Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

34 889 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

Nr. 3 **MEMORIE VAN TOELICHTING**

1. Inleiding

Met dit wetsvoorstel wordt uitvoering gegeven aan 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, L119). Deze richtlijn wordt in de Kamerstukken aangeduid als de richtlijn gegevensbescherming opsporing en vervolging (hierna ook: de richtlijn). Dit wetsvoorstel voorziet in aanpassing van de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Het wetsvoorstel bevat wijzigingen in verplichtingen voor de verwerkingsverantwoordelijke die in samenhang bezien tot een verbeterd beschermingsniveau leiden van degene op wie de verwerking van een politiegegeven of een gegeven als bedoeld in de Wjsg betrekking heeft. Uitgangspunt hierbij is minimumimplementatie van de richtlijn, met dien verstande dat voor enkele specifieke kwesties de implementatie doorwerking heeft en daarnaast aan een eerdere toezegging van het kabinet aan de Tweede Kamer uitvoering wordt gegeven die te bezien bij de omzetting van de implementatie van de richtlijn (zie nader paragraaf 5.2.2). Mede namens de Minister van Defensie licht ik dit wetsvoorstel hieronder nader toe.
Dit wetsvoorstel is onderdeel van een breder pakket, dat in zijn geheel de richtlijn gegevensbescherming opsporing en vervolging en de Algemene verordening gegevensbescherming[1] (hierna: ook de verordening gegevensbescherming, of: de verordening) zal implementeren. Dit pakket bestaat uit:

a. het voorliggende wetsvoorstel, waarmee de richtlijn gegevensbescherming opsporing en vervolging wordt geïmplementeerd;

[1] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (PbEU 2016, L 119).

kst-34889-3
ISSN 0921 - 7371
's-Gravenhage 2018

b. de uitvoeringswet, waarin uitvoering wordt gegeven aan de verordening gegevensbescherming en de Wet bescherming persoonsgegevens wordt ingetrokken;
c. een invoeringswet met een technisch karakter, dat de terminologie in het bestaande wettenbestand aanpast aan de verordening en aan het wegvallen van de Wbp als de algemene wet voor bescherming van persoonsgegevens, alsmede aan gewijzigde verwijzingen als gevolg van dit wetsvoorstel.

In de memorie van toelichting bij het wetsvoorstel ter uitvoering van de verordening gegevensbescherming wordt nader ingegaan op de Europeesrechtelijke grondslag van de verordening gegevensbescherming en de richtlijn gegevensbescherming opsporing en vervolging en op de verhouding tussen de verordening en de richtlijn. In deze memorie van toelichting wordt ingegaan op:
- De Europeesrechtelijke achtergrond van de richtlijn;
- De richtlijn in vogelvlucht;
- De consequenties van de richtlijn voor de wetgeving op het gebied van de bescherming van persoonsgegevens;
- Het toepassingsgebied van de richtlijn en doelbinding;
- De richtlijn en de herziening van de privacywetgeving voor opsporing en vervolging;
- De consequenties van de richtlijn voor de wetgeving op het gebied van de bescherming van persoonsgegevens;
- Uitvoeringsgevolgen van de richtlijn;
- Implementatietabellen.

2. De Europeesrechtelijke achtergrond van de richtlijn

2.1. Voorgeschiedenis

Op 27 november 2008 heeft de Raad van de Europese Unie een kaderbesluit aangenomen over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken[2] (hierna: het kaderbesluit dataprotectie, of: het kaderbesluit). Het kaderbesluit dataprotectie, dat met deze richtlijn is ingetrokken, gaf regels over de verwerking van persoonsgegevens in het kader van de politiële en justitiële samenwerking in strafzaken (artikel 59, eerste lid, RI). Het toepassingsgebied van het voormalige kaderbesluit was beperkt tot de verwerking van persoonsgegevens die werden verstrekt of beschikbaar gesteld tussen de lidstaten. Het voormalige kaderbesluit is destijds geïmplementeerd in de Wpg en de Wjsg[3] (Stb. 2011, 490). Daarbij is uitgegaan van een zoveel mogelijk extensieve werking van de regels van het kaderbesluit voor de verwerking en verstrekking van de persoonsgegevens, dat wil zeggen dat de regels van het voormalige kaderbesluit ook golden voor de gegevens die uitsluitend op nationaal niveau werden verwerkt. Aldus is met deze wet reeds een belangrijke stap gezet ter implementatie van de Europese regels op het gebied van de bescherming van persoonsgegevens. Daardoor is de implementatie van de richtlijn gegevensbescherming opsporing en vervolging beperkt tot aanpassing van de bepaalde onderdelen van de bestaande nationale wetgeving, in

[2] Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken (PbEU 2008, L 350/60).

[3] Wet tot wijziging van de Wet politiegegevens en van de Wet justitiële en strafvorderlijke gegevens in verband met de implementatie van het kaderbesluit van de Raad van de Europese Unie 2008/977/JBZ over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken en de implementatie van het Besluit van de Raad 2009/371/JBZ van 6 april 2009 tot oprichting van de Europese politiedienst (Europol), Kamerstukken II 32 554.

aanvulling op hetgeen reeds naar aanleiding van het voormalige kaderbesluit dataprotectie is aangepast. Wel wordt het niveau van gegevensbescherming bij de verwerking van persoonsgegevens ten behoeve van de strafrechtspleging hiermee verder verhoogd.
Op 4 november 2010 heeft de Commissie een Mededeling uitgebracht waarin de kaders worden geschetst voor een herziening van de zogenoemde Privacyrichtlijn (Richtlijn nr. 95/46/EG)[4]. In de Mededeling is een uitgewerkt voorstel tot herziening van het wettelijk kader voor gegevensbescherming in de EU aangekondigd. Naar aanleiding van de mededeling is een zogenaamd fiche opgesteld aan de Kamer gezonden (Kamerstukken II 2010/11, 22 112, nr. 1116). De op 25 januari 2012 door de Commissie gepresenteerde orstellen strekken tot uitvoering van de in de Mededeling aangekondigde voornemens.
Op 27 april 2016 hebben het Europees Parlement en de Raad de richtlijn gegevensbescherming opsporing en vervolging aangenomen[5]. Deze richtlijn treedt in de plaats van het kaderbesluit dataprotectie. Naast de richtlijn gegevensbescherming opsporing en vervolging is de verordening gegevensbescherming tot stand gekomen, die van toepassing is op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Deze verordening heeft rechtstreekse werking, zodat voor de uitvoering daarvan kan worden volstaan met de Uitvoeringswet Algemene verordening gegevensbescherming (Uitvoeringswet Avg).
Met dit wetsvoorstel wordt de richtlijn geïmplementeerd. De bepalingen uit de richtlijn met betrekking tot de nationale toezichthouder zijn echter deels opgenomen in de Uitvoeringswet Avg. Verder zullen de bepalingen van de richtlijn worden geïmplementeerd door middel van aanpassing van specifieke wetten op het terrein van het strafrecht.

2.2. De verhouding tot de Algemene verordening gegevensbescherming

Voor wat betreft het toepassingsbereik sluiten de verordening en de richtlijn elkaar wederzijds uit: waar de richtlijn geldt is de verordening niet van toepassing en andersom. Materieel is er sprake van een zekere mate van overlap tussen de richtlijn en de verordening voor wat betreft de verplichtingen van de verwerkingsverantwoordelijke.
De verordening gegevensbescherming reguleert de verwerking van persoonsgegevens die gebaseerd zijn op privaatrechtelijke en bestuurlijke rechtsverhoudingen. De aard van de rechtsverhouding die ten grondslag kan liggen aan de verwerking van persoonsgegevens is ruimer dan onder de richtlijn. Op basis van de verordening kan de grondslag voor de verwerking van persoonsgegevens berusten op een wettelijke verplichting, maar ook op toestemming van een betrokkene of een contractuele verplichting. De richtlijn is toegesneden op de rechtshandhaving, waarbij er geen ruimte is voor instemming van de betrokkene met de gegevensverwerking. Bepaalde verplichtingen zijn onder de richtlijn en de verordening materieel gelijk, zoals de verplichte melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit en aan de betrokkene (vgl. de artikelen 30 en 31 RI en 33 en 34 Avg). Andere verplichtingen zijn vergelijkbaar maar kennen verschillen in de concrete uitwerking, zoals de verplichting voor de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen te

[4] COM2010 609.
[5] Richtlijn 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 (Richtlijn 2016/680 van 27 april 2016, Pb EU L 119/89).

treffen ter bescherming en beveiliging van de gegevens (vgl. de artikelen 19, 20, 29 Rl en 24, 25 en 32 Avg). Voor meer onderwerpen geldt dat die zowel in de richtlijn als de verordening worden geregeld, maar niet op identieke wijze. Dit leidt tot verschillen van uiteenlopende aard en omvang, bijvoorbeeld ten aanzien van de verplichting inzake een gegevensbeschermingseffectbeoordeling (vgl. artikel 27 Rl en 35 Avg), de door een verwerkingsverantwoordelijke bij te houden verwerkingsactiviteiten in een register (vgl. artikelen 24 Rl en 30 Avg), de verwerking voor andere doelen (vgl. artikelen 9 Rl en 6 Avg), de informatieverstrekking aan de betrokkene (vgl. artikelen 13 Rl en 13, 14 Avg) en de kennisgeving van rectificatie (vgl. artikelen 16 Rl en 19 Avg). Anders dan onder de richtlijn bevat de verordening geen verplichting tot geautomatiseerde vastlegging van gegevens over de gegevensverwerking (logging) en het recht voor betrokkene een klacht bij de toezichthoudende autoriteit in te dienen. De verplichte aanwijzing van de functionaris voor gegevensbescherming op grond van de richtlijn sluit niet uit dat voor die verplichting op grond van de verordening dezelfde functionaris wordt aangewezen (vgl. artikelen 33 en 34 Rl en 37 tot en met 39 Avg).
Een complicerende factor is dat de verplichtingen van de richtlijn moeten worden omgezet in nationale wetgeving, terwijl de verplichtingen van de verordening rechtsreeks werken. Instanties die onder het toepassingsgebied van de richtlijn vallen, zoals de politie en de Koninklijke marechaussee, krijgen niet alleen te maken met de nationale regelgeving ter implementatie van de richtlijn maar ook met zowel de bepalingen van de verordening die rechtstreeks werken als de nationale bepalingen die uitvoering geven aan de verordening, voor zover dit taken betreft die geen betrekking hebben op 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 (hierna ook: de richtlijntaken). Ook een instantie als het Centraal Justitieel Incasso Bureau zal met onderscheidenlijke regimes van regelgeving moeten werken bij de afdoening van overtredingen op grond van de Wet administratiefrechtelijke handhaving verkeersvoorschriften (zie nader de toelichting bij artikel 1, onderdeel d, Wjsg).
Uitgangspunt voor de implementatie is dat zoveel mogelijk moet worden voorkomen dat de instanties binnen de strafrechtsketen worden geconfronteerd met verschillende verwerkingsregimes, met het oog op de uitvoerbaarheid van de regels voor de verwerking van persoonsgegevens door de betreffende instanties. Daarbij is zoveel mogelijk aangesloten bij de bestaande privacywetgeving voor die instanties. Dit betreft de Wpg voor de politie, de Koninklijke marechaussee en de bijzondere opsporingsdiensten, en de Wjsg voor het openbaar ministerie en het CJIB. Deze wetten geven regels voor de verwerking van persoonsgegevens door de personen en instanties die zijn belast met de opsporing en vervolging van strafbare feiten. Met de aanpassing van deze wetten ter implementatie van de richtlijn wordt aldus uitgegaan van een meer organisatiegerichte benadering, gericht op de strafrechtspleging. Voor zover sprake is van de verwerking van persoonsgegevens met het oog op andere vormen van handhaving, door middel van het bestuurs- of civiele recht, is de verordening van toepassing.

3. De richtlijn gegevensbescherming opsporing en vervolging in vogelvlucht

Bij brief van 7 januari 2016 is reeds een korte schets van de belangrijkste onderdelen van de richtlijn gegevensbescherming opsporing en vervolging gegeven, en een eerste, algemene waardering van het onderhandelingsresultaat (Kamerstukken II 2015/16, 32 761, nr. 91).
De richtlijn bestaat uit tien hoofdstukken. *Hoofdstuk I* bevat de algemene bepalingen. Dit betreft het toepassingsgebied van de richtlijn en de

definities (artikelen 2 en 3 RI). De belangrijkste definities zijn gelijk aan die van de verordening.
Hoofdstuk II bevat de beginselen. Dit betreft beginselen inzake verwerking van persoonsgegevens, specifieke verwerkingsvoorwaarden en de verwerking van bijzondere categorieën van persoonsgegevens (artikelen 4, 9 en 10 RI).
In *Hoofdstuk III* zijn de rechten van de betrokkene neergelegd. Dit betreft algemene regels voor de communicatie, zoals het beginsel dat deze kosteloos geschiedt en dat de betrokkene schriftelijk in kennis wordt gesteld van de opvolging van zijn verzoek (artikel 12 RI). Verder is voorzien in een verplichting voor de verwerkingsverantwoordelijke om bepaalde informatie ter beschikking te stellen (artikel 13 RI). Aanvullend is voorzien in een recht op inzage van de betrokkene (artikel 14 RI) en in de mogelijkheid van beperking van het inzagerecht in het belang van (onder meer) het opsporingsonderzoek of de strafvervolging (artikel 15 RI). Tevens is in dit hoofdstuk voorzien in een recht op rectificatie of wissing van persoonsgegevens, waarbij eveneens weigeringsgronden kunnen worden ingeroepen (artikel 16 RI).
Hoofdstuk IV bevat algemene verplichtingen voor de verwerkingsverantwoordelijke en de verwerker (afdeling 1), de beveiliging van persoonsgegevens (afdeling 2) en de functionaris voor gegevensbescherming (afdeling 3). De verwerker verwerkt de persoonsgegevens namens de verantwoordelijke en uitsluitend volgens de instructies van de laatstgenoemde (artikel 21 RI). De verwerkingsverantwoordelijke en de verwerker zijn gehouden maatregelen te treffen ter beveiliging van persoonsgegevens (artikelen 20 en 29 RI). Van geautomatiseerde verwerkingen worden logbestanden bijgehouden (artikel 25 RI). Tevens is voorzien in verplichtingen tot het verrichten van een gegevensbeschermingseffectbeoordeling, de voorafgaande raadpleging van de toezichthoudende autoriteit en de melding van datalekken (artikelen 27, 28, 30 en 31 RI). Er moet een functionaris voor gegevensbescherming worden aangewezen die toeziet op de naleving van de richtlijn (artikelen 32 en 34 RI).
Hoofdstuk V heeft betrekking op doorgiften van persoonsgegevens aan derde landen of internationale organisaties. Het uitgangspunt is dat persoonsgegevens slechts mogen worden doorgegeven op basis van een adequaatheidsbesluit van de Commissie (artikel 36 RI). Bij ontstentenis van een adequaatheidsbesluit kunnen persoonsgegevens worden doorgegeven op basis van passende waarborgen voor de bescherming van persoonsgegevens (artikel 37 RI). In afzonderlijke in de richtlijn omschreven gevallen is doorgifte aan derde landen of een internationale organisatie mogelijk, onder andere met het oog op de richtlijntaken (artikel 38 RI).
Hoofdstuk VI regelt de instelling van onafhankelijke toezichthoudende autoriteiten. Dit omvat onder meer de onafhankelijkheid (artikel 42 RI), de competentie (artikel 45 RI), de taken (artikel 46 RI) en bevoegdheden (artikel 47 RI).
Hoofdstuk VII voorziet in de samenwerking tussen de nationale toezichthoudende autoriteiten, onder meer door het verstrekken van relevante informatie en het verlenen van wederzijdse bijstand (artkel 50 RI). Het op grond van de verordening opgerichte Europees Comité voor gegevensbescherming wordt belast met het adviseren van de Commissie over aangelegenheden in verband met de bescherming van persoonsgegevens in de Europese Unie (artikel 51 RI). Dit Comité wordt gevormd door de bestaande zogenaamde «artikel 29-werkgroep», die is samengesteld uit alle nationale toezichthoudende autoriteiten.
Hoofdstuk VIII regelt beroep, aansprakelijkheid en straffen. De betrokkene heeft het recht om, als hij van mening is dat inbreuk wordt gemaakt op de krachtens de richtlijn vastgestelde bepalingen, een klacht in te dienen bij een toezichthoudende autoriteit (artikel 52 RI). Tevens heeft de betrokkene

het recht om een doeltreffende voorziening in rechte in te stellen (artikel 53 en 54 RI).
Hoofdstuk IX bevat bepalingen over uitvoeringshandelingen. De commissie krijgt op een tweetal terreinen de gedelegeerde bevoegdheid om nadere regels te stellen. Dit betreft de intrekking, wijziging of schorsing van een zogenaamd adequaatheidsbesluit met betrekking tot het beschermingsniveau in een derde land (artikel 36, vijfde lid, RI) en de vastlegging van het model en de procedures voor de wederzijde bijstand tussen de toezichthoudende autoriteiten van de lidstaten (artikel 50, achtste lid, RI). De uitvoeringshandelingen worden vastgesteld volgens de onderzoeksprocedure, genoemd in artikel 2 van Verordening nr. 182/2011, aangezien dit handelingen van algemene strekking zijn (overweging 91 RI)[6].
Hoofdstuk X bevat de slotbepalingen. Hierin is onder andere voorzien in de intrekking van het kaderbesluit dataprotectie (artikel 59 RI), het van kracht blijven van specifieke bepalingen voor de bescherming van persoonsgegevens in reeds geldende rechtshandelingen van de Europese Unie (artikel 60 RI), de periodieke evaluatie van de richtlijn (artikel 62 RI) en de inwerkingtreding (artikel 64 RI).
De richtlijn moet op 6 mei 2018 zijn geïmplementeerd (artikel 63, eerste lid, RI).

4. De consequenties van de richtlijn voor de wetgeving op het gebied van de bescherming van persoonsgegevens

De richtlijn heeft consequenties voor de wetgeving van de lidstaten op het gebied van de bescherming van persoonsgegevens die worden verwerkt ten behoeve van 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. In de eerste plaats kan worden gewezen op het ruimere toepassingsgebied van de richtlijn ten opzichte van het voormalige kaderbesluit dataprotectie, omdat de richtlijn ook van toepassing is op de verwerking van persoonsgegevens die uitsluitend op nationaal niveau plaatsvindt. Zoals hierboven reeds aan de orde is gekomen, is dit onderscheid voor Nederland minder van belang omdat destijds is gekozen voor een zo veel mogelijk extensieve implementatie van het voormalige kaderbesluit dataprotectie.
In de tweede plaats maakt de richtlijn onderscheid tussen de verwerking van persoonsgegevens in de lidstaten van de Europese Unie enerzijds en de doorgifte van persoonsgegevens aan derde landen en internationale organisaties anderzijds. Met dit onderscheid wordt afgeweken van de structuur van de Wpg en de Wet justitiële en strafvorderlijke gegevens, waarin onderscheid wordt gemaakt tussen de verwerking van gegevens op nationaal niveau en de verstrekking van gegevens aan derde landen en internationale organisaties, waarbij nader onderscheid werd gemaakt tussen de verstrekking aan andere lidstaten en de verstrekking aan derde landen. Dit betekent dat de regels van de Wpg met betrekking tot een vrije uitwisseling van gegevens met het oog op de uitvoering van de politietaak («free flow of information»), op basis van hoofdstuk III van die wet, onverkort van toepassing zijn op de uitwisseling van gegevens met opsporingsambtenaren in andere lidstaten. Voor de verstrekking van politiegegevens aan opsporingsambtenaren in andere landen geldt het regime voor de verstrekking van politiegegevens aan derde landen en internationale organisaties (Paragraaf 3 Wpg). Voor de Wjsg geldt

[6] Verordening nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren (Pb L55 van 20-02-2017, blz. 13).

hetzelfde ten aanzien van onder die wet vallende gegevens. Hierbij moet nog worden opgemerkt dat het begrip «lidstaat» niet eenduidig kan worden gedefinieerd, vanwege de bijzondere positie van landen als het Verenigd Koninkrijk, Ierland, Denemarken als EU-lidstaten enerzijds en van landen als Noorwegen, IJsland en Zwitserland als niet-lidstaten anderzijds. In het wetsvoorstel wordt met de definitie van het begrip derde land hiermee rekening gehouden.
In de derde plaats bevat de richtlijn nieuwe verplichtingen voor de verwerkingsverantwoordelijke. Dit betreft verplichtingen als de (actieve) beschikbaarstelling van informatie over de gegevensverwerking aan de betrokkene, het bijhouden van logbestanden, de registratie van gegevens over de gegevensverwerkingen, het verrichten van gegevensbeschermingseffectbeoordelingen en het melden van datalekken aan de betrokkene en aan de toezichthoudende autoriteit. Op deze punten behoeven de Wpg en de Wjsg aanpassing, de betreffende verplichtingen van de richtlijn zijn in dit wetsvoorstel opgenomen.
In de vierde plaats bevat de richtlijn uitgebreide regels over de positie, de taken en bevoegdheden van de toezichthoudende instantie. Voor Nederland betreft dit de Autoriteit persoonsgegevens (AP). Voor zover de regels van de richtlijn aanleiding geven tot aanpassing van de Wpg en de Wjsg, zijn de betreffende regels in dit wetsvoorstel opgenomen.
Ten slotte kan worden opgemerkt dat de richtlijn niet belet in het nationale recht uitgebreidere waarborgen te bieden dan die waarin de richtlijn voorziet (artikel 1, derde lid, Rl). Dit betekent dat, daar waar de Wpg en de Wjsg thans uitgebreidere waarborgen bieden dan die welke uit de richtlijn voortvloeien, die waarborgen kunnen worden gehandhaafd.

5. Het toepassingsgebied van de richtlijn gegevensbescherming opsporing en vervolging en doelbinding

5.1. Het toepassingsbereik van de richtlijn

De richtlijn is van toepassing op 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 (artikel 2, eerste lid, Rl). De Algemene verordening gegevensbescherming is van toepassing op de verwerking van persoonsgegevens voor andere doeleinden, die binnen de werkingssfeer van het Unierecht vallen.
Van de toepasselijkheid van zowel de richtlijn als de verordening is uitgezonderd de verwerking van persoonsgegevens in het kader van activiteiten die buiten de werkingssfeer van het recht van de Europese Unie vallen, zoals activiteiten van de Algemene inlichtingen- en veiligheidsdienst en de Militaire inlichtingen- en veiligheidsdienst (artikel 2 Rl en artikel 2 Avg). De richtlijn en de verordening zijn evenmin van toepassing op de verwerking van persoonsgegevens door de lidstaten bij de uitvoering van activiteiten die onder het gemeenschappelijk buitenlands- en veiligheidsbeleid vallen en op de verwerking van persoonsgegevens door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit. Tot slot is van de toepasselijkheid van de richtlijn uitgezonderd de verwerking van persoonsgegevens bij inzet of beschikbaarstelling door de krijgsmacht. Hierop wordt de Algemene verordening gegevensbescherming van overeenkomstige toepassing verklaard (artikel 4 Uitvoeringswet Avg).
Bepalend voor de toepasselijkheid van de richtlijn zijn (1) het zijn van bevoegde autoriteit in de zin van de richtlijn, en (2) de doeleinden waarop de verwerking van persoonsgegevens door een bevoegde instantie betrekking hebben. Deze twee voorwaarden zijn cumulatief.

Bevoegde autoriteit is (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 recht van de lidstaten is gemachtigd openbaar gezag en openbare bevoegdheden uit te oefenen met het oog op de onder punt a genoemde doelen (artikel 3, zevende lid, RI).
De doeleinden van de richtlijn hebben betrekking op de strafrechtspleging, dit blijkt ook uit de verwijzing naar Verklaring betreffende de bescherming van persoonsgegevens op het gebied van justitiële samenwerking in strafzaken en op het gebied van politiële samenwerking bij het Verdrag van Lissabon[7]. De voorkoming van strafbare feiten betreft de verwerking van persoonsgegevens door de bevoegde autoriteiten ter voorkoming dat een strafbaar feit wordt gepleegd, zoals het verwerken van persoonsgegevens door de criminele inlichtingen eenheid van de politie of een bijzondere opsporingsdienst. De gegevensverwerking in het kader van de vervolging van strafbare feiten omvat tevens de strafrechtspraak. De richtlijn is namelijk zowel op nationale gerechten als op andere rechterlijke autoriteiten die bij de uitvoering van gerechtelijke taken in het kader van rechtszaken op strafrechtelijk gebied actief zijn, van toepassing (artikel 45, eerste lid en overwegingen 11 en 80 RI).
De richtlijn voegt aan de opsomming van doeleinden, waarvoor persoonsgegevens gebruikt kunnen worden, toe de zinsnede «met inbegrip van de bescherming tegen en voorkoming van gevaren van openbare veiligheid». Daarbij kan 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 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 RI). 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.
Binnen het toepassingsgebied van de richtlijn valt de verwerking van persoonsgegevens door ambtenaren van politie, militairen van de Koninklijke marechaussee, opsporingsambtenaren van de bijzondere opsporingsdiensten, buitengewoon opsporingsambtenaren, officieren van justitie, strafrechters of het Ministerie van Justitie en Veiligheid met het oog op de opsporing en vervolging van strafbare feiten. De verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de tenuitvoerlegging van strafrechtelijke sancties valt eveneens binnen de richtlijntaken en daarmee het toepassingsgebied van de richtlijn. Dit omvat de verwerking van gegevens ten behoeve van de tenuitvoerlegging van vrijheidsbenemende straffen en maatregelen en andere strafrechtelijke sancties door of namens Onze Minister of het College procureurs-generaal. Bij wijze van specifiek voorbeeld volgt uit voorgaande opsomming dat ook binnen het toepassingsgebied van de richtlijn valt de verwerking van persoonsgegevens in het kader van activiteiten als:

---

[7] Verklaring nr. 21: De Conferentie erkent dat op het gebied van justitiële samenwerking in strafzaken en op het gebied van politiële samenwerking specifieke voorschriften inzake de bescherming van persoonsgegevens en het vrije verkeer van die gegevens op basis van artikel 16 van het Verdrag betreffende de werking van de Europese Unie nodig zouden kunnen blijken vanwege de specifieke aard van deze gebieden.

a. de opsporing van de in de akte of aanwijzing, bedoeld in artikel 142, tweede lid, Sv aangeduide strafbare feiten door een buitengewoon opsporingsambtenaar;
b. de uitvaardiging van een bestuurlijke strafbeschikking door een opsporingsambtenaar, op basis van artikel 257a Sv, of door een buitengewoon opsporingsambtenaar in dienst van een bestuursorgaan, op basis van artikel 257ba Sv, onder toezicht van het openbaar ministerie;
c. de tenuitvoerlegging van strafrechtelijke sancties door het CJIB (zie hiervoor ook de artikelsgewijze toelichting bij artikel 1, onderdeel d, Wjsg).

Buiten het toepassingsgebied van de richtlijn valt de verwerking van persoonsgegevens met het oog op doeleinden als de inzet van bestuurlijke, bestuursrechtelijke of privaatrechtelijke bevoegdheden. De verwerking is dan niet gericht op de strafrechtspleging. Buiten het toepassingsgebied van de richtlijn valt de verwerking van persoonsgegevens in het kader van activiteiten die niet onder de richtlijntaken vallen, als:

a. de screening van personen aan de hand van geregistreerde persoonsgegevens door het Bureau bevordering integriteitsbeoordelingen openbaar bestuur (Bibob) of Justis bij de afgifte van een verklaring omtrent het gedrag;
b. het toezicht op de naleving van wetgeving door de politie, ook als de politie op grond van een bijzondere wet is belast met dit toezicht;
c. de uitvoering van de vreemdelingenwetgeving.

Ook voor verwerkingen in het kader van verlening en uitvoering van zorg geldt dat die in beginsel niet tot de richtlijntaken worden gerekend, zodat de richtlijn daarop niet van toepassing is. Een machtiging van de burgerlijke rechter tot opneming van een persoon, die gestoord is in zijn geestvermogens, in een psychiatrisch ziekenhuis of tot het doen verblijven van die persoon in dat ziekenhuis, op grond van de Wet bijzondere opnemingen in psychiatrische ziekenhuizen (WBOPZ), heeft geen betrekking op de uitvoering van de richtlijntaken door een daartoe bevoegde autoriteit. Nadat de wetsvoorstellen Wet forensische zorg (Kamerstukken 32 398), Wet verplichte geestelijke gezondheidszorg (hierna: Wvgg) (Kamerstukken 32 399) en Wet zorg en dwang psychogeriatrische en verstandelijk gehandicapte cliënten (hierna: Wzd) (Kamerstukken 31 996) tot wet zijn verheven en in werking zijn getreden en de WBPOZ is ingetrokken, zal de richtlijn daardoor niet van toepassing zijn op de verwerking van persoonsgegevens in het kader van de uitvoering van andere zorg dan forensische zorg. Indien de strafrechter bevoegd is te oordelen over de afgifte van een zorgmachtiging, op grond van de Wvgg, of over de afgifte van een rechterlijke machtiging, op grond van de Wzd, heeft de verwerking betrekking op de uitvoering van de richtlijntaken door een daartoe bevoegde autoriteit. De richtlijn is dan wel van toepassing. Als de verwerking van persoonsgegevens binnen de doeleinden van de richtlijn valt is echter niet altijd voldaan aan het vereiste van bevoegde autoriteit. Buiten het toepassingsgebied van de richtlijn valt dan ook de verwerking van persoonsgegevens door een andere autoriteit dan een bevoegde autoriteit in de zin van de richtlijn, als:

a. de Raad voor de Strafrechtstoepassing (RSJ) bij de beslissing op bezwaar- of beroepschriften van gedetineerden met betrekking tot de tenuitvoerlegging van een vrijheidsstraf of vrijheidsbenemende maatregel;
b. instellingen voor slachtofferhulp of het schadefonds geweldsmisdrijven bij de hulpverlening aan veroordeelde personen en aan slachtoffers van strafbare feiten;
c. de Stichting HALT bij de bijstand bij de tenuitvoerlegging van een leer- of werkopdracht door een jeugdige, in het kader van een beslissing van de officier van justitie tot voorwaardelijk sepot of de resocialisatie

door instanties als de reclassering, zoals bijvoorbeeld controle op naleving van voorwaarden bij vrijlating en bij taakstraffen.

Tenslotte is de richtlijn van toepassing op de verwerking van persoonsgegevens op het grondgebied van de lidstaten. De richtlijn is dus niet van toepassing op de verwerking van persoonsgegevens op Bonaire, Sint Eustatius en Saba (BES).

5.2. De gevolgen van het toepassingsbereik van de richtlijn voor de Wpg, de Wjsg en andere wetten die betrekking hebben op de verwerking van persoonsgegevens ten behoeve van opsporing en vervolging.

5.2.1. De Wet politiegegevens

De Wpg is thans van toepassing op de verwerking van persoonsgegevens ten behoeve van de uitvoering van de politietaak als bedoeld in de artikelen 3 en 4, eerste lid, van de Politiewet 2012, door ambtenaren van de politie en de militairen Koninklijke marechaussee en militairen van andere onderdelen van de krijgsmacht die op grond van de Politiewet 2012 bijstand verlenen aan de politie. Deze taak omvat de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven (artikel 3 PW 2012). De daadwerkelijke handhaving van de rechtsorde heeft zowel betrekking op de handhaving van de openbare orde als op strafrechtelijke handhaving van de rechtsorde (artikel 12 PW 2012). De verwerking van persoonsgegevens door de ambtenaren van de rijksrecherche met het oog op hun wettelijke taak (artikel 49, eerste lid, PW 2012: het doen van onderzoek in opdracht van het College van procureurs-generaal, naar feiten of gedragingen die mogelijk een strafbaar feit opleveren) heeft betrekking op de strafrechtelijke handhaving van de rechtsorde en valt onder de reikwijdte van de Wpg. De Wpg is tevens van toepassing op de verwerking van persoonsgegevens door ambtenaren van een bijzondere opsporingsdienst, voor wat betreft de verwerking van persoonsgegevens ten behoeve van de opsporing van bepaalde categorieën van strafbare feiten, die verband houden met het beleidsterrein van de Minister onder wie de opsporingsdienst ressorteert (artikel 46 Wpg). Dit is uitgewerkt in het Besluit politiegegevens bijzondere opsporingsdiensten[8].

Zoals hierboven is aangegeven is de richtlijn van toepassing op de verwerking van persoonsgegevens met het oog op de voorkoming van gevaren voor de openbare veiligheid, als onderdeel van de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen. Dit ligt ook voor de hand omdat er een nauwe samenhang is tussen de handhaving van de openbare orde en de strafrechtelijke handhaving van de rechtsorde in zoverre, dat een inbreuk op de openbare orde tevens een strafbaar feit kan opleveren, of met het plegen van strafbare feiten gepaard kan gaan, maar ook doordat het plegen van strafbare feiten en de opsporing daarvan repercussies hebben op de handhaving van de openbare orde. Mede gelet op overweging 12 van de richtlijn ligt het in de rede dat ook het deel van de politietaak dat betrekking heeft op de handhaving van de openbare orde onder de reikwijdte van de richtlijn valt. De hulpverleningstaak, die thans ook onder de reikwijdte van de Wpg valt, vormt onderdeel van de politietaak. Deze taak moet worden gezien in samenhang met de opdracht aan de politie de rechtsorde te handhaven, en de daaruit voortvloeiende aanwezigheid en bereikbaarheid van de politie en het vertrouwen dat de burgerij in de politie pleegt te stellen (Kamerstukken 991/92, 22 562, nr. 3, blz. 34). Dit houdt verband met het feit dat de hulpverlening in de praktijk niet goed is te onderscheiden van de andere onderdelen van de politietaak. Zo kan de vermissing van een persoon nauwe raakvlakken hebben met een strafbaar feit en kan juist het

[8] Stb. 2009, 305.

onderling met elkaar in verband brengen van gegevens, die de politie in het kader van de verschillende activiteiten ter kennis zijn gekomen, bijdragen een aan goede uitvoering van de politietaak (Kamerstukken II 30 327, nr. 3, blz. 39). Aldus betreft de verwerking van persoonsgegevens in het kader van de hulpverleningstaak eveneens activiteiten van de politie waarbij vooraf niet bekend is of een voorval al dan niet een strafbaar feit is, en ligt het mede in het licht van de eergenoemde overweging 12 van de richtlijn in de rede om deze taak als onderdeel van de politietaak onder de reikwijdte van de richtlijn te vatten.
Onder de politietaak als bedoeld in artikel 3 Politiewet 2012, valt tevens de verwerking van persoonsgegevens ten behoeve van de uitvoering van de taken ten dienste van de justitie, zoals genoemd in artikel 1, onderdeel i, van de Politiewet 2012, als onderdeel van de handhaving van de rechtsorde. Dit onderdeel omvat de uitvoering van wettelijke voorschriften waarmee Onze Minister is belast alsmede de uitvoering van wettelijke voorschriften gesteld bij of krachtens de Vreemdelingenwet 2000 (artikel 1, onderdeel i, onder 1°, PW 2012). Onder «de uitvoering van wettelijke voorschriften waarmee Onze Minister is belast» wordt verstaan de Wet wapens en munitie, de Wet particuliere beveiligingsorganisaties en recherchebureaus en de Wet natuurbescherming, voor zover het betreft het besluit van de korpschef als bedoeld in artikel 3.28 of 5.4, vierde lid, ingeval de jachtakte is geweigerd of ingetrokken of mede is geweigerd of ingetrokken om redenen als bedoeld in artikel 3.28, derde lid, onderdeel a, of 5.4, vierde lid, onderdeel c. Dit onderdeel omvat tevens de administratiefrechtelijke afdoening van inbreuken op wettelijke voorschriften, voor zover in die voorschriften het toezicht op de uitvoering van de politietaak is opgedragen aan het openbaar ministerie (artikel 1, onderdeel i, onder 2°, PW 2012). Dit punt heeft vooral betrekking op de Wet administratiefrechtelijke handhaving verkeersvoorschriften (Kamerstukken II 2005/06, 30 327, nr. 3, blz. 28/29). Tot de taken ten dienste van de justitie behoren tenslotte de betekening van gerechtelijke stukken in strafzaken, het vervoer van rechtens van hun vrijheid beroofde personen, en de dienst bij de gerechten (artikel 1, onderdeel i, onder 3°, PW 2012).
De richtlijn gegevensbescherming opsporing en vervolging noopt tot aanpassing van de reikwijdte van de Wpg. Dit betreft in de eerste plaats de verwerking van persoonsgegevens door opsporingsambtenaren, die niet behoren tot de politie, de Koninklijke marechaussee of een bijzondere opsporingsdienst. Dit betreft de zogenaamde buitengewone opsporingsambtenaren (boa's) die zijn belast met de opsporing van bepaalde categorieën strafbare feiten. Deze opsporingsambtenaren kunnen in dienst zijn van de overheid maar dit is niet strikt vereist. Zoals eerder opgemerkt is de richtlijn ook van toepassing op ieder ander orgaan dat krachtens het recht van de lidstaat is gemachtigd openbaar gezag of openbare bevoegdheden uit te oefenen met het oog op de opsporing van strafbare feiten. Dit betekent dat de verwerking van persoonsgegevens met het oog op de opsporing door de boa's, die in dienst zijn van bijvoorbeeld de Nederlandse Spoorwegen, Natuurmonumenten of een ander bedrijf of instelling, voortaan onder de reikwijdte van de Wpg zal vallen.
De politie is belast met de uitvoering van de politietaak als bedoeld in artikel 3 Politiewet 2012. Dit betreft de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven. De daadwerkelijke handhaving van de rechtsorde valt uiteen in de strafrechtelijke handhaving van de rechtsorde, alsmede de taken ten dienste van de justitie, en de handhaving van de openbare orde. De handhaving van de openbare orde en de hulpverleningstaak zijn nauw gelieerd aan de opsporing van strafbare feiten. Deze taken blijven onder de reikwijdte van de Wpg vallen. Zoals eerder opgemerkt, laat de richtlijn hiervoor de ruimte.

Dit betreft in de tweede plaats de taken ten dienste van de justitie. Voor wat betreft deze taken heeft de uitvoering van wettelijke voorschriften waarmee Onze Minister is belast alsmede de uitvoering van wettelijke voorschriften gesteld bij of krachtens de Vreemdelingenwet 2000, bedoeld in artikel 1, onderdeel i, onder punt 1, van de Politiewet 2012, in beginsel geen betrekking op de opsporing of vervolging van strafbare feiten. Nu de gegevensverwerking met het oog op dit doel onder het toepassingsgebied van de verordening valt, is deze taak uitgezonderd van de reikwijdte van de Wpg.

Tot de wettelijke voorschriften met de uitvoering waarvan Onze Minister is belast, worden gerekend: de Wet wapens en munitie, de Wet natuurbescherming, de Wet particuliere beveiligings- en recherchebureaus en de Wet explosieven voor civiel gebruik. Deze taken hebben evenmin betrekking op de opsporing of vervolging van strafbare feiten. Dit betekent dat de verwerking van persoonsgegevens onder deze wetten door de politie voortaan niet onder de reikwijdte van de Wpg zal vallen maar onder de reikwijdte van de verordening. Waar nodig, zullen de genoemde wetten worden aangepast teneinde de bestaande mogelijkheden voor gegevensuitwisseling ook bij toepasselijkheid van de verordening te behouden.

Voor de Wet administratiefrechtelijke handhaving verkeersvoorschriften (ook bekend als de Wet Mulder) geldt dat deze in de praktijk een 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 strafrechtelijk 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 en de verordening hierop niet van toepassing is. De richtlijn biedt hiervoor de ruimte, nu in de overwegingen wordt erkend dat de activiteiten van de politie ook de rechts- en ordehandhaving omvatten als een, zo nodig, aan de politie toevertrouwde taak ter bescherming tegen en voorkoming van gevaren voor de openbare veiligheid en voor bij de wet beschermde fundamentele belangen van de samenleving, die tot strafbare feiten kunnen leiden (overweging 12 RI). Als wordt besloten tot een administratiefrechtelijke afdoening van de overtreding dan is de verordening van toepassing op de gegevensverwerking voor dat doel. Als wordt besloten tot een strafrechtelijke afdoening dan is de richtlijn van toepassing. Alsdan valt de verwerking van gegevens in het kader van de tenuitvoerlegging onder de reikwijdte van de Wjsg (zie hierna paragraaf 5.2.2.).

De Wpg is van toepassing op de verwerking van persoonsgegevens door de bevoegde autoriteiten op Bonaire, Sint Eustatius en Saba (BES). In de wet is een afzonderlijke paragraaf opgenomen over de gegevensverwerking op de BES (paragraaf 5a). Deze paragraaf bevat specifieke bepalingen voor de BES. De richtlijn heeft echter ook gevolgen voor de gegevensverwerking op de BES.

Dit betreft vooraleerst de mogelijke «doorwerking» van de implementatie op de regels voor de BES. De richtlijn en de verordening gegevensbescherming zijn niet van toepassing op de BES. Aanpassing van de bepalingen van de wet heeft echter, op grond van artikel 36a Wpg, tot gevolg dat deze aanpassingen ook gelden voor de BES. Het ongewijzigd overnemen van de verplichtingen van de richtlijn voor de BES is echter minder wenselijk, omdat sommige verplichtingen voor de BES minder goed uitvoerbaar zijn. Bovendien worden dan andere regels in de wet opgenomen dan voor de implementatie van de richtlijn noodzakelijk zijn (Ar 331). Daarom wordt voorgesteld in paragraaf 5a van de wet een aantal bepalingen van de richtlijn uit te zonderen van toepassing op de BES.

Dit betreft voorts het onderscheid tussen lidstaten en derde landen. In dit systeem gelden Bonaire, Sint Eustatius en Saba als derde land. In de richtlijn is een afzonderlijke regime opgenomen voor de verstrekking van persoonsgegevens aan derde landen, op grond van dit regime is de verstrekking van persoonsgegevens aan de BES mogelijk.
Dit betreft tenslotte het vervallen van de Wet bescherming persoonsgegevens. Omdat in paragraaf 5a naar die wet wordt verwezen (artikel 36c, eerste lid, onderdeel a, Wpg) behoeft de betreffende bepaling aanpassing.

5.2.2. De Wet justitiële en strafvorderlijke gegevens

De Wjsg is thans van toepassing op justitiële gegevens, strafvorderlijke gegevens en rapporten in persoonsdossiers. De Minister van Justitie en Veiligheid is verantwoordelijk voor de strafrechtspleging en verantwoordelijke voor de verwerking van justitiële gegevens en de verwerking van persoonsgegevens in persoonsdossiers. Het College van procureurs-generaal is verantwoordelijke voor de verwerking van strafvorderlijke gegevens. De richtlijn strekt tot aanpassing van de reikwijdte van de Wjsg. Dit heeft betrekking op de kring van personen of instanties die als bevoegde autoriteit zijn betrokken bij de verwerking van persoonsgegevens ten behoeve van de vervolging (en berechting) van strafbare feiten of de tenuitvoerlegging van straffen. Hierbij volgt de implementatie de huidige structuur van de Wjsg door aan de bestaande indeling van justitiële gegevens, strafvorderlijke gegevens en rapporten in persoonsdossiers enkele nieuwe gegevenscategorieën toe te voegen. Voor iedere in de Wjsg te onderscheiden categorie van gegevens wordt telkens bepaald wie verwerkingsverantwoordelijke is en welke voorschriften op de verwerking van de gegevens die binnen een categorie vallen van (overeenkomstige) toepassing zijn. Door dit zowel voor de bestaande als voor de nieuwe gegevenscategorieën te doen wordt materieel invulling gegeven aan de reikwijdte en inhoud van de richtlijn op een wijze die de bestaande wettelijke systematiek van de Wjsg aanhoudt. De gegevensverwerking waarop de doeleinden van de richtlijn betrekking heeft voor vervolging (en berechting) van strafbare feiten en de tenuitvoerlegging van straffen wordt in het voorstel op die wijze door een samenstel aan te onderscheiden gegevenscategorieën in de Wjsg geïncorporeerd. De volgende gegevenscategorieën worden aan de Wjsg toegevoegd om die doeleinden van de richtlijn volledig te kunnen implementeren.
In de eerste plaats wordt het toepassingsbereik van de Wjsg verruimd tot verwerking van tenuitvoerleggingsgegevens. Dit betreft persoonsgegevens en gegevens van rechtspersonen die betrekking hebben op de tenuitvoerlegging van straffen en maatregelen. Anders dan tijdens de opsporing is tijdens de tenuitvoerlegging de aard van de beslissing bekend waarop de afdoening berust. Tenuitvoerleggingsgegevens omvatten de verwerking van gegevens van personen bij de uitvoering van vrijheidsbenemende of -beperkende straffen en maatregelen. De verwerking van persoonsgegevens ter uitvoering van de Penitentiaire beginselenwet, de Beginselenwet justitiële jeugdinrichtingen en de Beginselenwet verpleging ter beschikking gestelden vallen hieronder. Ook de gegevens van personen die worden verwerkt ter uitvoering van een strafbeschikking zijn te rekenen tot tenuitvoerleggingsgegevens. Op de verwerking van deze gegevens is voortaan de Wjsg van toepassing, in het bijzonder hetgeen wordt voorgesteld in de nieuw in te voegen titel over tenuitvoerleggingsgegevens. Voor de Wet administratiefrechtelijke handhaving verkeersvoorschriften geldt dat het afhangt van de aard van de beslissing of daarop de Wjsg van toepassing is. De Wjsg is uitsluitend van toepassing als de beslissing een strafrechtelijke afdoening inhoudt. Indien gelet op de geringere aard en ernst van de overtreding een administratiefrechtelijke beslissing is getroffen, is op de tenuitvoerlegging daarvan de verordening en de Uitvoeringswet Avg van toepassing. In

algemene zin geldt dat als de verwerking van gegevens de tenuitvoerlegging betreft van een administratiefrechtelijke beslissing de Wjsg daarop niet van toepassing zal zijn; dit zijn geen tenuitvoerleggingsgegevens in de zin van de wet. De Minister van Justitie en Veiligheid zal worden aangewezen als de verwerkingsverantwoordelijke voor de verwerking van gegevens van personen ten behoeve van de tenuitvoerlegging van straffen en maatregelen. Dit vloeit mede voort uit het wetsvoorstel herziening tenuitvoerlegging strafrechtelijke beslissingen, dat thans bij de Eerste Kamer aanhangig is (Kamerstukken 34 086). Zodra dit wetsvoorstel kracht van wet heeft verkregen zal de aanwijzing van de Minister van Justitie en Veiligheid als verwerkingsverantwoordelijke zoals die in het voorliggende wetsvoorstel is geregeld, van kracht worden. Het College van procureurs-generaal is dan uitsluitend verwerkingsverantwoordelijke voor tenuitvoerleggingsgegevens in de gevallen dat dit uit de verantwoordelijkheid voor de uitvoering van een specifieke wettelijke taak volgt. Daartoe wordt voorzien in een zogenaamde samenloopbepaling.
In de tweede plaats wordt het toepassingsbereik van de Wjsg verruimd tot verwerking van persoonsgegevens en gegevens van rechtspersonen door gerechten op strafrechtelijk gebied bij de uitvoering van gerechtelijke taken. Dit betreft de verwerking van gegevens van natuurlijke personen en van rechtspersonen (vgl. artikel 51 van het WvSr) door de gerechtelijke instanties in het kader van de behandeling van strafzaken. In het wetsvoorstel worden dit gerechtelijke strafgegevens genoemd. Ook voor deze categorie gegevens is in het wetsvoorstel voorzien in een aparte titel in de Wjsg ter implementatie van de richtlijn.
De reikwijdte van de richtlijn heeft daarmee tot gevolg dat naast justitiële gegevens, strafvorderlijke gegevens en rapporten in persoonsdossiers, ook tenuitvoerleggingsgegevens en gerechtelijke strafgegevens onder het toepassingsbereik van de Wjsg worden gebracht. De huidige Wjsg rekent tot justitiële gegevens en strafvorderlijke gegevens ook gegevens over een rechtspersoon, terwijl de richtlijn op de verwerking van persoonsgegevens betrekking heeft. Om te voorkomen dat de bestaande rechtsbescherming ten aanzien van deze gegevens wordt aangetast, blijft deze wettelijke afbakening ongewijzigd en wordt eenzelfde benadering hierin aangehouden voor tenuitvoerleggingsgegevens en gerechtelijke strafgegevens. Een ander uitgangspunt zou, evenals in de vorige paragraaf is toegelicht voor de doorwerking van de implementatie van de Wpg op de regels voor de BES, tot een onbevredigende uitkomst leiden.
Dit gaat ook op voor de bepalingen in het wetsvoorstel over het recht van een betrokkene op het verstrekken van informatie over het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en over een uit te voeren «review» na een uitgevoerde gegevensbeschermingseffectbeoordeling. Deze voorschriften dienen tot uitvoering van de eerder gedane toezegging van het kabinet, in reactie op het rapport «Big Data in een vrije en veilige samenleving» van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR). In die reactie is toegezegd dat bij de implementatie van de Richtlijn zal worden bezien of enkele verplichtingen in de verordening ook in de implementatie van de richtlijn zouden moeten worden opgenomen (Kamerstukken II 2016/17, 26 643, nr. 426, bijlage par. 6). Dit betreft de verplichtingen van de verwerkingsverantwoordelijke om te toetsen of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling wordt uitgevoerd, ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden (artikel 35, elfde lid, Avg) en om bij Big Data analyses en de daarop gebaseerde beslissing aan te kunnen tonen waarop deze beslissing is gebaseerd en welke factoren en wegingen daarin zijn meegenomen (artikel 14, tweede lid, onder g, AVG). Het gaat in deze gevallen om regels die sterk verband houden met de bindende EU-rechtshandelingen die duidelijkheid scheppen over de werkingssfeer en de rechtsbescherming.
De richtlijn bevat tot slot voorschriften die lidstaten de keuze bieden

bepaalde rechten aan betrokkenen onder omstandigheden te beperken of uit te zonderen, zoals ten aanzien van informatieverstrekking, het inzagerecht en het recht op rectificatie. Waar dit passend is, is hieraan in het wetsvoorstel nadere invulling gegeven voor zowel de Wjsg als de Wpg.

