikwijdte van de Richtlijn dient te vallen en daarmee onder het bereik van de Wpg.

Conclusie afbakening Verordening/ Uitvoeringswet en Wijzigingswet: uitvoerbaarheid voor de praktijk
De vraag is of de gekozen afbakening in de uitvoeringspraktijk werkbaar en/of uitvoerbaar is. Het is aan de AP om daar in de praktijk invulling aan te geven. De verwerkingsverantwoordelijken zullen zich te allen tijde bewust moeten zijn van de vraag welke gegevens zij verwerken, in verband met welke taak en voor welk doel zij gegevens aan anderen willen verstrekken.

2 Boetebevoegdheid in Wijzigingswet in relatie tot de Verordening
In de Wijzigingswet is slechts een bevoegdheid gegeven om een boete op te leggen vanwege een overtreding van artikel 32 Wpg (de documentatieplicht). Het boetemaximum voor een overtreding van deze bepaling bedraagt ten hoogste het bedrag van de geldboete van de vierde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht, hetgeen thans neerkomt op EUR 20.500,-. Hoewel de AP ten

aanzien van eventuele overtredingen van de Wpg en Wjsg meerdere handhavingsinstrumenten ter beschikking staan, wijkt het voorgaande zeer af van hetgeen ingevolge de Verordening is toegestaan. De maximumboetebedragen in de Verordening variëren van EUR 10 miljoen tot EUR 20 miljoen (voor overheidsorganisaties) en gelden voor een groot aantal bepalingen uit de Verordening.

De Europese wetgever heeft met de goedkeuring van het pakket van gegevensbeschermingswetgeving tot doel gehad om een samenhangend pakket aan regelgeving voor te schrijven. De voorschriften van de Verordening en de Richtlijn voorzien dan ook in een overeenkomend stelsel van bepalingen dat voor wat betreft de Richtlijn slechts bedoeld is af te wijken van de in de Verordening gegeven voorschriften voor zover dit overeenkomt met het karakter van de specifieke sector waarop deze regelgeving ziet. Op grond van artikel 83, eerste lid, van de Verordening moeten de door de toezichthoudende autoriteit op te leggen administratieve geldboeten in elke zaak doeltreffend, evenredig en afschrikkend zijn. In lijn hiermee dienen ingevolge artikel 57 van de Richtlijn de door de lidstaten vast te stellen straffen op inbreuken op de Richtlijn dan ook evenzeer doeltreffend, evenredig en afschrikkend zijn. Gelet op de in artikel 83 van de Verordening gegeven opsomming van de onderscheiden verplichtingen, waarvan inbreuken daarop uit hoofde van dit artikel onderworpen zijn aan administratieve geldboeten, ligt het daarom voor de hand om de uitwerking van de overeenkomstige bepaling in de Richtlijn in artikel 57 op vergelijkbare wijze uit te leggen. De AP ziet dan ook geen aanleiding om van deze lijst – voor zover overeenkomend met de voorschriften van de Richtlijn – af te wijken.

Om die reden adviseert de AP de bepalingen waarvoor een administratieve boete kan worden opgelegd aan te vullen en aldus vast te stellen dat deze zien op overtreding van de volgende rechten en verplichtingen.

Categorie A (minder ernstige overtredingen):

- bepalingen inzake de verplichtingen van de verwerkingsverantwoordelijke en de verwerker, voortvloeiend uit Hoofdstuk IV, waaronder die inzake gegevensbescherming door ontwerp en door standaardinstellingen, gezamenlijke verwerkingsverantwoordelijken, register van de verwerkingsactiviteiten, bijhouden van logbestanden, medewerking met de toezichthoudende autoriteit, gegevensbeschermingseffectbeoordeling, voorafgaande raadpleging, beveiliging van de verwerking, melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit en mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene, en inzake de aanwijzing, positie en taken van de functionaris voor gegevensbescherming.

Categorie B (ernstige overtredingen):

- bepalingen inzake beginselen inzake verwerking van persoonsgegevens voortvloeiend uit Hoofdstuk II, waaronder die inzake de rechtmatigheid van de verwerking, termijnen voor opslag en evaluatie, onderscheid tussen verschillende categorieën van betrokkenen, onderscheid tussen persoonsgegevens en controle van de kwaliteit van persoonsgegevens, specifieke verwerkingsvoorwaarden, verwerking van bijzondere categorieën van persoonsgegevens en geautomatiseerde individuele besluitvorming;
- bepalingen inzake rechten van de betrokkene voortvloeiend uit Hoofdstuk III, waaronder het recht op informatie, inzage, rectificatie en wissing van persoonsgegevens;
- bepalingen inzake doorgifte van persoonsgegevens aan derde landen of internationale organisaties voortvloeiend uit Hoofdstuk V;

- niet-naleving van een bevel of een tijdelijke of definitieve verwerkingsbeperking of een opschorting van gegevensstromen door de toezichthoudende autoriteit (op basis van corrigerende maatregelen), of niet-verlening van toegang in strijd met bepalingen inzake onderzoeksbevoegdheden van de toezichthoudende autoriteit.

Conclusie boetebevoegdheid Wijzigingswet in relatie tot de Verordening
De AP verzoekt om het aantal in de Wpg en Wjsg beboetbare overtredingen en de daarvoor geldende boetemaxima te heroverwegen en in dat verband aansluiting te zoeken bij de Verordening zoals hierboven vermeld.

3 Beveiliging van politiegegevens

Binnen de toepassing van het fundamentele recht op bescherming van persoonsgegevens neemt de beveiliging van gegevens een centrale plaats in. Naast voorschriften die zien op onder meer de rechtmatigheid en kwaliteit van de verwerkte gegevens, zijn de bepalingen die een effectieve informatiebeveiliging voorschrijven van groot belang. In het bijzonder in deze tijd van toenemende digitalisering van de informatievoorziening en kwetsbaarheid daarvan voor inbreuken op de beveiliging, is een gedegen informatiebeveiliging cruciaal voor een behoorlijke gegevensverwerking. Het niveau van de technische en organisatorische maatregelen die een organisatie moet treffen ter beveiliging van door haar verwerkte persoonsgegevens hangt sterk samen met factoren als de gevoeligheid van die gegevens. De rechtshandhavingsorganisaties verwerken persoonsgegevens die bij uitstek als gevoelig te karakteriseren zijn, onder meer gegevens over de uitvoering van de politietaak en gegevens over strafrechtelijke veroordelingen en de tenuitvoerlegging daarvan, en kennen daarbinnen ook gegevensverwerkingen met een hoog afbreukrisico, zoals bijvoorbeeld onderzoeken naar zware criminaliteit en terrorisme, informantengegevens en gespreksverslagen, en zogenaamde embargo-onderzoeken.