5.2.3. Andere wetten die betrekking hebben op de verwerking van persoonsgegevens voor opsporing en vervolging

Naast de Wpg en de Wjsg zijn er andere wetten die voorschriften bevatten over de verwerking van persoonsgegevens in het kader van de doelen waarop de richtlijn van toepassing is. Dit betreft de volgende gegevensverwerkingen:
Het strafrechtsketennummer wordt gebruikt voor het uitwisselen van persoonsgegevens van verdachten en veroordeelden ten behoeve van de toepassing van het strafrecht. De Minister van Justitie en Veiligheid is verwerkingsverantwoordelijke voor de strafrechtketendatabank (artikel 27b, vierde lid, Sv). Thans is de Wet bescherming persoonsgegevens (Wbp) van toepassing op de verwerking van persoonsgegevens voor dit doel. De verwerking van persoonsgegevens van verdachten en veroordeelden door de Minister van Justitie en Veiligheid ten behoeve van de toepassing van het strafrecht valt echter onder het toepassingsgebied van de richtlijn. In dit wetvoorstel wordt voorzien in aanpassing van het Wetboek van Strafvordering, zodat de verwerking van persoonsgegevens door de Minister van Justitie en Veiligheid voor dit doel in overeenstemming is met de richtlijn.
De Penitentiaire beginselenwet bepaalt dat bij of krachtens algemene maatregel van bestuur regels worden gesteld omtrent de aanleg van dossiers waarin ook persoonsgegevens zijn opgenomen (artikel 59 Pbw). De Beginselenwet verpleging ter beschikking gestelden bevat een vergelijkbare grondslag voor het verpleegdedossier (artikel 19, tweede lid, Bvt). Ook de Beginselenwet justitiële jeugdinrichtingen bevat voorschriften over verwerking van persoonsgegevens en over dossiers waarin persoonsgegevens zijn opgenomen (artikelen 33 en 63, eerste lid, Bjj). Thans is de Wet bescherming persoonsgegevens van toepassing op de verwerking van persoonsgegevens voor dit doel. De verwerking van persoonsgegevens van verdachten en veroordeelden door de Minister van Justitie en Veiligheid ten behoeve van de tenuitvoerlegging van een opgelegde straf valt echter onder het toepassingsgebied van de richtlijn. In dit wetvoorstel wordt voorzien in aanpassing van het Wetboek van Strafvordering, zodat de verwerking van persoonsgegevens door de Minister van Justitie en Veiligheid voor dit doel in overeenstemming is met de richtlijn.

5.3. Doelbinding

De richtlijn gegevensbescherming opsporing en vervolging stelt eisen aan de proportionaliteit en rechtmatigheid van de gegevensverwerking (artikel 4 RI). Essentieel is dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en legitieme doeleinden worden verzameld en niet op een met de doelen onverenigbare wijze worden verwerkt. De verwerking voor een ander doel binnen het toepassingsgebied van de richtlijn is toegelaten voor zover de verwerkingsverantwoordelijke overeenkomstig het Unierecht of het nationale recht gemachtigd is de persoonsgegevens voor dat doel te verwerken en de verwerking noodzakelijk is en in verhouding staat tot dat andere doel (artikel 4, tweede lid, RI). Voor de Wpg en de Wjsg betekent dit dat de richtlijn toelaat dat gegevens die met het oog op een opsporingsonderzoek worden verwerkt, verder worden verwerkt met het oog op de handhaving van de openbare

orde, het instellen van strafvervolging of de tenuitvoerlegging van een opgelegde straf.
De richtlijn gegevensbescherming opsporing en vervolging biedt de mogelijkheid om de persoonsgegevens, die worden verwerkt met het oog op de doelen binnen het toepassingsgebied van de richtlijn, verder te verwerken voor andere doelen voor zover die verwerking krachtens het Unierecht of het recht van de lidstaten is toegestaan. De verordening is dan van toepassing op de verdere verwerking door de ontvanger van de gegevens (artikel 9 RI). Voor de Wpg en de Wjsg betekent dit dat de richtlijn de verstrekking van gegevens aan derden toelaat met het oog op andere doelen dan de opsporing of vervolging van strafbare feiten, voor zover die verstrekking bij of krachtens de wet is voorzien. Aan dit vereiste is in de Wpg en de Wjsg reeds voldaan (artikelen 18, 19 en 20 Wpg en 9 tot en met 14 Wjsg). Voor verstrekking van gegevens inzake tenuitvoerlegging en berechting van strafbare feiten sluit het wetsvoorstel hierbij aan.
Als een bevoegde autoriteit is belast met taken die geen betrekking hebben op de doeleinden van de richtlijn gegevensbescherming opsporing en vervolging, is de verordening gegevensbescherming van toepassing op de verwerking van persoonsgegevens voor die doeleinden (overweging 12 RI). Voor de Nederlandse situatie kan daarbij worden gedacht aan de verwerking van persoonsgegevens door een ambtenaar van politie met het oog op het toezicht op de naleving van wetgeving (toezichthoudende taak op grond van bijzondere wet), of aan het gebruik van justitiële gegevens door de Minister van Justitie en Veiligheid ten behoeve van het geven van een positieve of negatieve verklaring aan buitenlandse autoriteiten over te verlenen visa.

6. De implementatie van de richtlijn en de herziening van de privacywetgeving voor opsporing en vervolging

De Wpg is van toepassing op persoonsgegevens die door opsporingsambtenaren in het kader van de uitvoering van de politietaak worden verwerkt, de Wjsg is van toepassing op persoonsgegevens die door het openbaar ministerie in een strafzaak worden verwerkt. De persoonsgegevens die worden verwerkt met het oog op opsporing, vervolging of tenuitvoerlegging en die niet onder de Wpg of de Wjsg vallen, vallen thans onder de reikwijdte van de Wet bescherming persoonsgegevens. Deze wet wordt vervangen door de verordening gegevensbescherming. Het feit dat persoonsgegevens, die binnen de strafrechtsketen worden verwerkt, onder verschillende wettelijke privacyregimes vallen is niet bevorderlijk voor de samenhang en de uitvoerbaarheid van de wettelijke regels in de praktijk. De persoonsgegevens in een proces-verbaal van een opsporingsambtenaar, dat aanleiding geeft tot strafvervolging, vallen achtereenvolgens onder de reikwijdte van de Wpg (opsporing door een opsporingsambtenaar van de politie, de Koninklijke marechaussee of een bijzondere opsporingsdienst) dan wel de Wet bescherming persoonsgegevens (opsporing door een buitengewoon opsporingsambtenaar), de Wjsg (vervolging door het openbaar ministerie), de Wet bescherming persoonsgegevens (berechting door de strafkamer van een gerecht en tenuitvoerlegging van straffen). Aldus is één en hetzelfde persoonsgegeven aan verschillende regimes voor verstrekking en bewaring onderworpen, naar gelang het zich bevindt bij een bepaalde persoon of instantie binnen de strafrechtsketen. Enerzijds sluiten de verschillende privacyregimes niet goed op elkaar aan terwijl anderzijds de bestaande juridische schotten de verwerking van de gegevens bemoeilijken. Zeker in het digitale tijdperk, waarin gegevens niet meer aan een plaats gebonden zijn, is dit niet langer te rechtvaardigen. De Wpg en de Wjsg zijn, in hun onderling verband en samenhang, aan een grondige heroverweging toe (Kamerstukken II 2013/14, 33 842, nr. 2).

In het licht van de voortgaande integratie van de activiteiten van de verschillende partijen in de strafrechtsketen, onder meer in het kader van het project verbetering prestaties strafrechtsketen (VPS), is één enkel privacyregime voor de gegevensverwerking binnen die keten wenselijk. De digitalisering van de strafrechtsketen heeft tot gevolg dat informatie in beginsel eenmalig kan worden ingevoerd en technisch op één plaats opgeslagen en onderhouden. In de visie op de digitalisering van de strafrechtspleging, die aan de Tweede Kamer is aangeboden, zijn de contouren geschetst van de ontwikkeling naar het digitaal werken in de strafrechtsketen. Vanaf een centrale plaats zal de informatie digitaal beschikbaar worden gesteld met het oog op het gebruik door de belanghebbende personen en instanties binnen de strafrechtsketen (Kamerstukken II 2015/16, 29 279, nr. 298).
Met de richtlijn gegevensbescherming opsporing en vervolging en de verordening gegevensbescherming is een Europeesrechtelijk kader voor de verwerking van persoonsgegevens tot stand gekomen. Het van toepassing zijn van één enkel Europeesrechtelijk privacyregime op de verwerking van persoonsgegevens binnen de strafrechtsketen, biedt de basis en de grondslag voor de integratie van de Wpg en de Wjsg in één enkele wet. Hierbij zullen ook de regels voor de verwerking van persoonsgegevens in het Wetboek van Strafvordering worden betrokken vanwege de nauwe relatie tussen de privacywetgeving en de regels voor de verwerking van persoonsgegevens in het kader van de strafvordering. Hiervoor kan worden verwezen naar de toelichting op artikel 2.1.5.1 van het nieuwe Boek 2 van het Wetboek van Strafvordering, dat in februari 2017 in consultatie is gegeven en dat een grondslag bevat om bij of krachtens algemene maatregel van bestuur regels te stellen over de verwerking van gegevens die door de uitoefening van de bevoegdheden van Boek 2 zijn verkregen. In die algemene maatregel van bestuur kunnen de gegevensverwerkingsregels worden samengenomen die bij of krachtens het huidige wetboek zijn gesteld[9]. Het is de bedoeling dat deze grondslag tijdelijk van aard is en komt te vervallen zodra een gegevensverwerkingswet tot stand is gebracht waarin de Wpg en de Wjsg opgaan. Zoals in de eerdergenoemde brief is aangegeven is in deze herziening tevens een herziening van de bewaartermijnen aan de orde. Daarbij zal niet zozeer de termijn voor de bewaring van gegevens voorop staan als wel de voorwaarden voor het gebruik van de gegevens. Gedurende de gehele bewaartermijn mag het gegeven in beginsel worden gebruikt voor alle in de wet omschreven doelen, waarbij vanwege de proportionaliteit wordt gedifferentieerd naar het specifieke doel en aan dat gebruik nadere voorwaarden kunnen worden verbonden, bijvoorbeeld dat het gebruik alleen is toegestaan voor bepaalde categorieën zeer ernstige delicten of door bepaalde personen (autorisaties). Na afloop van de verwerkingstermijn zullen de persoonsgegevens moeten worden vernietigd.
De termijn voor de implementatie van de richtlijn gegevensbescherming opsporing en vervolging staat er aan in de weg om deze herziening te betrekken in de implementatie van de richtlijn. Zodra de implementatiewetgeving kracht van wet heeft verkregen zal de herziening en integratie van de Wpg en de Wjsg in voorbereiding kunnen worden genomen.

[9] Het betreft thans de artikelen 27a, 27b en 55c (gegevensverwerking identiteitsgegevens), 61a (verwerking handpalmafdrukken) 125m (vernietigen gegevens tijdens doorzoeking ter vastlegging gegevens en gebruik ander onderzoek), 126nb (vernietiging gegevens inzet scanapparatuur), 126cc en 126dd (verwerken van gegevens die door de uitoefening van enkele bijzondere opsporingsbevoegdheden zijn verkregen) en 151a (verwerking DNA-gegevens), en de onderliggende uitvoeringsbesluiten.

7. De consequenties van de richtlijn gegevensbescherming opsporing en vervolging voor de wetgeving op het gebied van de bescherming van persoonsgegevens

Zoals in paragraaf 2.1. reeds is opgemerkt heeft het voormalige kaderbesluit dataprotectie reeds aanleiding gegeven tot aanpassing van de Wpg, de Wjsg en de op basis van deze wetten vastgestelde algemene maatregelen van bestuur. De richtlijn geeft aanleiding tot verdere aanpassing van de wetgeving op onderdelen. Over het geheel bezien zullen deze aanpassingen resulteren in een beter beschermingsniveau voor de betrokkenen dan onder de huidige wetgeving, onder meer ten aanzien van de beveiliging van hun gegevens, de uitoefening van hun rechten en de mogelijkheden voor rechtsbescherming. De belangrijkste wijzigingen betreffen het volgende:

7.1. Verplichtingen voor de verwerkingsverantwoordelijke en de verwerker

De verwerkingsverantwoordelijke en de verwerker zijn gehouden een register bij te houden van verwerkingsactiviteiten (artikel 24 RI). Dit betreft een meer algemene beschrijving rond de gegevensverwerking, zoals de naam en contactgegevens van de verwerkingsverantwoordelijke, de verwerkingsdoeleinden en de categorieën van ontvangers aan wie persoonsgegevens zijn of zullen worden bekend gemaakt. In de Wpg en het daarop gebaseerde Besluit politiegegevens (Bpg) zijn thans reeds verplichtingen opgenomen tot de registratie van dergelijke gegevens. De betreffende bepalingen zullen waar nodig worden aangevuld. Daarbij zullen bepaalde verplichtingen kunnen worden samengevoegd omdat deze weliswaar reeds in de huidige Wpg zijn opgenomen, maar niet volledig stroken met de richtlijn.
Voorts voorziet de richtlijn in een verplichting tot de geautomatiseerde vastlegging van gegevens over de gegevensverwerking (logging). Dit ten behoeve van de controle van de rechtmatigheid van de gegevensverwerking, de waarborging van de integriteit van de beveiliging van de gegevens en voor strafrechtelijke procedures. Thans kennen de Wpg en de Wjsg geen verplichting tot de logging van gegevens. Op dit punt zullen deze wetten worden aangevuld. Daarbij moet worden opgemerkt dat het thans niet volledig duidelijk is in hoeverre de informatiesystemen die door de bevoegde autoriteiten (opsporingsdiensten, openbaar ministerie, Minister van Justitie en Veiligheid) worden gebruikt voldoende zijn voorbereid om aan de loggingplicht te voldoen. De richtlijn voorziet in de mogelijkheid voor de lidstaten om, als dit buitengewone inspanningen met zich zou brengen, de geautomatiseerde systemen uiterlijk in 2023 in overeenstemming te brengen met de verplichting tot logging (artikel 63, tweede lid, RI). In uitzonderlijke omstandigheden is verder uitstel mogelijk, tot uiterlijk 6 mei 2026. Het wetsvoorstel voorziet in de mogelijkheid van gedifferentieerde inwerkingtreding.
De verwerkingsverantwoordelijke is gehouden verschillende maatregelen te treffen ter beveiliging van de verwerkte persoonsgegevens. Dit betreft technische en organisatorische maatregelen om te waarborgen dat de verwerking in overeenstemming met de richtlijn wordt verricht en de rechten van de betrokkenen worden beschermd (artikelen 19 en 20 RI). Ten aanzien van de geautomatiseerde verwerking wordt in meer concrete verplichtingen voorzien, die erop zijn gericht te verhinderen dat onbevoegden toegang verkrijgen tot de persoonsgegevens of deze gegevens onbevoegd kunnen wijzigen (artikel 29 RI). Voor de invulling van deze verplichtingen dient rekening te worden gehouden met de aard, reikwijdte, context en de doeleinden van de verwerking, alsmede met de risico's en vrijheden van de betrokkene. Op dit punt laat de richtlijn de verwerkingsverantwoordelijke dus een zekere marge voor afweging.

Thans bevatten de Wpg en de Wjsg meer algemene regels over de beveiliging van de verwerkte persoonsgegevens. De verdergaande verplichtingen, die uit de richtlijn voortvloeien, zullen deels worden opgenomen in de Wpg en de Wjsg en, vanwege het meer technische karakter van de voorschriften, deels in het Bpg en het Besluit justitiële en strafvorderlijke gegevens (Bjsg).
De verwerkingsverantwoordelijke is gehouden een inbreuk in verband met persoonsgegevens, ook bekend als een datalek, te melden aan de toezichthoudende autoriteit (artikel 31 RI). Van melding kan worden afgezien als het niet waarschijnlijk is dat de inbreuk een risico voor de betrokken personen met zich meebrengt. De verwerkingsverantwoordelijke dient tevens te melden welke maatregelen worden of zijn getroffen om de inbreuk ongedaan te maken. Wanneer het datalek waarschijnlijk een hoog risico met zich meebrengt voor de rechten en vrijheden van natuurlijke personen, wordt de inbreuk zonder onnodige vertraging aan de betrokkene meegedeeld. Onder bepaalde voorwaarden kan van de melding worden afgezien, onder meer als passende technische en organisatorische maatregelen zijn getroffen welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling, of als mededeling aan de betrokken een onevenredige inspanning zou vergen. In het laatste geval kan worden volstaan met een openbare mededeling of een vergelijkbare maatregel. De Wpg en de Wjsg kennen thans geen verplichting tot het melden van datalekken. Op dit punt moeten deze wetten worden aangevuld.
De verwerkingsverantwoordelijke is voorts gehouden tot een beoordeling van het effect van risicovolle verwerkingsactiviteiten op de bescherming van persoonsgegevens (gegevensbeschermingseffectbeoordeling). Dit betreft in het bijzonder verwerkingen waarbij nieuwe technologieën worden gebruikt (artikel 27 RI). Thans moeten instanties die tot de rijksdienst behoren reeds met een toetsmodel werken bij ontwikkeling van nieuwe wetgeving en beleid waarmee de bouw van nieuwe ICT-systemen of de aanleg van grote databestanden wordt voorzien; het «Privacy Impact Assessment». De richtlijn voorziet tevens in de verplichting om in bepaalde gevallen de toezichthoudende autoriteit te raadplegen voordat persoonsgegevens in een nieuw bestand worden opgenomen (artikel 28 RI). Dit is onder meer aan de orde als uit een gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico zou opleveren als geen maatregelen worden getroffen ter beperking daarvan. Thans kennen de Wpg en de Wjsg reeds een dergelijke verplichting. Als de toezichthoudende autoriteit van oordeel is dat de voorgenomen verwerking indruist tegen de richtlijn, dan wordt de verwerkingsverantwoordelijke hierover van advies gediend.
Ten slotte kan worden gewezen op de verplichting voor de verwerkingsverantwoordelijke om een functionaris voor gegevensbescherming aan te wijzen (artikel 32 RI). Deze wordt belast met het adviseren van de verwerkingsverantwoordelijke over de naleving van de wettelijke verplichtingen op basis van de richtlijn, het toezicht op de naleving van die verplichtingen en het optreden als contactpunt voor de toezichthoudende autoriteit. De Wpg en de Wjsg voorzien thans niet in de verplichting tot aanwijzing van een functionaris voor gegevensbescherming, thans voorziet de Wpg in de mogelijkheid daartoe en in een verplichting tot het aanwijzen van een privacyfunctionaris. Op dit punt behoeven de Wpg en de Wjsg aanvulling. De functionaris voor gegevensbescherming richt zich met name op het uitoefenen van toezicht op de gegevensverwerking binnen een organisatie en bekleedt in dit kader een onafhankelijke positie. De privacyfunctionaris richt zich met name op interne advisering op dit gebied.

7.2. Rechten van de betrokkene

De richtlijn gegevensbescherming opsporing en vervolging geeft een uitgebreide regeling voor het recht van de betrokkene op informatie over de verwerking van de hem of haar betreffende persoonsgegevens. De verstrekking van informatie over de verwerking van politiegegevens geschiedt in een beknopte en toegankelijke vorm en is kosteloos. Ingeval van vexatoire verzoeken, die kennelijk ongegrond of buitensporig zijn, kan de verwerkingsverantwoordelijke een redelijke vergoeding aanrekenen of weigeren gevolg te geven aan het verzoek. Hierbij is niet alleen voorzien in een meer passieve informatieplicht, naar aanleiding van een verzoek van de betrokkene, maar ook een meer actieve informatieplicht. Dit laatste betreft de verplichting om de betrokkene bepaalde gegevens ter beschikking te stellen, zoals de identiteit van de verwerkingsverantwoordelijke en de doeleinden van de verwerking en het recht op inzage van de gegevens (artikel 13 RI). Dit kan worden gedaan op een website (overweging 42 RI). In specifieke gevallen dient de betrokkene te worden ingelicht over aspecten als de rechtsgrond voor de verwerking, de bewaartermijnen en de categorieën van de ontvangers van de gegevens. De Wpg en de Wjsg voorzien weliswaar in het recht van inzage voor de betrokkene, maar dit is niet kosteloos en betreft de passieve variant. Deze wetten voorzien evenmin in de mogelijkheid van weigering bij een vexatoir verzoek. Voor de transparante en kosteloze verstrekking van informatie, de mogelijkheid van weigering bij vexatoire verzoeken en het actief ter beschikking stellen van bepaalde persoonsgegevens is aanpassing van deze wetten aangewezen.
Aanvullend heeft de betrokkene het recht op inzage van de verwerkte persoonsgegevens (artikel 14 RI). Dit recht kan worden ingeperkt, onder meer ter voorkoming van nadelige gevolgen voor de opsporing en vervolging van strafbare feiten en de bescherming van de rechten en vrijheden van derden (artikel 15 RI). De lidstaten kunnen bepaalde verwerkingscategorieën geheel of gedeeltelijk onder deze beperking brengen. Voorts heeft de betrokkene het recht op rectificatie of wissing van onjuiste persoonsgegevens (artikel 16 RI). De eerdergenoemde gronden ter beperking kunnen hier worden ingeroepen. De betrokkene kan zijn rechten ook uitoefenen via de toezichthoudende autoriteit. De Wpg en de Wjsg voorzien reeds in een regeling voor het recht van inzage voor de betrokkene. De formulering van de weigeringsgronden en de mogelijkheid van uitsluiting van bepaalde categorieën van persoonsgegevens van het recht op inzage en rectificatie nopen echter tot aanpassing van deze wetten. Ditzelfde geldt voor de mogelijkheid deze rechten via de toezichthoudende autoriteit uit te oefenen.

7.3. Het toezicht op de naleving van de richtlijn gegevensbescherming opsporing en vervolging

De richtlijn gegevensbescherming opsporing en vervolging bepaalt dat iedere lidstaat erin voorziet dat één of meer onafhankelijke overheidsinstanties worden belast met het toezicht op de toepassing van de richtlijn. Dit kan dezelfde autoriteit betreffen als die welke is belast met het toezicht op de naleving van de verordening gegevensbescherming (artikel 41 RI). De toezichthoudende autoriteit treedt volledig onafhankelijk op bij de uitvoering van haar taken en de uitoefening van haar bevoegdheden (artikel 42 RI). Iedere toezichthoudende autoriteit heeft de competentie om op het grondgebied van haar lidstaat de taken en de bevoegdheden van de richtlijn uit te oefenen. Van het toezicht is uitgezonderd de gegevensverwerking door gerechten in het kader van hun rechterlijke taken (artikel 45 RI).
Het toezicht op de naleving van de Wpg en de Wjsg is thans opgedragen aan de AP. Voor de regeling van de taken en bevoegdheden van de AP

wordt in de Wpg en de Wjsg verwezen naar de regeling in de Wbp. Nu de Wet bescherming persoonsgegevens vervalt is een eigenstandige regeling in de Wpg en de Wjsg aangewezen. Dit klemt temeer daar de regeling van de taken en bevoegdheden van de AP op basis van de verordening gegevensbescherming op onderdelen afwijkt van die op basis van de richtlijn. Voorgesteld wordt in de Wpg te voorzien in een zelfstandige regeling van de positie, taken en bevoegdheden van de AP, ter implementatie van de richtlijn. Voor enkele onderdelen van de richtlijn die overeenkomen met de regels die op basis van de verordening zijn uitgewerkt in de Uitvoeringswet Avg, wordt volstaan met verwijzing naar die wet. Een voorbeeld hiervan is de verplichting de AP advies te vragen over voorstellen van wet en ontwerpen van algemene maatregelen van bestuur die betrekking hebben op de verwerking van persoonsgegevens. In de Wjsg wordt vervolgens verwezen naar de regeling van de Wpg, zodat de regels inzake het toezicht op de naleving van de beide wetten door de AP identiek zijn.
Voor wat betreft de bevoegdheden van de toezichthoudende autoriteit laat de richtlijn, anders dan de verordening, een grote mate van vrijheid aan de lidstaten om de bevoegdheden vorm te geven. De lidstaten zijn gehouden bij wet te voorzien in effectieve onderzoeksbevoegdheden. Dit omvat ten minste de bevoegdheid om toegang te verkrijgen tot alle persoonsgegevens die worden verwerkt en tot alle informatie die noodzakelijk is voor de uitoefening van haar taken (artikel 47, eerste lid, RI). Tevens dient bij wet te worden voorzien in effectieve bevoegdheden tot het treffen van corrigerende maatregelen, zoals het waarschuwen van de verwerkingsverantwoordelijke of de verwerker, het gelasten de verwerkingen in overeenstemming te brengen met de richtlijn en een tijdelijke of definitieve begrenzing van het verwerken, waaronder een verwerkingsverbod (artikel 47, tweede lid, RI). Uitgangspunt is aan de verplichtingen van de richtlijn op dit punt uitvoering te geven door de bestaande bevoegdheden van de Autoriteit persoonsgegevens op basis van de Wpg en de Wjsg te continueren. Voor deze bevoegdheden wordt thans verwezen naar de artikelen 51, tweede lid, 60, 61 en 65 van de Wet bescherming persoonsgegevens. Voorgesteld wordt deze bepalingen materieel over te nemen in de Wpg, en aan te vullen met de relevante bepalingen van de richtlijn. Tevens wordt voorgesteld de bevoegdheden van de Autoriteit persoonsgegevens tot het opleggen van bestuurlijke boetes te verruimen en de maximale boetebedragen te verhogen, zodat de regeling meer in balans is met die van de verordening. Aanvullend beschikt de AP als toezichthouder in de zin van de Algemene wet bestuursrecht over de bevoegdheden met betrekking tot het toezicht op de naleving, bedoeld in Titel 5.2. van die wet.

8. Het advies van de Autoriteit persoonsgegevens

Het conceptwetsvoorstel is voor advies voorgelegd aan de AP. Bij brief van 7 april 2017 heeft de AP zijn advies aan mij doen toekomen[10]. De AP verzoekt de voorgenomen wijziging van het Bpg en het Bjsg te zijner tijd voor advies voorgelegd te krijgen. Aan dit verzoek zal gevolg worden gegeven.

I. Rechtsgrondslag en reikwijdte van de richtlijn

Onder verwijzing naar de audits en evaluaties rond de Wpg en de Wjsg wijst de AP erop dat naleving van de thans geldende normen op problemen stuit; de AP acht de gemaakte keuze voor een minimumimplementatie niet bevorderlijk voor de tussentijdse naleving van de geldende normen. Met de AP gaat mijn voorkeur uit naar herziening van de Wpg en

[10] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

de Wjsg, tegelijk met de implementatie van de richtlijn gegevensbescherming opsporing en vervolging zodat de uitvoeringspraktijk slechts eenmaal wordt geconfronteerd met wijzigingen in het wettelijk kader van gegevensbescherming. De implementatietermijn van twee jaar biedt echter geen ruimte voor de integratie van de nationale wetten omdat hierbij verstrekkende afwegingen aan de orde zijn, bijvoorbeeld rond de bewaartermijnen. Gelet op de noodzaak van tijdige implementatie moet worden vermeden dat de implementatie van bindende EU-rechtshandelingen wordt «meegenomen» in een bredere herziening van de desbetreffende regelgeving of dat in de implementatieregeling «extra» nationaal beleid wordt meegenomen (Ar 331).
Voorts is de AP van oordeel dat de implementatie van de richtlijn is gebaseerd op een onjuiste opvatting over de grondslag en reikwijdte van de richtlijn en hierdoor niet voldoet aan de vereiste nauwgezette omzetting van de richtlijn in nationaal recht. De AP heeft reeds om die reden bezwaar tegen het in deze vorm indienen van het voorliggende wetsvoorstel. Dit betreft de volgende aspecten:

– Betekenis van het autonoom Unierechtelijk begrip «strafbaar feit» voor de reikwijdte van de Richtlijn.
De AP wijst op overweging 13 bij de Richtlijn waarin staat vermeld dat het begrip strafbaar feit in de zin van de richtlijn een autonoom Unierechtelijk begrip moet zijn zoals uitgelegd door het Hof van Justitie. Op grond van de jurisprudentie van het Europese Hof van Justitie is volgens de AP een functionele interpretatie van het begrip «strafbaar feit» aangewezen, op grond waarvan aangesloten moet worden bij de jurisprudentie van het EHRM over dit begrip. Dit betreft in het bijzonder de criteria als geformuleerd in de zaak Engel e.a. tegen Nederland (EHRM 8 juni 1976, nr. 5370/72, Engel tegen Nederland, NJ 1978/223). 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 Nederlandse recht. Dit heeft volgens de AP tot gevolg dat de richtlijn ook van toepassing is op feiten waarop met bestraffende bestuurlijks sancties (waaronder in ieder geval een bestuurlijke boete) of zwaarder kan worden gereageerd. Doordat in het wetsvoorstel is miskend dat de reikwijdte van de Richtlijn breder is, acht de AP een heroverweging van de gemaakte keuzes op zijn plaats.
De richtlijn heeft betrekking op de politiële en justitiële samenwerking in strafzaken. In het licht van verklaring 21 bij het Verdrag van Lissabon zijn op die gebieden specifieke voorschriften vereist inzake de bescherming van persoonsgegevens en het vrije verkeer van die gegevens (overweging 10). Vanwege de specifieke aard van de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten is het aangewezen dat die gebieden worden behandeld in een richtlijn waarin specifieke regels worden vastgesteld voor de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens voor die doelen (overweging 11). Tijdens de onderhandelingen is nimmer sprake geweest van een toepassingsbereik buiten de traditionele strafrechtsketen. Op basis van de tekst van de richtlijn en de ontstaansgeschiedenis gaat de regering er van uit dat de Richtlijn van toepassing is op de verwerking van persoonsgegevens door de politie en de Koninklijke marechaussee bij de uitoefening van de politietaak, de bijzondere opsporingsdiensten bij de opsporing van strafbare feiten en het openbaar ministerie bij de vervolging van strafbare feiten en de tenuitvoerlegging van straffen, zoals ook in de memorie van toelichting is toegelicht. Dit is in lijn met de implementatie van het eerdere Kaderbesluit 2008/977/JBZ, dat inmiddels is vervangen door de richtlijn, en ligt ook voor de hand vanuit het oogpunt van de rechtsbescherming.

Een belangrijk aandachtspunt bij implementatie is immers dat de reikwijdte van de richtlijn niet te ruim wordt uitgelegd, omdat hiermee het sterke beschermingsregime van de Algemene verordening gegevensbescherming zou kunnen worden ondergraven. Dit wordt bevestigd door de expertbijeenkomst van 7 november 2016, waarin de juridische dienst van de Commissie heeft gewezen op het belang van onderscheid tussen bestuurlijke feiten (onder de verordening) en strafbare feiten (onder de richtlijn), en de expertbijeenkomst van 7 maart 2017 in Brussel waaruit is gebleken dat een meerderheid van de lidstaten voornemens is de Richtlijn toe te passen op de traditionele «derde pijler» rechtshandhavingsautoriteiten (politiële en justitiële autoriteiten), zij het met enkele uitzonderingen, zoals de Douane voor zover deze optreedt met het oog op de doeleinden van de richtlijn.
De door de AP voorgestelde verruiming van de toepassing van de richtlijn op bestraffende bestuurlijke sancties zou voor burgers leiden tot een lager beschermingsniveau, omdat de richtlijn, vanwege het belang van opsporing en vervolging andere accenten legt dan de verordening, bijvoorbeeld op het gebied van de transparantie jegens de betrokkene (minder informatieplichten van de verantwoordelijke) en de bevoegdheden van de toezichthoudende autoriteit.
Op grond van de tekst, ontstaansgeschiedenis en het voorkomen van ondergraving van het maximale beschermingsregime van de algemene verordening gegevensbescherming acht de regering de gekozen interpretatie van de reikwijdte een getrouwe implementatie van de richtlijn.

– Implementatie begrip «verwerkingsverantwoordelijke».
De AP wijst erop dat het begrip «verwerkingsverantwoordelijke» volgens het advies van de «Artikel 29 werkgroep» een autonoom begrip betreft maar ook functioneel is, in die zin dat het bedoeld is om de verantwoordelijkheden te leggen waar de feitelijke invloed ligt. In de Richtlijn is de definitie van het begrip «verwerkingsverantwoordelijke» gekoppeld aan de definitie van het begrip «bevoegde autoriteit». Een bevoegde autoriteit is – kort gezegd – iedere overheidsinstantie die bevoegd is voor de doeleinden van de richtlijn of 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 die doeleinden (artikel 3, zevende lid, Rl). De AP stelt vast dat in de Wpg en de Wjsg enkele verwerkingsverantwoordelijken worden aangewezen die niet tevens ook bevoegde autoriteit zijn, zoals de Minister van Justitie en Veiligheid voor de verwerking van justitiële gegevens. Daarmee heeft het begrip verwerkingsverantwoordelijke volgens de AP op nationaal niveau een andere invulling gekregen dan in de richtlijn. Vanuit meer praktisch perspectief roept dit de vraag op naar de bevoegdheid van de verwerkingsverantwoordelijke om zelf de betreffende persoonsgegevens te kunnen verwerken. Hierbij wordt verwezen naar de gegevensverwerking door de boa's, waarbij de werkgever als verwerkingsverantwoordelijke zal worden aangewezen. De AP is van oordeel dat de implementatie van de begrippen bevoegde autoriteit en verwerkingsverantwoordelijke in het wetsvoorstel niet in overeenstemming zijn met hetgeen de richtlijn hierover bepaalt en adviseert de richtlijn alsnog als zodanig te implementeren.
Verder wijst de AP er op dat op verschillende plaatsen in de Wpg en Wjsg en in het wetsvoorstel dan wel de Politiewet het onderscheid tussen de begrippen beheer en gezag voorkomt. Volgens de AP heeft gezag betrekking op het bepalen van het doel van de verwerking en ziet beheer op het vaststellen van middelen. In het nationale recht zijn degenen die het beheer voeren, aangemerkt als verwerkingsverantwoordelijken. De Richtlijn kent dit onderscheid in doel en middelen niet. Daarom dient volgens de AP de verwerkingsverantwoordelijke niet alleen het beheer,

maar ook het gezag te hebben. Bovendien ontbreekt in het nationale recht de koppeling met «bevoegde autoriteit». Dit roept voor de AP de vraag op of het begrip verwerkingsverantwoordelijke op de juiste manier is geïmplementeerd. Op grond van het voorgaande meent de AP dat ook de burgemeester onder de definitie van bevoegde autoriteit van de richtlijn valt: indien de feitelijke gezagsverhouding over de politie tot uitgangspunt wordt genomen, is de burgemeester tevens verwerkingsverantwoordelijke.
Naar aanleiding van dit advies moet worden opgemerkt dat het begrip «verwerkingsverantwoordelijke» niet bij voorbaat is beperkt tot de bevoegde autoriteit. De richtlijn biedt de mogelijkheid om in de nationale wetgeving te bepalen wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen (artikel 3, achtste lid, Rl). Van deze mogelijkheid wordt gebruik gemaakt om in de Wpg de Minister van Defensie aan te wijzen als de verwerkingsverantwoordelijke voor de verwerking van politiegegevens door de Koninklijke marechaussee en in de Wjsg de Minister van Justitie en Veiligheid voor de verwerking van justitiële gegevens. De Minister van Defensie en de Minister van Justitie en Veiligheid hebben zowel beheersmatig als hiërarchisch zeggenschap over de bedrijfsvoering door respectievelijk de Koninklijke marechaussee en de Justitiële Informatiedienst, zodat het aanwijzen van deze Ministers als verwerkingsverantwoordelijke voor de hand ligt.
Voor de boa's geldt dat de bevoegdheid tot het opsporen van strafbare feiten is gebaseerd op een akte van opsporingsbevoegdheid, verleend door Onze Minister van Justitie en Veiligheid of het College van procureurs-generaal (artikel 141, eerste lid, Sv). De opsporing van strafbare feiten door een boa vindt plaats onder gezag van de officier van justitie. De officier van justitie is echter niet betrokken bij de bedrijfsvoering van de organisatie waar de boa in dienst is en heeft evenmin een hiërarchische relatie met de boa. Ditzelfde geldt voor de korpschef van de Nationale politie. Vanwege de beheersmatige en hiërarchische zeggenschap zal de verwerkingsverantwoordelijkheid voor de gegevensverwerking door een boa worden belegd bij diens werkgever. Voor wat betreft de bevoegdheid van de verantwoordelijke om zelf de politiegegevens te verwerken geldt dat de Wpg reeds voorziet in toegang van de verantwoordelijke tot de politiegegevens die onder zijn beheer worden verwerkt ten behoeve van het toezicht op de naleving van het bij of krachtens deze wet bepaalde (artikel 4, vierde lid, Wpg).
Voor wat betreft het onderscheid tussen beheer en gezag kan voorts worden opgemerkt dat de organisatorische inbedding van de gegevensverwerkingsverantwoordelijke bij het beheer van de politie – of van een bijzondere opsporingsdienst – voor de hand ligt omdat de rol van de verwerkingsverantwoordelijke betrekking heeft op de beschikbaarstelling van de middelen voor een adequate gegevensverwerking. Dit raakt aan de bedrijfsvoering van de betreffende opsporingsdienst. Daarbij ligt de nadruk meer op de middelen dan op het doel van de verwerking.
Vanwege de wettelijke taken van de politie of van de bijzondere opsporingsdienst is het doel van de verwerking bij voorbaat gegeven, te weten de opsporing van strafbare feiten. Indien de gezagslijn op basis van de Politiewet 2012 (mede)bepalend zou zijn voor de toedeling van de verantwoordelijkheid voor de gegevensverwerking, dan zou iedere officier van justitie en iedere burgemeester slechts verantwoordelijk zijn voor een beperkt onderdeel van de gegevensverwerking, namelijk de verwerking die onder zijn gezag plaatsvindt. De individuele officier van justitie of burgemeester is dan slechts voor een zeer klein deel van de gegevensverwerking verantwoordelijk. In de praktijk zal dit betekenen dat niemand aanspreekbaar is voor de meer algemene verplichtingen voor de verwerkingsverantwoordelijke, bijvoorbeeld op het gebied van de beveiliging van de verwerking. Vooralsnog is niet goed in te zien op welke wijze meer dan 1.100 verwerkingsverantwoordelijken (ruim 300 burge-

meesters 800 officieren van justitie) op een gecoördineerde wijze zouden kunnen worden betrokken bij de gegevensverwerking door de politie, voor zover de gegevensverwerking betrekking heeft op de uitvoering van de politietaak waarover zij het gezag uitoefenen. Ook voor de burger zou het niet duidelijk zijn tot wie hij zich moet wenden voor de uitoefening van zijn fundamentele rechten. De burger zou dan immers zelf moeten uitzoeken welke officier verwerkingsverantwoordelijke is voor de verwerking van zijn persoonsgegevens. Een dergelijke wijziging van het systeem van de Wpg en de Wjsg vloeit niet voort uit de richtlijn, raakt aan de verdeling van de beheersmatige en gezagsmatige verantwoordelijkheden op basis van de Politiewet 2012, is vanuit het perspectief van de uitvoerbaarheid niet wenselijk en zou de mogelijkheden voor burgers om hun rechten uit te oefenen feitelijk bemoeilijken.
Dit laat overigens onverlet dat het voor zowel de officier van justitie als de burgemeester van essentieel belang is te kunnen beschikken over politiegegevens om invulling te kunnen geven aan hun gezagsrol op grond van de Politiewet 2012. In de Wpg is voorzien in een verplichting voor de verantwoordelijke om politiegegevens te verstrekken aan leden van het openbaar ministerie en de burgemeesters voor zover zij deze behoeven in verband met hun gezag en zeggenschap over de politie (artikel 16, eerste lid, onderdelen b en c, onder 1°, Wpg). Ik verwijs daarvoor tot slot naar overweging 54 van de richtlijn, waarin wordt overwogen dat het voor de bescherming van de rechten en vrijheden van betrokkenen en de verantwoordelijkheid en aansprakelijkheid van verwerkingsverantwoordelijken en verwerkers, onder meer wat de monitoring door en de maatregelen van toezichthoudende autoriteiten betreft, noodzakelijk is dat de bij de richtlijn vastgestelde verantwoordelijkheden op duidelijke wijze worden toegekend.

II. Uitvoeringstoets op onderwerp

1. Afbakening Verordening/Uitvoeringswet en het voorliggende wetsvoorstel: uitvoerbaarheid voor de praktijk

a. Onder verwijzing naar de tekst van overweging 12 vraagt de AP zich af of de doeleinden die zien op de strafrechtelijke handhaving berusten bij het openbaar ministerie, en de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid bij de burgemeester. Zoals eerder reeds is opgemerkt heeft de richtlijn geen betrekking op het gezag en beheer over de politie, op dat punt is de Politiewet 2012 leidend. Omdat gedragingen van burgers in de openbare ruimte betrekking kunnen hebben op zowel de strafrechtelijke handhaving van de rechtsorde (bijvoorbeeld het plegen van openlijk geweld of het vernielen van goederen) als de handhaving van de openbare orde (bijvoorbeeld demonstraties of rellen) is de taakafbakening tussen officier van justitie enerzijds en burgemeester anderzijds niet altijd scherp te maken. Dit houdt echter geen verband met de richtlijn als wel met het systeem van de Politiewet 2012.
b. De AP acht de keuze in dit wetsvoorstel verdedigbaar dat de hulpverleningstaak van de politie, als onlosmakelijk onderdeel van de handhaving van de openbare orde en ook van de strafrechtelijke handhaving van de rechtsorde, 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.
   Dit punt behoeft geen reactie, behoudens dat het oordeel van de AP wordt onderschreven.
c. De AP merkt op dat het uitzonderen van de vreemdelingentaken van de politietaak gevolgen heeft voor de taakuitvoering door de Koninк-

lijke marechaussee en werpt de vraag op of de grensbewakingstaak (die nog wel onder de politietaak valt) en de vreemdelingentaken (die niet meer onder de politietaak vallen) vanwege hun onderlinge vervlechting in de praktijk onder de verschillende privacyregimes (Avg en richtlijn) op toereikende wijze gescheiden kunnen worden.
In de Wpg worden de vreemdelingentaak en daarmee samenhangende grensbewakingstaak uitgezonderd. De daarbij behorende verwerking van persoonsgegevens valt daarom onder het regime van de verordening. Zodra de uitvoering van deze taken aanleiding geeft tot opsporing en vervolging van strafbare feiten of het voorkomen van bedreiging van de openbare veiligheid, valt de daarmee gemoeide verwerking van de persoonsgegevens wel onder het regime van de richtlijn.
Een hiermee samenhangend punt vormt het toepasselijke regime voor de vreemdelingensignaleringen in het Schengen Informatiesysteem van de tweede generatie (SIS II). De AP vreest een bijzonder ondoorzichtige, en mogelijk onwerkbare, situatie nu de vreemdelingensignaleringen onder het Verordeningsregime zullen vallen en de overige signaleringen onder de richtlijn, en daarmee onder de werking van de Wpg.
Met het toepassingsbereik van de richtlijn wordt echter aangesloten bij de systematiek van de EU-regelgeving op het gebied van asiel en migratie enerzijds en opsporing en vervolging van strafbare feiten anderzijds. De verwerking van persoonsgegevens in het SIS met het oog op weigering van toegang tot of verblijf op het grondgebied van de lidstaten is thans geregeld in een verordening. De verwerking van persoonsgegevens met het oog op de politiële en justitiële samenwerking in strafzaken is thans geregeld in een Besluit. De verordening en het besluit bevatten afzonderlijke regels voor gegevensbescherming (respectievelijk Hoofdstukken VI en XII). In het voorstel van de Commissie voor een nieuwe verordening voor het SIS worden de verschillende gegevensbeschermingsregimes voor de verschillende doeleinden van het SIS gehandhaafd (artikel 64, tweede en derde lid, Vo). Ook hierbij geldt dat als het doel van de gegevensverwerking is gericht op asiel- en migratie, de verordening van toepassing is op de gegevensverwerking voor dat doel; als de gegevens worden geraadpleegd voor opsporing en vervolging dan valt de verdere verwerking onder het regime van de richtlijn en daarmee van de Wpg of Wjsg.

d. De AP verzoekt om opheldering over het toepasselijke regime voor de Wet administratieve handhaving verkeersvoorschriften (Whav).
In reactie hierop moet worden vooropgesteld dat, zoals in de memorie van toelichting is vermeld, de gegevensverwerking door ambtenaren van politie met betrekking tot de Whav onder de reikwijdte van de Wpg zal blijven vallen. Dit is abusievelijk niet betrokken in de voorgestelde aanpassing van artikel 1, onderdeel a, van de Wpg. Deze omissie zal worden hersteld.
De AP concludeert dat het de vraag is of de gekozen afbakening in de uitvoeringspraktijk werkbaar en/of uitvoerbaar is. Naar aanleiding daarvan meen ik dat de afbakening tussen twee regimes voortvloeit uit de keuze voor twee verschillende regimes voor de verwerking van persoonsgegevens. Dit probleem is echter niet nieuw, dit is ook thans aan orde bij het onderscheid tussen de Wbp enerzijds en de Wpg en Wjsg anderzijds. Ik meen echter dat met de voorgestelde afbakening zo veel mogelijk tegemoet wordt gekomen aan zowel de bedoeling van de Europese wetgever als de noodzaak van een heldere afbakening tussen richtlijn en verordening. Dit betekent inderdaad wel dat de verwerkingsverantwoordelijke en de verwerkers zich te allen tijde bewust moeten zijn van de vraag welke gegevens zij verwerken, in verband met welke taak en voor wel doel zij gegevens aan anderen willen verstrekken.

2. Boetebevoegdheid

De AP merkt op dat in het wetsvoorstel slechts een bevoegdheid is gegeven om een boete op te leggen vanwege een overtreding van de documentatieplicht (artikel 32 Wpg). Het boetemaximum bedraagt ten hoogste het bedrag van de vierde boetecategorie van artikel 23, vierde lid, Sr (€ 20.500). De maximum boetebedragen in de Verordening variëren van 10 to 20 miljoen euro. De AP wijst op de samenhang met de Verordening en de verplichting voor de lidstaten om inbreuken op de Richtlijn te bestraffen met doeltreffende, evenredige en afschrikkende sancties (artikel 57 RI) en stelt voor om voor de administratieve geldboeten aan te sluiten bij de regeling van artikel 83 van de Verordening. Om die reden adviseert de AP de bepalingen waarvoor een administratieve boete kan worden opgelegd aan te vullen en de boetemaxima te heroverwegen en in dat verband aansluiting te zoeken bij de Verordening. Daarbij wordt een lijst van overtredingen voorgesteld, waarvoor een bestuurlijke boete kan worden opgelegd.
Naar aanleiding van dit advies wordt opgemerkt dat, anders dan de verordening, de richtlijn de lidstaten niet verplicht om bepaalde bevoegdheden tot handhaving toe te delen aan de toezichthoudende instantie. De richtlijn volstaat met een verplichting voor de lidstaten om te voorzien in effectieve bevoegdheden terzake waarbij rekening gehouden kan worden met de specifieke nationale situatie. Voor de implementatie van dit onderdeel van de richtlijn is aangesloten bij de huidige regeling op basis van de Wpg en de Wjsg. De huidige regeling voorziet in vergaande bevoegdheden voor de AP ter handhaving, zoals het opleggen van een last onder bestuursdwang. Niettemin wordt naar aanleiding van het advies van de AP voorgesteld om de bevoegdheid van de AP tot het opleggen van een bestuurlijke boete te verruimen tot het niet-naleven van de verplichting tot het melden van datalekken (artikelen 33a Wpg, 27, vierde lid, 39r, derde lid, 51, derde lid, 51d, derde lid, en 51h, derde lid, Wjsg, 27b, vijfde lid, Sv en 14, derde lid, Wet ter voorkoming van witwassen en financieren van terrorisme). Tevens wordt voorgesteld het maximum boetebedrag met het oog op de afschrikkende werking te verhogen van de vierde tot de vijfde boetecategorie van artikel 23, vierde lid, Sr (€ 82.000). Mede in het licht van de andere bevoegdheden van de AP wordt de AP hiermee naar mijn oordeel een evenwichtig en voldoende voldragen instrumentarium geboden ter handhaving van deze voorschriften.

3. Beveiliging van politiegegevens

De AP adviseert om bij voorkeur de algemene verplichting tot beveiliging van politiegegevens van artikel 19 van de richtlijn, en de uitwerking daarvan, in 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 «Data Protection Impact Assessment» in afzonderlijke artikelen onder te brengen. Tevens adviseert de AP om af te zien van de in de richtlijn geboden mogelijkheid tot uitstel van invoering van de loggingplicht.
Aan dit advies is reeds gevolg gegeven doordat de gegevensbeveiliging door ontwerp, de gegevensbescherming door standaardinstellingen en de verplichting tot een gegevensbeschermingseffectbeoordeling zijn geregeld in respectievelijk de artikelen 4a, 4b en 4c Wpg. De verplichting tot beveiliging van politiegegevens is eveneens opgenomen in artikel 4a Wpg. De uitwerking van deze verplichting in artikel 29, tweede lid, van de richtlijn, is dermate gedetailleerd en uitgebreid dat dit niet goed past in een wet in formele zin. Deze uitwerking zal dan ook worden opgenomen in het Bpg.

De verplichting tot logging van gegevens over de verwerking van politiegegevens en van justitiële-, strafvorderlijke- en strafzaakgegevens betreft een verstrekkende verplichting, vanwege het grote aantal informatiesystemen bij de opsporingsdiensten en het openbaar ministerie waarvoor deze verplichting geldt (alleen voor de politie ruim 400 systemen), het aantal informatiesystemen dat daadwerkelijk aanpassing behoeft om aan deze verplichting te voldoen en de hoge kosten die hieraan zijn verbonden. Deze stand van zaken noopt tot opneming in het wetsvoorstel van de mogelijkheid tot uitstel van invoering van de betreffende bepalingen van de Wpg en de Wjsg, binnen de bandbreedte die daarvoor in de richtlijn wordt geboden.

4. Passende waarborgen

De AP wijst erop dat ten aanzien van de verwerking van bijzondere categorieën van persoonsgegevens, op grond van artikel 5 Wpg, het thans gehanteerde criterium – dat die verwerking mogelijk is voor zover die voor het doel van de verwerking «onvermijdelijk» is – wordt vervangen door het criterium dat de verwerking «strikt noodzakelijk» is. De richtlijn vereist tevens dat passende waarborgen worden geboden. De AP stelt vast dat in het wetsvoorstel de passende waarborgen zijn beperkt tot het vereiste dat de verwerking voor dit doel slechts plaatsvindt in aanvulling op de verwerking van andere politiegegevens, en adviseert te voorzien in verdergaande waarborgen dan de thans voorgestelde tekst.
Naar aanleiding van dit advies wordt opgemerkt dat het vereiste van de strikte noodzaak impliceert dat strenge regels gelden voor de toegang tot de gegevens, omdat die toegang afhankelijk is van de noodzaak om die gegevens te verwerken. Niettemin is de tekst van het voorgestelde artikel 5 Wpg nader aangepast. Gekozen is het criterium van de onvermijdelijkheid, dat thans in de wet wordt gesteld, te handhaven.
Verder wijst de AP erop dat ten aanzien van de profilering, op grond van artikel 7a, eerste lid, Wpg, de vereiste passende waarborgen slechts uitwerking hebben gekregen in «het recht op menselijke tussenkomst», terwijl een voorwaarde die voorziet in specifieke voorlichting aan de betrokkene ontbreekt. Weliswaar wordt in de toelichting op artikel 24b, tweede lid, onder e, Wpg voorzien in de verplichting de betrokkene te informeren over het bestaan van geautomatiseerde besluitvorming, maar de AP concludeert dat met deze bepalingen onvoldoende invulling wordt gegeven aan de vereiste passende waarborgen voor de betrokkene. De AP adviseert om die reden de genoemde bepalingen en de bijbehorende toelichting op adequate wijze aan te vullen.
Naar aanleiding van dit advies is de tekst van het voorgestelde artikel 7a, eerste lid, Wpg, aangevuld met de verplichting te voorzien in specifieke voorlichting aan de betrokkene. De toelichting is dienovereenkomstig aangevuld.

5. Rechten betrokkene inzake geautomatiseerde besluitvorming en datalekken

Ter implementatie van artikel 12, eerste lid, van de richtlijn bepaalt het wetsvoorstel in artikel 24a, eerste lid, eerste volzin, Wpg dat de verwerkingsverantwoordelijke aan de betrokkene informatie verstrekt over de verwerking van politiegegevens in een beknopte en toegankelijke vorm. De AP wijst er – kort weergegeven – op dat dit artikellid niet voldoende tegemoet komt aan het bepaalde in artikel 12 van de richtlijn. Volgens de AP gaat de strekking van artikel 12 van de richtlijn verder dan een loutere informatieverplichting als weergegeven. De AP adviseert artikel 12 van de richtlijn alsnog op toereikende wijze om te zetten in het wetsvoorstel. Artikel 24a, eerste lid, Wpg is in algemene bewoordingen opgesteld en bevat geen specifieke beperking ten aanzien van de informatie die in een

beknopte en toegankelijk vorm dient te worden opgesteld. Het heeft daarmee niet een beperktere reikwijdte dan hetgeen waarop artikel 24a, derde lid, Wpg over kosteloze verstrekking betrekking heeft. Om dit te benadrukken is in de toelichting op artikel 24a, eerste lid, Wpg alsnog verduidelijkt welke aspecten tot de verplichtingen als bedoeld in dat lid worden gerekend. Dit komt overeen met de aspecten waaraan in artikel 12 van de richtlijn wordt gerefereerd. Ten aanzien van hetgeen de AP heeft opgemerkt over artikel 24b, tweede lid, onder e, Wpg wordt voor de goede orde onder de aandacht gebracht dat dit artikellid niet de implementatie van artikel 12 maar van artikel 13, tweede lid, van de richtlijn betreft. Dit betreft de meer actieve informatieplicht in specifieke gevallen. Dit laat de aanvulling van de toelichting op artikel 24a, eerste lid, Wpg onverlet.

6. Gegevensverwerking door gerechten

De AP merkt op dat het bereik van de richtlijn mede ziet op de verwerking van persoonsgegevens door de gerechten, 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.
Het standpunt van de AP wordt onderschreven. De AP is niet belast met het toezicht op de verwerking van gerechtelijke strafgegevens door de gerechten, bedoeld in artikel 2 van de Wet op de rechterlijke organisatie, in het kader van de uitoefening van hun rechterlijke taken. In de toelichting op artikel 51 Wjsg van het wetsvoorstel wordt hierop nader ingegaan. Daarin wordt ook aangegeven dat enkel in gevallen waarin duidelijk is dat het toezicht door AP op geen enkele wijze van invloed kan zijn op de rechterlijke oordeelsvorming in de strafzaak die bij een gerecht in behandeling is, de bevoegdheid bestaat dit toezicht uit te oefenen.

7. Doorgifte aan derde landen en internationale organisaties

De AP geeft een beschrijving van de inrichting van het systeem van verstrekking van politiegegevens, justitiële en strafvorderlijke gegevens aan andere bevoegde autoriteiten. Hierbij wijst de AP er op dat bij de buiten de EU gelegen landen thans niet voorzien is in een omvattend beoordelingsmechanisme dat alle relevante factoren daarbij in beschouwing neemt. Onder de nieuwe richtlijn is dezelfde systematiek aanvaard als onder richtlijn 95/46 gebruikelijk was en zoals deze in de verordening wordt voortgezet. De systematiek zoals die in de voorgestelde wetswijzigingen is uiteengezet vormt volgens de AP een juiste uitwerking van de voorschriften van de richtlijn, maar de in de memorie van toelichting daarop gegeven toelichting sluit op die systematiek niet aan. De AP adviseert de toelichting in overeenstemming te brengen met de toepasselijke systematiek voor doorgiften aan derde landen of internationale organisaties zoals in artikel 17a van de Wpg 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.
Naar aanleiding van dit advies is de tekst van het voorgestelde artikel 17a, tweede lid, Wpg, en 16b, tweede lid, Wjsg gewijzigd door daarin aan te geven dat uitsluitend bij ontstentenis van een adequaatheidsbesluit van de Europese Commissie, gegevens kunnen worden doorgegeven op basis van passende waarborgen. Daarmee wordt uitdrukkelijk bepaald dat uitsluitend in geval een adequaatheidsbesluit ontbreekt aan de toepassing van het tweede lid kan worden toegekomen. De toelichting op artikel 17a, tweede lid, Wpg is overeenkomstig het advies van AP aangepast.

8. Artikelsgewijs commentaar

Aan het artikelsgewijze commentaar, de redactionele opmerkingen en de voorgestelde wijzigingen in de implementatietabel, die deel uitmaakt van het algemeen deel van de toelichting, is uitvoering gegeven door aanpassing van de voorgestelde artikelen of van deze toelichting.

9. Uitvoeringsgevolgen van de richtlijn gegevensbescherming opsporing en vervolging

De richtlijn heeft, behalve gevolgen voor de wet- en regelgeving, ook gevolgen voor de uitvoering van de gegevensverwerking die onder gezag van de bevoegde autoriteiten plaatsvindt. Deze richtlijn leidt tot incidentele en structurele kosten bij de bevoegde autoriteiten. In het onderstaande wordt nader ingegaan op de belangrijkste gevolgen. De implementatie van de richtlijn leidt niet tot administratieve lasten en overige lasten voor het bedrijfsleven. Het wetsvoorstel bevat geen directe of indirecte verplichtingen voor ondernemingen.

9.1 Impact wetsvoorstel

De richtlijn heeft een andere reikwijdte dan de thans geldende Wpg en de Wet justitiële en strafvorderlijke gegevens. Op bepaalde categorieën gegevens die met toepassing van de Wet bescherming persoonsgegevens worden verwerkt zal dit wetsvoorstel ter implementatie van de richtlijn van toepassing worden. Ook de tegenovergestelde situatie doet zich voor: sommige taken van de politie waarvoor nu gegevens worden verwerkt met toepassing van de Wpg, vallen niet binnen de reikwijdte van de richtlijn. Op deze gegevensverwerkingen is de verordening in het vervolg van toepassing. Ten opzichte van de huidige Wpg en de Wjsg biedt de richtlijn een uitbreiding van de huidige regels, bijvoorbeeld ten aanzien van de rechten van betrokkene, en ook nieuwe verplichtingen, zoals een meldplicht voor inbreuken op de beveiliging van persoonsgegevens.
Om inzicht te krijgen in de gevolgen van het wetvoorstel voor de uitvoering is eerst onderzocht of het wettelijk kader dat van toepassing is ook van toepassing blijft op de gegevensverwerkingen door deze organisaties. Dit geldt voor de bevoegde autoriteiten die in de oude situatie gegevens verwerkten onder het regime van de Wpg en de Wjsg: de politie, de rijksrecherche, de Koninklijke marechaussee, het openbaar ministerie en de Justitiële Informatie Dienst. Hoewel de richtlijn van toepassing is op een groot deel van de taken die door deze organisaties worden uitgevoerd, geldt dit niet voor alle taken. De handhaving van de Vreemdelingenwet 2000 valt bijvoorbeeld niet binnen de reikwijdte van de richtlijn. Op dit punt verandert de situatie voor politie en Koninklijke marechaussee, dit betreft in het bijzonder het binnenlands vreemdelingentoezicht en de grensbewakingstaak die door de politie en de Koninklijke marechaussee worden uitgevoerd. Dit betekent dat de gegevensverwerking voor dit doel door politie en Koninklijke marechaussee voortaan onder de verordening valt. Dit geldt ook voor de gegevensverwerking door de politie ten behoeve van de taken die bij wet aan de korpschef zijn opgedragen.
Andere organisaties zijn bevoegde autoriteiten in het kader van de richtlijn terwijl zij onder de huidige wet gegevens verwerken binnen het regime van de Wet bescherming persoonsgegevens. Dit geldt bijvoorbeeld voor de verwerking van persoonsgegevens in het kader van opsporing door buitengewoon opsporingsambtenaren. De Wpg wordt daarom bij besluit van toepassing verklaard op de gegevensverwerking die in dit kader plaatsvindt. Hetzelfde geldt voor gegevens die worden verwerkt ten behoeve van de strafrechtspraak en de tenuitvoerlegging van straffen, de gerechtelijke strafgegevens en de tenuitvoerleggingsgegevens. Hierop is

de Wet bescherming persoonsgegevens van toepassing en dit wordt de Wet justitiële en strafvorderlijke gegevens. Zo worden de persoonsgegevens in het penitentiair dossier of inrichtingsdossier als tenuitvoerleggingsgegevens gekwalificeerd. Hierop wordt de Wet justitiële en strafvorderlijke gegevens, en in aanvulling daarop de voorschriften in de betreffende Beginselenwet over persoonsgegevens, van toepassing. De wijzigingen die met de overgang naar een ander wettelijk regime optreden zijn niet helemaal hetzelfde als de wijzigingen voor de organisaties die al werkten op basis van de Wpg of de Wjsg. De Wet bescherming persoonsgegevens kende bijvoorbeeld al een meldplicht voor datalekken, zodat dit materieel geen nieuwe verplichting zal inhouden bij de overgang naar het richtlijn regime.
De wijziging in de reikwijdte van de wettelijke regimes maakt de situatie voor sommige organisaties complex: het CJIB verwerkt bijvoorbeeld gegevens binnen drie verschillende regimes. De verordening is onder andere van toepassing op de gegevensverwerking in het kader van de afdoening op basis van de Wet administratiefrechtelijke handhaving verkeersvoorschriften, de Wpg op de verwerking van gegevens door buitengewone opsporingsambtenaren en de Wjsg op de gegevensverwerking in het kader van de inning van strafbeschikkingen.
De impact van de richtlijn op de taken die hieronder vallen verschilt per verplichting en per organisatie. Een aantal verplichtingen heeft een grote ICT-component. De impact van deze verplichtingen is mede afhankelijk van met de mogelijkheden die de huidige ICT-systemen bieden. De bevoegde autoriteiten hebben een voorlopige schatting gedaan van de impact voor de organisaties. Hiervoor is eerst in kaart gebracht welke taken onder de richtlijn vallen en welke taken onder de verordening vallen. Voor de taken die binnen de richtlijn vallen is onderzocht wat de wijzigingen zijn ten opzichte van de huidige situatie. Vervolgens is gekeken in hoeverre op dit moment al aan de nieuwe of gewijzigde verplichting wordt voldaan en welke wijzigingen nodig zijn om aan de verplichting te voldoen. Dat leidt tot een inschatting van de impact en waar mogelijk tot een kwantificering van de incidentele en structurele kosten. De impact analyses zijn een voorlopige beoordeling van de impact per organisatie. Vanwege de complexiteit van de regelgeving en omvang van de ICT voorzieningen, en de korte implementatietermijn van de richtlijn is het op dit moment niet mogelijk tot een meer nauwkeurige impactbeoordeling te komen.

9.2 Financiële gevolgen

De uitkomst van de impactanalyses kan worden onderverdeeld in twee categorieën verplichtingen, de verplichting logbestanden bij te houden en de overige verplichtingen. Deze onderverdeling is relevant omdat voor het voldoen aan de loggingsverplichting een langere implementatietermijn geldt, tot 2023 (of in uiterst geval tot 6 mei 2026), indien dit noodzakelijk is. Hoewel de impact van deze verplichting op veel organisaties groot is, omdat hogere eisen aan ICT-systemen worden gesteld en maatwerkaanpassingen nodig zijn, is er meer tijd om aan deze verplichting te voldoen. Waar mogelijk kan bij implementatie van de richtlijn hierdoor worden aangesloten bij de vernieuwing van ICT-systemen.
De kosten voor het voldoen aan de verplichting logbestanden bij te houden, hebben er mee te maken dat alle informatie die op basis van de richtlijn moet worden geregistreerd ook moet worden bewaard zodat hier ook de nodige informatie uit kan worden afgeleid. Hierbij geldt dat de snelheid en functionaliteit van de systemen niet achteruit mag gaan. Omdat meer gegevens op toegankelijke wijze moeten worden opgeslagen, is ook meer opslagcapaciteit nodig. De hoogte van de bedragen wordt mede bepaald door het aantal systemen, de ouderdom en functionaliteit van de systemen, en de aantallen gebruikers en

bevragingen van deze systemen. Daarnaast is een systeem nodig waarmee toezicht wordt gehouden op de verwerking, op basis van de logginggegevens.
De impact van de overige verplichtingen is sterk afhankelijk van de werkzaamheden en omvang van de organisaties. Organisaties die vanwege de aard van hun werkzaamheden veel gegevens verwerken, zoals de Justitiële Informatie Dienst, hebben de impact van de overige verplichtingen als groot beoordeeld. Dit komt onder andere omdat meer verzoeken om informatie over de gegevensverwerking worden verwacht. Het beantwoorden van deze verzoeken vergt een individuele beoordeling en afstemming met andere ketenpartners. De impact uit de overige verplichtingen betreft bijvoorbeeld ook de uitbreiding van de verplichting om gegevensbeschermingseffectbeoordelingen uit te voeren en het nemen van extra beveiligingsmaatregelen. Doordat de richtlijn hogere eisen stelt aan gegevensbescherming en daarmee aan ICT-systemen, kunnen de kosten van het gehele ICT-portfolio omhoog gaan. Tenslotte is mogelijk extra capaciteit nodig om aan de overige verplichtingen uit de richtlijn te kunnen voldoen. Zo moet bijvoorbeeld een functionaris voor de gegevensbescherming worden benoemd.

Het totaal aan verplichtingen leidt voor de verschillende organisaties tot de volgende kosteninschatting:

bedragen x € mln.

	incidenteel	structureel
DJI	5	1
CJIB	5	1
JustID	17	7
Rechtspraak	-	-
Hoge Raad	1	0
OM	11	14
Politie	35	8
Kmar	5	2
FIU	-	-
totaal	**77**	**33**
waarvan		
- verplichtingen rond logging	58	15
- overige verplichtingen	19	18

Over de jaren heen is een tentatieve inschatting dat de kosten als volgt zijn verdeeld:

bedragen x € mln.

	2017	2018	2019	2020	2021	2022	struc.
verdeling kosten meerjarig	10	10	10	15	20	25	33

Een eerste inventarisatie wijst uit dat de rechtspraak op dit moment reeds voldoet aan de verplichtingen uit de richtlijn. Hoewel de grondslag voor de verwerking van gegevens ten behoeve van de strafrechtspraak wijzigt, lijkt dit dus geen financiële gevolgen te hebben. De FIU-Nederland maakt gebruik van systemen van de politie en van een internationale organisatie. Deze systemen worden door de eigenaar aangepast, deze kosten komen niet voor rekening van de FIU-Nederland. De rijksrecherche maakt gebruik van ICT-voorzieningen die worden beheerd door het openbaar ministerie. De kosten voor de aanpassing van deze systemen maken onderdeel uit van de kosten die door het openbaar ministerie in kaart zijn gebracht.

Hoewel de richtlijn ook van toepassing is op de bijzondere opsporingsdiensten en de buitengewone opsporingsambtenaren, wordt niet in dit wetsvoorstel maar in een algemene maatregel van bestuur geregeld aan welke verplichtingen zij moeten voldoen. In de toelichting bij deze algemene maatregel van bestuur wordt de impact van de richtlijn op deze organisaties beschreven.
Het wetsvoorstel ter uitvoering van de verordening en dit wetsvoorstel ter implementatie van de richtlijn leiden tot een toename in de toezichtslasten voor de AP. Op deze toename, met inbegrip die als gevolg van de richtlijn, wordt in de toelichting op het wetsvoorstel ter uitvoering van de verordening nader ingegaan, zodat daarnaar wordt verwezen.
De kosten voor de organisaties die worden geraakt door dit wetsvoorstel, dienen te worden gedekt vanuit de bedrijfsvoeringsbudgetten van de betreffende organisaties. Een groot deel van de kosten vloeit voort uit de implementatie van de loggingsverplichting. De richtlijn kent voor deze verplichting een langere implementatietermijn tot 2023, en in uitzonderlijke gevallen tot 2026. Van deze termijn wordt gemaakt om bij de reguliere ICT-vervanging aan te sluiten.

9.3 Uitvoeringsaspecten

De Afdeling advisering van de Raad van State constateert dat uit onderzoek blijkt dat de toepassing van de gegevensbeschermingswetgeving op het gebied van politie en justitie al langere tijd een bron van aandacht en zorg is. Zij adviseert om in de toelichting nader in te gaan op de uitvoering van het voorstel in de praktijk, in het bijzonder de vraag op welke wijze de vage normen zullen worden gehanteerd en op de realisering van de voor een goede uitvoering noodzakelijke ICT-voorzieningen. Voorts adviseert de Afdeling om in de toelichting in te gaan op het punt van opleiding en scholing van degenen die met gegevensverwerking te maken hebben.
De Afdeling advisering van de Raad van State geeft in haar advies terecht aan dat de toepassing van de gegevensbeschermingswetgeving op het gebied van politie en justitie al langere tijd een bron van aandacht en zorg is. Bij de evaluatie van de Wpg in 2013 constateerden de onderzoekers dat sprake is van «een worstelende praktijk». De uitkomsten van een externe audit van de Auditdienst Rijk (ADR) naar de naleving van de Wpg door de politie bevestigden dit beeld (Kamerstukken II, 2015/16, 33 842, nr. 3). De doelstellingen en de hoofdlijnen van de wet worden weliswaar breed onderschreven, maar de invulling en de toepassing ervan loopt vast in de operationalisering en de implementatie. De oorzaak hiervan ligt deels in de complexiteit van de wetgeving, deels in de politieorganisatie.

9.3.1 Wet politiegegevens

Zoals ik eerder aan de Kamer heb gemeld, hecht ik veel belang aan een nauwgezette naleving van de regels van de Wet politiegegevens door de politie. Burgers moeten erop kunnen vertrouwen dat de politie correct en zorgvuldig met persoonsgegevens omgaat. Een goede naleving van de Wpg leidt tot een evenwicht waarin de politie voldoende middelen ter beschikking staan om te werken aan de veiligheid van onze samenleving, zonder daarbij onnodig een inbreuk te maken op de grondrechten van burgers. Binnen de politie zijn een Gegevensautoriteit en een Informatiebeveiligingsautoriteit ingericht, waardoor centrale regie mogelijk is op de kwaliteit en beveiliging van de informatie. Naar aanleiding van de eerdergenoemde audit van de ADR is een meerjarig verbeterplan opgesteld, dat inmiddels aan Uw Kamer is aangeboden (Kamerstukken II 2015/16, 33 842, nr. 4). In het verbeterplan zijn maatregelen opgenomen om te komen tot verbetering van de naleving van de Wpg. Daartoe bevat het verbeterplan maatregelen op het gebied van de beveiliging van

gegevens, de rechten van de betrokkene, de verstrekking van gegevens, de protocolplicht, de kwaliteit van gegevens, gevoelige gegevens en audits. De maatregelen hebben onder andere betrekking op het aanpassen van ICT systemen en het inrichten van procedures. De opleiding en scholing van medewerkers is tevens een integraal onderdeel van het verbeterplan.
De maatregelen uit het verbeterplan beginnen inmiddels tot resultaten te leiden. Zo werkt de politie aan een geautomatiseerde oplossing voor het proces van verstrekken en intrekken van autorisaties voor politiesystemen bij (ver)plaatsing of uitdiensttreding («Identity & Accessmanagement tooling»), die voor een aantal applicaties reeds wordt toegepast. Voorts is inmiddels een uitvoeringskader «Privacy & Security by Design» vastgesteld, dat momenteel binnen de politieorganisatie wordt geïmplementeerd.
Het verbeterplan heeft betrekking op de periode 2016–2019 en wordt projectmatig aangestuurd. Daartoe is een stuurgroep opgericht en zijn verschillende deelprogramma's ingericht. Ten behoeve van de implementatie van deze richtlijn is de scope van het verbeterplan uitgebreid en zijn aanvullende maatregelen in het plan opgenomen, waardoor de implementatie van de normen van de richtlijn onderdeel vormt van het lopende verbetertraject. Dit betreft onderwerpen als de verplichting tot het loggen van gegevens (artikel 32a Wpg), de ontwikkeling van een model voor het registreren van gegevens (artikel 31d Wpg) en voor het opstellen van een gegevensbeschermingseffectbeoordeling (artikel 4c Wpg).
Binnen de politie bestaat het Privacyplatform, waarin zowel meer algemene privacyvraagstukken, invulling van open normen als concrete casussen aan de orde komen en worden afgestemd. Naast de privacyfunctionarissen, juristen en beleidsadviseurs van de politie, worden voor dit overleg ook vertegenwoordigers van de Koninklijke marechaussee, de rijksrecherche en de vertegenwoordigers van bijzondere opsporingsdiensten uitgenodigd. Dit gremium kan een belangrijke rol spelen ter ondersteuning van de implementatie van de maatregelen die uit het voorliggende wetsvoorstel voortvloeien, een eenduidige toepassing van de normen en het adresseren van vragen vanuit de uitvoeringspraktijk.
Het volledig kunnen naleven van de Wpg vergt echter niet alleen maatregelen ter implementatie van wet- en regelgeving. Een adequate naleving hangt tevens nauw samen met aanpassing of vervanging van oudere informatiesystemen en aanpassing in de huidige wetgeving. In de beleidsreactie op de evaluaties van de Wpg en de Wjsg (Kamerstukken II 2013/2014, 33 842, nr. 2) heeft mijn ambtsvoorganger aangekondigd om beide wetten op termijn in onderling verband te zullen herzien en moderniseren, zodat gekomen wordt tot een eenduidig en eenvormig regime voor de verwerking van persoonsgegevens binnen de strafrechtsketen. Nadat de implementatie van deze richtlijn in de Wpg en Wjsg is afgerond, zullen de voorbereidingen voor de eerder aangekondigde herziening van de beide wetten in gang worden gezet.

9.3.2 Wet justitiële en strafvorderlijke gegevens

In 2013 is de Wjsg geëvalueerd. De onderzoekers constateerden, onder andere, dat de justitiële en strafvorderlijke gegevens aan het einde van de bewaartermijn (niet) of niet altijd worden vernietigd. Naar aanleiding daarvan zijn verbeterplannen opgesteld, met als doel conform de wet- en regelgeving te schonen. De Justitiële Informatiedienst heeft in dat kader voorzieningen getroffen waardoor de gegevens niet meer toegankelijk zijn voor gebruikers van het justitieel documentatiesysteem en voor functioneel beheerders.
De organisaties die onder de Wjsg vallen en die moeten voldoen aan de verplichtingen die voortvloeien uit de richtlijn, zijn hiermee inmiddels van start gegaan. Projectleiders zijn geworven en projectplannen zijn

opgesteld. Grofweg kan onderscheid worden gemaakt tussen drie categorieën activiteiten: bewustwording en voorlichting, wijzigen processen en werven personeel en ICT-aanpassingen.
Zo heeft het openbaar ministerie in 2017 een programma ingericht om zich voor te bereiden op de inwerkingtreding van de verordening en de richtlijn gegevensbescherming. Het programma ondersteunt het openbaar ministerie om te kunnen voldoen aan de nieuwe verplichtingen door o.a. modelovereenkomsten en protocollen op te stellen, het inrichten van een landelijk verwerkingsregister, het (laten) uitvoeren van «privacy impact assessments» en het aanstellen van een functionaris gegevensbescherming. De komende periode zal meer concreet in kaart worden gebracht welke aanpassingen nodig zijn in de systemen van het openbaar ministerie om te kunnen voldoen aan de nieuwe loggingverplichting.
De medewerkers van het openbaar ministerie zullen vanuit het programma worden geïnformeerd over de nieuwe wetgeving en de nodige aandacht zal uitgaan naar het vergroten van bewustzijn hoe om te gaan met persoonsgegevens en eventuele datalekken. In de communicatie met de burger wordt expliciet rekening gehouden met de richtlijn en de verordening. Bij de voorbereiding op de inwerkingtreding van de richtlijn en de verordening werkt het openbaar ministerie samen met ketenpartners en het zogenoemde AVG-team van het Ministerie van Justitie en Veiligheid.
Ook bij de Hoge Raad is een project gestart. Het project richt zich onder meer op het organiseren van awareness sessies, het op orde hebben van het register met gegevensverwerkingen en het in kaart brengen van het autorisatiemodel.
Bij de Justitiële informatiedienst (JustID) wordt één medewerker opgeleid tot information privacy manager. Er wordt ook een privacy officer aangesteld. Daarnaast is een awareness campagne begonnen onder medewerkers en is er voorlichting gegeven. Inmiddels is Justid begonnen met het Project Vernieuwing Kernsystemen (PVK) waarbij wordt beginnen met het systeem JDS. Dit systeem wordt ontwikkeld onder architectuur. In de doelarchitectuur is een tweetal applicatiecomponenten opgenomen:

- Verstrekkingen: het registreren van alle verstrekkingen van informatieproducten, gegevenssets, aan de afnemers conform de verordening/ richtlijn.
- Wet & regelgeving: module waarin alle relevante wet- en regelgeving is opgenomen die als toetsingskader dient voor het verstrekken van informatieproducten aan de afnemers.

Bij de Dienst Justitiële Inrichtingen is per 1 januari 2018 een «privacy officer» aangesteld, daarnaast zijn verschillende PIA's uitgevoerd.
Het Ministerie van Justitie en Veiligheid ondersteunt de organisaties waar mogelijk bij de implementatie van de nieuwe verplichtingen. Voor dit doel is het eerdergenoemde JenV-brede AVG-team uitgebreid met een richtlijn-team. Organisaties kunnen terecht bij dit team voor praktische tips en goede voorbeelden. Desgewenst kan het team ondersteuning op maat bieden bij de implementatie van de verplichtingen. Het team wordt ondersteund door een aantal juristen die vragen over de interpretatie van de verplichtingen kunnen beantwoorden. Tijdens bijeenkomsten worden knelpunten gedeeld en «best practices» besproken. Daarnaast is het voornemen om ten behoeve van een eenduidige toepassing van de vage normen in de Wpg en Wjsg met alle betrokken ketenpartners de uitleg die aan belangrijke begrippen wordt gegeven, af te stemmen.

De Afdeling advisering merkt tevens op dat technologische ontwikkelingen, zoals big data analyses, vergaande gevolgen lijken te hebben voor de wetgeving en de basisprincipes die daaraan ten grondslag liggen. Ondanks de aanpassingen vanwege de richtlijn is het de vraag in hoeverre de richtlijn en het voorstel op deze ontwikkelingen zijn toegerust, in het bijzonder of deze leiden tot een effectieve bescherming van de algemene

beginselen van gegevensbescherming en tegelijk bruikbaar zijn voor de uitvoeringspraktijk. In de uitvoeringsbegeleiding zou nadrukkelijk aandacht besteed moeten worden aan de wijze waarop de technische ontwikkelingen worden geïncorporeerd in de praktische toepassing van het wetsvoorstel of geregeld in andere wetgeving. De Afdeling adviseert in de toelichting hierop in te gaan, in het bijzonder op de wijze waarop de onderhavige regelgeving is toegesneden op de genoemde technische ontwikkelingen.
Naar aanleiding van dit advies kan worden opgemerkt dat de zienswijze dat technologische ontwikkelingen gevolgen kunnen hebben voor de bescherming van persoonsgegevens, wordt onderschreven. Hierbij moet worden bedacht dat het verzamelen van persoonsgegevens ten behoeve van de opsporing of vervolging van strafbare feiten, zeker als het grote hoeveelheden gegevens betreft van personen die (nog) niet in verband kunnen worden gebracht met het beramen of plegen van strafbare feiten, een ingrijpende inbreuk op de bescherming van de persoonlijke levenssfeer met zich mee kan brengen die een adequate wettelijke grondslag vereist. Een dergelijke wettelijke grondslag heeft nauwe raakvlakken met de bevoegdheden tot het opsporen van strafbare feiten, en behoort dan te worden opgenomen in het Wetboek van Strafvordering. Een voorbeeld van een dergelijke bevoegdheid betreft het stelselmatig met een technisch hulpmiddel vastleggen van gegevens betreffende een persoon uit open bronnen, in het kader van een verkennend onderzoek. Een dergelijke bevoegdheid is opgenomen in het conceptwetsvoorstel Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering (Het opsporingsonderzoek), dat vorig jaar in consultatie is gegeven (artikel 2.9.1). Alsdan ligt het opnemen van garanties waarborgen ter bescherming van de persoonlijke levenssfeer in het kader van een dergelijke wettelijke bevoegdheid in de rede.
Voorts wordt opgemerkt dat het uitgangspunt van de Wpg, dat politiegegevens uitsluitend worden verwerkt voor welomschreven en gerechtvaardigde doelen, heeft geleid tot het onderscheiden van doelen binnen de politietaak waarvoor politiegegevens mogen worden verwerkt. Eén van die doelen betreft de uitvoering van de dagelijkse politietaak (artikel 8 Wpg). Naast (of in vervolg op) de uitvoering van de dagelijkse politietaak is er de gerichte verwerking van politiegegevens, zoals bij een onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval (artikel 9 Wpg). De Wpg staat er aan in de weg dat persoonsgegevens, die worden verwerkt met het oog op een bepaald doel binnen de politietaak, vrijelijk met elkaar in verband worden gebracht. De Wpg bevat echter wel specifieke regels voor het geautomatiseerd vergelijken en in combinatie zoeken van politiegegevens (artikel 11 Wpg). Die regels voorzien in de mogelijkheid de politiegegevens die worden verwerkt met het oog op een bepaald doel binnen de politietaak, geautomatiseerd te vergelijken met politiegegevens die worden verwerkt voor een ander doel, teneinde vast te stellen of verbanden bestaan tussen de betreffende gegevens. Het verdere gebruik van de gerelateerde gegevens is gekoppeld aan instemming van een daartoe bevoegde functionaris. Alleen de daartoe geautoriseerde ambtenaren van politie kunnen worden belast met de gegevensvergelijking. Indien dit noodzakelijk is ten behoeve van een bepaald onderzoek of een bepaald doel binnen de politietaak kunnen alle beschikbare politiegegevens, inclusief de gegevens van onverdachte personen, in combinatie met elkaar worden verwerkt. Deze zoekmogelijkheid dient op grond van de wet te worden voorbehouden aan een zeer beperkte kring van politieambtenaren die daarvoor de vereiste deskundigheid en ervaring bezitten. Bovendien is voor het gebruik van deze mogelijkheid een opdracht van het bevoegde gezag vereist. Dit is de officier van justitie of de burgemeester; afhankelijk van het doel van de verwerking. Tot slot valt te wijzen op artikel 22 Wpg, op grond waarvan politiegegevens kunnen worden verwerkt ten behoeve van beleidsinfor-

matie, wetenschappelijk onderzoek of statistiek met het oog op de taak, bedoeld in artikel 1, eerste lid, onder a, Wpg. Ook bij een dergelijke verwerking kan het om grote hoeveelheden gegevens gaan. De wet verbindt hieraan de voorwaarde dat de resultaten daarvan geen persoonsgegevens mogen bevatten, terwijl ook het Bpg een aantal nadere voorwaarden voor een dergelijke verwerking bevat.
De waarborgen uit de richtlijn zijn techniekonafhankelijk en bieden daarmee ook bescherming bij het gebruik van nieuwe technische toepassingen waarmee op grote schaal persoonsgegevens kunnen worden verwerkt. Het betreft hier waarborgen ten aanzien van geautomatiseerde individuele besluitvorming (artikel 11 RI), «privacy by design» (artikel 20 RI), gegevensbeschermingseffectbeoordeling (artikel 27 RI), het voorafgaand consulteren van de toezichthoudende autoriteit (artikel 28 RI) en de beveiliging van gegevens (artikel 29 RI). Met dit wetsvoorstel worden deze waarborgen in de Wpg en de Wjsg opgenomen.
Niettemin roept de ontwikkeling op het gebied van informatie- en communicatietechnologie fundamentele vragen op over de (toekomstige) verhouding tussen technische mogelijkheden en de mogelijkheden om de persoonsgegevens effectief te blijven beschermen. Met het oog hierop heeft het toenmalige kabinet in zijn standpunt over het WRR-rapport: »Big Data in een vrije en veilige samenleving» een aantal beleidsuitgangspunten geformuleerd voor het kabinetsbeleid met betrekking tot «Big Data» in het veiligheidsdomein, waarbij is aangetekend dat sommige van deze beleidsuitgangspunten ook betekenis kunnen hebben voor andere domeinen, zoals dienstverlening en zorg. Er is bewust gekozen voor beleidsuitgangspunten, omdat het terrein van Big Data nog zo in beweging is dat het – zeker in dit stadium – lastig is om, in aanvulling op de algemene waarborgen in de richtlijn, meer specifieke waarborgen in de Nederlandse wetgeving vast te leggen die niet alleen voldoende sturend maar ook voldoende flexibel (en daarmee toekomstbestendig) zijn. Ook de richtlijn zelf bevat relatief weinig specifieke waarborgen met betrekking tot de verwerking van persoonsgegevens ten behoeve van geavanceerde data-analyses.
Eén en ander neemt niet weg dat bezien wordt of de wettelijke basis voor het uitvoeren en gebruiken van data-analyses versterking behoeft, met inbegrip van de waarborgen die daarbij gehanteerd dienen te worden. Dit is één van de actiepunten uit voornoemd kabinetsstandpunt, waarvan de uitvoering moet bijdragen aan een effectieve bescherming van algemene beginselen van gegevensbescherming bij toepassing van «Big Data».
De Afdeling advisering adviseert verder om ook in de noodzakelijke uitvoeringsbegeleiding aandacht te besteden aan de wijze waarop technologische ontwikkelingen kunnen worden geïncorporeerd in de praktische toepassing van deze wet. De incorporatie hiervan vergt deels nog nader onderzoek. Zo is een van de andere actiepunten uit voornoemd kabinetsstandpunt het uitvoeren van een onderzoek naar het verschaffen van voldoende inzicht in gebruikte algoritmen en analysemethoden ten behoeve van toezicht en rechterlijke toetsing. Ook wordt gezocht naar wegen om de transparantie rond «Big Data» toepassingen door de overheid, inclusief politie en openbaar ministerie, te vergroten. De uitvoeringsbegeleiding op genoemd vlak heeft al wel concretere vormen aangenomen in het kader van experimenten die met betrekking tot «Big Data» worden uitgevoerd. Zo is op het terrein van justitie en veiligheid een broedkamer (Living Lab) voor «Big Data» experimenten ingericht (Kamerstukken II, 2016/17, 26 643, nr. 426, p. 4). Een ander voorbeeld is de City Deal « Zicht op ondermijning», een traject waarin met behulp van data-analyses wordt getracht een beter zicht te krijgen in patronen met betrekking tot ondermijnende criminaliteit (Stcrt. Nr. 48699, 29 augustus 2017). In deze experimenten, waar politie en het openbaar ministerie ook bij zijn betrokken, zijn principes uit het gegevensbeschermingsrecht, zoals terug te vinden zijn in de richtlijn en de verordening, in toetsingskaders

vertaald naar stappen die bij het uitvoeren van data-analyses gezet dienen te worden. Afhankelijk van de ervaringen in deze experimenten zal worden bezien of een meer generiek kader kan worden opgesteld waarvan mogelijk elementen naderhand in wetgeving kunnen worden vastgelegd.
Ook in de noodzakelijke uitvoeringsbegeleiding is nadrukkelijk aandacht voor de vraag hoe bepaalde technologische ontwikkelingen kunnen worden geïncorporeerd in de praktische toepassing van dit wetsvoorstel. In dit verband kan worden gewezen op het recent door de minsterraad vastgestelde nieuwe Model gegevensbeschermingseffectbeoordeling rijksdienst (PIA), waarin apart aandacht wordt besteed aan «Big Data» verwerkingen en de maatregelen die in dat kader moeten worden overwogen. Ook het opstellen van dit model was een toezegging uit de kabinetsreactie op het advies van de WRR over «Big Data». Overigens voorziet dit wetsvoorstel in een evaluatiebepaling, waarbij wordt voorgesteld de termijn voor de eerste evaluatie te stellen op drie jaar, zodat de bevindingen en uitkomsten van die evaluatie kunnen worden betrokken in de herziening van de privacywetgeving en tevens ter kennis van de Commissie kunnen worden ingebracht ten behoeve van de evaluatie van de richtlijn.