De Richtlijn schrijft voor dat de verwerkingsverantwoordelijke het niveau van de gegevensbescherming dient af te stemmen op de risico's voor de verwerking en de ernst en waarschijnlijkheid daarvan, door middel van uitvoeren van een risicoanalyse. Hij moet daartoe dan ook passende technische en organisatorische maatregelen treffen en deze risicoanalyse periodiek herhalen en de getroffen beveiligingsmaatregelen hierop blijven afstemmen.

Om de risico's die aan de gegevensverwerking verbonden zijn het hoofd te bieden, dient intern beveiligingsbeleid worden vastgesteld en moeten maatregelen worden geïmplementeerd die uitvoering geven aan gegevensbeschermingsbeginselen als dataminimalisatie, en maatregelen die de integriteit en betrouwbaarheid van de gegevens waarborgen. De Richtlijn stelt daartoe tevens verplicht dat gegevensbescherming door ontwerp – Privacy by design – en gegevensbescherming door standaardinstelling – Privacy by default – worden toegepast. Wanneer te voorzien is dat de gegevensverwerking zal leiden tot een hoog risico voor de rechten en vrijheden van burgers wordt de uitvoering van een gegevensbeschermingseffectbeoordeling – Data Protection Impact Assessment, DPIA – voorgeschreven.

De Richtlijn geeft in artikel 19, eerste lid, een algemene verplichting voor verwerkingsverantwoordelijken om zodanige technische en organisatorische maatregelen te treffen dat deze de naleving van de voorschriften van de richtlijn kunnen garanderen. In artikel 29 van de Richtlijn is deze verplichting tot beveiliging van de gegevensverwerking uitgewerkt in specifieke voorschriften welke maatregelen de

verwerkingsverantwoordelijke en de verwerker moeten treffen om een op het risico afgestemd beveiligingsniveau te waarborgen voor de diverse – in het tweede lid, onder a) tot en met j) beschreven – doeleinden. Het betreft hier de voorschriften met het oog op a) controle op de toegang tot de apparatuur, b) controle op de gegevensdragers, c) opslagcontrole, d) gebruikerscontrole, e) controle op de toegang tot de gegevens, f) transmissiecontrole, g) invoercontrole, h) transportcontrole, i) herstel en j) betrouwbaarheid en integriteit van de systemen en de verwerkte persoonsgegevens.
Hoewel de Richtlijn de lidstaten verplicht het treffen van deze voorzieningen voor te schrijven, voorziet de Wijzigingswet hier niet uitdrukkelijk in. Hoewel enkele onderdelen hiervan zijn omschreven in verschillende specifieke artikelen van de Wpg, ontbreekt een centraal en afzonderlijk artikel waarin de geldende verplichtingen in verband met informatiebeveiliging op overzichtelijke wijze bijeen zijn gebracht en omschreven.

Uit de resultaten van eerder door de AP uitgevoerde onderzoeken op het terrein van de verwerking van politiegegevens volgt dat sprake is van structurele tekortkomingen ten aanzien van de beveiliging van politiegegevens, daaronder begrepen de uitvoering van logging en het ontbreken van toereikende werkprocedures en beveiligingsbeleid. De uitkomsten van de Wpg-auditrapportages sluiten hier ook op aan. Om die reden is het van het grootste belang dat al de relevante onderdelen van de verplichting tot beveiliging van gegevens voldoende effectief worden geïmplementeerd. Een afzonderlijk en centraal gesteld artikel in de Wpg waarin een heldere uiteenzetting wordt gegeven van de door de Richtlijn voorgeschreven aspecten van gegevensbeveiliging kan daaraan bijdragen alsmede een voor de praktijk duidelijke maatstaf die, techniek en tijdonafhankelijk, voldoende houvast geeft voor de uitvoering van die verplichtingen in de praktijk.

De hiervoor genoemde bevindingen van de AP als toezichthouder sluiten aan bij het in december 2016 uitgebrachte rapport van de Algemene Rekenkamer ten aanzien van de "ICT politie 2016".[8] Ten opzichte van het eerdere rapport uit 2011 constateert de Rekenkamer onder meer dat de ICT-governance van de politie, mede door de vorming van de nationale politie op onderdelen is verbeterd, maar dit nog niet optimaal functioneert.[9] Ook laat een strikte uitvoering van de bestaande meerjarige begroting voor ICT financieel en inhoudelijk nauwelijks ruimte voor verdere vernieuwing.[10] Daarnaast zijn verbeteringen in het functioneren van de IT-auditfunctie nodig, waarbij de politie in een Herijkt Auditjaarplan 2015 aangeeft dat er in de huidige bezetting een tekort bestaat aan specifieke kennis over IT-audit en de Wet Politiegegevens (Wpg).[11]

De logging vormt een belangrijk onderdeel van de implementatie van het beveiligingsbeleid en is als zodanig onlosmakelijk verbonden met de overige beveiligingsmaatregelen. Aldus is in de logbestanden na te gaan wie, wanneer, welke gegevens heeft geraadpleegd of gewijzigd. Dit vormt noodzakelijke informatie bij de controle op de rechtmatigheid van de toegang tot en het gebruik van de verwerkte gegevens. Uitstel van de verplichting om de loggingsvoorschriften tijdig geïmplementeerd te hebben, zoals in de Wijzigingswet bij de toelichting bij artikel VI is verwoord, zou hierbij onmiskenbaar een verkeerd signaal

[8] "ICT politie 2016; Vervolgonderzoek naar de ICT-governance en de basisvoorzieningen voor handhaving en opsporing bij de nationale politie", Algemene Rekenkamer, Den Haag december 2016.
[9] T.a.p., p.21.
[10] T.a.p., p. 30.
[11] T.a.p., p.25.

afgeven. Gelet op de hiervoor vermelde tekortkomingen ten aanzien van de naleving op dit punt, dient aan dit onderdeel eerder prioriteit te worden gegeven.