10. Implementatietabellen

10.1 Implementatietabel van de Wet politiegegevens

Richtlijn	Wet politiegegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
1(1) Onderwerp	Aan dit artikelonderdeel wordt uitvoering gegeven door de algehele implementatie van de richtlijn bij en krachtens de Wpg, waaronder voorschriften over te verwerken politiegegevens, over de bevoegde autoriteiten die deze gegevens mogen verwerken voor nader te bepalen doeleinden die binnen de reikwijdte van de richtlijn vallen, en over de toepasselijkheid van het bij en krachtens de Wpg bepaalde op de verwerking van politiege-gevens		
1(2a) Verplichtingen	Behoeft geen afzonderlijke implementatie; aan dit artikelonderdeel wordt uitvoering gegeven door de algehele implementatie van de richtlijn		
1(2b) Verplichtingen	Behoeft geen implementatie; de huidige wet voorziet niet in een verbod of beperking op uitwisseling van politiegegevens tussen bevoegde autoriteiten als bedoeld in dit artikelonderdeel		
1(3) Uitgebreidere waarborgen op nationaal niveau	Artikel 4c, derde lid	Lidstaten mogen uitgebreidere waarborgen bieden ter bescherming in verband met verwerking van persoonsgegevens dan de richtlijn voorschrijft	De implementatie van de richtlijn biedt voldoende waarborgen en het uitgangspunt van minimumimplementatie wordt gerespecteerd
2(1) Reikwijdte – doeleinden	Artikelen 1, onderdeel a, en 2, eerste lid		
2(2) Reikwijdte – bestand	Artikel 2, eerste lid		
2(3) Reikwijdte – uitsluiting activiteiten buiten Unierecht	Behoeft geen implementatie		
3(1) Persoonsgegeven	Artikel 1, onderdelen b en g		
3(2) Verwerking	Artikel 1, onderdeel c		
3(3) Verwerkingsbeperking	Artikel 1, onderdeel n*		

Richtlijn	Wet politiegegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
3(4) Profilering	Artikel 1, onderdeel u		
3(5) Pseudonimisering	Dit behoeft geen implementatie; dit begrip keert terug in artikel 20, eerste lid, van de richtlijn, waarbij het als voorbeeld wordt aangehaald		
3(6) Bestand	Artikel 1, onderdeel o		
3(7) Bevoegde autoriteit	Artikel 1, onderdeel l		
3(8) Verwerkingsverantwoordelijke	Artikel 1, onderdeel f		
3(9) Verwerker (voorheen bewerker)	Artikel 1, onderdeel i		
3(10) Ontvanger	Artikel 1, onderdeel p		
3(11) Inbreuk op persoonsgegevens	Artikel 1, onderdeel q		
3(12) Genetische gegevens	Artikel 1, onderdeel r		
3(13) Biometrische gegevens	Artikel 1, onderdeel s		
3(14) Gegevens gezondheid	Artikel 1, onderdeel t		
3(15) Toezichthoudende autoriteit	Artikel 1, onderdeel h		
3(16) Internationale organisatie	Artikel 1, onderdeel w		
4(1)(a) Behoorlijk en rechtmatig	Artikel 3, tweede lid		
4(1)(b) Welbepaalde en gerechtvaardigde doelen	Artikel 3, eerste lid*		
4(1)(c) Toereikend en proportioneel	Artikel 3, tweede lid		
4(1)(d) Juist en zonodig geactualiseerd	Artikel 4, eerste lid		
4(1)(e) Niet langer bewaard dan nodig	Artikel 4, tweede lid*		
4(1)(fb) Passende middelen ter beveiliging	Artikel 4a		
4(2) Verwerking voor ander doel dan doel artikel 1(1)	Artikel 3, derde lid		
4(3) Archivering en wetenschappelijk onderzoek	Artikelen 14, vierde lid*, en 22, eerste lid		
4(4) Naleving leden 1 – 3	Artikel 4a, eerste lid, onderdeel a		
5 Termijnen voor opslag en evaluatie	Artikelen 8, zesde lid*, 9, vierde lid*, 10, zesde lid*, 12, zesde lid*, 13, vierde lid* en 14, eerste en vierde lid*		
6(1) Onderscheid categorieën betrokkenen	Artikel 6b		
7(1) Onderscheid tussen persoonsgegevens en betrouwbaarheid	Artikel 4, derde lid		
7(2) Controle gegevens voor doorzending	Artikel 4, eerste lid		

Richtlijn	Wet politiegegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
7(3) Kennisgeving ontvanger na op onrechtmatige wijze doorgezonden + rectificatie	Artikel 4, vierde lid		
8(1) Rechtmatigheid	Artikel 3, eerste lid* en tweede lid		
8(2) Wetgeving lidstaten	Implementatie bestaat uit de gehele Wpg en het Bpg		
9(1) Verwerking voor andere doelen dan die van 1(1)	Artikelen 3, vierde lid, 18, eerste lid*, 19* en 20*		
9(2) Avg van toepassing op die verwerking	Behoeft geen implementatie gelet op de recht-streekse toepasselijkheid van verordening 2016/679/EU in het Nederlandse recht		
9(3) Specifieke voorwaarden	Artikelen 15, tweede lid en 15a, tweede lid		
9(4) Zelfde voorwaarden als nationaal	Artikel 15, tweede lid (AMvB)		
10(1) Gevoelige persoonsgege-vens	Artikel 5		
11(1) Profilering	Artikel 7a, eerste lid		
11(2) Gevoelige persoonsgege-vens	Artikel 7a, tweede lid		
11(3) Geen discriminatie	Artikel 7a, derde lid		
12(1) Heldere informatie	Artikel 24a, eerste lid		
12(2) Faciliteren	Bepaling verwerkt in paragraaf 4 en paragraaf 4a		
12(3) Schriftelijk in kennis stellen m.b.t. opvolging verzoek	Artikel 24a, tweede lid		
12(4) Verstrekking informatie kosteloos en mogelijkheid weigering kennelijk ongegronde of buitensporige verzoeken	Artikel 24a, derde lid en vierde lid		
12(5) Aanvullende informatie	Artikel 26, eerste lid		
13(1) Algemene informatie	Artikel 24b, eerste lid		
13(2) Speciale informatie	Artikel 24b, tweede lid		
13(3) Weigeringsgronden speciale informatie	Mogelijkheid om verstrekking bepaalde informatie aan betrokkene uit te stellen, te beperken of achterwege te laten op bepaalde gronden	Mogelijkheid om verstrekking bepaalde informatie aan betrokkene uit te stellen, te beperken of achterwege te laten op bepaalde gronden	In het kader van mini-mumimplementatie is van deze mogelijkheid geen gebruik gemaakt
13(4) Generieke uitzonderingen	Artikel 24b, derde lid	Mogelijkheid om verwerkingscategorieën vast te stellen waarvoor verstrekking van bepaalde informatie aan betrokkene niet van toepassing is	In het kader van mini-mumimplementatie is van deze mogelijkheid beperkt gebruik gemaakt
14 Recht op inzage	Artikel 25, eerste lid		
15(1) Weigeringsgronden inzage	Artikel 27, eerste lid	Mogelijkheid tot beperking van inzagerecht voor betrokkene om bepaalde redenen	Gelet op het zwaarwe-gende karakter van de redenen, waaronder die inzake nationale veilig-heid, is dit onderdeel van de implementatie

Richtlijn	Wet politiegegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
15(2) Generieke uitzonderingen	Artikel 27, derde lid	Mogelijkheid voor lidstaten te bepalen welke verwerkingscategorieën onder een beperking van het inzagerecht kunnen vallen	Van deze mogelijkheid is gebruik gemaakt voor gegevens betreffende informanten, infiltranten en getuigenbescherming
15(3) Weigering schriftelijk + klacht	Artikel 27, tweede lid en artikel 24a, tweede lid		
15(4) Documentatie	Artikel 32, eerste lid, onderdeel c		
16(1) Correctie	Artikel 28, eerste lid		
16(2) Wissen	Artikel 28, tweede lid		
16(3) Verwerkingsbeperking	artikel 28, tweede lid		
16(4) Niet informeren Informeren over indienen klacht	Artikel 27, eerste en tweede lid Artikel 24a, tweede lid	Tweede volzin 16(4): mogelijkheid tot beperking van rectificatie, wissing of verwerkingsbeperking om bepaalde redenen	Gelet op het zwaarwegende karakter van die redenen, waaronder de nationale veiligheid, is dit onderdeel van de implementatie
16(5) Doorgeven rectificatie aan verstrekker	Artikel 28, vierde lid		
16(6) Informeren ontvangers	Artikel 28, vijfde lid		
17(1) Controle TA	Artikelen 29, tweede lid, 31a, eerste lid		
17(2) In kennis stellen betrokkene	Artikel 24a, tweede lid en artikel 24b, eerste lid, onderdeel d		
17(3) Informatie aan de betrokkene	Behoeft geen implementatie. Besluit van de AP is besluit in de zin van Awb, waarvoor motiveringsplicht geldt (o.g.v. 3:46 Awb) en verplichting tot kennisgeving mogelijkheid bezwaar en beroep (o.g.v. 3:45 Awb)		
18 Strafzaak	Artikel 24a, vijfde lid		
19(1) Technische maatregelen Evaluatie en actualiseren	Artikel 4a, eerste lid, onderdeel a Artikel 4a, derde en vijfde lid		
19(2) Passend geg. beschermingsbeleid	Artikel 4a, eerste lid, onderdeel b		
20(1) Waarborgen privacy	Artikel 4a, eerste lid, onderdeel c, derde lid, en vierde lid		
20(2)Gegevens bescherming d.m.v. standaardinstellingen	Artikel 4b, eerste lid, onderdelen a en b, en tweede lid		
21(1) Gezamenlijke verwerkers + verplichtingen jegens betrokkene («kunnen bepaling»)	Artikel 1, onderdeel f, onder 4°; behoeft geen implementatie omdat er o.g.v. die bepaling maar één gegevensverwerkingsverantwoordelijke is		
21(2) Uitoefening rechten jegens iedere verantwoordelijke («kunnen bepaling»)	Behoeft geen implementatie omdat dit geen verplichting betreft maar een mogelijkheid		
22(1) Garanties verwerker passende maatregelen	Artikel 6c, eerste lid		
22(2) Schriftelijke toestemming verantwoordelijke	artikel 6c, vierde lid		
22(3) Inhoud contract met verwerker	Artikel 6c, tweede lid (AMvB)		

Richtlijn	Wet politiegegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
22(4) Schriftelijk contract	Artikel 6c, tweede lid		
22(5) Verwerker bepaalt middelen >> verantwoordelijke	Artikel 1, onderdeel i		
23 Instructies verantwoordelijke	Artikel 6c, derde lid		
24(1) Register verantwoordelijke	Artikel 31d, eerste lid, onderdelen a tot en met j		
24(2) Register verwerker	Artikel 31d, tweede lid, onderdelen a tot en met d		
24(3) Schriftelijk	Artikel 31d, eerste en tweede lid		
24(3) Register beschikbaar aan AP	Artikel 5:17, eerste lid, Awb		
25(1) Logging	Artikel 32a, eerste lid		
25(2) Gebruik logbestanden	Artikel 32a, tweede lid		
25(3) Logbestanden beschikbaar AP	Artikel 5:17, eerste lid, Awb*		
26 Samenwerking met AP	Artikel 5.20 Awb*		
27(1) PIA	Artikel 4c, eerste lid		
27(2) Inhoud PIA	Artikel 4c, tweede lid		
28(1) Consultatie AP	Artikel 33b, eerste lid		
28(2) Consultatie wetgeving	Artikel 35b, eerste lid, onderdeel b		
28(3) Lijst consultatie	Artikel 33b, tweede lid		
28(4) PIA beschikbaar AP	Artikel 33b, derde lid		
28(5) Advies AP	Artikel 33b, vierde en vijfde lid		
29(1) Beveiliging verwerking	Artikel 4a, tweede en derde lid		
29(2) Maatregelen beveiliging	Artikel 4a, zesde lid (AMvB)		
30(1) Notificatie inbreuk gegevensverwerking	Artikel 33a, eerste lid		
30(2) Verwerker informeert verantwoordelijke	Artikel 6c, vijfde lid		
30(3) Inhoud notificatie	Artikel 33a, tweede lid		
30(4) In fasen	Artikel 33a, derde lid		
30(5) Documentatie inbreuk	Artikel 32, eerste lid, onderdeel d		
30(6) Informeren verantwoordelijke andere LS	Artikel 33a, vierde lid		
31(1) Mededeling inbreuk aan betrokkene	Artikel 33a, vijfde lid		
31(2) Inhoud mededeling	Artikel 33a, vijfde lid		
31(3) Uitzonderingen mededeling	Artikel 33a, zesde lid		
31(4) Mededeling in opdracht van AP	artikel 35c, eerste lid, onderdeel e		
31(5) Uitstel c.q. afstel mededeling aan betrokkene	Artikel 33a, zevende lid		

Richtlijn	Wet politiegegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
32(1) Aanwijzing functionaris voor gegevensbescherming (FG)	Artikel 36, eerste lid	Mogelijkheid gerechten en andere onafhankelijke rechterlijke autoriteiten vrij te stellen van verplichting tot aanwijzing gegevens-beschermingsfunctionaris bij uitoefening van hun rechterlijke taken	Politiegegevens worden niet verwerkt door gerechten, zodat van deze mogelijkheid geen gebruik is gemaakt
32(2) Expertise FG	Artikel 36, tweede lid		
32(3) Een FG voor verschillende instanties	Artikel 36, eerste lid		
32(4) Publicatie contactgegevens	Artikel 36, vijfde lid		
33(1) Positie FG	Artikel 36, eerste lid		
33(2) Voldoende middelen FG	Artikel 36, vijfde lid		
34 Taken FG	Artikel 36, derde lid		
35(1) Algemene beginselen	Artikel 17a, eerste, tweede, derde, vierde en zesde lid		
35(2) Doorgiften zonder voorafgaande toestemming	Artikel 17a, vierde lid		
35(3) Toepassing zonder niveau RI te ondermijnen	Artikel 17a		
36(1) Adequaat beschermingsniveau	Artikel 17a, eerste lid		
36(2–6) Beoordeling adequaat beschermingsniveau	Behoeft geen implementatie. De voorschriften richten zich tot de Europese Commissie		
36(7) Intrekking laat uitzonderingen o.g.v. artikelen 35 en 36 onverlet	Artikel 17a, tweede en derde lid		
36(8) Publicatie besluit Commissie	Behoeft geen implementatie		
37(1) Voldoende waarborgen	Artikel 17a, tweede lid		
37(2) Informeren AP	Artikel 17a, tweede lid, onderdeel b		
37(3) Documentatie	Artikel 32, tweede lid en artikel 5:17 Awb*		
38(1) Afwijking specifieke situatie	Artikel 17a, derde lid		
38(2) Grondrechten prevaleren	Artikel 17a, derde lid		
38(3) Documentatie	Artikel 32, tweede lid		
39(1) Ontvanger in derde land	Artikelen 17a, vijfde lid en artikel 5:11, eerste lid, Bpg		
39(2) Internationale overeenkomst	Artikel 17a, vijfde lid (AMvB)		
39(3) Informeren AP	Artikel 17a, zevende lid (AMvB)		
39(4) Documentatie	Artikel 32, eerste lid, onderdeel b		
40 Internationale samenwerking	Behoeft geen afzonderlijke implementatie in wetgeving		
41(1) Aanwijzing toezichthoudende autoriteit (TA)	Artikel 35, eerste lid		

Richtlijn	Wet politiegegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
41(2) Samenwerking TA's	Artikel 35d, eerste lid		
41(3) TA op basis Avg	Mogelijkheid voor lidstaten om te kiezen dat toezichthoudende autoriteit als bedoeld in de richtlijn, dezelfde is als die op grond van de verordening is aangewezen. Van deze mogelijkheid is gebruik gemaakt; zie artikel 35, eerste lid	Mogelijkheid voor lidstaten om te kiezen dat toezichthoudende autoriteit als bedoeld in de richtlijn, dezelfde is als die op grond van de verordening is aangewezen	Van deze mogelijkheid is gebruik gemaakt. Dit sluit aan bij de bestaande situatie waarin het College bescherming persoonsgegevens toezicht houdt
41(4) Meerdere TA's opgericht	Mogelijkheid voor lidstaat meer dan een toezichthoudende autoriteit op te richten. Van deze mogelijkheid is geen gebruik gemaakt, zodat dit aansluit bij de huidige situatie waarin voor het toezicht op de Wet bescherming persoonsgegevens en de Wpg eveneens sprake is van dezelfde toezichthouder. Zie artikel 35, eerste lid, Wpg	Mogelijkheid voor lidstaat meer dan één toezichthoudende autoriteit op te richten	Van deze mogelijkheid is geen gebruik gemaakt. Dit sluit aan bij de huidige situatie waarin voor het toezicht op de Wet bescherming persoonsgegevens en de Wjsg sprake is van dezelfde toezichthouder
42(1) Onafhankelijk optreden	Artikel 35a, eerste lid		
42(2) Positie leden	Artikel 35a, derde lid		
42(3) Onthouden van handelingen	Artikel 35a, vierde lid en artikel 7, vierde en zesde lid, van de Uitvoeringswet Avg		
42(4) Voldoende middelen	Artikel 10, eerste lid, Uitvoeringswet Avg		
42(5) Eigen medewerkers	Artikel 10, eerste lid, Uitvoeringswet Avg		
42(6) Financiële controle	Artikel 13, tweede lid, Uitvoeringswet Avg		
43(1) Algemene voorwaarden	Artikel 7, derde lid, Uitvoeringswet Avg		
43(2) Kwaliteiten leden	Artikel 35a, tweede lid		
43(3) Einde taken lid	Artikel 7, vijfde lid, Uitvoeringswet Avg		
43(4) Ontslag lid	Artikel 8, eerste lid, Uitvoeringswet Avg		
44(1a) Wettelijke regeling	Artikelen 6 en 7 Uitvoeringswet Avg		
44(1b) Kwalificaties leden TA	Artikel 35a, tweede lid en artikel 7, tweede lid, Uitvoeringswet Avg		
44(1c) Benoeming leden TA	Artikel 7, derde lid, uitvoeringswet Avg		
44(1d) Ambtstermijn leden TA	Artikel 7, vierde lid, Uitvoeringswet Avg		
44(1e) Herbenoeming leden TA	Artikel 7, vijfde lid, Uitvoeringswet Avg		
44(1f) Voorwaarden plichten leden TA	Artikel 8 en artikel 10 Uitvoeringswet Avg		
44(2) Beroepsgeheim	Artikel 125, derde lid, Ambtenarenwet* en artikel 2:5 Awb*		
45(1) Bevoegdheid	Artikel 35, eerste lid		
45(2) Uitzondering gerechten	Artikel 51h, derde lid, Wjsg; gerechten verwerken in het kader van hun gerechtelijke taken gerechtelijke strafgegevens die te onderscheiden zijn van politiegegevens		
46(1) Taken TA	Artikel 35b, eerste lid		
46(2) Faciliteren klachten	Artikel 31a, vierde lid		
46(3) kosteloos	Artikel 35b, tweede lid		

Richtlijn	Wet politiegegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
46(4) Ongegronde verzoeken	Artikel 31a, zesde lid		
47(1) Bevoegdheden	Artikel 35, eerste lid en Titel 5.2 Awb		
47(2) Corrigeren	Artikel 35c		
47(3) Advies	Artikelen 35b, eerste lid, onderdeel b, j.o. 15 Uitvoeringswet Avg c.q. Kaderwet adviescolleges		
47(4) Rechterlijke toetsing	Artikelen 29, tweede lid, 31a, vijfde lid en 35c, derde lid; besluit in de zin van Awb		
47(5) Rechterlijke tussenkomst	Implementatietraject n.a.v. zaak C-362/14 (Schrems)		
48 Vertrouwelijke melding	Artikelen 2 en 3j Wet Huis voor klokkenluiders* (Stb. 2016, 147)		
49 Activiteitenverslag	Artikel 18 Kaderwet ZBO's*		
50(1) Wederzijdse hulp	Artikel 35d, eerste lid		
50(2) Zonder vertraging	Artikel 35d, tweede lid		
50(3) Verzoek om bijstand	Artikel 35d, derde lid		
50(4) Weigering	Artikel 35d, vierde lid		
50(5) Reactie	Artikel 35d, tweede lid		
50(6) Standaardformulier	Artikel 35d, zesde lid (AMvB)		
50(7) Bijstand kosteloos	Artikel 35d, vijfde lid		
50(8) Vastlegging model en procedures bijstand	Behoeft geen implementatie		
51(1–4) Comité gegevensbe-scherming	Behoeft geen implementatie. Voorschriften richten zich niet tot de lidstaten		
52(1) Klacht bij TA	Artikel 31a, eerste lid		
52(2) Doorsturen klacht	Artikel 31a, tweede lid		
52(3) Assistentie	Artikel 31a, derde lid		
52(4) Informatie subject	Artikel 31a en overigens Awb		
53(1) Rechterlijke tussenkomst TA	Artikel 35c, derde lid (zie 47, vierde lid) en Awb		
53(2) Idem bij niet reageren TA	Artikel 31a, vijfde lid en Awb		
53(3) Bevoegdheid gerecht bij TA	Artikel 31b		
54 Rechterlijke tussenkomst algemeen	Awb en Wetboek burgerlijke rechtsvordering		
55 Namens subject	Artikel 2:1 Awb* (en begrip belanghebbende)		
56 Recht op schadevergoeding	Artikel 31c		
57 Passende straffen	Artikel 35c, eerste lid, onderdeel b (bestuurlijke boete) en Wetboek van Strafrecht (o.a. ambtsmis-drijven)		
58 Comitéprocedure	Behoeft naar zijn aard geen implementatie		
59 Intrekking kaderbesluit	Behoeft naar zijn aard geen implementatie		

Richtlijn	Wet politiegegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
60 Reeds van kracht zijnde Unierechtshandelingen	Behoeft naar zijn aard geen implementatie in wetgeving gelet op respecterende werking van Unierechtshandelingen		
61 Verhouding tot reeds gesloten overeenkomsten	Behoeft naar zijn aard geen implementatie in wetgeving gelet op respecterende werking van Unierechtshandelingen		
62 Commissieverslagen	Behoeft geen implementatie. Voorschriften richten zich tot de Europese Commissie		
63(1) Omzetting	Behoeft naar zijn aard geen implementatie in wetgeving		
63(2 en 3) Extra termijn art. 25, eerste lid	Facultatieve bepaling	Mogelijkheid voor lidstaten tot latere implementatie ten aanzien van functies voor het bijhouden van logbestanden bij systemen voor geautomatiseerde verwerking	Zie artikel 32a Wpg jo. artikel VII
63(4) Extra termijn art. 25, eerste lid vanwege uitzonderlijke omstandigheden	Uitvoering door middel van feitelijk handelen		
64 Inwerkintreding	Behoeft naar zijn aard geen implementatie in wetgeving		
65 Adressanten	Behoeft naar zijn aard geen implementatie in wetgeving		

* Betreft bestaande wetsbepaling.

10.2 Implementatietabel van de Wet justitiële en strafvorderlijke gegevens

Richtlijn	Wet justitiële en strafvorderlijke gegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
Artikel 1(1) onderwerp	Aan dit artikelonderdeel wordt uitvoering gegeven door de algehele implementatie van de richtlijn bij en krachtens de Wjsg, waaronder voorschriften over te verwerken justitiële en strafvorderlijke gegevens, rapporten in persoonsdossiers, tenuitvoerleggingsgegevens en gerechtelijke strafgegevens		
Artikel 1(2a) verplichtingen	Behoeft geen afzonderlijke implementatie; aan dit artikelonderdeel wordt uitvoering gegeven door de algehele implementatie van de richtlijn		
Artikel 1(2b) verplichtingen	Behoeft geen implementatie; de huidige wet voorziet niet in een verbod of beperking op uitwisseling van persoonsgegevens tussen bevoegde autoriteiten als bedoeld in dit artikelonderdeel		
Artikel 1(3) uitgebreidere waarborgen op nationaal niveau	Van mogelijkheid is geen gebruik gemaakt	Lidstaten mogen uitgebreidere waarborgen bieden ter bescherming in verband met verwerking van persoonsgegevens dan de richtlijn voorschrijft	De implementatie van de richtlijn biedt voldoende waarborgen en het uitgangspunt van minimumimplementatie wordt gerespecteerd
Artikel 2(1) toepassingsgebied doeleinden	Artikelen 2, eerste lid*, 39a, eerste lid*, 40, eerste lid*, 51a, eerste lid en 51e		
Artikel 2(2) toepassing op persoonsgegevens in bestanden	Artikel 1, onderdelen a tot en met e		

Richtlijn	Wet justitiële en strafvorderlijke gegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
Artikel 2(3) uitsluiting activiteiten buiten Unierecht	Behoeft geen implementatie		
Artikel 3(1) definitie persoonsgegeven	Artikel 1, onderdelen i en j		
Artikel 3(2) definitie verwerking	Artikel 1, onderdeel m		
Artikel 3(3) definitie verwerkingsbeperking	Artikel 1, onderdeel n		
Artikel 3(4) definitie profilering	Artikel 1, onderdeel t		
Artikel 3(5) definitie pseudonimisering	Behoeft geen implementatie. Dit begrip keert terug in artikel 20, eerste lid, waarbij het als voorbeeld wordt aangehaald		
Artikel 3(6) definitie bestand	Artikel 1, onderdeel o		
Artikel 3(7) definitie bevoegde autoriteit	Artikel 1, onderdeel v		
Artikel 3(8) definitie verwerkingsverantwoordelijke	Artikel 1, onderdeel k		
Artikel 3(9) definitie verwerker	Artikel 1, onderdeel l		
Artikel 3(10) ontvanger	Artikel 1, onderdeel u		
Artikel 3(11) inbreuk op beveiliging	Artikel 1, onderdeel p		
Artikel 3(12) genetische gegevens	Artikel 1, onderdeel q		
Artikel 3(13) biometrische gegevens	Artikel 1, onderdeel r		
Artikel 3(14) gezondheidsgegevens	Artikel 1, onderdeel s		
Artikel 3(15) toezichthoudende autoriteit	Artikel 1, onderdeel z		
Artikel 3(16) internationale organisatie	Artikel 1, onderdeel x		
Artikel 4(1a) behoorlijk en rechtmatig	Artikelen 3, derde lid*, 39c, tweede lid, 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 4(1b) welbepaalde en gerechtvaardigde doelen	Artikelen 3, tweede lid*, 39b, eerste lid*, 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 4(1c) toereikend en proportioneel	Artikelen 3, derde lid*, 39c, tweede lid, 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 4(1d) juist en zo nodig geactualiseerd	Artikelen 3, eerste lid, 39c, eerste lid, 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 4(1e) niet langer bewaard dan nodig	Artikelen 3, zesde lid, 39c, eerste lid, 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 4(1f) passende middelen ter beveiliging	Artikelen 7, 39c, eerste lid, 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 4(2) verwerking voor ander doel dan doel 1(1)	Artikelen 3, vierde lid, 39c, eerste lid, 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 4(3) archivering en wetenschappelijk onderzoek	Reeds geïmplementeerd in artikel 15; zie voorts artikel 31 van het Bjsg		

Richtlijn	Wet justitiële en strafvorderlijke gegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
Artikel 4(4) naleving leden 1–3	Artikelen 7, eerste lid, onderdeel a, 39c, eerste lid, 40, derde lid, 51b, eerste lid en 51f		
Artikel 5 termijnen voor opslag en evaluatie	Artikelen 4* en 6*, 39d*, 41*, 51c, eerste lid en 51g		
Artikel 6 onderscheid categorieën betrokkenen	Artikelen 7c en 39b, tweede lid		
Artikel 7(1) onderscheid tussen persoonsgegevens en betrouwbaarheid	Behoeft geen implementatie. Dit onderscheid volgt voor zover mogelijk uit het onderscheid tussen de verschillende gedefinieerde gegevens. Justitiële gegevens zijn bijvoorbeeld veelal gegevens die gebaseerd zijn op een rechterlijke vaststelling en berusten niet op een persoonlijk subjectief oordeel		
Artikel 7(2) controle gegevens voor doorzending	Artikelen 3, eerste en vijfde lid, 39c, eerste lid, 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 7(3) kennisgeving ontvanger na op rechtmatige wijze doorgezonden en rectificatie	Artikelen 24, eerste lid, 39o, eerste lid, 48, 51b, eerste en derde lid en 51f		
Artikel 8(1) rechtmatigheid	Artikelen 3, derde lid, 39c, eerste lid, 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 8(2) wetgeving lidstaten	Implementatie bestaat uit de gehele Wjsg en het Bjsg voorziet hierin		
Artikel 9(1) verwerking voor andere doelen dan die van 1(1)	Artikelen 3, vierde lid, 39c, eerste lid, 40, derde lid en 51b, eerste en derde lid en 51f		
Artikel 9(2) Avg van toepassing op die verwerking	Behoeft geen implementatie gelet op de rechtstreekse toepasselijkheid van verordening 2016/679/EU in het Nederlandse recht		
Artikel 9(3) specifieke voorwaarden	Artikelen 16a, tweede lid, 39ga, eerste lid, 42a, eerste lid, 51b, eerste en derde lid en 51f		
Artikel 9(4) zelfde voorwaarden als nationaal	Artikelen 16a, eerste en tweede lid (AMvB), 39ga, eerste lid, 42a, eerste lid, 51b, eerste en derde lid en 51f		
Artikel 10 gevoelige persoonsgegevens	Artikelen 39c, derde lid, 40, derde lid, 51b eerste en derde lid en 51h, eerste lid. Behoeft geen implementatie voor wat betreft justitiële gegevens		
Artikel 11(1) profilering	Artikelen 7e, 39c, eerste lid, 40, derde lid, 51b, eerste en derde lid		
Artikel 11(2) gevoelige persoonsgegevens	Artikelen 39c, vierde lid, 40, derde lid, 51b, eerste en derde lid, 51h, eerste lid. Behoeft geen implementatie voor wat betreft justitiële gegevens. Dit zijn geen gevoelige persoonsgegevens		
Artikel 11(3) geen discriminatie	Artikelen 7e, tweede lid, 39c, vijfde lid en 40 derde lid, 51b, eerste en derde lid, en 51f		
Artikel 12(1) heldere informatie	Artikelen 17a en 17b, eerste lid, 39ha, eerste en tweede lid, 42b, 51b, eerste en derde lid en 51f		
Artikel 12(2) faciliteren	Verwerkt in titel 2, afdeling 3, titel 2a, afdeling 3, 43 e.v.		
Artikel 12(3) schriftelijk	Artikelen 21, eerste lid, 39l, eerste lid, 46a, eerste lid, 51b, eerste en derde lid, 51f		
Artikel 12(4) kosteloos en kennelijk ongegrond	Artikelen 25, 39p, 49, 51b, eerste en derde lid, 51f		

Richtlijn	Wet justitiële en strafvorderlijke gegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
Artikel 12(5) aanvullende informatie	Artikelen 20, eerste lid, 39k, eerste lid, tweede volzin, 45, 51b, eerste en derde lid, 51f		
Artikel 13(1) algemene informatie	Artikelen 17a, 39ha, eerste lid en 42b, 51b, eerste en derde lid, 51f		
Artikel 13(2) speciale informatie	Artikel 17b, tweede lid, 39ha, tweede lid, 42b, eerste lid, 51b, eerste en derde lid, 51f		
Artikel 13(3) weigeringsgronden speciale informatie	Mogelijkheid om verstrekking bepaalde informatie aan betrokkene uit te stellen, te beperken of achterwege te laten op bepaalde gronden	Mogelijkheid om verstrekking bepaalde informatie aan betrokkene uit te stellen, te beperken of achterwege te laten op bepaalde gronden	In het kader van minimumimplementatie is van deze mogelijkheid geen gebruik gemaakt
Artikel 13(4) generieke uitzonderingen	Mogelijkheid tot uitzondering	Mogelijkheid om verwerkingscategorieën vast te stellen waarvoor verstrekking van bepaalde informatie aan betrokkene niet van toepassing is	In het kader van minimumimplementatie is geen noodzaak gebleken van deze mogelijkheid gebruik te maken voor gegevens die onder Wjsg vallen
Artikel 14 recht op inzage	Artikel 18, 39i, eerste lid, 43, 51b, tweede lid en 51f		
Artikel 15(1) weigeringsgronden inzage	Artikelen 21, tweede lid, 39l, tweede lid, 46a, tweede lid, 51b, eerste en derde lid en 51f	Mogelijkheid tot beperking van inzagerecht voor betrokkene om bepaalde redenen	Gelet op het zwaarwegende karakter van de redenen, waaronder die inzake nationale veiligheid, is dit onderdeel van de implementatie
Artikel 15(2) generieke uitzonderingen	Mogelijkheid tot uitzondering	Mogelijkheid voor lidstaten te bepalen welke verwerkingscategorieën onder een beperking van het inzagerecht kunnen vallen	Er is geen noodzaak gebleken van deze mogelijkheid gebruik te maken voor gegevens die onder Wjsg vallen
Artikel 15(3) weigering schriftelijk en klacht	Artikelen 21, derde lid, 39l, derde lid, 46a, tweede lid, 51b, eerste en derde lid en 51f		
Artikel 15(4) documentatie	Artikelen 26d, eerste lid, onderdeel a, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		
Artikel 16(1) correctie	Artikelen 22, eerste lid, 39m, eerste lid, 46, eerste lid, 51b, eerste en derde lid en 51f		
Artikel 16(2) wissen	Artikelen 22, tweede lid, 39m, tweede lid, 46, tweede lid, 51b, eerste en derde lid en 51f		
Artikel 16(3) verwerkingsbeperking	Artikelen 22, derde lid, 39m, derde lid, 46, derde lid, 51b, eerste en derde lid en 51f		
Artikel 16(4) niet informeren	Artikelen 21, tweede en derde lid, 39l, tweede en derde lid, 46a, tweede lid, 51b, eerste en derde lid en 51f	Tweede volzin 16(4): mogelijkheid tot beperking van rectificatie, wissing of verwerkingsbeperking om bepaalde redenen	Gelet op het zwaarwegende karakter van die redenen, waaronder de nationale veiligheid, is dit onderdeel van de implementatie
Artikel 16(5) doorgeven rectificatie aan verstrekker	Artikelen 22, vijfde lid, 39m, vijfde lid, 46, vijfde lid, 51b, eerste en derde lid en 51f		
Artikel 16(6) informeren ontvangers	Artikelen 24, 39o, 48, 51b, eerste en derde lid en 51f		

Richtlijn	Wet justitiële en strafvorderlijke gegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
Artikel 17(1) controle TA	Artikelen 23, tweede lid, 26a, eerste lid, 39n, tweede lid, 39r, eerste lid, 47, tweede lid, 51, tweede lid, 51b, eerste lid, 51d, eerste lid, 51f en 51h, eerste en derde lid		
Artikel 17(2) in kennis stellen betrokkene	Artikelen 21, eerste lid, 39l, eerste lid, 46a, eerste lid, 51b, eerste en derde lid en 51f		
Artikel 17(3) informatie aan betrokkene	Behoeft geen implementatie. Betreft besluiten in de zin van de Awb waarvoor gelden plicht tot motivering (3:46 Awb*) en plicht tot kennisgeving van bezwaar en beroep (3:45 Awb*)		
Artikel 18	39ha, derde lid		
Artikel 19(1) technische maatregelen	Artikelen 7, eerste lid, onder a, derde en vijfde lid, 39c, eerste lid, 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 19(2) gegevensbescher-mingsbeleid	Artikelen 7, eerste lid, onder b en derde lid, 39c, eerste lid, 40 derde lid, 51b, eerste en derde lid en 51f		
Artikel 20(1) waarborgen privacy	Artikel 7, eerste lid, en derde lid, 39c, eerste lid, 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 20(2) standaardinstellin-gen	Artikel 7a, 39c, eerste lid, 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 21(1) gezamenlijke verwerkers + verplichtingen jegens betrokkene («kunnen bepaling»)	Behoeft geen implementatie. De situatie dat twee of meer verwerkingsverantwoordelijken gezamen-lijk de doeleinden en middelen bepalen voor verwerkingen onder de richtlijn, doet zich niet voor		
Artikel 21(2) uitoefening rechten jegens iedere verantwoordelijke («kunnen bepaling»)	Behoeft geen implementatie omdat dit geen verplichting betreft maar een mogelijkheid		
Artikel 22(1) garanties verwerker passende maatregelen	Artikelen 7d, eerste lid, 39c, eerste lid, 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 22(2) schriftelijke toestemming verantwoordelijke	Artikelen 7d, vierde lid, 39c, eerste lid en 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 22(3) inhoud contract met verwerker	Artikelen 7d, tweede lid, 39c, eerste lid en 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 22(4) schriftelijk contract	Artikel 7d, tweede lid, 39c, eerste lid en 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 22(5)	Artikel 1, onderdeel l		
Artikel 23	Artikel 7d, derde lid, 39c, eerste lid, 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 24(1) register verantwoor-delijke	Artikelen 26c, eerste lid, onderdelen a tot en met i, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		
Artikel 24(2) register verwerker	Artikelen 26c, tweede lid, onderdelen a tot en met d, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		
Artikel 24(3) schriftelijk	Artikelen 26c, eerste en tweede lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		
Artikel 24(4) register beschikbaar aan AP	Artikel 5:17, eerste lid, Awb		
Artikel 25(1) logging	Artikelen 26e, eerste lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		

Richtlijn	Wet justitiële en strafvorderlijke gegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
Artikel 25(2) gebruik logbestanden	Artikelen 26e, tweede lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		
Artikel 25(3) logbestanden beschikbaar AP	Artikel 5:17, eerste lid, Awb*		
Artikel 26 samenwerking met AP	Artikel 5.20 Awb*		
Artikel 27(1) PIA	Artikelen 7b, eerste lid, 39c, eerste lid, 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 27(2) inhoud PIA	Artikelen 7b, tweede lid, 39c, eerste lid, 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 28(1) consultatie AP	Artikelen 26h, eerste lid, 39r, tweede lid, 51, eerste lid,51d, eerste lid en 51h, eerste lid		
Artikel 28(2) consultatie wetgeving	Artikelen 27, tweede lid, jo. artikel 15 van de Uitvoeringswet Avg, 39r, eerste lid, 51, eerste lid en 51d, eerste lid en 51h, eerste lid		
Artikel 28(3) lijst consultatie	Artikelen 26h, tweede lid, 39r, tweede lid, 51, eerste lid,51d, eerste lid en 51h, eerste lid		
Artikel 28(4) PIA beschikbaar AP	Artikelen 26h, derde lid, 39r, tweede lid, 51, eerste lid, 51d, eerste lid, en 51h, eerste lid		
Artikel 28(5) advies AP	Artikelen 26h, vierde en vijfde lid, 39r, tweede lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		
Artikel 29(1) beveiliging verwerking	Artikelen 7, tweede en derde lid, 39c, eerste lid, 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 29(2) maatregelen beveiliging	Artikelen 7, zesde lid, 39c, eerste lid, 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 30(1) notificatie inbreuk gegevensverwerking	Artikelen 26g, eerste lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		
Artikel 30(2) verwerker informeert verantwoordelijke	Artikel 7d, vijfde lid, 39c, eerste lid en 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 30(3) inhoud notificatie	Artikelen 26g, tweede lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		
Artikel 30(4) in fasen	Artikelen 26g, derde lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		
Artikel 30(5) documentatie inbreuk	Artikelen 26d, eerste lid, onder c, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		
Artikel 30(6) informeren verantwoordelijke andere LS	Artikelen 26g, vierde lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		
Artikel 31(1) mededeling inbreuk aan betrokkene	Artikelen 26g, vijfde lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		
Artikel 31(2) inhoud mededeling	Artikelen 26g, vijfde lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		
Artikel 31(3) uitzonderingen mededeling	Artikelen 26g, zesde lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		
Artikel 31(4) mededeling in opdracht van AP	Artikelen 27, derde lid jo. artikel 35c, eerste lid, onderdeel e, van de Wpg, 39r, tweede lid, 51, tweede lid, 51d, tweede lid en 51h, tweede lid		
Artikel 31(5) uitstel c.q. afstel mededeling aan betrokkene	Artikelen 26g, zevende lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		

Richtlijn	Wet justitiële en strafvorderlijke gegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
Artikel 32(1) aanwijzing functionaris gegevensbescher-ming (FG)	Artikelen 26f, eerste lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid	Mogelijkheid gerechten en andere onafhankelijke rechterlijke autoriteiten vrij te stellen van verplichting tot aanwijzing gegevens-beschermingsfunctionaris bij uitoefening van hun rechterlijke taken	In het kader van mini-mumimplementatie is van deze mogelijkheid gebruik gemaakt voor gerechte-lijke strafgegevens
Artikel 32(2) expertise FG	Artikelen 26f, tweede lid, 39r, eerste lid, 51, eerste lid en 51d, eerste lid		
Artikel 32(3) een FG voor verschillende instanties	Artikel 26f, eerste lid, artikel 39r, eerste lid, 51, eerste lid en 51d, eerste lid		
Artikel 32(4) publicatie contact-gegevens	Artikelen 26f, vijfde lid, 39r, eerste lid, 51, eerste lid en 51d, eerste lid		
Artikel 33(1) positie FG	Artikel 26f, eerste lid, 39r, eerste lid, 51, tweede lid en 51d, eerste lid		
Artikel 33(2) voldoende middelen FG	Artikel 26f, zesde lid, 39r, eerste lid, 51, eerste lid en 51d, eerste lid		
Artikel 34 Taken FG	Artikelen 26f, derde lid, 39r, eerste lid, 51, eerste lid en 51d, eerste lid		
Artikel 35(1) algemene beginse-len	Artikelen 16a, 39e, 42a, tweede lid, 51b, eerste en derde lid en 51f		
Artikel 35(2) doorgiften zonder voorafgaande toestemming	Artikel 16a, vijfde lid, 39ga, tweede lid, 42a, tweede lid, 51b, eerste en derde lid en 51f		
Artikel 35(3) toepassing zonder niveau RI te ondermijnen	Artikel 16a, 39ga, tweede lid, 42a, tweede lid, 51b, eerste en derde lid en 51f		
Artikel 36(1) adequaat niveau	Artikelen 16a, eerste lid, 39ga, tweede lid, 42a, tweede lid, 51b, eerste en derde lid en 51f		
Artikel 36(2–6)	Behoeft geen implementatie. De voorschriften richten zich tot de Europese Commissie		
Artikel 36(7) intrekking laat uitzonderingen o.g.v. artikelen 37 en 38 onverlet	Artikel 16a, tweede en derde lid, 39ga, tweede lid, 42a, tweede lid, 51b, eerste en derde lid en 51f		
Artikel 36(8) publicatie besluit Commissie	Behoeft geen implementatie		
Artikel 37(1) voldoende waarborgen	Artikelen 16a, tweede lid, 39ga, tweede lid, 42a, tweede lid, 51b, eerste en derde lid en 51f		
Artikel 37(2) informeren AP	Artikelen 16a, tweede lid, laatste volzin, 39ga, tweede lid, 42a, tweede lid, 51b, eerste en derde lid en 51f		
Artikel 37(3) documentatie	Artikelen 26d, eerste lid, onderdeel b en tweede lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		
Artikel 38(1) afwijking specifieke situatie	Artikelen 16a, derde lid, 39ga, tweede lid, 42a, tweede lid, 51b, eerste en derde lid en 51f		
Artikel 38(2) grondrechten prevaleren	Artikelen 16a, derde lid, 39ga, tweede lid, 42a, tweede lid, 51b, eerste en derde lid en 51f		
Artikel 38(3) documentatie	Artikelen 26d, eerste lid, onderdeel b en tweede lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		

Richtlijn	Wet justitiële en strafvorderlijke gegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
Artikel 39(1) ontvanger in derde land	Artikelen 16a, vierde lid, 39ga, tweede lid, 42a, tweede lid, 51b, eerste en derde lid en 51f		
Artikel 39(2) – definitie	Artikel 16a, vierde lid (AmvB), 39ga, tweede lid, 42a, tweede lid, 51b, eerste en derde lid en 51f		
Artikel 39(3) informeren TA	Artikelen 16a, vierde lid (AmvB), 39ga, tweede lid, 42a, tweede lid, 51b, eerste en derde lid en 51f		
Artikel 39(4) documentatie	Artikelen 26d, eerste lid, onderdeel b, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		
Artikel 40 samenwerking derde landen	Behoeft geen afzonderlijke implementatie in wetgeving		
Artikel 41(1) aanwijzing toezichthoudende autoriteit (TA)	Artikelen 27, eerste lid, 39r, eerste lid, 51, eerste lid en 51d, eerste lid en 51h, eerste en zesde lid		
Artikel 41(2) samenwerking TA's	Artikelen 27, derde lid, jo. 35d, eerste lid, van de Wpg, 39r, tweede lid, 51, tweede lid en 51d, tweede lid en 51h, tweede lid		
Artikel 41(3) TA op basis Vo	Artikelen 27, eerste lid, 39r, tweede lid, 51, tweede lid en 51d, tweede lid en 51h, eerste en derde lid	Mogelijkheid voor lidstaten om te kiezen dat toezichthoudende autoriteit als bedoeld in de richtlijn, dezelfde is als die op grond van de verordening is aangewezen	Van deze mogelijkheid is gebruik gemaakt. Dit sluit aan bij de bestaande situatie waarin het College bescherming persoonsgegevens (in het wetsvoorstel de AP) toezicht houdt
Artikel 41(4) meerdere TA's opgericht	Facultatieve bepaling	Mogelijkheid voor lidstaat meer dan één toezichthoudende autoriteit op te richten	Van deze mogelijkheid is geen gebruik gemaakt. Dit sluit aan bij de huidige situatie waarin voor het toezicht op de Wet bescherming persoonsgegevens en de Wjsg sprake is van dezelfde toezichthouder
Artikel 42(1) onafhankelijkheid TA	Artikelen 27, derde lid jo. 35a, eerste lid, van de Wpg, 39r, tweede lid, 51, tweede lid,51d, tweede lid en 51h, tweede lid		
Artikel 42(2) positie leden	Artikelen 27, derde lid jo. 35a, derde lid, van de Wpg, 39r, tweede lid, 51, tweede lid,51d, tweede lid en 51h, tweede lid		
Artikel 42(3) onthouden van handelingen	Artikelen 27, derde lid jo. 35a, vierde lid, van de Wpg, 39r, tweede lid, 51, tweede lid,51d, tweede lid en 51h, tweede lid		
Artikel 42(4 en 5) voldoende middelen en eigen medewerkers	Artikel 10, eerste lid, Uitvoeringswet Avg		
Artikel 42(6) financiële controle	Artikel 13, tweede lid, Uitvoeringswet Avg		
Artikel 43(1) benoeming	Artikel 7, derde lid, Uitvoeringswet Avg		
Artikel 43(2) kwaliteit leden	Artikelen 27, derde lid jo. 35a, tweede lid, van de Wpg, 39r, tweede lid, 51, tweede lid, 51d, tweede lid en 51h, tweede lid		
Artikel 43(3)	Artikel 7, vijfde lid, Uitvoeringswet Avg		
Artikel 43(4)	Artikel 8, eerste lid, Uitvoeringswet Avg		
Artikel 44(1a) oprichting TA	Artikel 6 Uitvoeringswet Avg		

Richtlijn	Wet justitiële en strafvorderlijke gegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
Artikel 44(1b) kwalificaties leden TA	Artikel 7, tweede lid, Uitvoeringswet Avg		
Artikel 44(1c) benoeming leden TA	Artikel 7, derde lid, Uitvoeringswet Avg		
Artikel 44(1d) ambtstermijn leden TA	Artikel 7, vierde lid, Uitvoeringswet Avg		
Artikel 44(1e) herbenoeming leden TA	Artikel 7, vijfde lid, Uitvoeringswet Avg		
Artikel 44(1f) voorwaarden plichten leden TA	Artikel 8, Uitvoeringswet Avg		
Artikel 44(2) beroepsgeheim	Artikel 125a, derde lid, van de Ambtenarenwet* en artikel 2:5 Awb*		
Artikel 45(1) competentie	Artikelen 27, eerste lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste en zesde lid		
Artikel 45(2) geen TA op gerechten In de Nederlandse vertaling moet staan «niet belast» i.p.v. «belast»	Het toezicht door de AP strekt zich in het voorstel niet uit tot gerechtelijke strafgegevens ter uitoefening van gerechtelijke taken; Artikel 51h, zesde lid		
Artikel 46(1) taken TA	Artikel 27, derde lid, jo. 35b, eerste lid, van de Wpg, 39r, tweede lid, 51, tweede lid, 51d, tweede lid en 51h, tweede lid		
Artikel 46(2) faciliteren klachten	Artikelen 26a, vierde lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste en zesde lid		
Artikel 46(3) Kosteloos	Artikelen 27, derde lid, jo. 35b, tweede lid, van de Wpg, 39r, tweede lid, 51, tweede lid, 51d, tweede lid en 51h, tweede lid		
Artikel 46(4) ongegronde verzoeken	Artikelen 26a, zesde lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid		
Artikel 47(1) onderzoeksbe-voegdheden	Artikel 27, eerste lid, 39r, tweede lid, 51, tweede lid, 51d, tweede lid, 51h, tweede en derde lid, artikel 16 Uitvoeringswet Avg en Titel 5.2 van de Awb		
Artikel 47(2) corrigerende maatregelen TA	Artikelen 27, vierde lid, 39r, derde lid, 51, derde lid, 51d, derde lid en 51h, derde en zesde lid		
Artikel 47(3) adviezen	Artikelen 27, tweede lid, 27, vierde lid, onderdeel d, 39r, eerste lid en derde lid, onderdeel d, 51, eerste lid en derde lid, onderdeel d, 51d, eerste lid en derde lid, onderdeel d, 51h, eerste lid en derde lid, onderdeel d, c.q. Kaderwet adviescolleges		
Artikel 47(4) passende waarbor-gen bevoegdheden	Artikelen 23, tweede lid, 26a, vijfde lid, 27, vijfde en zesde lid, 39n, tweede lid, 39r, eerste lid, 47, tweede lid, 51, eerste, vierde en vijfde lid, 51b, eerste lid, 51d, eerste, vierde en vijfde lid en 51h, vierde en vijfde lid; besluit in de zin van de Awb waartegen bezwaar en beroep openstaat		
Artikel 47(5)	Implementatietraject n.a.v. zaak C-362/14 (Schrems)		
Artikel 48 vertrouwelijke melding	Artikelen 2 en 3j Wet Huis voor klokkenluiders* (Stb. 2016, 147)		
Artikel 49 activiteitenverslag	Artikel 18 Kaderwet ZBO's*		

Richtlijn	Wet justitiële en strafvorderlijke gegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
Artikel 50 (1)wederzijdse bijstand	Artikelen 27, derde lid jo. 35d, eerste lid, van de Wpg, 39r, tweede lid, 51, tweede lid, 51d, tweede lid en 51h, tweede en zesde lid		
Artikel 50(2) zonder vertraging	Artikelen 27, derde lid jo. 35d, tweede lid, van de Wpg, 39r, tweede lid, 51, tweede lid, 51d, tweede lid en 51h, tweede en zesde lid		
Artikel 50(3) verzoek om bijstand	Artikelen 27, derde lid jo. 35d, derde lid, van de Wpg, 39r, tweede lid, 51, tweede lid, 51d, tweede lid en 51h, tweede en zesde lid		
Artikel 50(4) weigering	Artikelen 27, derde lid jo. 35d, vierde lid, van de Wpg, 39r, tweede lid, 51, tweede lid, 51d, tweede lid en 51h, tweede en zesde lid		
Artikel 50(5) reactie	Artikelen 27, derde lid jo. 35d, tweede lid, van de Wpg, 39r, tweede lid, 51, eerste lid, 51d, tweede lid en 51h, tweede en zesde lid		
Artikel 50(6) standaardformulier	Artikelen 27, derde lid jo. 35d, zesde lid (amvb), van de Wpg, 39r, tweede lid, 51h, tweede lid, 51d, tweede lid en 51h, tweede en zesde lid		
Artikel 50(7)	Artikelen 26h, eerste lid jo. 35d, vijfde lid, van de Wpg, 39r, tweede lid, 51, tweede lid, 51d, tweede lid en 51h, tweede en zesde lid		
Artikel 50(8)	Behoeft geen implementatie		
Artikel 51(1–4) Comité gegevens-bescherming	Behoeft geen implementatie. Voorschriften richten zich niet tot de lidstaten		
Artikel 52(1) klacht bij TA	26a, eerste lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste en zesde lid		
Artikel 52(2) doorzending bij indiening verkeerde TA	26a, tweede lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste en zesde lid		
Artikel 52(3) bijstand verlenen door TA	26a, derde lid, 39r, eerste lid, 51, eerste lid,51d, eerste lid en 51h, eerste en zesde lid		
Artikel 52(4) informeren voortgang en beroep	26a, vijfde lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste en zesde lid en de artikelen 3:45 en 6:23 Awb*		
Artikel 53(1) rechterlijke tussenkomst TA	Artikelen 26a, vijfde lid, tweede volzin, 39r, 51, 51d en 51h, eerste en zesde lid		
Artikel 53(2) voorziening in rechte bij niet behandelen klacht	Artikelen 26a,vijfde lid, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste en zesde lid, en Awb		
Artikel 53(3) Vordering instellen bij gerecht van lidstaat vestiging TA	Artikelen 26b, 39r, eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste en zesde lid		
Artikel 54 voorziening in rechte tegen verwerkingsverantwoorde-lijke of verwerker	Beroep bij de bestuursrechter op grond van artikel 8:1 Awb* en dagvaarding op grond van de tweede Titel van het Wetboek burgerlijke rechtsvordering		
Artikel 55 vertegenwoordiging «namens opgericht» orgaan	Artikel 2:1 Awb* (en begrip belanghebbende)		
Artikel 56 recht op schadever-goeding	Artikelen 7f, 39c, eerste lid en 40, derde lid, 51b, eerste en derde lid en 51f		
Artikel 57 Straffen	Artikelen 27, vierde lid, 39r, derde lid, 51, derde lid en 51d, derde lid, 51h, derde en zesde lid, en Awb		

Richtlijn	Wet justitiële en strafvorderlijke gegevens	Omschrijving beleids-ruimte	Toelichting op keuze bij invulling beleidsruimte
Artikel 58 Comitéprocedure	Behoeft naar zijn aard geen implementatie		
Artikel 59 intrekking kaderbesluit	Behoeft naar zijn aard geen implementatie		
Artikel 60 reeds van kracht zijnde Unierechtshandelingen	Behoeft naar zijn aard geen implementatie in wetgeving gelet op respecterende werking van Unierechtshandelingen		
Artikel 61 verhouding tot reeds gesloten overeenkomsten	Behoeft naar zijn aard geen implementatie in wetgeving gelet op respecterende werking van Unierechtshandelingen		
Artikel 62 Commissieverslagen	Behoeft geen implementatie. Voorschriften richten zich tot de Europese Commissie		
Artikel 63(1) omzetting	Behoeft naar zijn aard geen implementatie in wetgeving		
Artikel 63(2 en 3) extra termijn art. 25, eerste lid	Facultatieve bepaling	Mogelijkheid voor lidstaten tot latere implementatie ten aanzien van functies voor het bijhouden van logbestanden bij systemen voor geautomatiseerde verwerking	Artikelen 26e, 39r,eerste lid, 51, eerste lid, 51d, eerste lid en 51h, eerste lid, juncto artikel VII
Artikel 63(4) extra termijn art. 25, eerste lid vanwege uitzonderlijke omstandigheden	Uitvoering door middel van feitelijk handelen		
Artikel 64 Inwerkingtreding	Behoeft naar zijn aard geen implementatie in wetgeving		
Artikel 65 Adressanten	Behoeft naar zijn aard geen implementatie in wetgeving		

* Betreft bestaande wetsbepaling.

Artikelsgewijs

I. Wet politiegegevens

Artikel I, onderdeel A

Artikel 1 (definities)

In de richtlijn is een aantal begripsomschrijvingen opgenomen. De begripsomschrijvingen van de richtlijn geven aanleiding tot aanpassing van de omschrijving van een aantal begrippen in de Wpg. In de Wpg wordt thans voor een aantal begripsomschrijvingen verwezen naar de Wbp. De Wbp komt echter te vervallen. Aldus vloeit de noodzaak tot aanvulling van de begripsomschrijvingen voort uit de omschrijvingen in de richtlijn en uit het vervallen van de Wbp. Dit betreft het volgende:

Onderdeel a

Het begrip politiegegeven heeft betrekking op een persoonsgegeven dat wordt verwerkt met het oog op de voorkoming van, onderzoek naar en opsporing van strafbare feiten of de uitoefening van de politietaak, bedoeld in de artikelen 3 en 4 van de Politiewet 2012, met uitzondering van de taken en voorschriften met betrekking tot de uitvoering van de Vreemdelingenwet 2000. De uitvoering van wettelijke voorschriften gesteld bij of krachtens de Vreemdelingenwet 2000 behoren tot de taken ten dienste van de justitie, die onderdeel vormen van de politietaak als

bedoeld in artikel 3 PW 2012 (art. 1, eerste lid, onderdeel i, onder 1°, PW 2012). Aan de Koninklijke marechaussee is een aantal politietaken opgedragen, waaronder de uitvoering van de bij of krachtens de Vreemdelingenwet 2000 opgedragen taken, waaronder begrepen de bediening van de daartoe door Onze Minister voor Immigratie en Asiel aangewezen doorlaatposten en het, voor zover in dat verband noodzakelijk, uitvoeren van de politietaak op en nabij deze doorlaatposten, alsmede het verlenen van medewerking bij de aanhouding of voorgeleiding van een verdachte of veroordeelde (art. 4, eerste lid, onderdeel f, PW 2012).
De aanpassing van dit begrip is reeds in het algemeen deel aan de orde gekomen (par. 5.2.1.).
In aanvulling daarop kan nog worden opgemerkt dat de Wpg, op basis van de Wet ter voorkoming van witwassen en financieren van terrorisme (hierna: Wvwft), van toepassing blijft op de verwerking van persoonsgegevens door de zogenaamde Financiële inlichtingeneenheid. De Financiële inlichtingeneenheid valt onder de verantwoordelijkheid van het Ministerie van Justitie en Veiligheid en is belast met het verzamelen en analyseren van meldingen rond zogenoemde ongebruikelijke transacties door financiële instellingen. Op de verwerking van persoonsgegevens door de Financiële inlichtingen eenheid zijn een aantal artikelen van de Wpg overeenkomstige toepassing[11], met dien verstande dat voor de Financiële inlichtingeneenheid als verantwoordelijke in de zin van artikel 1, onderdeel f, van die wet wordt aangemerkt Onze Minister van Justitie en Veiligheid. De betreffende bepalingen in de Wvwft en het Bpg worden aangepast, voor zover dit voortvloeit uit de implementatie van de richtlijn.

Onderdeel b

In de richtlijn wordt het begrip persoonsgegeven omschreven als informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatiemiddel, zoals een naam, een identificatienummer, locatiegegevens, een online identificatiemiddel of van één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (art. 1, eerste lid, onderdeel 1, RI). Deze omschrijving is identiek aan die van de verordening (art. 4, onder 1, Avg).

Onderdeel c

Het begrip verwerken van politiegegevens behoeft redactionele aanpassing. Dit betreft de toevoeging van het element van het al dan niet op geautomatiseerde wijze uitvoeren van de verwerking van politiegegevens en van het structureren en het opslaan van politiegegevens.

Onderdeel f

In de richtlijn wordt het begrip verwerkingsverantwoordelijke gehanteerd (hierna ook: de verantwoordelijke). Met dit begrip wordt gedoeld op de persoon of instantie die thans in de Wpg en de Wjsg wordt aangeduid als de verantwoordelijke. De verwerkingsverantwoordelijke wordt omschreven als de bevoegde autoriteit die, alleen of samen met andere, de doeleinden van en de middelen voor de verwerking van persoonsgegevens vaststelt (art. 1, eerste lid, onderdeel 8, RI). De richtlijn biedt de

[11] Dit betreft thans de artikelen 1, 2, 3, eerste en tweede lid, 4, 5, 6, 7, 15, 16, eerste lid, onderdelen a, b en c, 17, 18, 22 en 23, 25 tot en met 31, alsmede artikel 33 Wpg.

lidstaten de mogelijkheid om de verwerkingsverantwoordelijke bij wet aan te wijzen (art. 3, eerste lid, onderdeel g, RI).
Het begrip verwerkingsverantwoordelijke is in de Wpg nader gespecificeerd. De richtlijn is van toepassing op de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid. Dit betekent dat de richtlijn ook van toepassing is op de verwerking van persoonsgegevens door buitengewoon opsporingsambtenaren. Dit is in het algemeen deel reeds aan de orde gekomen. Dit zal worden geregeld door aanpassing van artikel 46 van de wet, dat voorziet in de mogelijkheid om onderdelen van het bij of krachtens deze wet bepaalde van overeenkomstige toepassing te verklaren op de verwerking van persoonsgegevens door een bijzondere opsporingsdienst. In het Besluit politiegegevens bijzondere opsporingsdiensten is de verantwoordelijke aangewezen voor de verwerking van politiegegevens door een bijzondere opsporingsdienst. In dit besluit zal ook de van overeenkomstige toepassing van onderdelen van de Wpg op de verwerking van politiegegevens door een buitengewone 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.

Onderdeel h

De AP is belast met het toezicht op de naleving van het bij of krachtens deze wet gestelde. De instelling van de AP is geregeld in de Wet ter uitvoering van de Algemene verordening gegevensbescherming en ter implementatie van de hoofdstukken VI, VII en VIII van de richtlijn gegevensbescherming opsporing en vervolging. In aanvulling daarop wordt in deze wet de taken en bevoegdheden van de AP geregeld, voor zover dit betrekking heeft op de implementatie van de richtlijn gegevensbescherming opsporing en vervolging.

Onderdeel i

De richtlijn bevat een omschrijving van het begrip verwerker (art. 3, eerste lid, onder 9, RI). De verwerker is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, die of dat namens de verwerkingsverantwoordelijke persoonsgegevens verwerkt. In andere taalversies van de richtlijn gebezigde bewoordingen als in het Engels «on behalf of», in het Duits «im Auftrag»» en in het Frans «pour le compte» zijn in het Nederlands vertaald als: namens. Juister ware het geweest indien aangesloten was bij de Nederlandse vertaling uit de verordening door te kiezen voor de woorden «ten behoeve van», die eveneens werden gebruikt in de Privacyrichtlijn (art. 2, onderdeel e). Aangezien in andere taalversies op dit punt geen enkel verschil in bewoordingen bestaat tussen de verordening en de richtlijn, dient de richtlijn hierin niet op andere wijze te worden opgevat dan de verordening. Behoudens de wijziging van de term «bewerker» in die van «verwerker» verandert daarmee de afbakening van dit begrip ten opzichte van de huidige Wpg en Wjsg inhoudelijk niet.
In de richtlijn is bepaald dat als een verwerker als verwerkingsverantwoordelijke wordt beschouwd als hij in strijd met de richtlijn als zodanig optreedt (art. 22, vijfde lid, RI). De verplichtingen van de verwerkingsverantwoordelijke zijn dan van toepassing op de verwerker.
In de richtlijn worden soms verplichtingen opgelegd aan de verwerkingsverantwoordelijke (bijvoorbeeld artikelen 12, 13, 19, 20, 24, 30, 32 RI) en soms aan de verwerkingsverantwoordelijke en de verwerker (bijvoorbeeld

artikelen 25, tweede lid, 26, 28, 29 RI). Aangenomen moet worden dat in die gevallen waarin een verplichting uitsluitend geldt voor een verantwoordelijke, ook de verwerker gehouden is daaraan te voldoen. Dit zal in de overeenkomst kunnen worden vastgelegd.

Onderdeel l

De richtlijn bevat een omschrijving van het begrip bevoegde autoriteit (art. 3, eerste lid, onderdeel 7, RI). In het algemeen deel van deze memorie is reeds ingegaan op de invulling van dit begrip in de Wpg en de Wjsg (par. 5.2.1. en 5.2.2.).
In aanvulling hierop kan worden opgemerkt dat particuliere beveiligings- en recherchebureaus geen bevoegde autoriteiten zijn in de zin van de richtlijn. Deze bureaus zijn krachtens het recht niet gemachtigd openbaar gezag en openbare bevoegdheden uit te oefenen met het oog op de opsporing van strafbare feiten. De verwerking van persoonsgegevens door deze bureaus valt onder het toepassingsgebied van de verordening.

Onderdeel p

De richtlijn bevat een omschrijving van het begrip ontvanger (art. 3, eerste lid, onderdeel 10, RI). Dir betreft een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden bekendgemaakt.

Onderdeel q

In de richtlijn wordt een inbreuk op de beveiliging omschreven als een inbreuk op de beveiliging met de vernietiging, het verlies, de wijziging, de bekendmaking of de ter beschikkingstelling van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte politiegegevens, hetzij per ongeluk, hetzij onrechtmatig, tot gevolg. Deze omschrijving is identiek aan die van de verordening (art. 4, onderdeel 12, Avg).
Met de implementatie van de richtlijn wordt voorzien in een verplichting voor de melding van datalekken voor de instanties die zijn belast met de opsporing en vervolging van strafbare feiten en de tenuitvoerlegging van straffen.

Onderdeel r

De omschrijving van het begrip genetische gegevens is identiek aan die van de verordening. De omschrijving van dit begrip is relevant voor de verwerking van bijzondere categorieën van persoonsgegevens (art. 5 Wpg).

Onderdeel s

De omschrijving van het begrip biometrische gegevens is identiek aan die van de verordening. Deze omschrijving is eveneens relevant voor de verwerking van bijzondere categorieën van persoonsgegevens (art. 5 Wpg).

Onderdeel t

De omschrijving van het begrip gegevens over gezondheid is identiek aan die van de verordening. Deze omschrijving is eveneens relevant voor de verwerking van bijzondere categorieën van persoonsgegevens (art. 5 Wpg).

Onderdeel u

De richtlijn bevat een omschrijving van het begrip profilering (art. 3, eerste lid, onder 4, RI). Dit betreft elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van die gegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met de bedoeling met name aspecten betreffende zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen. Deze omschrijving is identiek aan die van de verordening en sluit nauw aan bij de huidige omschrijving in de Wbp.

Onderdeel v

De richtlijn bevat geen omschrijving van het begrip derde land. Opneming van een omschrijving van dit begrip in de Wpg is echter noodzakelijk vanwege de regeling in de richtlijn voor de doorgifte van persoonsgegevens aan derde landen. Daarbij gaat de richtlijn uit van een onderscheid tussen lidstaten en derde landen. Dit onderscheid is echter materieel minder eenduidig omdat sommige lidstaten ervoor kunnen kiezen om de richtlijn niet te implementeren. Voor de toepassing van de richtlijn gelden de betreffende lidstaten dan als een derde land. Dit betreft de lidstaten Denemarken, Ierland en het Verenigd Koninkrijk. Het Verenigd Koninkrijk en Ierland zijn niet gebonden door de richtlijn wanneer deze landen niet gebonden zijn door de regels betreffende de vormen van justitiële samenwerking in strafzaken of van politiële samenwerking in het kader waarvan de op grond van artikel 16 VWEU vastgestelde bepalingen moeten worden nageleefd (overweging 99 RI)[12]. Binnen een termijn van zes maanden na de vaststelling van deze richtlijn dient Denemarken te beslissen of het deze richtlijn in het nationale recht zal omzetten (overweging 100 RI)[13]. Andersom geldt dat bepaalde landen, die geen lid zijn van de Europese Unie, gebonden kunnen zijn door de richtlijn vanwege de deelname aan Schengen. Dit betreft landen als Noorwegen, IJsland en/of Zwitserland. Wat IJsland, Noorwegen, Zwitserland en Liechtenstein betreft vormt deze richtlijn een ontwikkeling van de bepalingen van het Schengenacquis[14] [15] [16].

Onderdeel w

De richtlijn bevat een omschrijving van het begrip internationale organisatie in (art. 3, eerste lid, onderdeel 16, RI). Dit vanwege de regeling in de richtlijn tot doorgifte van politiegegevens aan een internationale organisatie. Dit is een organisatie en de daaronder ressorterende

---

[12] Artikel 6bis van Protocol nr. 21. Betreffende de positie van het Verenigd Koninkrijk en Ierland ten aanzien van de ruimte van vrijheid, veiligheid en recht, dat gehecht is aan het VEU en het VWEU.

[13] Artikel 4 van Protocol Nr. 22 betreffende de positie van Denemarken, dat gehecht is aan het VEU en het VWEU.

[14] Overeenkomst tussen de Raad van de Europese Unie en de Republiek IJsland en het Koninkrijk Noorwegen inzake de wijze waarop IJsland en Noorwegen worden betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis (Pb L 176 van 10-07-1999, blz. 36).

[15] Overeenkomst tussen de Europese Unie, de Europese gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis (Pb L 53 van 27-02-2008, blz. 52).

[16] Protocol tussen de Europese Unie, de Europese gemeenschap, de Zwitserse Bondsstaat en het Vorstendom Liechtenstein betreffende de toetreding van het Vorstendom Liechtenstein tot de Overeenkomst tussen de Europese Unie, d Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis.

internationaalpubliekrechtelijke organen of andere organen die zijn opgericht bij of op grond van een overeenkomst tussen twee of meer landen. Voor een dergelijke instantie kan worden gedacht aan Interpol. Wanneer persoonsgegeven worden doorgegeven aan Interpol, en aan landen die vertegenwoordigers naar Interpol hebben afgevaardigd, dient deze richtlijn van toepassing te zijn (overweging 25 RI). De doorgifte van gegevens aan EU-organen valt hier niet onder.

Onderdeel y

De omschrijving van het begrip lidstaat sluit uit dat dit een derde land kan zijn. Zoals hiervoor bij het begrip derde land is toegelicht zijn niet alle lidstaten van de Europese Unie gehouden tot implementatie van de richtlijn. Indien een lidstaat de richtlijn niet heeft geïmplementeerd kan niet als vaststaand worden aangenomen dat een toereikend beschermingsniveau voor persoonsgegevens wordt geboden. De desbetreffende lidstaat is in dat geval voor de toepassing van de richtlijn op één lijn te stellen met een derde land, waarvoor specifieke voorschriften bij doorgifte gelden die gebaseerd zijn op een voorafgaande beoordeling van het beschermingsniveau. Een lidstaat in de zin van deze wet betreft daarmee uitsluitend lidstaten van de Europese Unie die de richtlijn hebben geïmplementeerd.

Artikel I, onderdeel B

Artikel 2 (reikwijdte)

Voor de toelichting op dit artikel wordt verwezen naar het algemeen deel van deze memorie (par. 4.1.). Aanvullend kan nog worden opgemerkt dat de wet van toepassing is op de verwerking van politiegegevens die in een bestand zijn opgenomen of bestemd zijn daarin te worden opgenomen. De bescherming van natuurlijke personen door de richtlijn dient te gelden bij zowel de geautomatiseerde verwerking van persoonsgegevens als handmatige verwerking daarvan als gegevens zijn opgeslagen of bedoeld zijn om te worden opgeslagen in een bestand. Dossiers of een verzameling van dossiers en de omslagen ervan die niet volgens specifieke criteria zijn gestructureerd, mogen niet onder het toepassingsgebied van de richtlijn vallen (overweging 18 RI).

Artikel I, onderdeel C

Artikel 3 (noodzakelijkheid, rechtmatigheid en doelbinding)

Tweede lid

In dit lid is het vereiste ingevoegd van een «behoorlijke» verwerking. Dit betreft de vertaling van het Engelse woord «fair», dat in de richtlijn wordt gebruikt maar dat in het Nederlandse recht echter geen specifieke juridische betekenis heeft (art. 4, eerste lid, onder a, RI). Mede op grond daarvan was dit beginsel in de Wet bescherming persoonsgegevens anders verwoord (art. 6 Wbp). Zouden persoonsgegevens «oneerlijk» worden verwerkt, dan is dit in het Nederlands recht in strijd met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt. Blijkens artikel 6:162 BW is er dan al sprake van onrechtmatigheid. Daardoor wordt het begrippenpaar «eerlijk en rechtmatig» een tautologie (Kamerstukken II 1997/98, 25 892, nr. 3., blz. 78). Het beginsel van behoorlijke verwerking is overigens een ander begrip dan het recht op een onpartijdig gerecht zoals omschreven in artikel 47 van het handvest van de grondrechten en artikel 6 van het Europees Verdrag tot bescherming

van de Rechten van de Mens en de fundamentele vrijheden (EVRM) (overweging 26 RI).

Derde lid

In dit lid wordt geregeld de verdere verwerking van de persoonsgegevens, die zijn verwerkt voor een doel binnen de richtlijntaak (art. 1, onderdeel a, RI) voor een ander doel binnen het toepassingsgebied van de richtlijn. Dit betreft bijvoorbeeld de verdere verwerking van politiegegevens, die zijn verzameld voor een opsporingsonderzoek, voor de strafvervolging of de verdere verwerking van gegevens, die zijn verwerkt in het kader van de strafvervolging, voor de tenuitvoerlegging van een straf. Op grond van de richtlijn is een wettelijke regeling vereist, binnen de kaders van de proportionaliteit. De verdere verwerking van politiegegevens ten behoeve van de strafvordering is geregeld in artikel 16, eerste lid, onder a, Wpg.

Vierde lid

In dit lid wordt geregeld de verdere verwerking van de persoonsgegevens, die zijn verwerkt voor een doel binnen de richtlijntaak voor een ander doel buiten het toepassingsgebied van de richtlijn. Dit betreft dus een doel dat geen betrekking heeft 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. Dit betreft bijvoorbeeld de verstrekking van persoonsgegevens aan andere personen en instanties met het oog op doelen die niet onverenigbaar zijn met de opsporing en vervolging van strafbare feiten. Deze verstrekking is geregeld in de artikelen 18 tot en met 20 Wpg, en nader uitgewerkt in paragraaf 4 Bpg.

Artikel I, onderdeel D

Artikel 4 (juistheid en volledigheid politiegegevens)

Eerste lid

In dit lid is de algemene verlichting voor de verwerkingsverantwoordelijke opgenomen om de nodige maatregelen te treffen opdat politiegegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist, onvolledig of niet meer actueel zijn, niet worden verstrekt of beschikbaar gesteld. Als de gegevens onjuist zijn, dan worden deze onverwijld vernietigd of gerectificeerd. Het beginsel van juistheid van gegevens moet worden toegepast met inachtneming van de aard en het doel van de verwerking in kwestie. In het bijzonder bij gerechtelijke procedures zijn verklaringen die persoonsgegevens bevatten, gebaseerd op de subjectieve perceptie van natuurlijke personen en niet altijd te controleren. Het vereiste van juistheid dient derhalve geen betrekking te hebben op de juistheid van een verklaring, maar alleen op het feit dat een specifieke verklaring is afgelegd (overweging 30 RI). De bevoegde autoriteit controleert, voor zover praktisch uitvoerbaar, de kwaliteit van politiegegevens voordat de gegevens worden verstrekt of beschikbaar gesteld. Voor zover mogelijk wordt bij de doorzending van politiegegevens de noodzakelijke informatie toegevoegd aan de hand waarvan de ontvangende bevoegde autoriteit de mate van juistheid, volledigheid en betrouwbaarheid van politiegegevens kan beoordelen, alsmede de mate waarin zij actueel zijn.

Derde lid

De richtlijn verplicht ertoe om persoonsgegevens die op feiten zijn gebaseerd, voor zover mogelijk te onderscheiden van persoonsgegevens die op een persoonlijk oordeel zijn gebaseerd (art. 7, eerste lid, RI). Met dit artikel wordt aan deze verplichting uitvoering gegeven. Met de woorden «voor zover mogelijk» wordt het relatieve karakter van de verplichting tot uitdrukking gebracht. Gedurende het onderzoek kunnen gegevens waarvan is aangenomen dat die op vaststaande feiten zijn gebaseerd, op persoonlijke opvattingen blijken te berusten en vice versa. Dit relatieve karakter wordt versterkt omdat de richtlijn aan dit onderscheid geen rechtsgevolgen verbindt. Overigens bevat een Aanbeveling van de Raad van Europa van 1987 reeds een soortgelijke verplichting (art. 3.2.)[17].

Vierde lid

In dit lid is vastgelegd dat, indien wordt vastgesteld dat onjuiste politiegegevens zijn verstrekt of dat de politiegegevens op onrechtmatige wijze zijn verstrekt, de ontvanger daarvan onverwijld in kennis wordt gesteld. In dat geval dienen de gegevens te worden gerectificeerd, vernietigd of afgeschermd.

Artikel I, onderdeel E

Artikel 4a (verplichting tot gegevensbescherming door beveiliging en ontwerp)

Eerste lid

De verwerkingsverantwoordelijke en de verwerker zijn gehouden passende technische en organisatorische maatregelen te treffen om de rechtmatigheid, proportionaliteit en beveiliging van de gegevensverwerking te garanderen. De verplichtingen van de richtlijn zijn erop gericht gegevensbeschermingsbeginselen, zoals dataminimalisatie, op een doeltreffende manier uit te voeren. De richtlijn maakt expliciet melding van de mogelijkheid van de pseudonimisering van gegevens. Hiermee wordt gedoeld op het verwerken van persoonsgegevens op zodanige wijze dat de gegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om niet-koppeling aan een geïdentificeerd of identificeerbaar proces te waarborgen (art. 3, eerste lid, onder 5, RI).

Tweede lid

In dit lid is de verplichting voor de verwerkingsverantwoordelijke en de verwerker opgenomen om passende technische en organisatorische maatregelen te treffen om een beveiligingsniveau te waarborgen dat op het risico is afgestemd, met name met betrekking tot de verwerking van de bijzondere categorieën van persoonsgegevens, bedoeld in artikel 5.

Derde lid

Bij persoonsgegevens die worden verwerkt met het oog op de opsporing en vervolging van strafbare feiten is de betrouwbaarheid en juistheid van de gegevens juistheid niet bij voorbaat te garanderen; het onderzoek is er

[17] Aanbeveling R(87)15 van het Comité van Ministers van 17 september 1987, tot regeling van het gebruik van persoonsgegevens op politieel gebied.

juist op gericht om die betrouwbaarheid vast te stellen. Voor wat betreft de beveiliging van gegevens geldt dat absolute onaantastbaarheid van gegevens bij voorbaat niet te garanderen is. Daarom wordt in dit lid bepaald dat bij het treffen van maatregelen rekening wordt gehouden met de aard, het toepassingsgebied, de context en de doeleinden van de verwerking, alsmede met de qua waarschijnlijkheid en ernst uitéénlopende risico's voor de rechten en vrijheden van natuurlijke personen. Het risico moet worden beoordeeld op basis van een objectieve evaluatie, aan de hand waarvan wordt bepaald of de gegevensverwerking een hoog risico inhoudt. Een hoog risico is een bijzonder risico op aantasting van de rechten en vrijheden van betrokkenen (overweging 52 RI).

Artikel 4b (verplichting tot gegevensbescherming door standaardinstellingen)

De tenuitvoerlegging van passende technische en organisatorische maatregelen om te waarborgen dat aan de voorschriften van de richtlijn wordt voldaan mag niet alleen van economische overwegingen afhangen. Om de naleving van de richtlijn te kunnen aantonen moet de verwerkingsverantwoordelijke intern beleid vaststellen en maatregelen implementeren die in het bijzonder voldoen aan de beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen («privacy by design and by default»). Bij de ontwikkeling van die maatregelen en procedures moeten de resultaten van gegevensbeschermingseffectbeoordelingen in acht worden genomen. Die maatregelen kunnen onder meer inhouden dat zo spoedig mogelijk wordt overgegaan tot pseudonimisering (overweging 53 RI).

Artikel 4c (gegevensbeschermingseffectbeoordeling)

Eerste lid

In dit lid is de verplichting opgenomen voor de verwerkingsverantwoordelijke om een beoordeling te verrichten van het effect van beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Dit is ook bekend als een gegevensbeschermingseffectbeoordeling (GEB), doorgaans bekend onder de Engelse term «privacy impact assessment» (PIA). Deze verplichting geldt wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, het toepassingsgebied, de context of de doeleinden daarvan, waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen oplevert. Hiervoor kan worden gedacht aan het onderzoek van DNA-profielen van grote aantallen personen of bevolkingsgroepen. Hierbij wordt met name gekeken naar de voorgenomen maatregelen, waarborgen en mechanismen voor het beschermen van persoonsgegevens en het aantonen dat aan de richtlijn is voldaan. Effectbeoordelingen dienen relevante systemen en procedures van verwerkingsactiviteiten te bestrijken maar geen individuele gevallen (overweging 58 RI).

Tweede lid

In dit lid is geregeld welke elementen in ieder geval in de PIA zijn opgenomen. Het gaat hier om zaken als een algemene beschrijving van de beoogde verwerkingen en verwerkingsdoeleinden, een beoordeling van de risico's voor de rechten van de betrokkenen, de beoogde maatregelen ter beperking van de risico's, de voorzorgsmaatregelen, de beveiligingsmaatregelen en de mechanismen die zijn ingesteld om de persoonsgegevens te beschermen en aan te tonen dat aan de wettelijke eisen wordt voldaan. Het blijft evenwel een abstracte normstelling, die in belangrijke

mate door de verwerkingsverantwoordelijke zelf geïnterpreteerd zal moeten worden. Voor de rijksoverheid zal aandacht worden besteed aan de vraag wanneer een PIA is vereist in het aangepaste toetsmodel PIA rijksdienst (Kamerstukken II 2016/17, 26 643, nr. 453).

Derde lid

Artikel 35, elfde lid, van de verordening schrijft voor dat, indien nodig, de verwerkingsverantwoordelijke toetst of de verwerking overeenkomstig een eventueel uitgevoerde gegevensbeschermingseffectbeoordeling wordt uitgevoerd, zulks ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden. Een hiermee vergelijkbare bepaling ontbreekt in de richtlijn. In zijn reactie op het WRR-rapport «Big Data in een vrije en veilige samenleving» heeft het kabinet aangekondigd bij de implementatie van de richtlijn te bezien of een dergelijke bepaling niettemin in de implementatiewetgeving dient te worden opgenomen (Kamerstukken II 2016/17, 26 643, nr. 426, bijlage par. 6). Daartoe bestaat inderdaad aanleiding. Er is immers geen goede reden om op dit punt af te wijken van de verordening, te meer nu een dergelijke «review» een voor de hand liggende aanvulling vormt op de privacy audits die in artikel 33 zijn geregeld. Daarom bevat dit lid de verplichting om onder de daarin genoemde omstandigheden een dergelijke review te houden.

Artikel I, onderdeel F

Artikel 5 (bijzondere categorieën van politiegegevens)

Dit artikel regelt de verwerking van bijzondere categorieën van politiegegevens, thans in de Wpg aangeduid als gevoelige persoonsgegevens. In de richtlijn is de aard van deze persoonsgegevens verder uitgewerkt. Dit betreft niet alleen persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, of het lidmaatschap van een vakvereniging maar ook gegevens betreffende etnische afkomst, genetische gegevens en biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon.
De verwerking vindt slechts plaats wanneer dit strikt noodzakelijk is, met inachtneming van passende waarborgen voor de rechten en vrijheden van de betrokkene. De passende waarborgen dienen bij wet te worden vastgelegd. De passende waarborgen voor de betrokkene kunnen bijvoorbeeld inhouden dat de gegevens enkel mogen worden verzameld in samenhang met andere gegevens over de natuurlijke persoon in kwestie, dat de verzamelde 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 (overweging 37 RI). Met de vereisten dat de gegevens worden verwerkt in aanvulling op de verwerking van andere politiegegevens en dat wordt voorzien in een afdoende niveau van beveiliging wordt hieraan invulling gegeven.
De Afdeling advisering van de Raad van State heeft opgemerkt dat de toelichting zoals hiervoor weergegeven er expliciet van uitgaat dat de passende waarborgen in de wet worden vastgelegd. In lijn hiermee is ook de verwerking in aanvulling op andere gegevens als passende waarborg in artikel 5 Wpg opgenomen. Voor zover de regering meent dat andere passende waarborgen (zoals geclausuleerde toegang tot de gegevens en de andere voorbeelden die in lijn met overweging 37 in de toelichting worden genoemd) in de eis van onvermijdelijkheid van de verwerking moeten worden «ingelezen», strookt dat volgens de Afdeling niet met de hiervoor geciteerde passages uit de toelichting. De Afdeling adviseert met het oog op de duidelijkheid van de regeling – het gaat hier immers om de verwerking van bijzondere persoonsgegevens – alle passende

waarborgen ook in het wetsvoorstel op te nemen. Naar aanleiding van dit advies wordt opgemerkt dat de regering, anders dan de Afdeling advisering kennelijk veronderstelt, niet meent dat andere passende waarborgen (zoals geclausuleerde toegang tot de gegevens en de andere voorbeelden die in lijn met overweging 37 in de toelichting worden genoemd) in de eis van onvermijdelijkheid van de verwerking moeten worden «ingelezen». De toelichting betreft namelijk een citaat uit overweging 37 van de richtlijn, welke overweging de lidstaten een keuze lijkt te bieden in de passende waarborgen die bij wet worden vastgelegd («Passende waarborgen voor de rechten en vrijheden van de betrokkene *kunnen bijvoorbeeld* inhouden»). In dat kader is gekozen voor de handhaving van het vereiste dat de verwerking slechts plaatsvindt in aanvulling op de verwerking van andere politiegegevens (art. 5 Wpg). Uit de tekst van artikel 10 van de richtlijn, en de toelichting daarop, kunnen geen verderstrekkende verplichtingen worden afgeleid. Niettemin is de regering bereid om, in het belang van een adequate bescherming van persoonsgegevens, verder te gaan en aanvullend eisen te stellen aan de toegang tot de gegevens. Daarom is het vereiste toegevoegd dat de gegevens afdoende zijn beveiligd. Hiermee wordt gedoeld op de verplichting van de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om een beveiligingsniveau te waarborgen dat op het risico is afgestemd, met name met betrekking tot de verwerking van de bijzondere categorieën van politiegegevens (artikel 4a, tweede lid, Wpg). Binnen de politie wordt dit betrokken bij het informatiebeveiligingsbeleid. Daarnaast is een uitvoeringskader «Privacy & Security by Design» vastgesteld dat momenteel binnen de politieorganisatie wordt geïmplementeerd.

Artikel I, onderdeel H

Artikel 6a (toegang tot politiegegevens)

In dit artikel zijn de bepalingen over de toegang tot politiegegevens samengebracht.

Derde lid

De aanpassing van dit lid, voorheen artikel 4, vijfde lid, voorziet in de toegang tot de gegevens voor de verwerker en de functionaris voor gegevensbescherming. De verwerkingsverantwoordelijke kan gebruik maken van de diensten van een verwerker. Dit wordt hieronder, in het voorgestelde artikel 6c, nader toegelicht. Alsdan dient de verwerker uiteraard toegang te hebben tot de betreffende politiegegevens. Met de regeling voor de toegang voor de functionaris voor gegevensbescherming wordt uitvoering gegeven aan de bepaling in de richtlijn, dat de verwerkingsverantwoordelijke de functionaris voor gegevensbescherming ondersteunt bij de vervulling van zijn taken door hem toegang te verschaffen tot persoonsgegevens en verwerkingsactiviteiten (art. 33, tweede lid, RI).

Artikel 6b (onderscheid tussen verschillende categorieën van betrokkenen)

De richtlijn verplicht ertoe om, in voorkomend geval en voor zover mogelijk, een duidelijk onderscheid te maken tussen politiegegevens betreffende verschillende categorieën van betrokkenen, zoals verdachten, slachtoffers en getuigen en veroordeelden. Met dit artikel wordt aan deze verplichting uitvoering gegeven. Uit de formulering blijkt van een zekere marge voor de verwerkingsverantwoordelijk bij de invulling van deze verplichting. In de informatiesystemen van de opsporingsdiensten wordt

doorgaans onderscheid gemaakt in de status van personen, al naar gelang het gaat om verdachten, getuigen of slachtoffers. Dit betreft echter geen absoluut onderscheid omdat een verdachte gedurende het opsporingsonderzoek tot getuige kan transformeren en andersom. Doorgaans zal een dergelijke verandering onverwijld in de systemen worden verwerkt.
Het is de Afdeling advisering van de Raad van State opgevallen dat in de voorgestelde artikelen 6b Wpg en 39b, tweede lid, Wjsg verschillende categorieën van personen worden gehanteerd voor de verwerking van respectievelijk politiegegevens en strafvorderlijke gegevens. De reden voor dit onderscheid is volgens de Afdeling niet duidelijk, het gaat immers vaak om dezelfde soort gegevens. Met het oog op duidelijkheid en uniformiteit adviseert de Afdeling in de Wpg en de Wjsg zoveel mogelijk uit te gaan van dezelfde categorieën personen voor wat betreft de verwerking van politiegegevens en de strafvorderlijke gegevens en de eventueel noodzakelijke verschillen in categorieën te motiveren.
In reactie op dit advies wordt opgemerkt dat de categorieën van personen voor politiegegevens en strafvorderlijke gegevens grotendeels gelijk zijn. Met inachtneming daarvan zijn de artikelen 6b Wpg en 39b Wjsg nauwer op elkaar aangesloten.

Artikel 6c (verwerker)

Eerste, tweede en derde lid

De verwerkingsverantwoordelijke kan gebruik maken van de diensten van een verwerker, die namens de verantwoordelijke persoonsgegevens verwerkt. De verwerker dient uitsluitend te handelen volgens de instructies van de verantwoordelijke. De verwerker mag geen andere verwerker in dienst nemen zonder de voorafgaande toestemming van de verwerkingsverantwoordelijke. De verwerking door de verwerker moet in een overeenkomst, of een andere rechtshandeling op basis van het Unierecht of het recht van de lidstaten, worden geregeld. In de overeenkomst wordt onder meer vastgelegd dat de verwerker uitsluitend volgens de instructies van de verwerkingsverantwoordelijke handelt.
De Wpg bevat thans de mogelijkheid van het gebruik van een bewerker, vanwege de overeenkomstige toepassing van de artikelen 14, eerste, tweede, derde en vijfde lid, 49 en 50 van de Wbp (art. 4, zesde lid, Wpg). Mede vanwege het vervallen van de Wbp is de regeling van de richtlijn in een afzonderlijk artikel ondergebracht. De regeling is deels gelijk aan de huidige regels, op basis van de Wbp.

Vierde lid

Nieuw is, in dit lid, de bepaling dat de verwerker geen andere verwerker in dienst neemt dan na voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke. In het geval van een algemene schriftelijke toestemming, informeert de verwerker de verwerkingsverantwoordelijke over de toevoeging of vervanging van andere verwerkers, met de mogelijkheid van bezwaar door de verwerkingsverantwoordelijke.

Vijfde lid

Nieuw is ook, in dit lid, dat de verwerker de verwerkingsverantwoordelijke zonder onredelijke vertraging in kennis stelt van een inbreuk op de bescherming van persoonsgegevens (datalek). Naar aanleiding van de richtlijn wordt voorgesteld een verplichting tot melding van een datalek aan de AP in de wet op te nemen. Hiervoor kan worden verwezen naar het voorgestelde artikel 33a.

Artikel I, onderdeel J

Artikel 7a (geautomatiseerde individuele besluitvorming)

Eerste lid

De richtlijn voorziet in een verbod op uitsluitend op geautomatiseerde verwerking gebaseerde besluiten, met inbegrip van profilering, die voor de betrokkene nadelige rechtsgevolgen hebben of hem in aanmerkelijke mate treffen. Dit verbod geldt echter niet als het betrokken besluit is toegestaan op grond van het recht van de lidstaten en het besluit voorziet in passende waarborgen voor de rechten en vrijheden van de betrokkene, waaronder ten minste het recht op menselijke tussenkomst van de verwerkingsverantwoordelijke (art. 11, eerste lid, RI). Anders dan de Wbp die een soortgelijke bepaling bevat (art. 42, eerste lid, Wbp), kennen de Wpg en de Wjsg tot nu toe een dergelijk verbod niet. Met dit artikel wordt uitvoering gegeven aan het verbod van de richtlijn. De passende waarborgen van de richtlijn omvatten 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 (overweging 38 RI). 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 en te voorzien in specifieke voorlichting aan de betrokkene, zodat de betrokkene in staat wordt gesteld zijn standpunt kenbaar te maken of uitleg over het na een dergelijke beoordeling genomen besluit te krijgen en om op te komen tegen het besluit.
De Afdeling advisering heeft erop gewezen dat de wijze waarop het recht van de betrokkene op menselijke tussenkomst – om zijn standpunt kenbaar te maken, uitleg over het na een dergelijke beoordeling genomen besluit te krijgen en eventueel op te kunnen komen tegen het besluit – wordt vormgegeven niet is uitgewerkt. De Afdeling adviseert in de toelichting te expliciteren op welke wijze het recht op menselijke tussenkomst nader wordt vormgegeven en het wetsvoorstel zo nodig aan te passen. Naar aanleiding van dit advies is in dit lid expliciet de verplichting van de verwerkingsverantwoordelijke vastgelegd om te voorzien in voorafgaande menselijke tussenkomst. Voorzover dit besluit wordt aangemerkt als een besluit in de zin van de Algemene wet bestuursrecht, kan de betrokkene de rechtsbescherming inroepen die op basis van die wet geldt en kan de betrokkene zich tevens tot de Autoriteit persoonsgegevens wenden met het verzoek te bemiddelen of te adviseren in zijn geschil met de verwerkingsverantwoordelijke.

Tweede lid

De richtlijn bepaalt dat een besluit, bedoeld in het eerste lid, niet wordt gebaseerd op de bijzondere categorieën van politiegegevens, bedoeld in artikel 5, tenzij passende maatregelen zijn getroffen ter bescherming van de rechten en vrijheden en van de gerechtvaardigde belangen van de betrokkene (art. 11, tweede lid, RI). De Afdeling advisering van de Raad van State is van oordeel dat met het vereiste van «passende maatregelen», als bedoeld in artikel 11, tweede lid, RI, klaarblijkelijk wordt bedoeld dat, in aanvulling op de passende waarborgen bedoeld in artikel 11, eerste lid, RI, wordt voorzien in extra maatregelen voor de geautomatiseerde verwerking met gebruikmaking van bijzondere gegevens. De Afdeling adviseert derhalve in het wetsvoorstel een nadere invulling te geven aan het vereiste van «passende maatregelen» als bedoeld in artikel 11, tweede lid, RI. Naar aanleiding van dit advies is het vereiste opgenomen dat de Autoriteit persoonsgegevens wordt geraad-

pleegd over de voorgenomen gegevensverwerking, overeenkomstig artikel 33b, eerste lid, van de wet. Wanneer de Autoriteit persoonsgegevens van oordeel is dat de voorgenomen verwerking, bedoeld in het eerste lid, niet voldoet aan het bij of krachtens deze wet bepaalde, geeft zij binnen een termijn van ten hoogste zes weken schriftelijk advies aan de verwerkingsverantwoordelijke (art. 33, vierde lid, Wpg).

Derde lid

Het Handvest van de grondrechten van de Europese Unie verbiedt elke discriminatie, met name op grond van geslacht, ras, kleur, etnische of sociale afkomst, genetische kenmerken, taal, godsdienst of overtuigingen, politieke of andere denkbeelden, het behoren tot een nationale minderheid, vermogen, geboorte, een handicap, leeftijd of seksuele geaardheid (art. 21 Handvest). Overeenkomstig dit verbod wordt in dit lid profilering die leidt tot discriminatie van personen op grond van de in artikel 5 bedoelde categorieën van politiegegevens, verboden.

Artikel I, onderdeel M

Artikel 15a (ter beschikkingstelling binnen de Europese Unie)

Eerste en tweede lid

De richtlijn geeft waarborgen voor de bescherming van persoonsgegevens, die van toepassing zijn in het geval dat persoonsgegevens tussen de lidstaten onderling worden uitgewisseld. De richtlijn bevat geen zelfstandige bevoegdheden of verplichtingen voor de uitwisseling van persoonsgegevens tussen de lidstaten. Dit is bij de implementatie van het voormalige kaderbesluit dataprotectie reeds aan de orde gekomen (Kamerstukken II, 2010/11, 32 554, nr. 3, blz. 2). In afzonderlijke rechtsinstrumenten kunnen afspraken worden opgenomen over de gevallen waarin, en de voorwaarden waaronder, persoonsgegevens door de bevoegde autoriteiten van de lidstaten onderling ter beschikking gesteld kunnen worden of ter beschikking gesteld moeten worden. Het Verdrag van Lissabon, dat op 1 december 2009 in werking is getreden, biedt het Europees Parlement en de Raad de mogelijkheid om maatregelen, verordeningen of voorschriften vast te stellen voor de uitwisseling van gegevens door de lidstaten. Deze Unierechtelijke verplichtingen zijn uitgewerkt in het Bpg.
De richtlijn biedt de mogelijkheid om specifieke voorwaarden te stellen aan de verwerking van politiegegevens. In dat geval stelt de verstrekkende bevoegde autoriteit de ontvanger in kennis van die voorwaarden en van de noodzaak tot eerbiediging ervan (art. 9, derde lid, RI). De voorwaarden kunnen bijvoorbeeld voorzien in een verbod om de persoonsgegevens aan anderen door te zenden, of deze voor andere doeleinden te gebruiken dan die waarvoor zij aan de ontvanger werden doorgezonden of de betrokkene zonder de voorafgaande instemming van de doorzendende autoriteit niet in kennis te stellen ingeval van een beperking van het recht op informatie (overweging 36 RI). Wanneer de voorwaarden worden toegepast op andere lidstaten of EU-organen mogen die voorwaarden niet afwijken van de voorwaarden voor vergelijkbare doorzendingen van gegevens binnen de lidstaat (art. 9, derde lid, RI). Het voormalige kaderbesluit dataprotectie kende een soortgelijke mogelijkheid (art. 12 Kb dataprotectie), die thans is opgenomen in het Bpg (art. 5:3, zevende lid, Bpg). Deze beperking laat specifieke voorzieningen, opgenomen in een rechtsinstrument op grond van het verdrag betreffende de werking van de Europese Unie, onverlet. Hiervoor kan worden gewezen op Kaderbesluit

2006/960/JBZ van de Raad van 18 december 2006[18], dat specifieke gronden bevat voor bevoegde rechtshandhavingsautoriteit om de verstrekking van informatie of inlichtingen aan een andere lidstaat te weigeren (art. 10 Kb 2006/960/JBZ). Deze gronden zijn opgenomen in het Besluit politiegegevens (art. 5:3, tweede lid, Bpg).