Conclusie beveiliging politiegegevens
De AP adviseert om bij voorkeur de algemene verplichting (uit artikel 19, eerste lid, van de Richtlijn) en de uitwerking daarvan (uit artikel 29, tweede lid, van de Richtlijn) in één artikel vast te stellen en de overige aspecten als Privacy by design, Privacy by default en DPIA in afzonderlijke artikelen onder te brengen. Bovendien adviseert de AP artikel VI niet op dit onderdeel te handhaven.

4 Passende waarborgen
a. ten aanzien van bijzondere persoonsgegevens
Artikel 10 van de Richtlijn bepaalt ten aanzien van de verwerking van bijzondere categorieën van persoonsgegevens het volgende. *Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijkt, en verwerking van genetische gegevens, met het oog op de unieke identificatie van een natuurlijke persoon, gegevens over gezondheid of gegevens over seksueel gedrag* (lees: *seksuele leven) of seksuele gerichtheid van een natuurlijke persoon zijn slechts toegelaten wanneer de verwerking strikt noodzakelijk is, geschiedt met inachtneming van passende waarborgen voor de rechten en vrijheden van de betrokkene, en bij het Unierecht of het lidstatelijke recht is toegestaan; [..].*
Overweging 37 geeft daarbij aan dat persoonsgegevens die door hun aard bijzonder gevoelig zijn wat betreft de grondrechten en fundamentele vrijheden specifieke bescherming verdienen aangezien de context van de verwerking ervan aanzienlijke risico's voor die rechten en vrijheden kan meebrengen. *Dergelijke persoonsgegevens mogen slechts worden verwerkt indien bij de verwerking passende bij wet neergelegde waarborgen gelden wat de rechten en vrijheden van de betrokkene betreft en zij is toegelaten in bij wet bepaalde gevallen. [...] Passende waarborgen voor de rechten en vrijheden van de betrokkene kunnen bijvoorbeeld inhouden dat die gegevens enkel mogen worden verzameld in samenhang met andere gegevens over de natuurlijke persoon in kwestie, dat de gegevens afdoende kunnen worden beveiligd, dat strengere regels gelden voor de toegang van het personeel van de bevoegde autoriteit tot de gegevens, en dat de doorzending van die gegevens wordt verboden.*

Het thans geldende artikel 5 van de Wpg luidt als volgt. *De verwerking van politiegegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging vindt slechts plaats in aanvulling op de verwerking van andere politiegegevens en voor zover dit voor het doel van de verwerking onvermijdelijk is.* Het voorstel vult de categorieën bijzondere persoonsgegevens aan overeenkomstig de Richtlijn en wijzigt voorts slechts de beperking 'voor zover dit voor het doel van de verwerking onvermijdelijk is' in '*wanneer dit strikt noodzakelijk is voor het doel van de verwerking*'. In de memorie van toelichting wordt betoogd dat met het vereiste dat de gegevens worden verwerkt in aanvulling op de verwerking van andere politiegegevens aan de vereiste passende waarborgen invulling wordt gegeven.
Het thans gehanteerde criterium 'onvermijdelijk' wordt daarmee verlaten en verlaagd tot 'strikt noodzakelijk', terwijl aan de vereiste passende waarborgen geen (nadere) invulling is gegeven dan de al bestaande voorwaarde dat verwerking slechts plaatsvindt in aanvulling op de verwerking van andere politiegegevens. In de uitbreiding van het aantal categorieën gegevens door de Richtlijn tot de verwerking van genetische gegevens en biometrische gegevens, welke gegevens tevens in geautomatiseerde systemen zoals bijvoorbeeld DNA-databanken en databases voor vingerafdrukken worden verwerkt, heeft het

voorstel evenmin aanleiding gevonden om in nadere passende waarborgen te voorzien. Gelet op de uit de Richtlijn volgende vereisten en de vorenstaande uitbreiding, kan naar het oordeel van de AP niet worden volstaan met het criterium 'in aanvulling op' maar dienen verdergaande waarborgen te worden getroffen zoals beperkingen van de toegang tot die gegevens of andere maatregelen ter verhoging van de beveiliging van die gegevens.

In het voorgestelde artikel 39c, derde lid, van de Wjsg is in het verder gelijkluidende artikel ten aanzien van de verwerking van strafvorderlijke gegevens bepaald dat deze verwerking slechts plaatsvindt 'in aanvulling op de verwerking van andere strafvorderlijke gegevens en voor zover dit voor het doel van de verwerking onvermijdelijk is'. Op dit punt is dus nog het 'oude' criterium gehandhaafd, terwijl de memorie van toelichting daarover niet uitweidt en slechts verwijst naar de hieromtrent gegeven toelichting bij artikel 5 van de Wpg. Ook hier acht de AP een aanvulling van de vereiste passende waarborgen aangewezen.

Conclusie ten aanzien van bijzondere persoonsgegevens
De AP adviseert om zowel in artikel 5 van de Wpg als in artikel 39c, derde lid, van de Wjsg, te voorzien in verdergaande waarborgen dan de thans voorgestelde tekst.

b. ten aanzien van geautomatiseerde individuele besluitvorming
Artikel 11 van de Richtlijn schrijft in het eerste lid voor dat uitsluitend op geautomatiseerde verwerking gebaseerde besluiten, met inbegrip van profilering, die voor de betrokkene nadelige rechtsgevolgen hebben of hem in aanmerkelijke mate treffen, verboden zijn, tenzij dat besluit is toegestaan krachtens Unierecht of lidstatelijke recht, en dat besluit voorzien in passende waarborgen voor de rechten en vrijheden van de betrokkene, waaronder tenminste het recht op menselijke tussenkomst van de verwerkingsverantwoordelijke. Daarbij – zo stelt overweging 38 – moeten voor die verwerking in ieder geval passende waarborgen worden geboden, waaronder specifieke voorlichting van de betrokkene en het recht op menselijke tussenkomst, met name om zijn standpunt kenbaar te maken, om uitleg over het na een dergelijke beoordeling genomen besluit te krijgen en om op te komen tegen het besluit.