Artikel I, onderdeel P

Artikel 16 (verstrekking aan gezagsdragers)

Eerste lid

De verwijzing naar de buitengewone opsporingsambtenaren, in het huidige onderdeel a, komt te vervallen omdat de gegevensverwerking door de boa's onder de reikwijdte van de Wpg valt. De verstrekking van politiegegevens aan een boa wordt dan geregeld door artikel 15. Voorgesteld wordt in onderdeel c, onder punt 1, een verwijzing op te nemen naar artikel 14 van de Wet op de bijzondere opsporingsdiensten. Dit betreft het herstel van een omissie. De opneming van de verwijzing naar de regelgeving die van toepassing is op de aanstelling of arbeidsovereenkomst van de bijzondere opsporingsambtenaar, onder punt 2, houdt verband met de verruiming van de reikwijdte van de Wpg.

Artikel I, onderdeel R

Artikel 17 (verstrekking aan inlichtingendiensten)

Dit artikel regelt thans de verstrekking van politiegegevens aan inlichtingendiensten en buitenlandse opsporingsinstanties. Zoals eerder opgemerkt, maakt de richtlijn voor de toepasselijkheid van de regels over gegevensverwerking geen onderscheid tussen Nederland en andere lidstaten. De bevoegdheid tot het ter beschikking stellen van politiegegevens aan andere lidstaten wordt geregeld in het voorgestelde artikel 15a. De richtlijn bevat verder een specifiek regime voor de doorgifte van persoonsgegevens aan derde landen (Hfst. V Rl). De regeling is dermate uitgebreid dat ervoor is gekozen dit in een afzonderlijke bepaling op te nemen. Dit betreft het voorgestelde artikel 17a. Aldus wordt dit artikel te beperken tot de verstrekking van politiegegevens aan inlichtingendiensten.

Artikel I, onderdeel S

Artikel 17a (doorgiften aan derde landen)

Eerste lid

Thans is in dit artikel voorzien in de mogelijkheid van verstrekking van politiegegevens aan de verwerkingsverantwoordelijken in de BES. In het systeem van de richtlijn gelden de BES als derde land. In het licht hiervan wordt voorgesteld de regeling voor de doorgifte van politiegegevens aan derde landen in de plaats te doen komen van die over de verstrekking van politiegegevens aan de BES. De doorgifte van politiegegevens aan de BES kan dan plaatsvinden binnen de kaders van deze regeling.
Wanneer persoonsgegevens worden doorgegeven aan derde landen of internationale organisaties, mag dit niet ten koste gaan van het beschermingsniveau voor natuurlijke personen waarin door de richtlijn wordt

[18] Kaderbesluit 2006/960/JBZ van de Raad van 18 december 2006 betreffende de vereenvoudiging van de uitwisseling van informatie en inlichtingen tussen de rechtshandhavingsautoriteiten van de lidstaten van de Europese Unie (PbEU L386/89).

voorzien (overweging 64 RI). Uitgangspunt is dat politiegegevens kunnen worden doorgegeven aan een verwerkingsverantwoordelijke in een derde land of in een internationale organisatie die belast met de uitvoering van de richtlijntaken, als de Commissie heeft besloten dat het derde land of de internationale organisatie een toereikend beschermingsniveau voor de voorgenomen gegevensverwerking verzekert (art. 35, eerste lid, onder d, en 36, eerste lid, RI). Dit betreft een zogenaamd adequaatheidsbesluit. Een soortgelijke regeling is opgenomen in de huidige Wbp (art. 76/78 Wbp), op basis van de voormalige Privacyrichtlijn, en ook terug te vinden in de verordening (art. 45 Avg). Bij de beoordeling of het beschermingsniveau adequaat is houdt de Commissie met name rekening met (1) de rechtsstatelijkheid, de eerbiediging van de mensenrechten en de fundamentele vrijheden, de toepasselijke algemene en sectorale wetgeving evenals de tenuitvoerlegging van die wetgeving, gegevensbeschermingsregels, beroepsregels en veiligheidsmaatregelen, (2) het bestaan en het effectief functioneren van een toezichthoudende autoriteit in het derde land en (3) de internationale verbintenissen, in het bijzonder met betrekking tot de bescherming van persoonsgegevens, die het derde land heeft aangegaan (art. 36, tweede lid, RI). Bij de boordeling van het beschermingsniveau dient de Commissie overleg te plegen met het Comité voor gegevensbescherming, dat is opgericht op basis van de verordening gegevensbescherming. Tevens wordt rekening gehouden met de adequaatheidsbesluiten die overeenkomstig die verordening zijn vastgesteld (overweging 68 RI). De beslissing van de Commissie wordt gepubliceerd en periodiek getoetst (art. 36, derde en achtste lid, RI). Als niet langer aan de vereisten wordt voldaan wordt het besluit ingetrokken, gewijzigd of geschorst (art. 36, vijfde lid, RI).
Als de doorgifte politiegegevens betreft die oorspronkelijk van een andere lidstaat afkomstig zijn, is voorafgaande toestemming van die lidstaat vereist voor de verdere doorgifte, ook als sprake is van een adequaat beschermingsniveau (overweging 66 RI). Daarbij kunnen specifieke voorwaarden worden gesteld aan de verdere doorgifte (overweging 65 RI). Dit vereiste van toestemming geldt echter niet wanneer de doorgifte noodzakelijk is met het oog op de voorkoming van een onmiddellijk en ernstig gevaar voor de openbare veiligheid.

Tweede lid

Tot nu toe zijn, op basis van de voormalige Privacyrichtlijn, slechts een tiental adequaatheidsbesluiten gepubliceerd[19]. Uitgangspunt is dat de Europese Commissie voor de richtlijn eveneens adequaatsheidsbesluiten zal vaststellen. Uitsluitend indien een dergelijk besluit ontbreekt, voorziet de richtlijn voor lidstaten in de mogelijkheid tot de uitwisseling van persoonsgegevens met derde landen ten behoeve van de opsporing en vervolging van strafbare feiten, op basis van passende waarborgen. Deze waarborgen kunnen zijn opgenomen in een juridisch bindend instrument, zoals een verdrag. Daarbij kan rekening worden gehouden met samenwerkingsovereenkomsten die zijn gesloten tussen Europol of Eurojust en derde landen, en kunnen voorwaarden worden gesteld ten aanzien van de vertrouwelijkheid en doelbinding (overweging 71). Voor de verstrekking van politiegegevens aan de BES geldt dat met de Wpg, die beschouwd wordt als een «juridisch bindend instrument» in de zin van de richtlijn, reeds in voldoende waarborgen is voorzien (paragraaf 5a). Daarnaast kan de verwerkingsverantwoordelijke op grond van alle omstandigheden concluderen dat er passende waarborgen bestaan voor de bescherming

[19] Op basis van artikel 25, zesde lid, van de Privacyrichtlijn zijn thans de volgende landen aangewezen: Andorra, Argentinië, Canada, Zwitserland, Faeröer eilanden, Guernsey, Israël, Eiland Man, Jersey, New Zeeland, VS Privacy Shield en Uruguay.

van persoonsgegevens (art. 17, eerste lid, RI). In dit laatste geval wordt de AP over de categorieën van doorgiften geïnformeerd.

Derde lid

De criminaliteit waarmee de lidstaten worden geconfronteerd vindt soms zijn oorsprong in een derde land dat rechtsstatelijk gezien minder ver ontwikkeld is dan de Europese Unie. Passende waarborgen voor de verwerking van persoonsgegevens kunnen dan problematisch zijn. Dit klemt temeer daar opsporing en vervolging tijdgebonden zijn terwijl de voorbereiding van een adequaatheidsbesluit of de vaststelling van passende waarborgen juist tijdrovend zijn. Om in voorkomende gevallen, bij het ontbreken van een adequaatheidsbesluit en van passende waarborgen, toch de mogelijkheid te bieden tot de uitwisseling van persoonsgegevens ten behoeve van opsporing en vervolging wordt in de richtlijn voorzien in afwijkingen voor specifieke situaties (art. 38, eerste lid, RI). In afzonderlijke gevallen is doorgifte mogelijk als dit noodzakelijk is met het oog op de doelen, bedoeld in artikel 1, eerste lid, onder a. Dit kan een afzonderlijk opsporingsonderzoek of een individuele strafzaak betreffen. Deze uitzonderlingen mogen geen frequente massale en structurele doorgifte van persoonsgegevens mogelijk maken maar dienen tot het strikt noodzakelijke te worden beperkt (overweging 72 RI).

Vierde lid

Als de door te geven gegevens afkomstig zijn van een andere lidstaat, dan is toestemming van de bevoegde autoriteit uit die lidstaat vereist, voor de doorgifte van de gegevens aan een derde land. Die toestemming is niet nodig ingeval van de voorkoming van een onmiddellijk en ernstig gevaar voor de openbare veiligheid, zoals bij het verijdelen van een aanslag. In dat geval dient de voor het geven van de toestemming verantwoordelijke autoriteit van die lidstaat onverwijld in kennis te worden gesteld van de doorgifte van de gegevens.

Vijfde lid

De uitwisseling van persoonsgegevens met derde landen vindt in beginsel plaats met de medewerking van de bevoegde autoriteiten van die landen, soms zelfs zonder internationale overeenkomst. In bepaalde omstandigheden kan het echter noodzakelijk zijn om persoonsgegevens rechtstreeks aan een ontvanger, gevestigd in een derde land, te verstrekken zonder de voorafgaande tussenkomst van een bevoegde autoriteit. Dit kan aan de orde zijn als de ontvanger over gegevens beschikt die van groot belang zijn voor het opsporingsonderzoek of voor de strafvervolging, en het doorlopen van een rechtshulpprocedure tijdrovend is of omdat de autoriteit in het derde land de internationale mensenrechtennormen en -regels niet eerbiedigt (overweging 73 RI). De richtlijn maakt een dergelijke rechtstreekse doorgifte onder voorwaarden mogelijk (art. 39, eerste lid, RI). In dit lid is vastgelegd dat in afzonderlijke en specifieke gevallen politiegegevens rechtstreeks kunnen worden doorgegeven aan een ontvanger in een derde land, indien dit strikt noodzakelijk is voor de uitvoering van de richtlijntaken en tevens is voldaan aan enkele nadere voorwaarden. Bij de rechtstreekse doorgifte van politiegegevens in afzonderlijke en specifieke gevallen aan een ontvanger in een derde land dienen de bilaterale of multilaterale overeenkomsten tussen lidstaten en derde landen op het gebied van justitiële samenwerking in strafzaken en politiële samenwerking te worden gerespecteerd. De bepalingen van de richtlijn gelden dan in aanvulling op de regels van die overeenkomsten,

met name de bepalingen betreffende de rechtmatigheid van de verwerking en de bepalingen van hoofdstuk V van de richtlijn (overweging 73 RI).
De in dit lid opgesomde voorwaarden zijn cumulatief, zodat rechtstreekse doorgifte aan een ontvanger is toegestaan als aan alle voorwaarden is voldaan. In onderdeel a is de voorwaarde opgenomen dat de doorgifte noodzakelijk dient te zijn ter uitvoering van een voorgeschreven taak die binnen de doeleinden van de richtlijn valt. Bij de doorgifte van politiegegevens kan hierbij worden gedacht aan de uitvoering van politietaken, bedoeld in de artikelen 3 en 4, eerste lid van de Politiewet 2012. De voorwaarde in onderdeel b vereist dat een afweging wordt gemaakt tussen het belang van betrokkene op bescherming van grondrechten en fundamentele vrijheid en het openbaar belang dat doorgifte in het specifieke geval noodzakelijk maakt. Dit zal telkens een beoordeling in het afzonderlijke geval vereisen. Uiteraard dient er gegronde reden te zijn om, met voorbijgaan van de autoriteit die in het derde land bevoegd, politiegegevens door te geven. Uit onderdeel c volgt dat dit uitsluitend mogelijk is als de tussenkomst van die autoriteit naar het oordeel van de verstrekkende autoriteit ondoeltreffend of ongeschikt is. Deze beide criteria dienen te worden toegepast in het licht van de hiervoor aangehaalde overweging uit de richtlijn. Op grond van onderdeel d geldt in beginsel de verplichting de in het derde land bevoegde autoriteit over de doorgifte te informeren, tenzij dit ondoeltreffend of ongeschikt is. Indien bijvoorbeeld een derde land internationale regels inzake mensenrechten schendt, kan onder omstandigheden de enkele bekendheid bij een bevoegde autoriteit in dat derde land over rechtstreekse doorgifte van politiegegevens aan een ontvanger reeds voldoende zijn om de identiteit van de ontvanger te achterhalen. Het is ongeschikt informatie over de doorgifte te verstrekken indien dit een risico vormt. Onderdeel e bevat een verplichting die verband houdt met de doelbinding door de ontvanger bij de verwerking van politiegegevens.

Zesde lid

De richtlijn bepaalt dat verdere doorgifte aan een ander derde land of een andere internationale organisatie afhankelijk is van toestemming van een bevoegde autoriteit in de lidstaat van oorsprong van de gegevens. Voor het verlenen van toestemming worden de relevante factoren naar behoren in aanmerking genomen, waaronder de ernst van het strafbare feit, het doel waarvoor de gegevens oorspronkelijk waren doorgegeven en het niveau van gegevensbescherming in het derde land of de internationale organisatie waaraan de gegevens verder worden doorgegeven.

Zevende lid

In het Bpg en het Bjsg worden nadere regels opgenomen over de doorgifte van politiegegevens aan derde landen, de verdere verwerking van die gegevens en de daarbij te stellen voorwaarden aan het gebruik daarvan door ontvangstgerechtigde autoriteiten of internationale organen.

Artikel I, onderdeel X

Artikel 22 (verwerking voor wetenschappelijk onderzoek en statistiek)

Eerste lid

De richtlijn regelt de verwerking van politiegegevens met het oog op archivering, wetenschappelijk of historisch onderzoek of gebruik door statistische doeleinden (art. 4, derde lid, RI). De tekst van de richtlijn strekt tot redactionele aanpassing van dit artikel, dat thans de verstrekking van politiegegevens regelt ten behoeve van beleidsinformatie en wetenschappelijk onderzoek en statistiek. De archivering van politiegegevens is geregeld in artikel 14 Wpg. Overigens is de verwerking van politiegegevens ten behoeve van beleidsinformatie, wetenschappelijk onderzoek of statistiek slechts mogelijk zolang de gegevens niet zijn overgebracht naar een archiefbewaarplaats. Tenslotte kan nog worden opgemerkt dat de richtlijn de mogelijkheid biedt politiegegevens ook te verwerken met het oog op deze doelen, anders dan ter verwezenlijking van de doelen binnen de richtlijntaken (art. 9, tweede lid). Dan is de verordening van toepassing op de verdere verwerking van de gegevens voor deze doelen.

Artikel I, onderdeel Y

Artikel 23 (rechtstreekse verstrekking)

Derde lid

In het algemeen deel van deze toelichting is aan de orde gekomen dat de uitvoering van de taken ten dienste van de justitie, zoals genoemd in artikel 1, onderdeel i, van de Politiewet 2012, als onderdeel van de handhaving van de rechtsorde onder de politietaak valt (als bedoeld in artikelen 3 en 4 Politiewet 2012). Onder de taken ten dienste van de justitie valt de uitvoering van de Wet wapens en munitie, de Wet particuliere beveiligingsorganisaties en recherchebureaus, de Wet natuurbescherming en de Wet explosieven voor civiel gebruik. In deze wetten zijn taken opgedragen aan de korpschef van de politie. Daarnaast voert de Koninklijke marechaussee toezichtstaken uit in het kader van genoemde wetten. Deze korpscheftaken hebben betrekking op het verlenen, verlengen of intrekken van een akte voor de jacht, een erkenning voor het bezit van een vuurwapen, de toestemming voor de tewerkstelling als beveiliger of het verlof voor het gebruik van explosieven. Voor een goede uitvoering van die taken moeten de korpschef en de Minister van Defensie kunnen beschikken over politiegegevens, omdat die gegevens onmisbaar zijn om een goed beeld te kunnen verkrijgen van de achtergrond van de betrokken personen. In het algemeen deel van deze toelichting is daarnaast aan de orde gekomen dat gegevensverwerking in het kader van de uitvoering van de bij of krachtens de Vreemdelingenweet 2000 opgedragen taken -vreemdelingentoezicht en grensbewaking- voortaan onder de verordening vallen. Deze taken worden uitgevoerd door de politie en door de Koninklijke marechaussee. Omwille van de efficiency en een zorgvuldige besluitvorming is het van essentieel belang dat de korpschef en de Minister van Defensie (als verwerkingsverantwoordelijke ten aanzien van de Koninklijke marechaussee) rechtstreeks langs geautomatiseerde weg toegang heeft tot alle beschikbare politiegegevens die relevant zijn voor een goede uitvoering van de eerdergenoemde taken. Vanwege de risico's op het gebied van de bescherming van de persoonlijke levenssfeer en de afscherming van gevoelige opsporingsinformatie is het rechtstreeks langs geautomatiseerde weg verstrekken van politiegegevens aan personen of instanties buiten de politieorganisatie gebonden aan strikte regels. Deze

vorm van vertrekking is gebonden aan de vergelijking van bepaalde categorieën van gegevens met politiegegevens, op basis van «hit/no hit». Door de verstrekking op basis van hit/no hit is gewaarborgd dat uitsluitend gegevens worden verstrekt over de vraag of over een persoon gegevens worden verwerkt bij de politie of de Koninklijke marechaussee; de verstrekking van de «achterliggende» gegevens dient plaats te vinden door middel van een traditionele verstrekking van politiegegevens.

De rechtstreekse verstrekking van politiegegevens aan de korpschef of de Minister van Defensie, op basis van hit/no hit, is echter niet toereikend voor een adequate uitvoering van de taken op grond van de bovenbedoelde bijzondere wetten. Dit klemt temeer daar de korpschef en de commandant van de Koninklijke marechaussee zelf zijn belast met de uitvoering van de politietaak en geen derde zijn. Daarom wordt een aanvulling van dit artikel voorgesteld, die erin voorziet dat de korpschef en de Minister van Defensie rechtstreeks langs geautomatiseerde weg kunnen beschikken over de politiegegevens die noodzakelijk zijn met het oog op het uitvoeren van de wettelijke taken waarmee zij zijn belast. Daarbij geldt geen beperking van de raadpleging op basis van hit/no hit. De betreffende wettelijke taken worden bij algemene maatregel van bestuur aangewezen, zodat deze eenvoudig kunnen worden aangepast als deze taken vanwege beleidsinhoudelijke of wetstechnische redenen wijziging ondergaan. Dit zal in het Bpg worden uitgewerkt. Voor wat betreft de aan te wijzen taken van de korpschef wordt thans gedacht aan de volgende taken, op grond van de volgende wetten die behoren tot de taken ten dienste van de justitie:

– de verlening van de jachtakte, bedoeld in artikel 3.28, eerste lid, en het nemen van beschikkingen tot intrekking van jachtakten, als bedoeld in artikel 5.4, zevende lid, van de Wet Natuurbescherming;
– het in bewaring nemen van een wapen of munitie, als bedoeld in artikel 8, het verlenen en intrekken van een erkenning, alsmede het verlengen van de geldigheidsduur daarvan, als bedoeld in artikel 9, tweede lid, het verlenen van een verlof tot vervoer, als bedoeld in artikel 24, eerste lid, het verlenen van een verlof tot het voorhanden hebben van een wapen en munitie, als bedoeld in artikel 28, eerste lid, de afgifte van de Europese vuurwapenpas, bedoeld in artikel 28a, derde lid, en het verlenen van verlof tot verkrijging van wapens, als bedoeld in artikel 32, eerste lid, van de Wet wapens en munitie;
– het verlenen van toestemming voor de tewerkstelling van personen, als bedoeld in artikel 7, tweede lid, het uitoefenen van de bevoegdheden, als bedoeld in artikel 9, zevende lid, het afgeven van een verklaring van betrouwbaarheid, als bedoeld in artikel 10, vijfde lid, het geven van aanwijzingen aan een beveiligingsorganisatie of recherchebureau, als bedoeld in artikel 12, eerste lid, van de Wet particuliere beveiligingsorganisaties en recherchebureaus;
– het verlenen en intrekken van een erkenning, alsmede het verlengen van de geldigheidsduur daarvan, als bedoeld in artikel 18, tweede lid, van de Wet explosieven voor civiel gebruik.

Voor wat betreft de Minister van Defensie wordt thans gedacht aan toezichtstaken die de Koninklijke marechaussee conform artikel 141 van het Wetboek van Strafvordering uitoefent op de naleving van de Wet Wapens Munitie (art. 45), de Wet particuliere beveiligingsorganisaties en recherchebureaus (art. 11) en de Wet explosieven voor civiel gebruik (art. 22).

Aan de korpschef en aan de Minister van Defensie kan voorts rechtstreekse verstrekking van gegevens plaatsvinden in het kader van de uitvoering van de bij of krachtens de Vreemdelingenwet 2000 opgedragen taken, voor zover deze niet als richtlijn-taak kunnen worden aangemerkt.

Dit is in de eerste plaats het vreemdelingentoezicht door politie en Koninklijke marechaussee, het onderzoek naar de identiteit en de verblijfsrechtelijke status van vreemdelingen. In de tweede plaats is dat de grensbewaking, bedoeld in artikel 4, eerste lid, onder f, van de Politiewet 2012.

Vierde lid

In het huidige derde lid is vastgelegd dat de verantwoordelijke passende maatregelen treft teneinde te waarborgen dat uitsluitend politiegegevens rechtstreeks kunnen worden verstrekt voor zover dit noodzakelijk is voor het doel waarvoor die gegevens worden verstrekt. Voorgesteld wordt dat deze verplichting eveneens geldt voor de rechtstreekse verstrekking langs geautomatiseerde weg aan de korpschef, als voorzien in het voorgestelde derde lid.

Artikel I, onderdeel AA

Artikel 24a (informatie aan betrokkenen)

Eerste lid

De richtlijn bevat een algemene bepaling over de verstrekking van informatie aan de betrokkene (art. 12 RI). Dit betreft de informatie die op initiatief van de verantwoordelijke aan de betrokkene ter beschikking wordt gesteld (meer actieve informatieplicht) en de informatie die wordt verstrekt naar aanleiding van een verzoek van de betrokkene (meer passieve informatieplicht). In zijn algemeenheid geldt dat de verantwoordelijke gehouden is aan de betrokkene informatie over de verwerking van politiegegevens te verstrekken in een beknopte, heldere en gemakkelijk toegankelijke vorm en in duidelijke en heldere taal. Deze verplichting is in het bijzonder van toepassing bij de verwerking van politiegegevens in het kader van geautomatiseerde besluitvorming, bij het inzagerecht en beperkingen daarop, bij het recht op rectificatie en vernietiging van gegevens en beperkingen daarop, bij de uitoefening van rechten door de betrokkene en controle door de toezichthouder, bij de rechten van de betrokkene bij de strafrechtelijke onderzoeken en procedures, en bij een mededeling van een inbreuk in verband met persoonsgegevens aan een betrokkene. De verstrekking van de informatie is kosteloos. De informatie wordt met passende middelen, waaronder elektronische, verstrekt en in het algemeen in dezelfde vorm als de vorm van het verzoek.

Tweede lid

In de richtlijn is bepaald dat de verwerkingsverantwoordelijke de betrokkene zonder onnodige vertraging schriftelijk in kennis stelt met betrekking tot de opvolging van zijn verzoek (art. 12, derde lid. RI). In het licht van de meer specifieke verplichting om de betrokkene schriftelijk in kennis te stellen van de weigering tot inzage (art. 15, derde lid, RI), moet deze bepaling als een voorschrift van meer procedurele aard worden gezien. Ter implementatie daarvan wordt in dit lid geregeld dat degene die verzoekt om inzage of rectificatie, schriftelijk in kennis wordt gesteld van de ontvangst van het verzoek, de termijn voor uitsluitsel en de mogelijkheid om naar aanleiding daarvan een klacht in te dienen bij de AP. De mogelijkheid van een klacht bij de AP wordt geregeld in het voorgestelde artikel 31a. Als het verzoek tot inzage of rectificatie geheel of gedeeltelijk wordt afgewezen, dan vindt de afwijzing schriftelijk plaats. Daarvoor kan worden verwezen naar artikel 27, tweede lid.

Vierde lid

De richtlijn bepaalt dat, wanneer verzoeken van een betrokkene kennelijk ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter, de verwerkingsverantwoordelijke een redelijke vergoeding mag rekenen in het licht van de administratieve kosten waarmee het verstrekken van de gevraagde informatie of communicatie en het treffen van de gevraagde maatregelen gepaard gaan of kan weigeren gevolg te geven aan het verzoek (art. 12, vierde lid, RI). In het licht van deze mogelijkheid wordt in dit lid geregeld dat in het geval van kennelijk ongegronde of buitensporige verzoeken, met name vanwege de geringe tussenpozen tussen de verschillende verzoeken, de verwerkingsverantwoordelijke kan weigeren gevolg te geven aan het verzoek.

Vijfde lid

De richtlijn voorziet in de mogelijkheid om de uitoefening van het recht op informatie, inzage rectificatie, wissing of afscherming van persoonsgegevens of overeenkomstig het nationale procesrecht van de lidstaten uit te oefenen wanneer persoonsgegevens in een rechterlijke beslissing, register of dossier zijn vervat en in het kader van strafrechtelijke onderzoeken en procedures worden verwerkt (art. 18 en overweging 49 RI). In dit lid is vastgelegd dat aan een verplichting tot verstrekking van politiegegevens, naar aanleiding van de meer actieve informatieplicht jegens de betrokkene of een verzoek van de betrokkene tot inzage of rectificatie van gegevens, is voldaan als de gegevens onderdeel vormen van de processtukken ten aanzien waarvan aan de verdachte kennisneming is verleend op grond van de regeling van de kennisneming van processtukken in het Wetboek van Strafvordering (art. 30–34 Sv). Deze regeling voorziet in het recht van de verdachte om, op diens verzoek, tijdens het voorbereidende onderzoek kennis te kunnen nemen van de processtukken. De officier van justitie kan, indien het belang van het onderzoek dit vordert, de verdachte de kennisneming van bepaalde processtukken onthouden (art. 30, derde lid, Sv). Om te voorkomen dat een verdachte op grond van de Wpg of de Wjsg probeert gegevens te bekomen die hem door de officier van justitie zijn geweigerd, is het van belang dat een goede afstemming plaatsvindt tussen de betrokken opsporingsinstantie en het openbaar ministerie bij de behandeling van verzoeken om inzage of correctie van gegevens, op basis van de Wpg of de Wjsg.

Artikel 24b (verstrekking van informatie)

Eerste lid

Dit lid betreft een meer actieve informatieplicht van de verantwoordelijke. De verstrekking van de informatie kan worden gedaan op de website van de bevoegde autoriteit (overweging 42 RI).

Tweede lid

De actieve informatieplicht van de verantwoordelijke strekt er in specifieke gevallen toe dat deze verdere informatie verstrekt om de betrokkene in staat te stellen zijn rechten uit te oefenen. Hieraan kan eveneens invulling worden gegevens door publicatie van de betreffende gegevens op de website van de verantwoordelijke. Eveneens mogelijk is dat de gegevens ter beschikking van de betrokkene worden gesteld zodra deze langs elektronische weg contact opneemt met de bevoegde autoriteit. Daarvoor kan bij de politie worden gedacht aan een elektronische aangifte.

Onderdeel e

In artikel 14, tweede lid, onder g, Avg, 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. Een equivalent van genoemde bepaling uit de verordening gegevensbescherming ontbreekt in de richtlijn. In zijn reactie op het WRR-rapport «Big Data in een vrije en veilige samenleving» heeft het kabinet aangekondigd bij de implementatie van de richtlijn te bezien of een bepaling als deze niet ook voor geautomatiseerde besluitvorming op grond van strafrechtelijke gegevens zou moeten gaan gelden (Kamerstukken II 2016/17, 26 643, nr. 426, bijlage par. 6). Een dergelijke bepaling behoort in de Wpg inderdaad niet te ontbreken. Het verstrekken van de hier bedoelde informatie kan immers worden gezien als een expliciete invulling van de passende waarborgen voor de rechten en vrijheden van de betrokkene waarop in artikel 7a wordt gedoeld. Daarom is in dit artikel voor de verwerkingsverantwoordelijke de verplichting opgenomen deze informatie aan betrokkene te verstrekken. Deze informatieverplichting is niet absoluut. Er zijn immers situaties denkbaar waarin de verstrekking van informatie achterwege dient te blijven. Daarbij gaat het om dezelfde situaties die in artikel 27, eerste lid, worden genoemd om een verzoek om inzage in politiegegevens af te wijzen. Voor een nadere uiteenzetting van die situaties wordt verwezen naar de artikelsgewijze toelichting op dat artikel.

Derde lid

De richtlijn biedt de mogelijkheid de ter beschikking stelling van informatie uit te stellen, te beperken of achterwege te laten vanwege de gronden die in de weg staan aan inzage door de betrokkene. Dit betreft een afweging in afzonderlijke gevallen. Van deze mogelijkheid is geen gebruik gemaakt omdat een dergelijke afweging niet goed verenigbaar is met de wijze van implementatie van de actieve informatieplicht voor specifieke gevallen. Als een belanghebbende langs elektronische weg in contact treedt met de politie, bijvoorbeeld voor het doen van aangifte, past daarbij geen afweging voor het afzonderlijke geval. Dit ligt echter anders voor de mogelijkheid van richtlijn om bepaalde verwerking categorieën geheel of gedeeltelijk uit te zonderen van de actieve informatieplicht voor specifieke gevallen (art. 13, vierde lid, RI). Het is niet wenselijk 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 van de actieve informatieplicht voor specifieke gevallen.

Artikel I, onderdeel AB

Artikel 25 (recht op inzage)

Eerste lid

De richtlijn kent aan de betrokkene het recht toe om van de verantwoordelijke uitsluitsel te verkrijgen over de al dan niet verwerking van de hem betreffende persoonsgegevens, die gegevens in te zien en bepaalde informatie te krijgen, zoals de doelen en de rechtsgrond van de verwerking, de betrokken categorieën van politiegegevens en de voorziene periode van opslag. De Wpg kent thans een soortgelijk recht voor de betrokkene. Om aan dit recht te voldoen volstaat het dat aan de betrokkene in begrijpelijk vorm een volledig overzicht van die gegevens wordt verstrekt, dat wil zeggen in een vorm die de betrokkene in staat stelt

kennis te nemen van deze gegevens en na te gaan of deze juist zijn en overeenkomstig de richtlijn worden verwerkt, zodat hij in voorkomend geval de hem uit hoofde van de richtlijn toegekende rechten kan uitoefenen (overweging 43 RI). Wanneer die mededelingen informatie behelzen over de oorsprong van de persoonsgegevens, mag die informatie de identiteit van natuurlijke personen, met name van vertrouwelijke bronnen, niet onthullen (overweging 43 RI). De tekst van de betreffende bepaling in de richtlijn geeft aanleiding tot redactionele aanpassing van dit lid (art. 14, eerste lid, RI). Daarmee blijft de periode waarover informatie wordt verstrekt over in het verleden gedane verstrekkingen van de betrokkene betreffende politiegegevens en over de ontvangers of categorieën van ontvangers daarvan, evenals nu het geval is gehandhaafd op vier jaar voorafgaande aan een verzoek. Deze in onderdeel c van dit lid ongewijzigd gebleven termijn van vier jaar is vastgesteld naar aanleiding van het arrest van het Hof van Justitie van de Europese Gemeenschappen van 7 mei 2009 (C-553/07 (Rijkeboer). In dat arrest ging het om de verstrekking van persoonsgegevens door gemeenten op grond van de Wet gemeentelijke basisadministratie persoonsgegevens (Wet GBA) (zie voor de inhoud van het arrest en de vaststelling van de termijn in de wet op vier jaar: Kamerstukken II 2010/11, 32 554, nr. 3, blz. 38 en 39, en nr. 6, blz. 32 en 33). Vanwege de reactietermijn voor de verwerkingsverantwoordelijke is het vereiste van schriftelijkheid gehandhaafd. De verantwoordelijke dient binnen zes weken uitsluitsel te geven, deze termijn wordt eveneens gehandhaafd.
De Afdeling advisering van de Raad van State heeft geconstateerd dat er een onderscheid is tussen de justitiële en de strafvorderlijke gegevens waar het gaat om de termijn voor inzage en rectificatie van de gegevens, namelijk 4 en 6 weken met de mogelijkheid van verlenging. Op het punt van de termijnen bestaat eveneens een onderscheid met betrekking tot de politiegegevens: op grond van het voorgestelde artikel 25 Wpg is de termijn zes weken met de mogelijkheid van verlenging voor vier tot zes weken. De toelichting gaat op deze verschillen niet in. De Afdeling adviseert dit alsnog te doen, dan wel uniforme termijnen te hanteren.
Naar aanleiding van het advies van de Afdeling advisering kan worden opgemerkt dat de verantwoordelijke is gehouden een ieder op diens schriftelijke verzoek binnen zes weken mede te delen of, en zo ja welke, deze persoon betreffende politiegegevens verwerking ondergaan. De verantwoordelijke kan zijn beslissing voor ten hoogste vier weken verdagen, dan wel voor ten hoogste zes weken indien blijkt dat bij verschillende regionale of landelijke eenheden van de politie politiegegevens over de verzoeker worden verwerkt (art. 25, eerste lid, Wpg). Destijds is gekozen voor een reactietermijn van zes weken – in plaats van de termijn van vier weken van de Wbp- in verband met de behoefte aan coördinatie van de – in soms meer algemene bewoordingen gestelde – verzoeken aan de politie. In het licht van het voormalige politiebestel betrof dit zowel de situatie dat een verzoek om kennisneming werd gericht aan meerdere regiokorpsen als de situatie dat een verzoek betrekking had op informatie die afkomstig is van een ander korps dan aan welk het verzoek tot kennisneming is gericht. Inmiddels is het politiebestel veranderd. De structuur van de regionale eenheden, als onderdeel van het landelijk politiekorps, is echter gehandhaafd. Voorts is, bij verzoeken om kennisneming die ook aan het openbaar ministerie zijn gericht, afstemming met het openbaar ministerie aan de orde. Teneinde de politie in staat te stellen om naar aanleiding van een verzoek om kennisneming na te gaan of informatie vanuit meerdere korpsen moet komen en, indien dat het geval is, om het antwoord op het verzoek om kennisneming tussen de korpsen onderling en eventueel ook met het openbaar ministerie te kunnen afstemmen, is destijds gekozen voor een termijn van zes weken voor het reageren op een verzoek tot kennisneming, die kan worden verlengd met maximaal zes weken (Kamerstukken II 2005/06,

30 327, nr. 3, blz. 84). Verderop, bij de toelichting op de artikelen 39i en 39j Wjsg (Artikel II, onderdelen AI en AJ) zal worden ingegaan op de reactietermijn bij een verzoek om inzage van justitiële en strafvorderlijke gegevens.

Artikel I, onderdeel AC

Artikel 26 (formaliteiten)

Eerste lid

Dit lid wordt aangevuld vanwege de mogelijkheid die de richtlijn biedt om, wanneer de verwerkingsverantwoordelijke redenen heeft om te twijfelen aan de identiteit van de persoon die een verzoek doet tot inzage of rectificatie van gegevens, de nodige aanvullende informatie vragen ter bevestiging van de identiteit van de betrokkene (art. 12, vijfde lid, RI).

Artikel I, onderdeel AD

Artikel 27 (uitzonderingen)

Eerste lid

Het recht op inzage en het recht op rectificatie zijn geen absolute rechten. Deze rechten kunnen worden beperkt vanwege zwaarder wegende belangen, zoals het belang van het opsporingsonderzoek of van de strafvervolging. Daarbij dient het belang van de betrokkene op inzage te worden afgewogen tegen het belang van de overheid om inzage of rectificatie te weigeren. Met de criteria van noodzakelijkheid en evenredigheid wordt dit tot uitdrukking gebracht. De richtlijn kent verschillende gronden voor de beperking van het recht op inzage of rectificatie (art. 15, eerste lid, en 16, vierde lid, RI). Deze gronden zijn in dit lid opgenomen. Hieraan is toegevoegd de mogelijkheid om inzage of rectificatie te weigeren ingeval van kennelijk ongegronde of buitensporige verzoeken van de betrokkene. In een dergelijk geval biedt de richtlijn de mogelijkheid te weigeren om gevolg te geven aan het verzoek (art. 12, vierde lid, RI). Dit is bij de toelichting op artikel 24a, derde lid, aan de orde gekomen.
Als inzage of rectificatie wordt geweigerd staat de betrokkene de mogelijkheid open van een verzoek tot bemiddeling aan de AP (art. 29, tweede lid) of indiening van een klacht bij de AP (art. 31a, eerste lid). De weigering geldt als een besluit in de zin van de Awb zodat voor de betrokkene tevens beroep open staat bij de bestuursrechter (art. 29 eerste lid).

Tweede lid

De richtlijn schrijft voor dat de verwerkingsverantwoordelijke de betrokkene zonder onnodige vertraging schriftelijk in kennis stelt van een eventuele weigering of beperking van de inzage en van de redenen voor die weigering of beperking (art. 15, derde lid, RI). De termijn voor de reactie van de verantwoordelijke is reeds opgenomen in de wet (art. 25, eerste lid, Wpg). In dit lid is reeds de verplichting opgenomen van de schriftelijkheid. In aanvulling daarop wordt voorgesteld een verplichting op te nemen tot motivering van de afwijzing.

Derde lid

De richtlijn biedt de mogelijkheid om bepaalde verwerkingscategorieën geheel of gedeeltelijk onder de vrijstelling van het eerste lid te laten vallen (art. 15, tweede lid, RI). In dit lid wordt voorgesteld enkele verwerkingsca-

tegorieën uit te zonderen van het recht op inzage en rectificatie. Dit betreft in de eerste plaats de verwerking van politiegegevens met het oog op de controle op en het beheer van een informant, alsmede de beoordeling en verantwoording van het gebruik van informantgegevens, op grond van artikel 12 van de wet. Dit betreft tevens de persoonsgegevens met betrekking tot infiltranten en personen die in aanmerking zijn gebracht voor beschermingsmaatregelen, als bedoeld in het Besluit getuigenbescherming (art. 6:1, eerste lid, Bpg). Verstrekking van deze persoonsgegevens aan de betrokkene is in zijn algemeenheid onwenselijk in het licht van de belangen van opsporing en vervolging.

Artikel 28 (recht op rectificatie en vernietiging van gegevens)

Eerste lid

Dit lid regelt het recht van de betrokkene op rectificatie van de hem betreffende onjuiste politiegegevens en, rekening houdend met het doel van de verwerking, het recht om onvolledige politiegegevens te laten aanvullen. De Wpg kent thans een soortgelijk recht voor de betrokkene. Het recht op rectificatie mag echter geen invloed hebben op, bijvoorbeeld, de inhoud van een getuigenverklaring (overweging 47 RI). De tekst van de betreffende bepaling in de richtlijn geeft aanleiding tot redactionele aanpassing van dit lid (art. 16, eerste lid, RI). Vanwege de reactietermijn voor de verwerkingsverantwoordelijke is het vereiste van schriftelijkheid gehandhaafd. Conform de huidige regeling dient het verzoek de aan te brengen wijzigingen te bevatten.

Tweede lid

Dit lid regelt de verplichting van de verwerkingsverantwoordelijke om politiegegevens te vernietigen als de gegevens feitelijk onjuist, voor het doel van de verwerking onvolledig of niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift worden verwerkt of om te voldoen aan een op de verantwoordelijke rustende wettelijke verplichting. Met de term «vernietiging», in plaats van de in de richtlijn gehanteerde term «wissing», wordt aangesloten bij de bestaande terminologie van de Wpg. Hiermee is materieel hetzelfde beoogd. In plaats van vernietiging draagt de verwerkingsverantwoordelijke zorg voor het afschermen van de verwerking van de politiegegevens, als de juistheid daarvan de gegevens door de betrokkene wordt betwist en de juistheid of onjuistheid niet kan worden geverifieerd, of als de politiegegevens moeten worden bewaard als bewijsmateriaal. Zoals hierboven aan de orde is gekomen, kan een beroep op de onjuistheid van gegevens slechts betrekking hebben op de objectieve juistheid, onafhankelijk van het persoonlijk oordeel. Dit betreft de feitelijke juistheid van de verwerkte politiegegevens en niet de subjectieve juistheid, zoals de juistheid van een verklaring van een getuige. Als de objectieve juistheid van de politiegegevens wordt betwist kunnen de afgeschermde gegevens alleen worden verwerkt voor het doel dat aan vernietiging in de weg staat, zoals het opsporingsonderzoek ten behoeve waarvan de gegevens zijn verzameld. De afscherming kan worden gerealiseerd door de betreffende politiegegevens over te brengen naar een ander verwerkingssysteem of door het niet-beschikbaar maken van de betreffende gegevens. In geautomatiseerde systemen moet de verwerking in beginsel met technische middelen worden beperkt. In afwachting van de verificatie van de juistheid van de gegevens dient verdere verspreiding van de gegevens achterwege te blijven (overweging 47 RI).

Derde lid

De verwerkingsverantwoordelijke stelt de betrokkene binnen vier weken schriftelijk in kennis met betrekking tot de opvolging van zijn verzoek. De tekst van dit lid is redactioneel in overeenstemming gebracht met die van de kennisgeving aan de betrokkene als deze gebruik maakt van het recht op inzage (art. 25, tweede lid).

Vierde en vijfde lid

De verantwoordelijke geeft de verbetering van onjuiste politiegegevens door aan de bevoegde autoriteit van wie de gegevens afkomstig zijn en stelt, wanneer hij politiegegevens heeft gerectificeerd, vernietigd of afgeschermd, de ontvangers daarvan in kennis.

Artikel I, onderdeel AF

Artikel 29 (toepasselijkheid Awb)

Tweede lid

Dit lid betreft de mogelijkheid van bemiddeling. Dit is thans geregeld door middel van een verwijzing naar de artikelen 47 en 48 Wbp. Vanwege het vervallen van de Wbp is de inhoud van artikel 47, eerste lid, Wbp in dit lid overgenomen. De mogelijkheid tot bemiddeling staat open, indien een betrokkene bijvoorbeeld zijn rechten tot inzage in of rectificatie van verwerkte politiegegevens wil uitoefenen en de verwerkingsverantwoordelijke dit weigert. De onderdelen van dit artikel en van artikel 48 Wbp, die betrekking hebben op het gebruik van een geschillenbeslechtingsregeling op grond van een gedragscode zijn niet overgenomen omdat de Wpg niet voorziet in de mogelijkheid van een gedragscode.

Artikel I, onderdeel AH

Artikel 31a (klacht bij Autoriteit Persoonsgegevens)

Eerste lid

In de richtlijn is voorgeschreven dat betrokkene, onverminderd andere mogelijkheden van administratief beroep of een voorziening in rechte, het recht heeft een klacht in te dienen bij de toezichthoudende autoriteit, als de betrokkene van mening is dat de verwerking van de hem betreffende persoonsgegevens inbreuk maakt op de krachtens deze richtlijn vastgestelde bepalingen (art. 52 RI). In dit lid is dit recht van de betrokkene vastgelegd.
De richtlijn schrijft voor dat de betrokkene ook het recht dient hebben op een doeltreffende voorziening in rechte wanneer de toezichthoudende autoriteit de klacht niet behandelt of de betrokkene niet binnen drie maanden van de voortgang of het resultaat van de klacht in kennis stelt (art. 53, tweede lid, RI). Zoals ook in de memorie van toelichting bij de Uitvoeringswet Avg is aangegeven, kent het begrip klacht onder de Awb een eigen betekenis. De klacht heeft daar betrekking op de wijze waarop een bestuursorgaan zich in een bepaalde aangelegenheid jegens hem of een ander heeft gedragen, en de klacht wordt ingediend bij het bestuursorgaan zelf. De klacht als bedoeld in de verordening en de richtlijn wijkt in verschillende opzichten hiervan af. De richtlijn spreekt over het indienen van een klacht bij de toezichthoudende autoriteit over de verwerking van persoonsgegevens door een verwerkingsverantwoordelijke. Het gaat hier niet zozeer om bejegening, maar om de rechtmatigheid van de verwerking. Naar voor het algemene bestuursrecht gebruikelijke termino-

logie gaat het hier niet om een klacht, maar om een verzoek tot handhaving aan de AP. Betrokkene vraagt immers bij de AP aandacht voor een verwerking van zijn persoonsgegevens, die mogelijk niet conform de regels ter implementatie van de richtlijn plaatsvindt. Waar in dit artikel wordt gesproken over klacht, gaat het hier in de terminologie van de Awb derhalve over een verzoek tot handhaving. De schriftelijke reactie van de AP dient dan ook te worden beschouwd als een besluit in de zin van de Awb, waartegen rechtsbescherming open staat langs de gebruikelijke bestuursrechtelijke weg. Dit is in het vijfde lid vastgelegd.

Tweede en derde lid

In dit lid is vastgelegd dat, als de AP niet bevoegd is de klacht te behandelen, de autoriteit is gehouden de klacht zonder onnodige vertraging door te zenden aan de bevoegde toezichthoudende autoriteit in een andere lidstaat. Dit is aan de orde als de klacht betrekking heeft op een gegevensverwerking die op het grondgebied van een andere lidstaat heeft plaatsgevonden. De AP is bevoegd voor het Nederlands grondgebied in Europa gelet op het bepaalde in het voorgestelde artikel 35 omtrent de toezichtsbevoegdheid van deze autoriteit. Op verzoek van de betrokkene verleent de AP verdere bijstand. Hierbij kan worden gedacht aan voorlichting over de verdere procedure, het op verzoek van de betrokkene onderhouden van contacten met de toezichthoudende autoriteit in de andere lidstaat over de afhandeling van de klacht of het verschaffen van informatie over het juridische systeem in de andere lidstaat.

Vierde lid

In de richtlijn is vastgelegd dat de toezichthoudende autoriteit het indienen van klachten faciliteert door maatregelen te nemen, zoals het ter beschikking stellen van een klachtformulier dat ook elektronisch kan worden ingevuld, zonder dat andere communicatiemiddelen worden uitgesloten. Met dit lid wordt deze verplichting geïmplementeerd.

Vijfde lid

Zoals in de toelichting op het eerste lid is aangegeven dient de schriftelijke reactie van de AP op een klacht te worden beschouwd als een besluit in de zin van de Awb, waartegen rechtsbescherming open staat langs de gebruikelijke bestuursrechtelijke weg. Met inachtneming van artikel 4:13 Awb is in dit lid is vastgelegd dat de AP binnen drie maanden een beslissing neemt op een klacht als bedoeld in het eerste lid. Bij een niet-tijdige beslissing kan een dwangsom worden verbeurd (art. 4:17, eerste lid, Awb). Tegen de beslissing van de AP zijn bezwaar en beroep mogelijk, op grond van Afdeling 7.1 Awb.

Zesde lid

De richtlijn bepaalt dat, wanneer een verzoek kennelijk ongegrond of buitensporig is, met name vanwege zijn repetitieve karakter, de toezichthoudende autoriteit op basis van haar administratieve kosten een redelijke vergoeding mag aanrekenen of weigeren aan het verzoek gevolg te geven (art. 46, vierde lid, RI). Ter implementatie van deze bepaling is in dit lid gekozen voor de mogelijkheid voor de AP om een dergelijk verzoek te weigeren. Van de mogelijkheid van het rekenen van een vergoeding is afgezien vanwege de betrekkelijke onbepaaldheid van het begrip «redelijke vergoeding» en het geringe aantal gevallen waarin een dergelijke vergoeding naar verwachting aan de orde zal kunnen zijn. Het is aan de AP om aan te tonen dat het verzoek kennelijk ongegrond of buitensporig is.