In het voorstel geeft artikel 7a, eerste lid, van de Wpg hieraan de volgende uitwerking. Een besluit dat uitsluitend op geautomatiseerde verwerking is gebaseerd, met inbegrip van profilering, dat voor de betrokkene nadelige rechtsgevolgen heeft of hem in aanmerkelijke mate treft, is verboden, tenzij het besluit voorziet in het recht op menselijke tussenkomst van de zijde van de verwerkingsverantwoordelijke. De memorie van toelichting stelt met verwijzing naar overweging 38 dat in het licht van de mogelijkheden die door de richtlijn wordt geboden wordt voorgesteld te voorzien in de verplichting de betrokkene in staat te stellen te verzoeken om menselijke tussenkomst van de verantwoordelijke, zodat de betrokkene in staat wordt gesteld zijn standpunt kenbaar te maken of uitleg te krijgen. In deze bepaling hebben de vereiste passende waarborgen slechts uitwerking gekregen in 'het recht op menselijke tussenkomst', terwijl een voorwaarde die voorziet in specifieke voorlichting aan de betrokkene ontbreekt.

De memorie van toelichting bij artikel 24b, tweede lid, onder e, verwijst naar artikel 14, tweede lid, onder g van de Verordening, waarin is vastgelegd dat betrokkenen recht hebben op informatie over het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en nuttige informatie over de

onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene, en stelt dat een equivalent van genoemde bepaling ontbreekt in de Richtlijn. Tevens wordt verwezen naar de reactie van het kabinet op het WRR-rapport "Big Data in een vrije en veilige samenleving", waarin het kabinet heeft aangekondigd te willen bezien of bij de implementatie van de Richtlijn een bepaling als voormeld artikel van de Verordening niet ook voor geautomatiseerde besluitvorming op grond van strafrechtelijke gegevens zou moeten gaan gelden. Vervolgens betoogt de memorie van toelichting dat een dergelijke bepaling in de Wpg niet behoort te ontbreken, en stelt dat het verstrekken van de hier bedoelde informatie immers kan worden gezien als een expliciete invulling van de passende waarborgen voor de rechten en vrijheden van de betrokkene waarop in artikel 7a wordt gedoeld. Hoewel dit voorschrift in letterlijke zin inderdaad niet in de Richtlijn is opgenomen, wordt in artikel 12 van de Richtlijn verwezen naar een recht op informatie dat uitdrukkelijk ook ziet op dat recht in geval van geautomatiseerde individuele besluitvorming.

Ten aanzien van de toepassing van geautomatiseerde individuele besluitvorming, met inbegrip van profilering, in de politie-justitiesector acht de AP het volgende van belang.
In de gehele samenleving en ook in het veiligheidsdomein, waarop het toepassingsgebied van de Richtlijn ziet, wordt in toenemende mate gebruik gemaakt van Big Data-toepassingen, met name door koppelingen van systemen en openbare informatie, surveillance-toepassingen en (nieuwe) toepassingen van *intelligence-led policing*. Een belangrijke studie in dit verband vormt het eerder genoemde rapport van de WRR, getiteld "Big Data in een vrije en veilige samenleving"[12]. Hierin wordt onder meer een beschrijving gegeven van de stand van zaken van Big Data in het veiligheidsdomein, een analyse van de in het geding zijnde belangen en grondrechten, een schets van het toepasselijk juridisch kader en een vooruitblik op (mogelijke) toekomstige ontwikkelingen.

Het WRR-rapport concludeert onder meer dat het gebruik van Big Data een substantiële verzwaring van het toezicht veronderstelt. Ook moeten burgers en organisaties mogelijkheden hebben om de juistheid en evenredigheid van beslissingen op basis van data-analyses door overheidsinstanties, ter discussie te stellen en eventueel te laten toetsen.[13] Als aanbeveling wordt dan ook geformuleerd dat de transparantie van de gegevensverwerking moet worden vergroot, en er een beter evenwicht moet komen tussen het vereiste van geheimhouding en het belang van openbaarheid over Big Data-toepassingen die aan fundamentele vrijheden raken.[14]

Gelet op het toegenomen en nog steeds toenemende gebruik door de politie en opsporingsdiensten van Big data-toepassingen en de eveneens toenemende impact daarvan op de persoonlijke levenssfeer van de burgers, dienen de waarborgen voor de bescherming van de rechten en vrijheden van de burger hiermee gelijke tred te houden. De te wijzigen wetgeving ten gevolge van de implementatie van de Richtlijn zou daarom tot een dienovereenkomstige verhoging van het beschermingsniveau voor individuen moeten leiden en voldoende juridische waarborgen moeten bieden.

[12] "Big Data in een vrije en veilige samenleving", Wetenschappelijke Raad voor het Regeringsbeleid, Amsterdam 2016.
[13] T.a.p., p.143.
[14] T.a.p., p.144.

Conclusie ten aanzien van geautomatiseerde individuele besluitvorming
De AP is van oordeel dat de voorgestelde bepalingen onvoldoende invulling geven aan de vereiste passende waarborgen voor de betrokkene, waardoor deze niet leiden tot de benodigde transparantie en het verkrijgen van inzicht in welke data op welke wijze zijn gebruikt om tot besluiten te komen die hem in aanmerkelijke mate treffen. De AP adviseert om die reden de genoemde bepalingen en de bijbehorende toelichting op een adequate wijze aan te vullen.

5 Rechten betrokkene inzake geautomatiseerde besluitvorming en informatie datalekken
Artikel 12 van de Richtlijn schrijft voor dat de verwerkingsverantwoordelijke redelijke maatregelen neemt om de betrokkene de in artikel 13 bedoelde informatie te verstrekken in een beknopte, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal. Dit voorschrift ziet op de informatievoorziening in het kader van de volgende artikelen: artikel 11 (geautomatiseerde individuele besluitvorming); artikel 14 (recht op inzage van de betrokkene); artikel 15 (beperkingen van het inzagerecht); artikel 16 (recht op rectificatie of wissing van persoonsgegevens en verwerkingsbeperking); artikel 17 (uitoefening van rechten door de betrokkene en controle door de toezichthouder); artikel 18 (rechten van de betrokkene bij strafrechtelijke onderzoeken en procedures) en artikel 31 (mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene).
Artikel 12 van de Richtlijn is in het voorstel – blijkens de implementatietabel – geïmplementeerd in artikel 24a van de Wpg en in de artikelen 17a en 17b, 39ha, 42b, 51b en 51f van de Wjsg. Voor de Wpg omschrijft artikel 24a de informatieverstrekking in geval van de artikelen 25, eerste lid (recht op inzage), 28, eerste lid (recht op rectificatie en vernietiging) en 33b, vierde lid (schriftelijk advies bij voorafgaande consultatie). Inmiddels heeft (in de laatste tekstversie) invoeging van een verwijzing naar de artikelen 7a (geautomatiseerde individuele besluitvorming) en 33a (melding datalekken aan de betrokkene) plaatsgevonden in het derde lid van artikel 24a van de Wpg. Dit artikellid heeft echter slechts betrekking op de kosteloze verstrekking van informatie.

Artikel 24b, tweede lid, onder e, van de Wpg bepaalt dat informatie aan de betrokkene moet worden verstrekt over het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene. Waarbij in de toelichting op dat artikellid wordt vermeld dat een equivalent van artikel 14, tweede lid, onder g, van de AVG ontbreekt voor de Richtlijn. Echter, de strekking van artikel 12 van de Richtlijn in dit verband gaat verder dan louter het informeren over het bestaan van geautomatiseerde besluitvorming en het overige in artikel 24b, tweede lid, onder e, bepaalde. Om die reden meent de AP dat invoeging in artikel 24a van een verwijzing naar de artikelen 7a en 33a van de Wpg niet voldoende tegemoetkomt aan het bepaalde in artikel 12 van de Richtlijn.

Ten aanzien van de voorgestelde wijziging van de Wjsg gelden dezelfde aanbevelingen waar het betreft de artikelen 17a en 17b met overeenkomstige aanpassing van de daarbij vermelde toelichting, mede gelet op het ontbreken van een soortgelijke bepaling als artikel 24a van de Wpg.

Conclusie rechten betrokkene inzake geautomatiseerde besluitvorming en informatie datalekken
De AP adviseert de bovenvermelde bepaling uit de Richtlijn alsnog op toereikende wijze om te zetten in de bepalingen van de Wijzigingswet.

6 Gegevensverwerking door de gerechten

Artikel 45, tweede lid, van de Richtlijn schrijft voor dat elke toezichthoudende autoriteit belast moet zijn met het toezicht op verwerkingen door gerechten in het kader van hun rechterlijke taken. Daarbij bepaalt overweging 80 het volgende. *Hoewel deze richtlijn ook van toepassing is op de activiteiten van nationale gerechten en andere rechterlijke autoriteiten, dient de competentie van de toezichthoudende autoriteiten zich niet uit te strekken tot de verwerking van persoonsgegevens door gerechten in het kader van hun taken, teneinde de onafhankelijkheid van rechters bij de uitvoering van hun gerechtelijke taken te vrijwaren. Die vrijstelling dient beperkt te blijven tot gerechtelijke activiteiten in het kader van rechtszaken en niet te gelden voor andere activiteiten die rechters overeenkomstig het lidstatelijke recht verrichten.* [...] *De naleving van de regels van deze richtlijn door gerechten en andere onafhankelijke rechterlijke autoriteiten is in elk geval altijd onderworpen aan onafhankelijk toezicht in overeenstemming met artikel 8, lid 3, van het Handvest.* En ten aanzien van de bevoegdheden van de toezichthoudende autoriteit vermeldt overweging 82: *Hun bevoegdheden mogen echter geen afbreuk doen aan de specifieke regels voor strafrechtelijke procedures, met inbegrip van het onderzoek en de vervolging van strafbare feiten, of aan de onafhankelijkheid van de rechterlijke macht. Onverminderd de bevoegdheden die krachtens het lidstatelijke recht aan de met vervolging belaste autoriteiten zijn toegekend, dienen de toezichthoudende autoriteiten tevens de bevoegdheid te hebben inbreuken op deze richtlijn ter kennis van de rechterlijke autoriteiten te brengen of gerechtelijke procedures te voeren.*

Het bereik van de Richtlijn ziet mede op de verwerking van persoonsgegevens door de gerechten, zoals hierboven vermeld, waarbij al hetgeen valt onder de taakuitvoering van de onafhankelijke rechter uitdrukkelijk is uitgezonderd, zodat de toezichthoudende taak van de toezichthouder zich beperkt tot de procedurele kant van de verwerking van persoonsgegevens bij de behandeling van strafzaken door de gerechten en daarmee op generlei wijze betrekking heeft op de rechterlijke taak in de beoordeling van die zaken.

7 Doorgifte aan derde landen en internationale organisaties

De huidige Wpg en Wjsg voorzien kort gezegd in de volgende inrichting van het systeem van verstrekking van politiegegevens, justitiële en strafvorderlijke gegevens aan andere bevoegde autoriteiten.

a) De Wpg kent een verstrekkingenregime dat binnen de kring van bevoegde Nederlandse autoriteiten ter uitvoering van de politietaak plaatsvindt door middel van terbeschikkingstelling. Internationale verstrekkingen vallen uiteen in verstrekkingen aan internationale gerechten en organisaties op grond van een verdrag, aan buitenlandse politieautoriteiten of aan organen van de EU die werkzaam zijn op het gebied van de criminaliteitsbestrijding en voor zover aangewezen in het Besluit politiegegevens (zoals aan gemeenschappelijke onderzoeksteams, Europol en Eurojust). Bij verstrekking aan buitenlandse politieautoriteiten en internationale organisaties dient een toereikend niveau van gegevensbescherming aanwezig te zijn. In het geval van politieautoriteiten in de EU wordt uitgegaan van een adequaat niveau van gegevensbescherming en vindt gegevensuitwisseling plaats op gelijke voet met de nationale politieautoriteiten.
Bij de buiten de EU gelegen landen is thans niet voorzien in een omvattend beoordelingsmechanisme dat alle relevante factoren daarbij in beschouwing neemt. Dit in tegenstelling tot de bij de Richtlijn 95/46 gehanteerde systematiek van adequaatheidsbesluiten, vastgesteld door de Europese

Commissie, op welke vaststelling de verstrekkende Europese lidstaten moeten kunnen varen. Een equivalent hiervan kent de Wpg thans niet.

b) Voor de Wjsg is een vergelijkbaar verstrekkingenregime van toepassing. Aan bevoegde autoriteiten binnen de EU en aan EU-organen belast met de criminaliteitsbestrijding vindt verstrekking plaats op dezelfde voet als nationale bevoegde autoriteiten. Verstrekking ten behoeve van de strafrechtspleging aan internationale gerechten, aan rechterlijke ambtenaren en andere autoriteiten in het buitenland vindt plaats indien sprake is van een toereikend niveau van gegevensbescherming. Ook hier geldt dat niet is voorzien in een systeem van adequaatheidsbesluiten, waarbij is vastgesteld dat in het desbetreffende land of bij het desbetreffende internationale orgaan sprake is van een toereikend niveau van gegevensbescherming.