Artikel 31b (rechtsvordering tegen de Autoriteit persoonsgegevens)

In dit artikel is vastgelegd dat een vordering tegen de AP bij de Nederlandse rechter wordt ingesteld. Doordat alle lidstaten zijn gehouden de daartoe strekkende bepaling van de richtlijn te implementeren (art. 53, derde lid, RI) dient de betrokkene, als hij een toezichthoudende autoriteit in rechte wil aanspreken, de vordering in te stellen bij het gerecht van de lidstaat waar die autoriteit is gevestigd.

Artikel 31c (schadevergoeding)

De richtlijn verplicht de lidstaten te regelen dat eenieder die materiele of immateriële schade heeft geleden ten gevolge van een onrechtmatige verwerking of van een andere handeling die onverenigbaar is met de krachtens deze richtlijn vastgestelde nationale voorschriften, het recht heeft van de verwerkingsverantwoordelijke of een andere volgens het lidstatelijke recht bevoegde autoriteit, vergoeding van de geleden schade te verkrijgen (art. 56 RI). Thans is eenzelfde bepaling opgenomen in de Wet bescherming persoonsgegevens (art. 49 Wbp). In de Wpg is deze bepaling van overeenkomstige toepassing is verklaard (art. 4, zesde lid, Wpg). Het voorgestelde artikel komt aldus in de plaats van het huidige zesde lid in artikel 4 Wpg.

Artikel I, onderdeel AJ

Artikel 31d (register)

Eerste en tweede lid

De richtlijn bepaalt dat de verwerkingsverantwoordelijke een register bijhoudt van alle categorieën van verwerkingsactiviteiten die onder zijn verantwoordelijkheid vallen (art. 24, eerste lid, RI). Dit betreft een meer algemene beschrijving en heeft geen betrekking op afzonderlijke verwerkingsactiviteiten in een specifiek geval. Ook de verwerker is gehouden een register bij te houden van alle categorieën van verwerkingsactiviteiten die hij namens een verwerkingsverantwoordelijke heeft verricht. In deze leden zijn de gegevens opgesomd die onder de registerplicht vallen.

Artikel I, onderdeel AK

Artikel 32 (documentatie)

Eerste lid

De wet kent thans een zogenaamde protocolplicht, dat wil zeggen dat bepaalde gegevensverwerkingen schriftelijk vastgelegd moeten worden. Anders dan de registerplicht, heeft de protocolplicht betrekking op afzonderlijke verwerkingsactiviteiten in een specifiek geval. De richtlijn schrijft documentatie, dat wil zeggen schriftelijke vastlegging, voor van bepaalde verwerkingsactiviteiten. Het begrip «schriftelijk» heeft betrekking op de vastlegging door middel van schrifttekens, hieronder valt ook de vastlegging in elektronische vorm.
De verplichtingen van de richtlijn vormen aanleiding tot aanpassing c.q. aanvulling van dit lid. De verplichting tot vastlegging van de gegevens die op grond van het bepaalde bij of krachtens artikel 13, vierde lid, worden vastgelegd, in onderdeel b van dit lid, is geschrapt omdat deze verplichting aldaar reeds is geregeld. De vastlegging van de toekenning van de autorisaties wordt overgeheveld naar het voorgestelde artikel 31,

omdat deze geen betrekking heeft op afzonderlijke verwerkingsactiviteiten in een specifiek geval. De vastlegging van de geautomatiseerde vergelijking of het in combinatie met elkaar verwerken van politiegegevens is geschrapt omdat deze vastlegging reeds onder de verplichting tot het langs elektronische weg vastleggen van gegevens valt (logging), op grond van het voorgestelde artikel 32a.
Voorgesteld wordt de vastlegging van de verstrekking van politiegegevens op grond van paragraaf 3, thans in onderdeel f, te verplaatsen naar onderdeel b. De vastlegging omvat de doorgifte van politiegegevens, bedoeld in artikel 17, zesde lid, onderdeel b, en zevende lid, en de rechtstreekse doorgifte, bedoeld in artikel 17, achtste lid.
Toegevoegd zijn de onderdelen c en d. Dit betreft de redenen voor weigering van het recht op inzage en de feiten, gevolgen en genomen maatregelen rond datalekken (art. 15, derde lid, en 30, vijfde lid).

Tweede lid

Dit lid geeft een specifieke regeling voor de vastlegging van specifieke gegevens rond de doorgifte van politiegegevens aan een derde land of internationale organisatie, in de gevallen waarin de gegevens zijn vertrekt op basis van een beoordeling van de passende waarborgen van dat land of die organisatie door de verwerkingsverantwoordelijke of bij afwijkingen voor specifieke situaties (art. 37, derde lid en 38, derde lid, RI). De vastlegging van deze gegevens dienst om de AP in staat te stellen de rechtmatigheid van de verstrekking te toetsen.

Vierde lid

De tekst van dit lid is aangepast vanwege de voorgestelde schrapping in het eerste lid van het huidige onderdeel d (geautomatiseerde vergelijking of het in combinatie met elkaar verwerken van politiegegevens, bedoeld in de artikelen 8, derde lid, en 11, eerste, tweede en vierde lid).

Artikel I, onderdeel AL

Artikel 32a (logging)

Eerste lid

De logging betreft het geautomatiseerd vastleggen van gegevens over de verwerking van persoonsgegevens. De richtlijn bevat een verplichting voor de verwerkingsverantwoordelijke om logbestanden bij te houden van ten minste de volgende activiteiten in systemen voor geautomatiseerde verwerking: de verzameling, wijziging, raadpleging, verstrekking onder meer in de vorm van doorgiften, combinatie en het vernietigen van politiegegevens. In dit lid is deze verplichting vastgelegd. De identificatie van de persoon die persoonsgegevens heeft geraadpleegd of bekendgemaakt, dient te worden geregistreerd en *op basis daarvan* moeten de redenen voor de verwerkingsactiviteiten kunnen worden vastgesteld (overweging 57 RI). Aldus maken de logbestanden van raadpleging en bekendmakingen het mogelijk de redenen, de datum en het tijdstip van die handelingen te achterhalen en indien mogelijk de identiteit van de persoon die persoonsgegevens heeft geraadpleegd of bekendgemaakt, en de identiteit van de ontvangers van die persoonsgegevens. De richtlijn gegevensbescherming opsporing en vervolging bevat geen bewaartermijn voor de logging, gelet op het doel van de gegevensverwerking is de verordening gegevensbescherming op die gegevens van toepassing. De loggingplicht omvat de schriftelijke vastlegging van bepaalde gegevens, op basis van de protocolplicht in het huidige artikel 32. Aldus vallen de in dit artikel vastgelegde verplichtingen tot vastlegging van de

geautomatiseerde vergelijking of het in combinatie met elkaar verwerken van politiegegevens (eerste lid, onderdeel d), de hernieuwde verwerking van politiegegevens (eerste lid, onderdeel e), verwerkingen ten aanzien waarvan aanwijzingen bestaan dat zij onbevoegd of onrechtmatig zijn verricht (eerste lid, onderdeel g) en de geautomatiseerde vergelijking van gegevens (eerste lid, onderdeel h) onder de voorgestelde loggingplicht. De logging betreft een geautomatiseerd proces, dat doorgaans standaard is ingebouwd in het informatiesysteem. Niettemin voorziet de richtlijn in een langere implementatietermijn voor de loggingplicht. Dit is in het algemeen deel van deze memorie aan de orde gekomen.
De verwerkingsverantwoordelijke dient de bewaartermijn voor de gelogde gegevens vast te stellen in overeenstemming met de verordening gegevensbescherming. Het ligt in de rede de bewaartermijn te koppelen aan de periodieke privacy audits (art. 33 Wpg). Voor deze audits geldt een termijn van vier jaar (art. 6:5, eerste lid, Bpg).

Tweede lid

De vastgelegde gegevens kunnen uitsluitend worden gebruikt voor de controle van de rechtmatigheid van de gegevensverwerking, interne controles, ter waarborging van de integriteit en de beveiliging van de politiegegevens en voor strafrechtelijke procedures. Voor dit laatste kan worden gedacht aan strafvervolging op grond van ambtelijke corruptie, waarbij de gelogde gegevens kunnen worden gebruikt om aan te tonen dat een persoon op een bepaald tijdstip in het systeem gegevens heeft geraadpleegd, gewijzigd of gewist.

Artikel I, onderdeel AN

Artikel 33a (melding datalekken)

Eerste lid

Een inbreuk in verband met persoonsgegevens kan, wanneer deze niet tijdig en adequaat wordt aangepakt, resulteren in lichamelijke, materiële of immateriële schade voor natuurlijk personen, zoals verlies van controle over hun persoonsgegevens, of beperking van hun rechten, discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, ongeoorloofde ongedaanmaking van pseudonimisering, reputatieschade, verlies van vertrouwelijkheid van door beroepsgeheim beschermde gegevens of enig ander aanzienlijk economische of maatschappelijk nadeel voor de natuurlijke persoon in kwestie (overweging 62 RI). Daarom moet de verwerkingsverantwoordelijke de AP zonder onnodige vertraging en waar mogelijk binnen 72 uur nadat hij er kennis van heeft genomen in kennis stellen van een inbreuk op de beveiliging (art. 30 en overweging 61 RI). De melding is mondeling of schriftelijk. Deze verplichting is niet van toepassing als het niet waarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van personen met zich meebrengt. Als de melding na 72 uur wordt gedaan wordt daarbij een motivering gegeven voor de vertraging.

Tweede en derde lid

De richtlijn stelt bepaalde eisen aan de inhoud van de melding. Die eisen zijn in dit lid vastgelegd. Als het niet mogelijk is de informatie gelijktijdig te verstrekken dan kan deze zonder onnodige vertraging in stappen worden verstrekt. Gelet op de tekst van de richtlijn kan de verantwoordelijke daarbij kiezen tussen mondelinge en schriftelijke melding.

Vierde lid

Niet uitgesloten is dat een datalek betrekking heeft op gegevens die van een andere lidstaat zijn ontvangen. In dat geval deelt de verwerkingsverantwoordelijke een inbreuk op de beveiliging mee aan de verantwoordelijke van deze lidstaat. De mededeling dient zonder onredelijke vertraging te worden verricht.

Vijfde, zesde en zevende lid

In het vijfde lid wordt voorzien in de verplichting voor de verantwoordelijke om een inbreuk op de beveiliging mede te delen aan de betrokkene. Deze verplichting is van toepassing als de inbreuk waarschijnlijk een hoog risico voor de rechten en vrijheden van personen met zich brengt. De mededeling bevat een omschrijving van de aard van de inbreuk op de beveiliging en ten minste de punten, bedoeld in het tweede lid, onderdelen b, c en d.
In het zesde lid is geregeld dat de verplichting tot melding van een datalek aan de betrokkene in bepaalde omstandigheden niet van toepassing is. Dit is het geval als passende technische en organisatorische beschermingsmaatregelen zijn getroffen en deze maatregelen zijn toegepast op de betreffende politiegegevens, zoals het gebruik van encryptie. Dit is eveneens het geval als achteraf maatregelen zijn getroffen om ervoor te zorgen dat het hoge risico zich waarschijnlijk niet meer zal voordoen, zoals het op afstand wissen van de gelekte gegevens. Dit is tenslotte het geval als de mededeling een onevenredige inspanning zou vergen. In dat geval volgt een openbare mededeling of vergelijke maatregel ter informering van de betrokkenen.
In bepaalde omstandigheden kan melding van een datalalek aan de betrokkene worden uitgesteld. Dit betreft de gevallen waarin een weigeringsgrond voor het recht van de betrokkene op inzage of rectificatie aan de orde is. Deze gronden zijn opgenomen in artikel 27, eerste lid.

Artikel 33b (voorafgaand consulteren Autoriteit persoonsgegevens)

Eerste, tweede en derde lid

De richtlijn bevat de verplichting in bepaalde omstandigheden de toezichthoudende autoriteit te raadplegen voordat politiegegevens worden verwerkt in een nieuw bestand en (1) uit een gegevensbeschermingseffectbeoordeling, ofwel Privacy Impact Assessment, blijkt dat de verwerking een hoog risico zou opleveren als de verantwoordelijke geen maatregelen treft om dat te beperken of (2) de aard van de verwerking, in het bijzonder wanneer gebruik wordt gemaakt van nieuwe technologieën, mechanismen of procedures, een hoog risico meebrengt voor de voor de rechten en vrijheden van betrokkenen (art. 28, eerste lid, RI). De laatstgenoemde grond vormt thans reeds onderdeel van de Wpg (art. 35, vierde lid, Wpg). De eerstgenoemde grond is nieuw, dit hangt samen met de introductie in de richtlijn van een verplichting tot het opstellen van een PIA. De AP kan een lijst opstellen van de verwerkingen waarvoor de voorafgaande consultatie vereist is. De verantwoordelijke is gehouden de AP de PIA te verstrekken en, desgevraagd alle andere informatie op grond waarvan de AP de conformiteit van de verwerking en met name de risico's voor de bescherming van persoonsgegevens van de betrokkene en de betrokken waarborgen kan beoordelen.

Vierde en vijfde lid

Wanneer de AP van oordeel is dat de voorgenomen verwerking van politiegegevens niet voldoet aan het bij of krachtens deze wet bepaalde, geeft zij binnen zes weken schriftelijk advies aan de verwerkingsverantwoordelijke en, in voorkomend geval, aan de verwerker. Deze termijn kan, rekening houdend met de complexiteit van de voorgenomen verwerking, worden verlengd met een termijn van een maand. In dit geval wordt de verwerkingsverantwoordelijke of de verwerker, binnen een maand na de ontvangst van het verzoek in kennis gesteld van onder meer de redenen voor de vertraging.

Artikel I, onderdeel AO

Artikel 34 (privacyfunctionaris)

Eerste lid

Op dit moment beschikken de politie, Koninklijke marechaussee en bijzondere opsporingsdiensten over privacyfunctionarissen met bijzondere deskundigheid ten aanzien van privacyrecht. Deze situatie blijft met dit wetsvoorstel gehandhaafd. Inmiddels is de Politiewet 2012 in werking getreden en is er nog maar één politiekorps en daarmee nog maar één verantwoordelijke. Gezien de omvang van dit korps is een enkele privacyfunctionaris bij de politie niet toereikend. Daarom is nu bepaald dat één verantwoordelijke ook meerdere privacyfunctionarissen kan benoemen.

Vierde lid

Voorgesteld wordt dit lid te schrappen omdat de verwerkingsverantwoordelijke, op grond van het voorgestelde artikel 36, vijfde lid, reeds gehouden zal zijn de functionaris voor gegevensbescherming aan te melden bij de AP.

Artikel I, onderdeel AP

Artikel 35 (toezicht Autoriteit persoonsgegevens)

Eerste lid

Voor de bescherming van natuurlijke personen in verband met de verwerking van hun persoonsgegevens is het wezenlijk belang dat in de lidstaten toezichthoudende autoriteiten worden ingesteld die toezien op de toepassing van de krachtens de richtlijn vastgestelde bepalingen en bijdragen aan een consequentie toepassing daarvan in de gehele Unie. In dit lid wordt geregeld dat de AP toezicht uitoefent op de verwerking van politiegegevens overeenkomstig het bij of krachtens deze wet bepaalde. Vanwege het vervallen van de Wet bescherming persoonsgegevens wordt verwezen naar de Uitvoeringswet Avg. Die wet bevat regels over de op- en inrichting van de AP, waardoor gewaarborgd is dat de AP bij de uitvoering van haar taken en de uitoefening van haar bevoegdheden volledig onafhankelijk optreedt. Het toezicht op de verwerking van politiegegevens is beperkt tot het Nederlandse grondgebied in Europa, en heeft geen betrekking op de overzeese delen van het Rijk (Bonaire, Sint Eustatius en Saba).

Tweede lid

Vanwege het vervallen van de Wbp wordt voor enkele taakbestanddelen van de AP verwezen naar de Uitvoeringswet Avg. Dit betreft in de eerste plaats de regeling omtrent het advies van de AP over voorstellen van wet en ontwerpen van algemene maatregelen van bestuur die geheel of voor een belangrijk deel betrekking hebben op de verwerking van persoonsgegevens. Dit is thans geregeld door middel van verwijzing naar in art. 52, tweede lid, Wbp. Dit betreft in de tweede plaats de regeling van het toezicht op de naleving door de leden en buitengewone leden van het College, de ambtenaren van het secretariaat van het College, alsmede de bij besluit van het College aangewezen personen. Dit is thans geregeld door middel van verwijzing naar artikel 61 Wbp.
De bevoegdheid van de AP tot het opleggen van een last onder bestuursdwang, thans geregeld door middel van verwijzing naar artikel 65 Wbp, wordt in artikel 35b geregeld. In dat artikel worden alle bevoegdheden van de AP samengebracht.

Derde lid

In dit lid is thans de bevoegdheid van de AP geregeld tot het opleggen van een bestuurlijke boete. Voorgesteld wordt deze bevoegdheid over te hevelen naar artikel 35b, waarin zijn alle bevoegdheden van de AP worden samengebracht.

Artikel I, onderdeel AQ

Artikel 35a (positie Autoriteit persoonsgegevens)

Eerste lid

De positie en taken van de AP worden geregeld in de Algemene verordening gegevensbescherming. In de verordening is bepaald dat de AP bij de uitvoering van haar taken en de uitoefening van haar bevoegdheden volledig onafhankelijk optreedt (art. 52, eerste lid, Avg). Een soortgelijke bepaling is opgenomen in de richtlijn (art. 42, eerste lid, RI), zodat de onafhankelijk positie van de AP ook verzekerd moet zijn bij het toezicht op de naleving van de richtlijn. In de huidige Wbp is de onafhankelijke positie van de AP overigens reeds vastgelegd (art. 52, tweede lid, Wbp).

Tweede lid

In de Kaderwet adviescolleges is reeds vastgelegd dat de leden van een adviescollege worden benoemd op grond van de deskundigheid die nodig is voor de advisering op het beleidsterrein waarvoor het adviescollege is ingesteld alsmede op grond van maatschappelijke kennis en ervaring (art. 12, eerste lid, Kaderwet adviescolleges). In de richtlijn is meer specifiek vastgelegd dat de leden van de AP over de nodige deskundigheid en ervaring te beschikken, met name op het gebied van de bescherming van persoonsgegevens (art. 43, tweede lid, RI). De verordening bevat een soortgelijk voorschrift (art. 53, tweede lid, Avg).

Derde en vierde lid

Ter implementatie van de richtlijn is in deze leden vastgelegd dat de leden van de AP vrij zijn van externe invloed, geen instructies aanvaarden van anderen bij de uitvoering van het toezicht en zich onthouden van handelingen die niet verenigbaar zijn met hun taken (art. 42, tweede en derde lid, RI).

Artikel 35b (taken Autoriteit persoonsgegevens)

Eerste lid

De richtlijn bevat een uitgebreide regeling van de taken van de toezichthoudende autoriteit (art. 46, eerste lid, RI). Deze taken zijn in dit lid opgenomen. Daarbij zijn de verwijzingen naar de andere artikelen van de richtlijn vervangen door verwijzingen naar de artikelen in deze wet, waarmee die andere artikelen zijn geïmplementeerd.

Tweede lid

In de richtlijn is vastgelegd dat elke toezichthoudende autoriteit haar taken kosteloos verricht voor de betrokkene en voor de functionaris voor gegevensbescherming (art. 46, derde lid, RI). Met dit lid wordt deze verplichting geïmplementeerd.

Artikel 35c (bevoegdheden Autoriteit persoonsgegevens)

In dit artikel zijn de bevoegdheden van de AP samengebracht. Dit betreft de huidige bevoegdheden van de AP, aangevuld met de bevoegdheden op basis van de richtlijn. Daarnaast beschikt de AP als toezichthouder in de zin van de Algemene wet bestuursrecht over de bevoegdheden met betrekking tot het toezicht op de naleving, bedoeld in Titel 5.2. van die wet.

Eerste lid

De richtlijn verplicht te voorzien in effectieve onderzoeksbevoegdheden, effectieve bevoegdheden tot het treffen van corrigerende maatregelen, zoals het waarschuwen van de verwerkingsverantwoordelijke, het gelasten de verwerking in overeenstemming te brengen met de richtlijn of het opleggen van een verwerkingsverbod, en effectieve adviesbevoegdheden (art. 47, eerste en tweede lid, RI).
De AP kan de verwerkingsverantwoordelijke of de verwerker waarschuwen dat met de voorgenomen verwerkingen waarschijnlijk een inbreuk wordt gemaakt op het bij of krachtens deze wet bepaalde.
De AP kan een last onder bestuursdwang opleggen ter handhaving van het bij of krachtens deze wet bepaalde. Deze bevoegdheid is thans geregeld doordat artikel 65 Wbp van overeenkomstige toepassing is.
De AP kan een bestuurlijke boete opleggen als de verwerkingsverantwoordelijke handelt in strijd met de verplichting tot de schriftelijke vastlegging rond de verwerking van politiegegevens. Deze bevoegdheid is thans vastgelegd in artikel 35, derde lid. Naar aanleiding van het advies van de AP is voorgesteld om de bevoegdheid van de AP tot het opleggen van een bestuurlijke boete te verruimen tot de melding van datalekken en het maximum boetebedrag met het oog op de afschrikkende werking te verhogen van de vierde tot de vijfde boetecategorie van artikel 23, vierde lid, Sr.
De Afdeling advisering heeft erop gewezen dat aansluiting bij de huidige regeling op basis van de Wpg en de Wjsg tot gevolg heeft dat de voorgestelde bestuurlijke boetes voor politie en justitie sterk afwijken van overtreding van soms dezelfde normen door andere overheidsorganen en instanties op grond van de verordening. Voorts is het gevolg dat voor tal van normen waarvoor op grond van de verordening een boete kan worden opgelegd een bestuurlijke boete op grond van de Wpg en de Wjsg niet mogelijk zal zijn. In het bijzonder is de vraag hoe deze verschillen zich verhouden tot het standpunt van de regering dat het bieden van de mogelijkheid tot het opleggen van boetes bij de inbreuk op de overheid het belangrijke signaal afgeeft dat ook de overheid zelf zich heeft te

houden aan de verplichtingen van het gegevensbeschermingsrecht en hierin niet anders wordt behandeld dan het bedrijfsleven (Kamerstukken II 2017/18, 34 851, nr. 3, blz. 100–101). Gelet oog het voorgaande adviseert de Afdeling in de toelichting nader in te gaan op de discrepantie tussen de regeling van de bestuurlijke boete in de verordening en die in het voorstel.
Naar aanleiding van dit advies wordt het volgende opgemerkt. De regeling van de bevoegdheden van de toezichthoudende autoriteit op basis van de verordening wijkt af van die van de richtlijn. Voor wat betreft de hoogte van de op te leggen bestuurlijke boetes voorziet de verordening in een regeling op grond waarvan inbreuken op de een aantal bepalingen is onderworpen aan administratieve geldboeten tot tien miljoen euro of, voor een onderneming, tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is (art. 83, vierde lid, Avg). Inbreuken op andere bepalingen zijn onderworpen aan administratieve geldboeten tot twintig miljoen euro of, voor een onderneming, tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is (art. 83, vijfde lid, Avg). De maximale bedragen van respectievelijk tien en twintig miljoen euro bieden de mogelijkheid om effectief op te treden als ondernemingen aanzienlijk geldelijk voordeel hebben behaald vanwege het niet naleven van de verplichtingen van de verordening. Voor overheidsorganen, en het openbaar ministerie en de opsporingsinstanties in het bijzonder, is dit echter minder aan de orde omdat de bedrijfsvoering niet is gericht op het behalen van profijt of winst. Hier komt bij dat een bestuurlijke boete voor politie en justitie ten koste gaat van de begroting van deze instanties, zodat een bestuurlijke boete van een maximale hoogte als in de verordening voorzien, serieuze gevolgen zal hebben voor de dienstverlening van deze organen. In de praktijk zal dit kunnen betekenen dat bezuinigd zal moeten worden op personeel en materieel, bijvoorbeeld op de inzet van agenten of de verbetering van de ICT-structuur, hetgeen ten koste zal gaan van de veiligheid in de samenleving. Daarbij is niemand gebaat. Uiteraard dient ook de overheid zich te houden aan de verplichtingen van het gegevensbeschermingsrecht, en hierin niet anders te worden behandeld dan het bedrijfsleven, maar dit neemt niet weg dat daarbij rekening wordt gehouden met de aard en omstandigheden van de gegevensverwerking met het oog op de opsporing en vervolging van strafbare feiten evenals het feit dat er thans – anders dan onder de Wet bescherming persoonsgegevens – op basis van de Wpg en de Wjsg een zeer beperkte bevoegdheid voor de AP is om een bestuurlijke boete op te leggen.
Dit klemt temeer daar de naleving van de privacywetgeving door de politie thans nog niet volledig op orde is. Het treffen van organisatorische en technische maatregelen, zoals aanpassing in de ICT-voorzieningen, is van essentieel belang voor de naleving van de normen op het gebied van de gegevensbescherming. De korpschef heeft hiertoe een meerjarig verbeterplan opgesteld waarover uw kamer bij brief is geïnformeerd (Kamerstukken II, 2015/16, 33 842, nr. 4). Er is sprake van een ontwikkeltraject, waarbij wordt gestreefd naar de volledige naleving van de bepalingen van de Wpg op termijn. In het licht van dit traject ligt het in de rede om thans niet volledig aan te sluiten bij de lijst van overtredingen, zoals door de AP voorgesteld. Daarbij moet ook worden opgemerkt dat de niet naleving van sommige voorschriften reeds is gesanctioneerd met de mogelijkheid van een bestuursrechtelijke boete, zoals de verplichting tot medewerking met de toezichthoudende autoriteit (artikel 5:20 Awb). In afwachting van de herziening van de Wpg en de Wjsg verdient het de voorkeur een voorlopige balans te vinden waarbij enerzijds wordt voorzien in afschrikwekkende en effectieve sancties en anderzijds rekening wordt gehouden met de draagkracht van de betreffende organen en de mogelijkheid om op korte termijn te voldoen aan de soms tamelijk complexe normen van de richtlijn.

Gelet op het voorgaande wordt voorgesteld langs de volgende lijn te komen tot aanpassing van de regeling voor het opleggen van een bestuurlijke boete. Voor wat betreft de hoogte van de bestuurlijke boete kan worden aangesloten bij de tweedeling van de verordening, met dien verstande dat de maximale bedragen naar beneden worden bijgesteld. Voor de hoogte van de bestuurlijke boetes verdient het de voorkeur de aansluiting bij de boetecategorieën van artikel 23 van het Wetboek van Strafrecht te handhaven. Dit is in overeenstemming met het uitgangspunt van de Boetewijzer voor het bepalen van de maximumboete in wetgeving en het streven van het kabinet naar meer eenheid in de hoogte van geldboetes op het terrein van het straf- en bestuursrecht en het zoveel mogelijk voorkomen van ongerechtvaardigde, niet verklaarbare verschillen (Kamerstukken II 2012/13, 33 400 VI, nr. 80). Aldus kan voor de minder zware overtredingen van de bepalingen van de richtlijn worden gekozen voor de mogelijkheid van een bestuurlijke boete van ten hoogste de vijfde categorie van artikel 23, eerste lid, Sr (€ 83.000.–) en voor de zwaardere overtredingen de mogelijkheid van een bestuurlijke boete van ten hoogste de zesde categorie van artikel 23, eerste lid, Sr (€ 830.000.–).
Voor wat betreft de gevallen waarin een bestuurlijke boete kan worden opgelegd kan worden uitgegaan van twee categorieën van normschendingen die vanuit het oogpunt van adequate gegevensbescherming in aanmerking komen voor sanctionering door middel van een bestuurlijke boete, te weten die welke betrekking hebben op de verplichtingen van de verwerkingsverantwoordelijke en die welke betrekking hebben op de rechten van de betrokkene. De eerstgenoemde categorie betreft de voorschriften van de richtlijn met betrekking tot de gegevensbescherming door ontwerp en door standaardinstellingen (art. 20 RI), de verwerking van gevoelige persoonsgegevens (art. 10 RI), de verwerker (art. 22 RI), het register van verwerkingsactiviteiten (art. 24 RI), de beveiliging van de verwerking (art. 29 RI), de melding van inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit en mededeling aan de betrokkene (art. 30 en 31 RI), de gegevensbeschermingseffectbeoordeling (art. 27 RI), de voorafgaande raadpleging (art. 28 RI) en de functionaris voor gegevensbescherming (art. 32–34 RI). De tweede categorie betreft de voorschriften van de richtlijn met betrekking tot de transparante informatie (art. 12 RI), de verstrekking van informatie aan de betrokkene (art. 13 RI), het recht op inzage van de betrokkene (art. 14 RI), het recht op rectificatie of wissing en op beperking van de verwerking en de kennisgeving daarvan aan de ontvangers (art. 16 RI) en de geautomatiseerde individuele besluitvorming (art. 11 RI).
Op basis van deze benadering wordt een regeling voorgesteld als volgt:

a. een bestuurlijke boete van ten hoogste de vijfde categorie van artikel 23, eerste lid, Sr (€ 83.000.–) kan worden opgelegd voor de overtreding van de artikelen 4a, eerste tot en met vijfde lid (gegevensbescherming door beveiliging en ontwerp), 4b (gegevensbescherming door standaardinstellingen), 4c (gegevensbeschermingseffectbeoordeling), 6c (verwerker), 31d (register van de verwerkingsactiviteiten, 32 (documentatie), 33a (melding inbreuk in verband met persoonsgegevens aan AP en mededeling aan de betrokkene), 33b (Voorafgaande raadpleging) en 36 (functionaris voor gegevensbescherming).
b. een bestuurlijke boete van ten hoogste de zesde categorie van artikel 23, eerste lid, Sr (€ 830.000.–) kan worden opgelegd voor de overtreding van de artikelen 5 (verwerking gevoelige persoonsgegevens), 7a, (geautomatiseerde besluitvorming), 24a (transparante informatie), 24b (te verstrekken informatie aan betrokkene), 25 (recht van inzage) en 28 (recht van rectificatie).

Verder is de AP bevoegd tot het verstrekken van een advies aan de verwerkingsverantwoordelijke naar aanleiding van een voorafgaande

consultatie. Hiervoor kan worden verwezen naar de toelichting op het voorgestelde artikel 33b.
Ten slotte kan de AP de verwerkingsverantwoordelijke verplichten een inbreuk in verband met persoonsgegevens te melden aan de betrokkene. Dit is aan de orde als de verwerkingsverantwoordelijke die inbreuk nog niet aan de betrokkene heeft meegedeeld en de kans bestaat dat deze een hoog risico met zich meebrengt (art. 31, vierde lid RI).

Tweede lid

In de verordening is de bevoegdheid van de toezichthoudende autoriteit geregeld om administratieve geldboetes op te leggen. Dergelijke boetes worden in Nederland bestuurlijke boetes genoemd. Bij het besluit over de vraag of op grond van de verordening een administratieve geldboete wordt opgelegd en over de hoogte daarvan wordt voor elk concreet geval naar behoren rekening gehouden met een aantal omstandigheden (art. 83, tweede lid, Avg). Omwille van de rechtszekerheid is de verplichting van de Autoriteit persoonsgegevens van de verordening, om rekening te houden met de bepaalde omstandigheden bij het besluit over het opleggen van een boete en over de hoogte daarvan, eveneens van toepassing bij een dergelijk besluit op grond van het eerste lid. Dit met dien verstande dat de betreffende omstandigheden zijn toegesneden op de verwerking van politiegegevens door de bevoegde autoriteiten. Dit betreft de omstandigheden, genoemd in artikel 83, tweede lid, onderdelen a tot en met i, Avg.

Derde lid

In dit lid is vastgelegd dat de werking van de beschikking tot oplegging van de bestuurlijke boete wordt opgeschort totdat de bezwaar- of beroepstermijn is verstreken of, indien bezwaar is gemaakt respectievelijk beroep is ingesteld, op het bezwaar respectievelijk het beroep is beslist. Deze regeling is identiek aan die van het huidige artikel 71 Wbp, dat thans van overeenkomstige toepassing is (art. 35, derde lid).

Vierde lid

In dit lid is vastgelegd dat de uitoefening van bepaalde bevoegdheden door de AP geldt als een besluit in de zin van de Algemene wet bestuursrecht. Dit betreft de bevoegdheid tot het verstrekken van advies aan de verwerkingsverantwoordelijke naar aanleiding van de voorafgaande consultatie, bedoeld in artikel 33b, en de bevoegdheid tot het verplichten van de verwerkingsverantwoordelijke tot het melden van een inbreuk in verband met persoonsgegevens, bedoeld in artikel 33a, aan de betrokkene. Aangesloten is bij de regeling van artikel 14 van de Uitvoeringswet Avg. Hiermee wordt onduidelijkheid over het rechtskarakter van de uitoefening van deze bevoegdheden door de AP voorkomen. Op grond van de Algemene wet bestuursrecht gelden de last onder bestuursdwang, de bestuurlijke boete reeds als een besluit in de zin van de Awb.

Artikel 35d (samenwerking met andere toezichthoudende autoriteiten)

Eerste lid

De richtlijn schrijft voor dat de toezichthoudende autoriteiten elkaar relevante informatie en wederzijdse bijstand verstrekken om de richtlijn op een consequente manier ten uitvoer te leggen en toe te passen, en maatregelen nemen om doeltreffend met elkaar samen te werken (art. 50, eerste lid, RI). Deze verplichting is in dit lid opgenomen.

Tweede lid

De richtlijn schrift voor dat dat de toezichthoudende autoriteit alle passende maatregelen neemt die nodig zijn om een verzoek om informatie of wederzijdse bijstand van een andere toezichthoudende autoriteit zonder onnodige vertraging en in ieder geval binnen één maand na de ontvangst ervan te beantwoorden (art. 50, tweede lid, RI). Deze verplichting is in dit lid opgenomen. De verzoekende autoriteit wordt geïnformeerd over de resultaten of, in voorkomend geval, de voortgang.

Derde tot en met het vijfde lid

Een verzoek om bijstand bevat ten minste het doel van en de redenen voor het verzoek. Het verzoek kan slechts onder bepaalde voorwaarden gemotiveerd worden afgewezen. De bijstand is in beginsel kosteloos, de toezichthoudende autoriteiten kunnen echter regels overeenkomen om elkaar te vergoeden voor specifieke uitgaven die voortvloeien uit het verstrekken van wederzijdse bijstand in uitzonderlijke omstandigheden (art. 50, zevende lid, RI). De verstrekte informatie wordt alleen gebruikt voor het doel waarvoor om die informatie is verzocht.

Zesde lid

In het Bpg kunnen nadere regels worden gesteld over de wijze van verstrekking van de informatie. Dit kan het gebruik van een standaardformulier betreffen dat langs elektronische weg wordt overgedragen (art. 50, zesde lid, RI). De Commissie kan aan de hand van de zogenaamde uitvoeringshandelingen het model en de procedures voor de wederzijdse bijstand vastleggen, alsmede de regelingen voor de elektronische uitwisseling van informatie tussen de toezichthoudende autoriteiten onderling. De uitvoeringshandelingen worden vastgesteld volgens de onderzoeksprocedure, als beschreven in artikel 5 van Verordening (EU) nr. 182/2011.

Artikel I, onderdeel AR

Artikel 36 (functionaris voor gegevensverwerking)

Eerste lid

De verwerkingsverantwoordelijke wijst een functionaris voor gegevensbescherming aan die hem bijstaat bij het interne toezicht op de naleving van het bij of krachtens deze wet bepaalde. Anders dan onder de huidige wet is het benoemen van een functionaris voor gegevensbescherming niet meer facultatief. De functionaris voor gegevensbescherming dient in staat te zijn taken en verplichtingen onafhankelijk en in overeenstemming met het nationale recht uit te voeren (overweging 63 RI). Deze functionaris heeft derhalve, anders dan de privacyfunctionaris, een meer onafhankelijke positie ten opzichte van de verwerkingsverantwoordelijke. In lijn met de richtlijn (art. 32, derde lid, RI) kan voor verschillende bevoegde autoriteiten, rekening houdend met hun organisatiestructuur en omvang, één functionaris voor gegevensbescherming worden aangewezen. De functionaris voor gegevensbescherming wordt tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van politiegegevens.
De functionaris voor gegevensbescherming wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wet- en regelgeving en de praktijk inzake de gegevensbescherming en zijn vermogen om de hem opgedragen taken uit te voeren. De aangewezen persoon kan zijn taken in deeltijd uitoefenen,

tevens kunnen verschillende verantwoordelijken samen een functionaris voor gegevensbescherming benoemen (overweging 63 RI).

Tweede lid

In dit lid zijn de geschiktheidseisen voor de functionaris gegevensbescherming vastgelegd. Daarbij zijn de deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en het vermogen de wettelijk vastgelegde taken te vervullen, van bijzonder belang.

Derde lid

In dit lid zijn de taken van de functionaris voor gegevensbescherming opgenomen. Dit is allereerst het toezicht op de naleving van het bij of krachtens de wet bepaalde door de verwerkingsverantwoordelijke. Dit toezicht ziet ook op de toewijzing van de autorisaties, de bewustmaking en opleiding van de ambtenaren van politie die zijn betrokken bij de verwerking van politiegegevens en de audits. Hierbij werkt de functionaris voor gegevensbescherming samen met de AP en treedt de functionaris op als contactpunt voor de AP voor aangelegenheden in verband met de verwerking van persoonsgegevens.
De functionaris is niet alleen belast met toezicht op de naleving van het bij of krachtens de wet bepaalde maar heeft ook taken op het gebied van de advisering van de verantwoordelijke en de werknemers die persoonsgegevens verwerken over de nakoming van hun verplichtingen inzake gegevensbescherming (overweging 63 RI).

Vierde lid

In dit lid is vastgelegd dat de functionaris voor gegevensbescherming jaarlijks een verslag opstelt van zijn bevindingen.

Vijfde lid

In dit lid is vastgelegd dat de verwerkingsverantwoordelijke de contactgegevens van de functionaris voor gegevensbescherming openbaar maakt en de functionaris voor gegevensbescherming aanmeldt bij de AP.

Zesde lid

In dit lid is vastgelegd dat de verwerkingsverantwoordelijke de functionaris voor gegevensbescherming de benodigde middelen ter beschikking stelt voor het vervullen van zijn wettelijke taken en het in standhouden van zijn deskundigheid.

Artikel I, onderdeel AT

Artikel 36c

Eerste lid

In onderdeel a wordt verwezen naar artikel 4, zesde lid, van de wet. Vanwege het voorstel om dit lid te schrappen behoeft de verwijzing aanpassing. Voorgesteld wordt om onderdeel a te schrappen, en de inhoud van dit lid op te nemen in een nieuw derde lid.
In onderdeel g, voorheen onderdeel h, wordt de opsomming van de artikelen, waarin wordt verwezen naar het College bescherming persoonsgegevens, thans de AP, aangepast. Toegevoegd worden de artikelen 17a, tweede lid, onder b, 25, eerste lid, 29, tweede lid, 32, tweede lid en 33, tweede lid. De verwijzing naar artikel 34, vierde lid is niet meer correct

vanwege de schrapping van dat artikel. Voorgesteld wordt de inhoud van dat lid over te hevelen naar het vijfde lid, zodat de verplichting tot aanmelding van de privacyfunctionaris bij de toezichthoudende autoriteit voor de BES van toepassing blijft.

Tweede lid

In het algemeen deel van deze memorie is reeds aan de orde gekomen dat de richtlijn en de verordening gegevensbescherming niet van toepassing zijn op de BES. In het systeem van de richtlijn gelden de BES als derde land. Implementatie van de voorschriften van de richtlijn werkt echter door op de regels voor de BES. Om te voorkomen dat een aantal bepalingen van toepassing is die voor de BES minder goed werkbaar zijn, wordt voorgesteld die bepalingen uit te zonderen van paragraaf 5a van de wet. Dit betreft de volgende bepalingen:
Artikel 4, derde lid, betreft de verplichting om, voor zover mogelijk, politiegegevens die op feiten zijn gebaseerd te onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd. Deze verplichting wordt uitgezonderd omdat deze thans niet geldt voor de BES.
De artikelen 4a en 4b regelen de gegevensbescherming door ontwerp en door standaardinstellingen. Deze artikelen worden uitgezonderd omdat de oorspronkelijke verplichting tot beveiliging van de gegevens, die thans is opgenomen in artikel 3, vierde lid, voor de BES wordt gehandhaafd.
Artikel 4c regelt de verplichting tot het opstellen van een gegevensbeschermingseffectbeoordeling. Deze verplichting wordt uitgezonderd omdat deze thans niet geldt voor de BES.
Artikel 6b betreft de verplichting om, voor zover mogelijk, onderscheid te maken tussen verschillende categorieën van betrokkenen. Deze verplichting wordt uitgezonderd omdat deze thans niet geldt voor de BES.
Artikel 6c regelt de positie van de verwerker. Voor de BES is reeds voorzien in de regeling van de positie van de verwerker, vanwege het van overeenkomstige toepassing zijn van artikel 14 van de Wet bescherming persoonsgegevens BES. Hiervoor wordt verwezen naar de toelichting op het vierde lid.
Artikel 7a bevat het verbod op een besluit dat is uitsluitend op geautomatiseerde verwerking is gebaseerd. Deze verplichting wordt uitgezonderd omdat deze thans niet geldt voor de BES.
Artikel 15a regelt de verplichting tot het ter beschikking stellen van politiegegevens aan andere bevoegde autoriteiten in andere lidstaten van de Europese Unie. Dit artikel wordt uitgezonderd omdat de BES geen lidstaat zijn van de Europese Unie.
Artikel 24a bevat procedurele voorschriften rond de verstrekking van informatie aan de betrokkene. Deze verplichting wordt uitgezonderd omdat deze thans niet geldt voor de BES.
Artikel 24b betreft de meer actieve verplichting tot het verstrekken van bepaalde informatie over de gegevensverwerking aan de betrokkene. Deze verplichting wordt uitgezonderd omdat deze thans niet geldt voor de BES.
Artikel 31a regelt de mogelijkheid om een klacht in te dienen bij de AP. Voor de BES betreft dit de Commissie van toezicht bescherming persoonsgegevens BES, waar de betrokkene dan een klacht kan indienen als hij van mening is dat de verwerking van persoonsgegevens niet in overeenstemming is met het bij of krachtens deze wet bepaalde.
Artikel 31b betreft de verplichting een schriftelijk register bij te houden dat de in dat artikel aangewezen gegevens bevat. Deze verplichting wordt uitgezonderd omdat deze thans niet geldt voor de BES.
Artikel 32 regelt de documentatie van bepaalde gegevens met betrekking tot de verwerking van politiegegevens. Deze verplichting wordt uitgezonderd omdat deze thans niet geldt voor de BES.

Artikel 32a bevat de verplicht tot de geautomatiseerde vastlegging (logging) van bepaalde gegevens met betrekking tot de gegevensverwerking. Deze verplichting wordt uitgezonderd omdat deze thans niet geldt voor de BES.
Artikel 33a regelt de verplichting tot melding van datalekken. Deze verplichting wordt uitgezonderd omdat deze thans niet geldt voor de BES.
Artikel 33b regelt de verplichting tot het voorafgaand consulteren van de AP. Deze verplichting is thans opgenomen in artikel 35. Deze bepaling is reeds uitgezonderd omdat het (voormalige) College bescherming persoonsgegevens geen taken krijgt in de BES. Het toezicht door de Commissie van toezicht bescherming persoonsgegevens BES wordt geregeld in artikel 36g. Vanwege dezelfde reden wordt voorgesteld ook de artikelen 35a en 36a, die de taken en bevoegdheden van de AP regelen, uit te zonderen.
Artikel 35c betreft de vertrouwelijke melding van inbreuken op de richtlijn. Deze bepaling uitgezonderd omdat de richtlijn niet geldt voor de BES.
Artikel 35d betreft de samenwerking met toezichthoudende autoriteiten in andere lidstaten. Deze bepaling is eveneens uitgezonderd omdat de richtlijn niet geldt voor de BES.

Derde lid

Dit lid bevat de verplichting tot beveiliging van de verwerkte politiegegevens, overeenkomstig het bestaande artikel 3, vierde lid, van de wet. Voorgesteld wordt deze bepaling te schrappen vanwege de implementatie van de richtlijn, die strekt tot opneming van nieuwe bepalingen omtrent de beveiliging van gegevens door ontwerp en door standaardinstellingen (artikelen 4a en 4b). Met dit lid wordt de oorspronkelijke verplichting tot beveiliging van de verwerkte gegevens gehandhaafd voor de BES.

Vierde lid

Dit lid regelt het van overeenkomstige toepassing zijn van enkele bepalingen van de Wet bescherming persoonsgegevens BES. Dit betreft artikel 14, eerste, tweede, derde en vijfde lid (de verwerking van persoonsgegevens door een bewerker), 39 (schadevergoeding) en 40 (rechterlijk verbod op handelen in strijd met de bij of krachtens die wet gegeven voorschriften) van de Wet bescherming persoonsgegevens BES.

Vijfde lid

Vanwege de voorgestelde verplichting tot benoeming van een functionaris voor gegevensbescherming (art. 36) komt de verplichting tot aanmelding van de privacyfunctionaris bij de Commissie van toezicht bescherming persoonsgegevens BES te vervallen. De benoeming van een functionaris voor gegevensbescherming, naast de privacyfunctionaris, is voor de BES echter minder goed uitvoerbaar. Daarom wordt voorgesteld de huidige regeling rond de benoeming van een privacyfunctionaris te handhaven. Met dit lid wordt de eerdergenoemde verplichting tot aanmelding van die functionaris bij de Commissie van toezicht bescherming persoonsgegevens BES gehandhaafd.

Artikel I, onderdeel AV

Artikel 36e (verstrekking aan Nederlandse opsporingsinstanties en het openbaar ministerie en aan derde landen en internationale organisaties)

In dit artikel wordt de verstrekking van politiegegevens door de BES aan de Nederlandse politie, openbaar ministerie en bijzondere opsporingsdiensten geregeld. Voor wat betreft de verstrekking van politiegegevens door de BES aan derde landen en internationale organisaties is de regeling in de Wpg voor de verstrekking van politiegegevens aan buitenlandse opsporingsinstanties van overeenkomstige toepassing (art. 17 en 36a Wpg). De verstrekking van politiegegevens aan Aruba, Curaçao en Sint Maarten valt onder deze regeling (art. 17, derde lid, Wpg). Het regime van de richtlijn gegevensbescherming gaat uit van een besluit van de Commissie van de Europese Unie over het toereikende beschermingsniveau in het betreffende land of organisatie (artikel 35, eerste lid, onder d, RI). Met het voorgestelde artikel 17a wordt de regeling van de richtlijn in de Wpg geïmplementeerd. Omdat de richtlijn niet van toepassing is op de BES kan deze regeling echter niet van overeenkomstige toepassing worden verklaard. Voorgesteld wordt aan dit artikel enkele nieuwe leden toe te voegen, die inhoudelijk gelijk zijn aan het huidige artikel 17, tweede, derde, vijfde, zesde en zevende lid, van de Wpg. Hiermee wordt de huidige regeling van de Wpg voor de verstrekking van gegevens door de BES aan derde landen en internationale organisaties gecontinueerd.