Onder de nieuwe Richtlijn is dezelfde systematiek aanvaard als onder Richtlijn 95/46 gebruikelijk was en zoals deze in de Verordening wordt voortgezet. Onder deze systematiek kan de Commissie dan ook, na een gedegen beoordeling van alle relevante aspecten van het rechtssysteem en in het bijzonder ten aanzien van de bescherming van persoonsgegevens, een adequaatheidsbesluit nemen ten aanzien van (bevoegde autoriteiten in) derde landen, dat wil zeggen buiten de aangesloten lidstaten van de EU.

Waar het voorstel de door de Richtlijn voorgeschreven systematiek voor verstrekkingen aan derde landen en internationale organisaties uiteenzet in artikel 17a van de Wpg, vormt dit een juiste uitwerking van de voorschriften van de Richtlijn. Primair wordt daarbij aangehouden de bepaling in het eerste lid dat doorgifte aan derde landen of internationale organisaties zal plaatsvinden op basis van de door de Commissie vastgestelde adequaatheidsbesluiten. Vervolgens wordt in het tweede lid bepaald dat, in afwijking hiervan, doorgiften kunnen plaatsvinden wanneer sprake is van passende waarborgen voor de bescherming van persoonsgegevens, al dan niet vastgelegd in een juridisch bindend besluit. Tot slot is in het derde lid bepaald dat, in afwijking van de voorgaande twee gevallen, doorgifte mogelijk is in specifieke gevallen en –kort gezegd – in geval van dringende noodzaak.

De in de memorie van toelichting gegeven toelichting sluit hier echter niet op aan. Bij het tweede lid wordt daarbij verwezen naar de tot nu toe op grond van Richtlijn 95/46 gepubliceerde adequaatheidsbesluiten. Deze zijn echter niet relevant voor de doorgifte van politie- en justitiegegevens, waarvoor immers door de Commissie nog een specifiek op die sector afgestemde beoordelingscyclus zal moeten worden uitgevoerd. Bij de huidige beoordeling of sprake is van een adequaat niveau van gegevensbescherming kan weliswaar steun gevonden worden bijvoorbeeld bij de door Europol of Eurojust uitgevoerde beoordelingen ten behoeve van de met derde landen gesloten uitwisselingsovereenkomsten, maar thans zijn er voor deze sector nog geen vastgestelde besluiten voorhanden. De toelichting gaat er vervolgens van uit dat doorgifte – bij gebreke van adequaatheidsbesluiten "aanvullend" – primair zal plaatsvinden op basis van passende waarborgen, maar dit vormt niet het uitgangspunt voor verstrekkingen aan derde landen of internationale organisaties. De toelichting dient dan ook in overeenstemming te worden gebracht met de toepasselijke systematiek voor doorgiften aan derde landen of internationale organisaties.

Voor de Wjsg gelden vergelijkbare bezwaren ten aanzien van de toelichting, waarnaar in de voorgestelde artikelen 16b, 39ga, tweede lid, 42a, tweede lid, 51b, eerste lid, en 51f van de Wjsg wordt verwezen.

Conclusie doorgifte aan derde landen en internationale organisaties
De AP adviseert om de toelichting bij artikel 17a van de Wpg in overeenstemming te brengen met de voor deze sector toepasselijke systematiek voor doorgiften aan derde landen of internationale organisaties zoals in dat artikel omschreven en daarbij toe te lichten wat dit inhoudt voor de uitwerking daarvan in de praktijk. Hetzelfde geldt voor de overeenkomstige bepalingen in de Wjsg.

8 Artikelsgewijs commentaar

- De titel van de Wijzigingswet

Deze titel vermeldt dat deze is "ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing, vervolging en berechting van strafbare feiten of de tenuitvoerlegging van straffen."
Weliswaar omvat het bereik van de Richtlijn mede de verwerking van persoonsgegevens door de gerechten zoals hierboven vermeld, maar daarbij is al hetgeen valt onder de taakuitvoering van de onafhankelijke rechter uitdrukkelijk uitgezonderd. Dit brengt mee dat 'de berechting van strafbare feiten' nu juist is uitgezonderd van de reikwijdte van de Richtlijn. De invoeging bij de titel die ziet op die berechting heeft daarentegen (overeenkomstig algemeen juridisch spraakgebruik) betrekking op de beoordeling door de strafrechter van het voorgelegde strafbare feit. Om die reden dient de toevoeging " .. en berechting .." dan ook uit de titel van de Wijzigingswet te worden verwijderd.

- Artikel 24b, derde lid, van de Wpg

Deze bepaling die ziet op weigering van informatieverstrekking indien de betrokkene behoort tot de categorie "personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen gaan plegen". De memorie van toelichting verwijst daarvoor naar artikel 13, vierde lid, van de Richtlijn en betoogt dat het niet wenselijk is dat verdachten van strafbare feiten langs elektronische weg op de hoogte kunnen komen van het feit dat jegens hen een opsporingsonderzoek loopt. Daarom wordt voorgesteld deze categorie uit te zonderen. Echter, artikel 13, vierde lid, heeft betrekking op "wettelijke maatregelen om te bepalen welke verwerkingscategorieën geheel of gedeeltelijk onder één van de punten van lid 3 kunnen vallen." Dit artikellid heeft echter betrekking op categorieën *gegevens* en niet op categorieën *betrokkenen*. Dat lijkt ook logisch gezien de constructie dat deze weigeringsgrond om belemmering van gerechtelijke onderzoeken te voorkomen, is opgenomen bij de afwijzingsgronden bij een concreet verzoek om inzage, rectificatie of vernietiging van politiegegevens.

- Artikel 25, eerste lid, onder c, van de Wpg

Dit artikellid geeft aan dat de betrokkene recht heeft om te vernemen of politiegegevens –kort gezegd – gedurende een periode van vier jaar voorafgaand aan het verzoek zijn verstrekt en aan wie. Dit artikel is niet gewijzigd ten opzichte van de huidige Wpg. Desgevraagd heeft het ministerie van Veiligheid en Justitie hiervoor verwezen naar het 'Rijkeboer-arrest'.
De relevante conclusie in Rijkeboer-arrest van het Europese Hof van Justitie van 7 mei 2009 (C-553/07; ECLI:EU:C:2009:293) stelt dat het aan de lidstaten is om een juiste termijn voor de bewaring van informatie en een daarop afgestemde toegang vast te stellen die een juist evenwicht vormen tussen het belang van de betrokkene enerzijds en het belang van de verantwoordelijke anderzijds.
Hieruit volgt dat het in deze aan de nationale wetgever is om een termijn vast te stellen die een juist evenwicht vormt. Uit de memorie van toelichting blijkt dat de tekst van artikel 25 is aangepast aan de tekst

van artikel 14 van de Richtlijn, en voor het overige is gehandhaafd. Hier lijkt geen aanleiding om in de gekozen bewaartermijn wijziging aan te brengen. De AP adviseert om in dat verband een aanvullende toelichting hierover op te nemen.
Voorts is een onderdeel van het bepaalde in artikel 14, aanhef en onder g, van de Richtlijn niet in artikel 25, eerste lid, van de Wpg opgenomen. Onderdeel g) heeft betrekking op informatie over "de persoonsgegevens die worden verwerkt, en alle beschikbare informatie over de oorsprong van die gegevens". De inhoud van het eerste zinsdeel hiervan is weliswaar verwerkt in de tekst van het eerste lid van artikel 25, het laatste onderdeel van de zin is hier echter niet opgenomen. De AP adviseert dit onderdeel alsnog op te nemen.

- Artikel 31a, tweede lid, Wpg

Verzoek om in de toelichting een aanvulling op te nemen om daarmee te verduidelijken dat dit artikellid betrekking heeft op de onbevoegdheid die verband houdt met het territoriale aspect "Nederlands grondgebied in Europa".

- Artikel 35b, eerste lid, onderdeel g, van de Wpg

Dit artikel luidt als volgt: 1. *De Autoriteit persoonsgegevens heeft tot taak: het naar aanleiding van een klacht, bedoeld in artikel 31a, eerste lid, controleren van de rechtmatigheid van de verwerking en de betrokkene binnen een redelijke termijn te informeren over het resultaat van de controle of van de redenen waarom de controle niet is verricht.*
Uit de implementatietabel wijziging Wpg blijkt dat artikel 31a van de Wpg een implementatie betreft van artikel 17, eerste lid van de Richtlijn. Dit artikel bepaalt:"*1. In de in artikel 13, lid 3, artikel 15, lid 3, en artikel 16, lid 4, bedoelde gevallen treffen de lidstaten maatregelen die ertoe strekken dat de betrokkene zijn rechten ook via de bevoegde toezichthoudende autoriteit kan uitoefenen. 2. De lidstaten schrijven voor dat de verwerkingsverantwoordelijke de betrokkene in kennis stelt van de mogelijkheid uit hoofde van lid 1 zijn rechten via de toezichthoudende autoriteit uit te oefenen. 3. Wanneer het in lid 1 bedoelde recht wordt uitgeoefend, stelt de toezichthoudende autoriteit de betrokkene er ten minste van in kennis dat alle noodzakelijke controles of een evaluatie door de toezichthoudende autoriteit hebben plaatsgevonden. De toezichthoudende autoriteit stelt de betrokkene tevens in kennis van zijn recht om beroep in te stellen bij de rechter.*"
De AP begrijpt dit artikel zo, dat het verzoek van een betrokkene door de verantwoordelijke, bijvoorbeeld de politie, kan worden geweigerd of beperkt bijvoorbeeld om de nationale veiligheid te beschermen (zie overweging 44) en in die gevallen de betrokkene naar de toezichthouder kan gaan met het verzoek om te controleren of het verzoek terecht is geweigerd. De AP merkt zo'n verzoek momenteel aan als een verzoek om *bemiddeling* en niet als een klacht in de zin van een handhavingsverzoek. De AP adviseert om die reden de aanduiding bemiddeling in de Wpg te hanteren. Dit sluit ook aan bij de rol van de AP zoals omschreven in overweging 48 van de Richtlijn waarin staat dat de AP in een voorkomend geval controleert of de weigering of beperking terecht is en waarbij zij de betrokkene informeert over het recht om een voorziening in rechte in te stellen.

- Artikel 26 van de Wjsg

Het huidige artikel 26 van de Wjsg biedt de mogelijkheid van verzet "wegens bijzondere persoonlijke omstandigheden" en heeft betrekking op de rechten van de betrokkene op kennisneming en verbetering van justitiële gegevens. In het voorstel voor de Wijzigingswet komt dit element niet terug. In de memorie

Datum
7 april 2017

Ons kenmerk
z2017-01571

van toelichting bij het nieuwe artikel 26 is dit als volgt gemotiveerd: "De richtlijn kent de mogelijkheid van verzet niet. De invoering van een klachtrecht bij de Autoriteit Persoonsgegevens leidt voorts tot aanvullende rechtsbescherming van betrokkenen. In het licht hiervan wordt voorgesteld de mogelijkheid van verzet wegens bijzondere persoonlijke omstandigheden te schrappen. Het artikel voorziet in het recht van een betrokkene een klacht in te dienen bij de AP."
De AP meent dat in de praktijk de mogelijkheid van verzet hier een effectief middel kan zijn om de betrokkene de gelegenheid te geven eerst bij de verantwoordelijke aanpassing van de verwerking van zijn justitiële gegevens te verzoeken, naast het recht om een klacht in te dienen bij de AP. Dat de Richtlijn dit rechtsmiddel niet kent is in dit verband niet doorslaggevend, aangezien de Richtlijn voorziet in minimumvereisten waar de lidstaten steeds kunnen voorzien in een hoger niveau van bescherming.
De AP adviseert de mogelijkheid van verzet hier te handhaven.

- Redactionele opmerkingen

Enkele redactionele opmerkingen zijn opgenomen in bijlage 1.

- Overzichtstabel

Een overzicht met voorgestelde wijzigingen in de overzichtstabel bij de Wijzigingswet is opgenomen in bijlage 2.

Dictum

De Autoriteit Persoonsgegevens heeft bezwaar tegen het voorstel van wet en adviseert u dit niet aldus in te dienen.

De AP verneemt graag op welke wijze u gevolg geeft aan het advies. De AP is beschikbaar indien nadere toelichting is vereist.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
Autoriteit persoonsgegevens,

Mr. W.B.M. Tomesen
Vicevoorzitter

Datum
7 april 2017

Ons kenmerk
z2017-01571

Bijlage 1 - Redactionele opmerkingen

- **Artikel 4a, eerste lid, onder b, Wpg**
  Een opmerking van taalkundige aard: (gegevensbeschermings)beleid wordt uitgevoerd en (gegevensbeschermings)beginselen worden toegepast; het betreft de implementatie van elementen uit artikel 19, tweede lid, en artikel 20, eerste lid, van de Richtlijn. Voorstel tot wijziging van de tekst: 'b. op een doeltreffende manier het gegevensbeschermingsbeleid uit te voeren en de gegevensbeschermingsbeginselen toe te passen;'.
- **Artikel 17a, eerste lid, Wpg**
  In regel 2 dient de formulering te luiden "aan een internationale organisatie" en niet "aan een verantwoordelijke *in* een internationale organisatie" (zie artikel 35, eerste lid, onder b, van de Richtlijn "to a controller in a third country or international organisation"); het betreft hier de doorgifte aan een internationale organisatie, niet aan een verwerkingsverantwoordelijke *in* een internationale organisatie.
- **Artikel 33a, tweede lid, onder d, Wpg**
  De formulering "om de inbreuk [..] *ongedaan te maken* en, in voorkomend geval, .." is een ongelukkige (aangezien de inbreuk niet ongedaan te maken is) en bovendien onvolledig. Verzoek om hierbij aan te sluiten bij de bewoordingen van de Richtlijn (in artikel 30, derde lid, onder d) en van de Verordening (in artikel 33, derde lid, onder d).
- **Artikel 1, onder e, Wjsg**
  Het begrip "gerechtelijke *straf*gegevens" is juridisch ondeugdelijk, aangezien deze persoonsgegevens geen betrekking hebben op straffen maar op strafzaken, en dient te worden gewijzigd. Voorstel om dit te wijzigen in "gerechtelijk strafzaakgegeven". Ook de term "Nederlandse *strafwet*" is juridisch onjuist en verdient aanpassing. Hoewel de wijziging van de gebruikte term in 'gerechtelijk strafzaakgegeven' aanvankelijk in de memorie van toelichting bij het definitieve conceptvoorstel was doorgevoerd, is deze wijziging in de laatste tekstversie ongedaan gemaakt en in de tekst van de Wijzigingswet ongewijzigd gebleven.
- **Artikel 7, eerste lid, onder b, Wjsg**
  Idem als bij artikel 4a Wpg.
- **Titel 3b, artikel 51e e.v. Wjsg**
  Ten aanzien van de term "gerechtelijke *straf*gegevens" idem als bij artikel 1: telkens te wijzigen in "gerechtelijke strafzaakgegevens".

AUTORITEIT
PERSOONSGEGEVENS

Datum
7 april 2017

Ons kenmerk
z2017-01571

Bijlage 2 - voorgestelde wijzigingen overzichtstabel bij Wijzigingswet

Richtlijn	**Wet politiegegevens**	**Opmerking AP**
32(4) Publicatie contactgegevens	Artikel 36, vierde lid	Onjuiste verwijzing: Artikel 36, vijfde lid, Wpg
34 Taken	Artikel 36, tweede lid,	Onjuiste verwijzing: Artikel 36, derde lid, Wpg
44 (2) Beroepsgeheim	Artikel 125, derde lid, Ambtenarenwet	Aanvullen: artikel 2:5 Awb
45(2) Uitzondering gerechten	Artikel 35, derde lid	Niet geïmplementeerd? Artikel 35 heeft maar twee leden. (zie soortgelijke tekst artikel 51h Wjsg)
45 (3) Kosteloos	Artikel 35b, tweede lid	Verwijzing naar artikel 45 (3) is onjuist. Wijzigen in artikel 46 (3) Ri
45 (4) Ongegronde verzoeken	Artikel 31a, zesde lid	Verwijzing naar artikel 45 (4) is onjuist. Wijzigen in artikel 46 (3) Ri.
47 (1) Bevoegden	Artikel 35, tweede lid, en titel 5.2 Awb	Onjuiste verwijzing artikel 35, tweede lid Awb ziet op de adviesbevoegdheid van de AP. Deze staat in artikel 47, derde lid, van de Ri en niet in het eerste lid. De onderzoeksbevoegdheden staan wel in titel 5.2 van de Awb.
47 (4)	Artikelen 29, eerste lid, 31a, vijfde lid en 35c, vijfde lid; besluit in de zin van Awb	In Wijzigingswet staat deze bepaling in artikel 29, tweede lid. Niet geïmplementeerd? De verwijzing naar artikel 35c, vijfde lid is onjuist. Dit artikel heeft maar drie leden.
50 (1)	Artikel 35d, eerste lid	Onjuiste verwijzing, betreft artikel 35 e eerste lid.
53 (1) rechterlijke tussenkomst	Artikel 35c, derde lid (zie 47, vierde lid)	Toevoegen: Awb
53 (3) Bevoegdheid	Artikel 31a, zevende lid	Onjuiste verwijzing. Dit artikellid ontbreekt. Staat in artikel 31b Wpg
56 Recht op schadevergoeding	Artikel 31b j.o. 36 Uitvoeringswet Avg	Onjuiste verwijzing naar artikel 36 Uitvoeringswet. Dit artikel gaat over geautomatiseerde individuele besluitvorming

Datum
7 april 2017

Ons kenmerk
z2017-01571

Richtlijn	**Wjsg**	
Artikel 53 (1) Rechterlijke tussenkomst TA	Artikelen 26, eerste lid, tweede volzin, 26d, eerste lid jo. 35c, derde lid, Wpg, 39r, 51, 51d en 51h, eerste en derde lid	Klopt de verwijzing naar artikel 26d eerste lid?
Artikel 53 (2) voorziening in rechte bij niet behandelen klacht	Artikelen 26, vijfde lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste en derde lid	Toevoegen: Awb.
Artikel 56 recht op schadevergoeding	Artikelen 7f jo. 36 wvs Uitvoeringswet Algemene verordening gegevensverwerking, 39c, tweede lid en 40, derde lid, 51b eerste en derde lid en 51f.	Verwijzing naar artikelen in Uitvoeringswet kloppen niet. Artikel 36 van de Uitvoeringswet ziet op geautomatiseerde individuele besluitvorming