Artikel I, onderdeel AX

Artikel 46 (toepassing gegevensverwerking bijzondere opsporingsdiensten)

Eerste lid

De bijzondere opsporingsdiensten zijn onder meer belast met de strafrechtelijke handhaving van de rechtsorde op de beleidsterreinen waarvoor de Minister van Financiën, de Minister van Infrastructuur en Milieu, de Minister van Economische Zaken en de Minister van Sociale Zaken en Werkgelegenheid verantwoordelijkheid dragen, en de opsporing van strafbare feiten die zijn geconstateerd in het kader van die taak (art. 3 Wet op de bijzondere opsporingsdiensten). De bijzondere opsporingsdiensten zijn dus niet belast met de uitvoering van de politietaak maar met een deel daarvan, namelijk de strafrechtelijke handhaving van de rechtsorde op een specifiek beleidsterrein. In dit lid is bepaald dat de artikelen 10, eerste lid, onder a, en 12 van de Wpg van overeenkomstige toepassing zijn op de verwerking van politiegegevens door een ambtenaar, werkzaam bij een bijzondere opsporingsdienst. Bij algemene maatregel van bestuur kunnen ook andere onderdelen van het bij of krachtens deze wet bepaalde van overeenkomstige toepassing worden verklaard op de verwerking van persoonsgegevens door een ambtenaar, werkzaam bij een bijzondere opsporingsdienst. Inmiddels is dit uitgewerkt in het Besluit politiegegevens bijzondere opsporingsdiensten. Daarmee is de Wpg materieel van toepassing op de gegevensverwerking van de bijzondere opsporingsdiensten voor de taken, bedoeld in artikel 3 van de Wet op de bijzondere opsporingsdiensten.
De implementatie van de richtlijn geeft aanleiding tot aanpassing van de bestaande bepalingen van de Wpg en tot invoeging van nieuwe bepalingen van die wet. Dit heeft gevolgen voor de van overeenkomstige toepassing van bepalingen van de Wpg op de gegevensverwerking door de bijzondere opsporingsdiensten. Daartoe zal het Besluit politiegegevens bijzondere opsporingsdiensten worden aangepast, zodat ook de

gegevensverwerking door de ambtenaren, werkzaam bij de bijzondere opsporingsdiensten volledig voldoet aan hetgeen in de richtlijn is voorgeschreven.
Tevens wordt voorgesteld dit lid aan te vullen vanwege de verwerking van politiegegevens door de buitengewoon opsporingsambtenaren, bedoeld in artikel 142, eerste lid, Sv. De buitengewoon opsporingsambtenaren zijn, evenmin als de bijzondere opsporingsdiensten, belast met de uitvoering van de politietaak maar met een deel daarvan, namelijk de opsporing van bepaalde aangewezen categorieën van strafbare feiten. De opsporingsbevoegdheid van deze opsporingsambtenaren strekt zich uit tot de in de akte of aanwijzing aangeduide strafbare feiten, de akte of aanwijzing kan bepalen dat de opsporingsbevoegdheid alle strafbare feiten omvat (art. 142, tweede lid, Sv). De voorgestelde aanpassing van dit lid voorziet er in dat Onze Ministers en Onze Minister wie het mede aangaat bij algemene maatregel van bestuur andere onderdelen van het bij of krachtens deze wet bepaalde van overeenkomstige toepassing verklaren op de verwerking van persoonsgegevens door een buitengewoon opsporingsambtenaar. Daartoe zal ook het Besluit politiegegevens bijzondere opsporingsdiensten worden aangepast. In dit besluit zal de verwerkingsverantwoordelijke worden aangewezen voor de verwerking van politiegegevens door een buitengewoon opsporingsambtenaar; dit is de werkgever, bedoeld in artikel 1, onderdeel h, van het Besluit buitengewoon opsporingsambtenaar. In dit besluit zal ook de van overeenkomstige toepassing van onderdelen van de Wpg op de verwerking van politiegegevens door een buitengewone opsporingsambtenaar, als bedoeld in artikel 142, eerste lid, Sv, worden uitgewerkt. Daarbij zal worden voorzien in specifieke regels voor de verstrekking van politiegegevens over de naleving of uitvoering van wetgeving op een bepaald beleidsterrein, die een buitengewoon opsporingsambtenaar worden verwerkt, ten behoeve van het toezicht op de naleving van wetgeving op dat beleidsterrein.

Tweede lid

In artikel 15 is voorzien in een verplichting voor de verwerkingsverantwoordelijke om politiegegevens beschikbaar te stellen aan zowel de personen die onder zijn beheer vallen als de personen die onder het beheer van een andere verantwoordelijke vallen en die zijn geautoriseerd voor de verwerking van politiegegevens, voor zover zij die gegevens behoeven voor de uitvoering van hun taak. Dit principe van de beschikbaarstelling van gegevens binnen de politie wordt ook wel aangeduid als de «free flow of information». Dit principe was oorspronkelijk bedoeld voor de uitwisseling van gegevens tussen de voormalige regionale politiekorpsen. Dit betreft de opsporingsambtenaren, bedoeld onder artikel 141, onderdelen b en c, Sv. Inmiddels is de verwerking van politiegegevens door de opsporingsambtenaren, werkzaam bij de bijzondere opsporingsdiensten, onder de reikwijdte van de Wpg gebracht. Dit betreft de opsporingsambtenaren, bedoeld in artikel 141, onderdeel d, Sv. Aldus is dit beginsel van toepassing op de uitwisseling van politiegegevens tussen de politie, de Koninklijke marechaussee en de bijzondere opsporingsdiensten.
De richtlijn strekt ertoe de verwerking van politiegegevens door opsporingsambtenaren met het oog op de richtlijntaken onder de reikwijdte van de Wpg te brengen, ook die door de buitengewone opsporingsambtenaren. Dit betekent dat het principe van de «free flow of information» ook voor deze opsporingsambtenaren zal gaan gelden, met dien verstande dat de «free flow» dan is beperkt tot de persoonsgegevens die worden verwerkt op grond van de artikelen van de wet die van toepassing zijn op die opsporingsambtenaren en voor zover niet is voorzien in aanvullende

gronden tot het weigeren of beperken van de ter beschikkingstelling van politiegegevens, op grond van artikel 15, tweede lid, van de wet.

II. De Wet justitiële en strafvorderlijke gegevens

Artikel II, onderdeel A

Artikel 1

Onderdelen a tot en met c

De voorgestelde wijzigingen in de definities van justitiële en strafvorderlijke gegevens maken duidelijk dat het dient te gaan om gegevens die zijn of worden verwerkt in een gegevensbestand. Deze nadere afbakening sluit aan bij het toepassingsgebied van de richtlijn die alleen van toepassing is op persoonsgegevens die in een bestand zijn of worden opgenomen (art. 2, tweede lid, RI). Een gegevensbestand kan zowel geautomatiseerd als in papieren vorm beschikbaar zijn. De voorgestelde aanpassing in de definitie van het begrip persoonsdossier is een technische verduidelijking, die voortvloeit uit de definitie van het begrip bestand in de richtlijn (art. 3, onderdeel 6, RI).

Onderdeel d

Op de verwerking van persoonsgegevens inzake de tenuitvoerlegging van straffen is de richtlijn van toepassing (art. 2, eerste lid, juncto art. 1, eerste lid, RI). Met de introductie van het begrip tenuitvoerleggingsgegevens kunnen voorschriften uit de richtlijn ook voor deze gegevens in dit wetsvoorstel worden geïmplementeerd. Persoonsgegevens die worden gebruikt voor de tenuitvoerlegging van strafrechtelijke beslissingen kunnen vrijheidsbenemende of beperkende straffen en maatregelen inhouden, alsook geldstraffen in de vorm van een strafbeschikking. Persoonsgegevens die op vrijheidsbenemende straffen en maatregelen betrekking hebben zijn in regelgeving nader omschreven, zoals in het besluit Penitentiaire maatregel, de Beginselenwet verpleging ter beschikking gestelden en de Beginselenwet justitiële jeugdinrichtingen. Uit deze specifieke wet- en regelgeving volgt welke persoonsgegevens voor de tenuitvoerlegging van de daarin bedoelde straffen en maatregelen worden gebruikt. Geen tenuitvoerleggingsgegevens zijn persoonsgegevens die worden gebruikt voor de tenuitvoerlegging van een andere dan een strafrechtelijke beslissing, zoals voor de inning van een opgelegde bestuurlijke boete. Evenals bij justitiële en strafvorderlijke gegevens omvatten tenuitvoerleggingsgegevens gegevens die op een rechtspersoon betrekking hebben.
In het kader van het toepassingsgebied van de richtlijn gegevensbescherming opsporing en vervolging verdient de verwerking van persoonsgegevens door het Centraal Justitieel Incassobureau (hierna: CJIB) specifieke aandacht. Het CJIB is een agentschap dat ressorteert onder de Minister van Justitie en Veiligheid en dat is belast met de ondersteuning van het openbaar ministerie bij de tenuitvoerlegging van opgelegde sancties, waaronder de inning van geldbedragen (art. 2 Instellingsbesluit CJIB). Daarnaast is het CJIB in opdracht van andere bestuursorganen betrokken bij de inning van opgelegde geldsancties. Thans valt de verwerking van persoonsgegevens door het CJIB ten behoeve van de afdoening van overtredingen van de Wet administratiefrechtelijke handhaving verkeersvoorschriften onder het regime van de Wet bescherming persoonsgegevens. Ditzelfde geldt voor de strafrechtelijke afdoening van overtredingen waarvoor boa's bevoegd zijn. De verwerking van persoonsgegevens rond de administratiefrechtelijke afdoening valt onder de reikwijdte van de verordening, de gegevensverwerking rond de

strafrechtelijke afdoening valt onder de reikwijdte van de richtlijn. Voor de gegevensverwerking rond de strafrechtelijke afdoening wordt het regime van de Wbp dus vervangen door dat van de Wjsg. De verwerking van persoonsgegevens door het CJIB ter ondersteuning van het openbaar ministerie in de fase van de tenuitvoerlegging gaat onder het regime van de Wjsg vallen. Deze gegevensverwerking valt onder de reikwijdte van de richtlijn. Thans valt de verwerking van persoonsgegevens ten behoeve van andere bestuursorganen onder het regime van de Wbp. Dit regime wordt vervangen door dat van de verordening.

Onderdeel e

De richtlijn is van toepassing op de verwerking van persoonsgegevens door nationale gerechten in het kader van hun gerechtelijke activiteiten die binnen de doeleinden van de richtlijn vallen (art. 45, eerste lid en overwegingen 11 en 80, RI). Op de verwerking van persoonsgegevens door gerechten in het kader van het behandelen en beslissen van zaken waarop de Nederlandse wetgeving inzake strafzaken van toepassing is, is thans de Wet bescherming persoonsgegevens van toepassing. Hierop is de richtlijn van toepassing. De verwerking van persoonsgegevens door gerechtelijke instanties in het kader van de behandeling van strafzaken is te onderscheiden van de verwerking van justitiële en strafvorderlijke gegevens. Om ook de verwerking van persoonsgegevens door gerechtelijke instanties in het kader van de behandeling van strafzaken onder het toepassingsbereik van het wetsvoorstel te brengen, bevat het voorstel een definitie van het begrip gerechtelijke strafgegevens. Geen gerechtelijke strafgegevens zijn persoonsgegevens die in het kader van burgerlijke of bestuursrechtelijke zaken worden verwerkt door gerechtelijke instanties. De richtlijn is daarop niet van toepassing.

Onderdeel i

Voor een toelichting op het begrip persoonsgegeven wordt verwezen naar de toelichting op artikel 1, onderdeel b, van de Wpg.

Onderdeel j

Een betrokkene kan bijvoorbeeld een verdachte, veroordeelde, slachtoffer of getuige zijn. Bepalend is dat een gegeven op een persoon betrekking heeft en dit gegeven onder een wettelijk gedefinieerde categorie gegevens valt.

Onderdeel k

Er zijn verschillende verwerkingsverantwoordelijken die persoonsgegevens verwerken waarop de richtlijn van toepassing is. In dit onderdeel zijn de verwerkingsverantwoordelijken voor achtereenvolgens justitiële gegevens, strafvorderlijke gegevens, persoonsdossiers, tenuitvoerleggingsgegevens en gerechtelijke strafgegevens benoemd. Daarmee wordt duidelijk wie voor welke gegevens verwerkingsverantwoordelijke is.
Voor wat betreft de verwerking van tenuitvoerleggingsgegevens berust thans op grond van de Beginselenwetten de verantwoordelijkheid voor de verwerking van tenuitvoerleggingsgegevens inzake vrijheidsstraffen en vrijheidsbenemende maatregelen bij de Minister van Justitie en Veiligheid. Voor andere sancties, zoals taakstraffen en strafbeschikkingen, berust de verantwoordelijkheid op grond van het Wetboek van Strafvordering bij het College procureurs-generaal. Deze verdeling in de verantwoordelijkheid voor de gegevensverwerking wijzigt indien de Wet herziening tenuitvoerlegging strafrechtelijke beslissingen in werking

treedt. Het wetsvoorstel voorziet in samenloop, bij de toelichting op artikel V wordt hierop nader in gegaan.
Voor de verwerking van gerechtelijke strafgegevens zijn de organen die met rechtspraak zijn belast verwerkingsverantwoordelijke. Dit sluit aan bij de huidige praktijk waarin deze organen als verantwoordelijke voor de verwerking van persoonsgegevens bepaalde systemen bij de AP hebben aangemeld, zoals die in het kader van de procesvoering van strafzaken en het gerechtelijk vooronderzoek. Daarnaast is een ontwikkeling waarin de feitelijke zorg en het beheer voor de systemen waarin gerechtelijke strafgegevens worden verwerkt bij de Raad voor de rechtspraak berust. De Raad voor de rechtspraak is op grond van artikel 91 van de Wet op de rechterlijke organisatie verantwoordelijk voor ondersteuning van de bedrijfsvoering van de gerechten, in het bijzonder gericht op automatisering en bestuurlijke informatievoorziening. De Raad voor de rechtspraak is eigenaar van een eigen ICT-bedrijf spir-it dat de ontwikkeling en het beheer van de digitale systemen van de rechtspraak uitvoert. Er is sprake van een centraal systeem met een centrale gegevensopslag, in tegenstelling tot situaties waarbij een gerecht over eigen databases en gegevenssystemen beschikt.
De Raad draagt zorg voor een zorgvuldige gegevensverwerking door onder meer de ontwikkeling van privacykaders. Daarnaast voldoet de Raad aan de informatieplicht jegens de betrokkene in de zin van thans nog de Wbp en geeft hij informatie over de wijze waarop deze betrokkene haar rechten kan uitoefenen, onder meer door informatieverschaffing via de website van de rechtspraak. De ontwikkeling van digitale systemen vindt plaats in samenspraak met de gerechtsbesturen. Ieder gerechtsbestuur moet persoonsgegevens in een zaaksdossier kunnen aanmaken en bijwerken dat bij dat betreffende gerecht aanhangig is. Door middel van interne afspraken tussen de Raad voor de rechtspraak en de gerechtsbesturen wordt recht gedaan aan de onderlinge verdeling van verantwoordelijkheden ten aanzien van de nakoming van de verplichtingen uit de richtlijn.

Onderdelen l en m

Deze onderdelen bevatten definities over de begrippen verwerker en verwerking. Degene die onder het rechtstreeks gezag van een verwerkingsverantwoordelijke persoonsgegevens verwerkt, is geen verwerker (art. 23 RI). Mandatering voor de verwerking van persoonsgegevens binnen bestuursrechtelijke gezagsverhoudingen, blijft daarmee mogelijk. Een voorbeeld hiervan betreft het CJIB. Het CJIB is een agentschap dat ressorteert onder de Minister van Justitie en Veiligheid, en dat is belast met de ondersteuning van het openbaar ministerie bij de tenuitvoerlegging van opgelegde sancties, waaronder de inning van geldbedragen (art. 2 Instellingsbesluit CJIB). Het CJIB is hiervoor gemandateerd. Op de mandaatverlener rust de verplichting de toepasselijke voorschriften inzake bescherming van persoonsgegevens na te komen voor de verwerkingen die aan het CJIB zijn gemandateerd. Dit is thans nog het College van procureurs-generaal. Daarnaast int het CJIB, in opdracht van andere bestuursorganen, opgelegde geldsancties. Hierbij fungeert het CJIB als verwerker, onder het regime van de verordening.
In de richtlijn worden in de definitie van het begrip verwerking (art. 3, onder 2, RI) de woorden «wissen of vernietigen» gebezigd. In de richtlijn wordt verder uitsluitend het woord «wissen» gebruikt. Bij de implementatie is er voor gekozen telkens het woord «vernietigen» te gebruiken daar waar de richtlijn verwijst naar «wissen». Dit sluit beter aan bij het Nederlandse taalgebruik; gegevens op papier kunnen worden vernietigd maar niet gewist.

Onderdeel n

In de richtlijn wordt het begrip «verwerkingsbeperking» gedefinieerd (art. 3, derde lid, RI). Om duidelijker tot uitdrukking te brengen wat hiermee wordt bedoeld, wordt in het wetsvoorstel hiervoor het begrip «afschermen» gebruikt. Het markeren van gegevens maakt herkenbaar voor welke gegevens het doel is de verwerking ervan in de toekomst verder te beperken.

Onderdelen p tot en met u

Deze onderdelen bevatten definities over achtereenvolgens de begrippen inbreuk op de beveiliging, genetische gegevens, biometrische gegevens, gegevens over gezondheid, profilering en ontvanger. Voor een toelichting op deze begrippen wordt verwezen naar de toelichting op artikel 1, onderdelen p tot en met u, van de Wpg.

Onderdelen v, w, x, z en aa

Deze onderdelen bevatten definities over de begrippen bevoegde autoriteit, derde land, internationale organisatie, Autoriteit persoonsgegevens en lidstaat. Voor een toelichting op deze begrippen wordt verwezen naar de toelichting op artikel 1, onderdelen h, k, v, w en y van de Wpg.

Artikel II, onderdelen B, C en D

Artikelen 3, 7, 7a en 7b

Voor een toelichting op deze artikelen over de juistheid en kwaliteit van gegevens, evenredigheid van en de doeleinden waarvoor verwerking mogelijk is, de verplichting tot het treffen van passende en technische organisatorische maatregelen, ontwerp en gegevensbescherming door standaardinstellingen en de gevallen waarin een effectbeoordeling dient te worden uitgevoerd wordt hier volstaan met te verwijzen naar de toelichting op de artikelen 3, 4 en 4a tot en met 4c, van de Wpg.

Artikel II, onderdeel D

Artikel 7c

De richtlijn verplicht er toe om, in voorkomend geval en voor zover mogelijk een duidelijk onderscheid te maken tussen gegevens betreffende verschillende categorieën van betrokkenen, zoals verdachten, slachtoffers, getuigen en veroordeelden (art. 6 RI). Dit onderscheid is niet dwingend of limitatief voorgeschreven. Voor de verwerking van justitiële gegevens benoemt het voorgestelde artikel een onderscheid tussen veroordeelden en vrijgesprokenen. Dit onderscheid is niet definitief maar dient te worden geplaatst in het perspectief van de strafrechtspleging. Een persoon kan voor een strafbaar feit worden veroordeeld en voor een ander strafbaar feit worden vrijgesproken. Ook is mogelijk dat geen veroordeling en ook geen vrijspraak volgt, maar ontslag van rechtsvervolging. Dezelfde persoon valt dan voor verschillende strafbare feiten in verschillende categorieën. Ook kunnen justitiële gegevens soms op verdachten betrekking hebben. Doordat het onderscheid geldt «in voorkomend geval» en «voor zover mogelijk» bestaat een zekere marge voor de verwerkingsverantwoordelijke bij de invulling van deze verplichting. Dit biedt ruimte om aan te sluiten bij en rekening te houden met wat haalbaar is voor de praktijk.

Artikelen 7d tot en met 7f

Voor een toelichting op deze artikelen over achtereenvolgens de inschakeling van een verwerker, geautomatiseerde besluiten en het verkrijgen van schadevergoeding wordt hier volstaan met te verwijzen naar de toelichting op de artikelen 6c, 7a en 31c van de Wpg.

Artikel II, onderdeel E

Artikel 8

Het huidige artikel regelt in het derde lid en daarop volgende leden de doorgifte van justitiële gegevens aan het buitenland, waarbij tevens een nader onderscheid wordt aangehouden voor verstrekkingen aan andere lidstaten en derde landen. De richtlijn maakt uitsluitend onderscheid tussen lidstaten en derde landen, met een uitgebreid eigen regime voor verstrekking aan derde landen. Gelet hierop is er voor gekozen de artikelleden of delen daarvan die betrekking hebben op grensoverschrijdende verstrekkingen te laten vervallen (eerste lid en vierde tot en met negende lid). In plaats daarvan worden de voorschriften uit de richtlijn over verstrekkingen van justitiële gegevens aan andere lidstaten en aan derde landen elders in de afdeling afzonderlijk geregeld. Het resterende artikel beperkt zich daarmee tot verstrekkingen aan Nederlandse rechterlijke ambtenaren, de Minister en de in dat artikel aangeduide personen en lichamen die bevoegd zijn een strafbeschikking uit te vaardigen.

Artikel II, onderdeel F

Artikel 8a

In dit artikel wordt voor de bevoegdheid tot verstrekking van justitiële gegevens door het College van procureurs-generaal verwezen naar gevallen waarin het op grond van artikel 39e of 39f bevoegd is tot verstrekking van strafvorderlijke gegevens. Hierbij is vereist dat dit noodzakelijk is met het oog op een zwaarwegend algemeen belang. Artikel 39e omvat ook grensoverschrijdende verstrekkingen en aan internationale organen of strafgerechten. Doordat de richtlijn onderscheid maakt tussen de verwerking van persoonsgegevens in de lidstaten van de Europese Unie enerzijds en de doorgifte van persoonsgegevens aan derde landen en internationale organisaties anderzijds, worden deze verstrekkingen in het wetsvoorstel apart geregeld (zie voor strafvorderlijke gegevens het nieuw voorgestelde artikel 39ga) en heeft het huidige artikel hierop niet langer betrekking. Als gevolg hiervan dienen de verwijzingen in het onderhavige artikel naar de gevallen waarin bevoegdheid tot verstrekking is toegestaan te worden aangepast. Door die aanpassing blijft verstrekking door het College van procureurs-generaal van justitiële gegevens in grensoverschrijdende situaties en aan internationale organen mogelijk, in de in het wetsvoorstel geregelde gevallen.

Artikel II, onderdelen G en H

Artikelen 9 en 13

De verwijzing in het tweede lid van beide artikelen naar een ander artikellid is technisch niet correct en met de voorgestelde aanpassingen wordt dit gecorrigeerd.

Artikel II, onderdeel J

Artikel 15

Voor een toelichting op de voorgestelde wijziging in dit artikel wordt verwezen naar de toelichting op artikel 22 van de Wpg.

Artikel II, onderdeel K

Artikelen 16 en 16a

Voor een toelichting op deze artikelen, over het ter beschikking stellen van justitiële gegevens aan andere lidstaten van de Europese Unie en doorgifte daarvan aan derde landen, wordt verwezen naar de toelichting op de artikelen 15a en 17a van de Wpg.

Artikel II, onderdeel M

Artikelen 17a en 17b

Voor de toelichting op het voorgestelde artikel 17a over informatieverplichtingen aan betrokkene wordt verwezen naar de toelichting op artikel 24a, eerste lid, van de Wpg. Voor de toelichting op het voorgestelde artikel 17b wordt verwezen naar de toelichting op artikel 24b eerste en tweede lid, van de Wpg.

Artikel II, onderdeel N

Artikel 18

De richtlijn kent aan de betrokkene het recht om van de verantwoordelijke uitsluitsel te verkrijgen over de al dan niet verwerking van de hem betreffende persoonsgegevens en die gegevens in te zien. De Wjsg kent thans een soortgelijk recht voor betrokkene, met dien verstande dat dit in de voorgestelde wijzigingen wordt uitgebreid met het krijgen van in de richtlijn nader omschreven informatie, zoals de doelen en de rechtsgrond van de verwerking, de betrokken categorieën van justitiële gegevens en de voorziene periode van de opslag (art. 14, eerste lid, van de RI). Vanwege de reactietermijn voor de verwerkingsverantwoordelijke is het vereiste van schriftelijkheid gehandhaafd. De verantwoordelijke dient binnen vier weken uitsluitsel te geven en inzage te bieden, deze termijn wordt gehandhaafd. De termijn geldt ook voor de afdoening van een verzoek dat zich uitstrekt tot de verkrijging van informatie, bedoeld in eerste lid, onderdelen a tot en met g. Die informatie kan schriftelijk worden verstrekt. De huidige wet bepaalt in het derde lid dat bij ministeriële regeling nadere regels kunnen worden gesteld omtrent het verzoek en de wijze van kennisneming. In het verleden is van die mogelijkheid geen gebruik gemaakt, zodat wordt voorgesteld de grondslag voor een ministeriële regeling te laten vervallen. Een dergelijke ministeriële regeling is voor de implementatie ook niet noodzakelijk.

Artikel II, onderdeel O

Artikel 19

Met de vastlegging en termijn van bewaring van verstrekkingen als bedoeld in het eerste lid, wordt gedoeld op verstrekkingen van justitiële gegevens aan andere personen, organen en instanties die op grond van afdeling 2 van de Wjsg zijn toegestaan. De voorgestelde wijziging verwijst naar de juiste afdeling waarin dit wordt geregeld.

Een verzoek tot inzage van in het verleden gedane verstrekkingen is thans onderwerp van artikel 19, tweede lid, van de Wet justitiële en strafvorderlijke gegevens. Dit is in het voorstel onderwerp van artikel 18, eerste lid, onderdeel c, zodat het tweede lid hier vervalt.

Artikel II, onderdeel Q

Artikel 21

De richtlijn bepaalt dat de verwerkingsverantwoordelijke de betrokkene zonder onnodige vertraging schriftelijk in kennis stelt van de opvolging van zijn verzoek (art. 12, derde lid, van de richtlijn). Het voorgestelde eerste lid geeft hieraan uitvoering. In het tweede lid wordt bepaald wanneer een verzoek tot inzage of het recht op rectificatie wordt afgewezen. Indien een verzoek betrekking heeft op het verkrijgen van overige voor betrokkene relevante informatie, zoals over de doelen en de rechtsgrond van de verwerking, de betrokken categorie van de gegevens, de voorziene periode van opslag, en over verscheidene andere zaken (zie daarvoor onderdelen a tot en met g van artikel 18, eerste lid), kan een afwijzing die aan de in het tweede lid aangegeven voorwaarden voldoet daarop eveneens betrekking hebben. De richtlijn kent verschillende gronden voor de beperking van het recht op inzage of rectificatie (art. 15, eerste lid, en 16, vierde lid, RI). Deze gronden zijn in het tweede lid opgenomen. Hieraan is toegevoegd de mogelijkheid om inzage of rectificatie te weigeren ingeval van kennelijk ongegronde of buitensporige verzoeken van de betrokkene. In een dergelijk geval biedt de richtlijn de mogelijkheid te weigeren om gevolg te geven aan het verzoek (art. 12, vierde lid, RI). In het derde lid wordt bepaald dat een gehele of gedeeltelijke weigering schriftelijk is en wordt gemotiveerd.

Artikel 22

Voor de toelichting op deze artikelen over het recht van een betrokkene op rectificatie van hem betreffende justitiële gegevens, over vernietiging van die gegevens of het afschermen daarvan wordt verwezen naar de toelichting op artikel 28 van de Wpg.

Artikel II, onderdeel R

Artikel 23

Voor de toelichting op de in dit artikel voorgestelde wijziging betreffende de mogelijkheid tot bemiddeling of advisering door de AP bij een geschil met een verwerkingsverantwoordelijke, wordt verwezen naar de toelichting op artikel 29 van de Wpg.

Artikel II, onderdeel S

Artikel 24

Indien blijkt dat onjuiste persoonsgegevens zijn doorgezonden, of dat de persoonsgegevens op onrechtmatige wijze zijn doorgezonden, bepaalt de richtlijn dat de ontvanger daarvan onverwijld in kennis wordt gesteld. In dat geval moeten de persoonsgegevens worden gerectificeerd of gewist, of de verwerking beperkt (art. 7, derde lid, RI). Anders dan de richtlijn bevat het thans geldende artikel een beperking in de tijd van de personen en instanties waaraan eerder gegevens zijn verstrekt en is er een voorbehoud indien het doen van een mededeling onmogelijk blijkt of een onevenredige inspanning kost. Doordat de richtlijn deze beperkingen niet kent, wordt voorgesteld deze te schrappen. Het vervallen van deze

beperking betekent niet dat bij de kennisgeving aan ontvangers in de praktijk daardoor geen enkele beperking in de tijd mag plaatsvinden. Een beperking hierin is evenwel niet a priori in overeenstemming met de richtlijn, aangezien die daarin niet uitdrukkelijk voorziet. Uit de rechtspraktijk zal moeten blijken wat hierin voldoende in overeenstemming is met de richtlijn.

Artikel II, onderdeel T

Artikel 25

Artikel 12, vierde lid, van de richtlijn verplicht de lidstaten dat het verstrekken van bepaalde informatie kosteloos geschiedt. Daarom vervalt de mogelijkheid een kostenvergoeding te verlangen voor het doen van bepaalde mededelingen op verzoek. Het voorgestelde eerste lid bepaalt dit voor het recht op inzage en rectificatie van strafvorderlijke gegevens. Voor de toelichting op het tweede lid wordt verwezen naar de toelichting op artikel 24a, derde lid, van de Wpg.

Artikel II, onderdeel U

Artikelen 26a en 26b

De richtlijn veronderstelt dat er buiten doeltreffende voorzieningen in rechte tegen inbreuken op de verwerking van persoonsgegevens, ook andere mogelijkheden van administratief of buitengerechtelijk beroep bestaan. Met de mogelijkheid van bezwaar en beroep tegen besluiten die op de verwerking van justitiële gegevens betrekking hebben, wordt hieraan invulling gegeven. Ook de bestaande mogelijkheid van verzet tegen bepaalde besluiten kan hiertoe worden gerekend. De invoering van een klachtrecht bij de AP leidt voorts tot aanvullende rechtsbescherming voor betrokkenen. Het in dit onderdeel als eerste nieuw ingevoegde artikel voorziet in het recht van een betrokkene een klacht in te dienen bij de AP. Voor de toelichting hierop over wordt verwezen naar de toelichting op het voorgestelde artikel 31a van de Wpg. Voor de toelichting op het in dit onderdeel als tweede nieuw ingevoegde artikel over het instellen van een vordering tegen de AP wordt verwezen naar de toelichting op artikel 31b van de Wpg.

Artikel II, onderdeel W

Artikel 26c

De verwerkingsverantwoordelijke heeft de verplichting een register bij te houden van alle categorieën van verwerkingsactiviteiten die onder zijn verantwoordelijkheid vallen (art. 24, eerste lid, RI). Dit betreft een meer algemene beschrijving en heeft geen betrekking op afzonderlijke verwerkingsactiviteiten in een specifiek geval. Ook de verwerker is gehouden een register bij te houden van alle categorieën van verwerkingsactiviteiten die hij namens een verwerkingsverantwoordelijke heeft verricht. In de leden zijn de gegevens opgesomd die onder de registerplicht vallen.

Artikel 26d

De in dit artikel vastgelegde verplichting tot schriftelijke vastlegging heeft betrekking op afzonderlijke activiteiten in een specifiek geval, zoals de afwijzing van een verzoek tot inzage of rectificatie. Ook is schriftelijke vastlegging vereist van doorgifte van gegevens aan ontvangers in derde landen die niet zijn gebaseerd op een besluit van de Europese Commissie

over het niveau van gegevensbescherming in dat land. Dit omvat de datum en tijd van doorgifte, informatie over de ontvangende bevoegde autoriteit, de reden van doorgifte en de doorgegeven gegevens zelf. Ook een inbreuk op de beveiliging van justitiële gegevens, inclusief de feiten omtrent de inbreuk, de gevolgen ervan en de maatregelen die zijn getroffen ter correctie, dient schriftelijk te worden vastgelegd.

Artikel 26e

Voor de toelichting op de logging door middel van het geautomatiseerd vastleggen van gegevens over de verwerking van persoonsgegevens wordt verwezen naar het eerste deel van de toelichting op artikel 32a van de Wpg. De logging betreft een geautomatiseerd proces, dat doorgaans standaard is ingebouwd in het informatiesysteem. Niettemin voorziet de richtlijn in een langere implementatietermijn voor de loggingplicht. Dit is in het algemeen deel van deze memorie aan de orde gekomen. De verwerkingsverantwoordelijke dient de bewaartermijn voor de gelogde gegevens vast te stellen in overeenstemming met de verordening gegevensbescherming. Voor de vaststelling van deze termijn kan wordt aangesloten bij de termijn van vier jaren die voor de bewaring van politiegegevens wordt aangehouden.

Artikelen 26f tot en met 26h

Voor de toelichting op deze artikelen in verband met de functionaris voor gegevensbescherming en de door hem te vervullen taken, over de verplichting tot het melden van een inbreuk in verband met persoonsgegevens, alsmede over het door de verwerkingsverantwoordelijke of de verwerker raadplegen van de AP over voorgenomen verwerkingen van justitiële gegevens, wordt verwezen naar de toelichting op de artikelen 36, 33a en 33b van de Wpg.

Artikel II, onderdeel X

Artikel 27

Met het toezicht op de verwerking van justitiële gegevens overeenkomstig het bij en krachtens deze wet bepaalde is de AP belast. Dit volgt uit het eerste lid. Vanwege het vervallen van de Wet bescherming persoonsgegevens wordt hierbij verwezen naar de Uitvoeringswet Avg. Voorts wordt vanwege het vervallen van de Wbp in het tweede lid voor enkele taakbestanddelen van de AP verwezen naar de Uitvoeringswet Avg. Voor een toelichting op deze leden wordt verwezen naar de toelichting op artikel 35, eerste en tweede lid, van de Wpg.
Paragraaf 5 van de Wpg heeft betrekking op controle en toezicht op de verwerking van politiegegevens. De in die paragraaf voorgestelde artikelen over toezicht zijn, waar passend, in het derde lid van overeenkomstige toepassing verklaard op de verwerking van justitiële gegevens. Het betreft achtereenvolgens de artikelen die betrekking hebben op de positie en toezichtstaken van de AP en de samenwerking met toezichthoudende autoriteiten in andere lidstaten van de Europese Unie. Voor een toelichting hierop wordt verwezen naar de toelichting op de artikelen 35a, 35b en 35d van de Wpg. Het vierde, vijfde en zevende lid bepalen de bevoegdheden waarover de AP beschikt, die in de toelichting op artikel 35c van de Wpg nader worden toegelicht. Die bevoegdheden strekken zich daarmee ook uit tot voorschriften in de Wjsg die op de verwerking van justitiële gegevens betrekking hebben, met dien verstande dat:

a. een bestuurlijke boete van ten hoogste de vijfde categorie (€ 83.000,–) kan worden opgelegd voor de overtreding van de

artikelen 7 (gegevensbescherming door beveiliging en ontwerp), 7a (gegevensbescherming door standaardinstellingen), 7b, (gegevensbeschermingseffectbeoordeling), 7d (verwerker), 26c (register van de verwerkingsactiviteiten), 26g (melding inbreuk in verband met persoonsgegevens aan toezichthoudende autoriteit en de betrokkene), 26h (voorafgaande raadpleging) en 26f (functionaris voor gegevensbescherming).

b. een bestuurlijke boete van ten hoogste de zesde categorie (€ 830.000,–) kan worden opgelegd voor de overtreding van de artikelen 24, eerste lid (kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens), 7e (geautomatiseerde besluitvorming), 17a en 17b (transparante informatie en te verstrekken informatie aan betrokkene), 18 (recht van inzage), 22 (recht van rectificatie).

Vijfde lid

Bij het besluit over het opleggen van een boete en over de hoogte daarvan wordt rekening gehouden met bepaalde omstandigheden, overeenkomstig de regeling van de verordening. Voor de toelichting wordt verwezen naar de toelichting op artikel 35c, tweede lid, van de Wpg.

Artikel II, onderdelen Y en Z

Artikelen 36 en 38

De in deze artikelen voorgestelde wijzigingen zijn uitsluitend van technische aard. Deze vloeien voort uit een voorgestelde wijziging elders in het wetsvoorstel en de vervanging van de Wet bescherming persoonsgegevens door de Uitvoeringswet Avg.

Artikel II, onderdeel AB

Artikel 39b

De verplichting in de richtlijn om, in voorkomend geval en voor zover mogelijk, een duidelijk onderscheid te maken tussen gegevens betreffende verschillende categorieën van betrokkenen strekt zich ook uit tot de verwerking van strafvorderlijke gegevens. Strafvorderlijke gegevens hebben betrekking op het strafrechtelijk onderzoek waardoor meerdere personen vanuit een verschillende status bij dat onderzoek betrokken kunnen zijn, zoals die van verdachte, getuige of slachtoffer. In het voorgestelde artikel is hiermee rekening gehouden. Anders dan bij justitiële gegevens zullen strafvorderlijke gegevens zich over het algemeen niet richten op veroordeelden, zodat dit niet als afzonderlijke categorie wordt genoemd. Er bestaat een zekere marge voor de verwerkingsverantwoordelijke bij de invulling van deze verplichting.
Naar aanleiding van het advies van de Afdeling advisering van de Raad van State is de tekst van het tweede lid nauwer aangesloten bij die van artikel 6b Wpg. Voor de toelichting wordt verwezen naar de toelichting op laatstgenoemd artikel (artikel I, onderdeel H).

Artikel II, onderdeel AC

Artikel 39c

In het eerste lid worden verscheidene artikelen die betrekking hebben op de verwerking van justitiële gegevens van overeenkomstige toepassing verklaard op strafvorderlijke gegevens. De aanpassing in het tweede lid strekt tot implementatie van artikel 4, eerste lid, onder a en c, van de

richtlijn, waarin is bepaald dat lidstaten voorschrijven dat persoonsgegevens rechtmatig en eerlijk worden verwerkt, en toereikend, ter zake dienend en niet bovenmatig in verhouding tot de doeleinden waarvoor zij worden verwerkt, zijn.
Van de verwerking van strafvorderlijke gegevens kunnen ook bijzondere persoonsgegevens, onder de huidige wet aangeduid als gevoelige persoonsgegevens, deel uitmaken. Dit is bij een eerdere wijziging van de Wjsg toegelicht (Kamerstukken II 2010/11, 32 554, nr. 3, blz. 15). Er is toen aangegeven dat het voorstelbaar is dat in het kader van een strafzaak persoonsgegevens worden verwerkt over iemands geloof of over iemands seksuele leven, hetgeen aan de hand van enkele voorbeelden werd verduidelijkt. Daarop werd geconcludeerd dat, anders dan voor justitiële gegevens, verwerking van deze bijzondere persoonsgegevens bij strafvorderlijke gegevens en persoonsdossiers aan de orde kan zijn en werd voorzien in het huidige artikel 39c. Gelet hierop wordt voorgesteld de voorschriften in de richtlijn die op de verwerking van bijzondere persoonsgegevens betrekking hebben voor strafvorderlijke gegevens in het derde tot en met vijfde lid van dit artikel te implementeren. Voor een toelichting hierop wordt volstaan met verwijzing naar de toelichting op de voorgestelde wijziging van artikel 5 van de Wpg. Bij het treffen van passende en organisatorische maatregelen om een beveiligingsniveau te waarborgen dat op het risico is afgestemd, dient met name ook rekening te worden gehouden met de verwerking van deze bijzondere persoonsgegevens.

Artikel II, onderdelen AD en AF

Artikelen 39e en 39ga

De doorgifte van strafvorderlijke gegevens aan het buitenland is evenals bij justitiële gegevens in het wetsvoorstel afzonderlijk geregeld en maakt niet langer deel uit van een artikel dat tevens betrekking heeft op verstrekkingen aan de daarin specifiek aangeduide ambtenaren, lichamen, personen, instanties en bewaarders. Dientengevolge vervallen in artikel 39e de artikelleden die op grensoverschrijdende doorgiften betrekking hebben en is een nieuw artikel toegevoegd dat betrekking heeft op het ter beschikking stellen van gegevens aan andere lidstaten van de Europese Unie, respectievelijk de doorgifte aan derde landen. Omdat de BES in het systeem van de richtlijn als derde land gelden, zal de verstrekking van strafvorderlijke gegevens aan de verwerkingsverantwoordelijken in de BES plaats kunnen vinden binnen de kaders van de in artikel 39ga, tweede lid, getroffen afzonderlijke regeling voor de doorgifte van strafvorderlijke gegevens aan derde landen.

Artikel II, onderdeel AH

Artikel 39ha

Voor de toelichting op de actieve en passieve informatieverplichtingen van de verwerkingsverantwoordelijke wordt verwezen naar de toelichting en verwijzingen in de artikelen 17a en 17b. Voor de toelichting op het voorgestelde derde lid, over de verwerking van strafvorderlijke gegevens in een processtuk, wordt verwezen naar de toelichting op artikel 24a, laatste lid, van de Wpg.

Artikel II, onderdelen AI en AJ

Artikelen 39i en 39j

Op een verzoek tot inzage door betrokkene betreffende strafvorderlijke gegevens dient het College procureurs-generaal binnen zes weken uitsluitsel te geven, met de mogelijkheid van verdaging van vier weken. Deze termijnen komen overeen met die in de huidige wet. Een verzoek kan zich ook uitstrekken tot het verkrijgen van inlichtingen over de verstrekking van strafvorderlijke gegevens betreffende de betrokkene gedurende een periode van vier jaar voorafgaande aan het verzoek en over de ontvangers of categorieën van ontvangers aan wie de gegevens zijn verstrekt. Hierover dient binnen vier weken uitsluitsel te worden gegeven. Ook deze termijn is dezelfde als die in de huidige wet, zodat die eveneens ongewijzigd is gebleven. Het desbetreffende voorschrift wordt in aangepaste vorm onderdeel van het voorgestelde nieuwe artikel 39i, eerste lid en vervalt in het huidige artikel 39j, tweede lid. Voor een verdere toelichting wordt verwezen naar de toelichting op artikel 25 van de Wpg.
De Afdeling advisering van de Raad van State heeft geconstateerd dat er een onderscheid is tussen de justitiële en de strafvorderlijke gegevens waar het gaat om de termijn voor inzage en rectificatie van de gegevens, namelijk vier en zes weken met de mogelijkheid van verlenging. Hoewel deze verschillende termijnen ook in de bestaande Wjsg voorkomen, is niet duidelijk waarom dit onderscheid noodzakelijk is. Op het punt van de termijnen bestaat eveneens een onderscheid met betrekking tot de politiegegevens: op grond van het voorgestelde artikel 25 Wpg is de termijn zes weken met de mogelijkheid van verlenging voor vier tot zes weken. De toelichting gaat op deze verschillen niet in. De Afdeling adviseert dit alsnog te doen, dan wel uniforme termijnen te hanteren.
Naar aanleiding van het advies van de Afdeling advisering kan worden opgemerkt dat hierboven, bij de toelichting op artikel 25 Wpg (Artikel I, onderdeel AB) is ingegaan op de redenen voor een reactietermijn van zes weken bij een verzoek tot inzage van politiegegevens. Voor justitiële gegevens kan een verzoek tot inzage worden gericht aan de Minister van Justitie en Veiligheid (art. 18 Wjsg). De noodzaak van coördinatie tussen de verschillende eenheden, die aanleiding vormde voor de verlenging van de reactietermijn voor een verzoek tot inzage van politiegegevens, doet zich daarbij echter niet voor omdat het verzoek tot inzage wordt afgehandeld door Just-ID. Bij strafvorderlijke gegevens ligt dit echter anders. Destijds is, bij de implementatie van het voormalige kaderbesluit dataprotectie, voorgesteld de reactietermijn van vier weken voor een verzoek om inzage van strafvorderlijke gegevens te verlengen tot zes weken omdat ook bij strafvorderlijke gegevens behoefte bestaat aan een langere reactietermijn. Daarbij kunnen verschillende parketten zijn betrokken. In de memorie van toelichting is aangegeven dat bij omvangrijke strafzaken veel gegevens gecontroleerd zullen moeten worden. Daarnaast kan het nodig zijn de voorgenomen beslissing af te stemmen met de betrokken politiekorpsen omdat de betreffende gegevens niet alleen in het kader van de strafzaak zijn verwerkt maar tevens in het kader van het opsporingsonderzoek van de politie (Kamerstukken II, 2010/11, 32 554, nr. 3, blz. 45). Daarbij is gekozen voor de mogelijkheid de beslissing te verdagen voor ten hoogste vier weken.
Ondanks dat destijds is aangegeven dat de reactietermijn hiermee in overeenstemming wordt gebracht met die voor de kennisneming van politiegegevens, is dit niet volledig het geval. Als blijkt dat bij verschillende eenheden van de politie gegevens over de verzoeker worden verwerkt kan de beslissing voor ten hoogste zes weken worden verdaagd (art. 25, eerste lid, Wpg). Dit kan bij strafvorderlijke gegevens ook aan de orde zijn, als bij verschillende parketten strafvorderlijke gegevens over de verzoeker worden verwerkt. Om de termijnen van de Wpg en de Wjsg op

dit punt volledig met elkaar in overeenstemming te brengen wordt voorgesteld de reactietermijn voor dat geval te verlengen tot maximaal zes weken, overeenkomstig de Wpg.

Artikel II, onderdeel AL

Artikel 39l

In de richtlijn is bepaald dat de verwerkingsverantwoordelijke de betrokkene zonder onnodige vertraging schriftelijk in kennis stelt met betrekking tot de opvolging van zijn verzoek (art. 12, derde lid. RI). Het eerste lid strekt tot implementatie daarvan door te bepalen dat degene die verzoekt om inzage of rectificatie, schriftelijk in kennis wordt gesteld van de ontvangst van het verzoek, de termijn voor uitsluitsel en de mogelijkheid om naar aanleiding daarvan een klacht in te dienen bij de AP. Dit moet ten opzichte van andere schriftelijke kennisgevingen als een voorschrift van meer procedurele aard worden gezien.
Het huidige wetsartikel bepaalt dat een mededeling op verzoek van een persoon inhoudende of, en zo ja, welke hem betreffende strafvorderlijke gegevens verwerking ondergaan achterwege blijft, indien dit noodzakelijk is op een van de in dat artikel genoemde gronden. Ditzelfde geldt voor mededelingen over de verstrekkingen en ontvangers daarvan, waarnaar in datzelfde artikel wordt verwezen. Uit de artikelen 15, eerste lid, en 16, vierde lid, van de richtlijn volgt dat de afwijzing van een verzoek, indien dit een noodzakelijke en evenredige maatregel is op een of meer van de aldaar genoemde gronden, zowel van toepassing is op een verzoek tot inzage als een verzoek tot rectificatie. Het tweede lid strekt tot implementatie hiervan. Indien een verzoek betrekking heeft op het verkrijgen van overige voor betrokkene relevante informatie, zoals over de doelen en de rechtsgrond van de verwerking, de betrokken categorie van de gegevens, de voorziene periode van opslag, en over verscheidene andere zaken (zie daarvoor onderdelen a tot en met g van artikel 39i, eerste lid), kan een afwijzing daarop eveneens betrekking hebben. Ook voor afwijzing hiervan dient een noodzakelijke en evenredige maatregel aanwezig te zijn op een of meer van de gronden waarnaar het tweede lid verwijst. Die in de richtlijn genoemde gronden tot afwijzing zijn vermijding van belemmering van de gerechtelijke onderzoeken of procedures, nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, bescherming van de openbare veiligheid, bescherming van de rechten en vrijheden van derden en bescherming van de nationale veiligheid. Hieraan is toegevoegd de mogelijkheid om inzage of rectificatie te weigeren ingeval van kennelijk ongegronde of buitensporige verzoeken van de betrokkene (zie voor de toevoeging van deze laatste grond: art. 12, vierde lid, RI). Het derde lid betreft implementatie van de meer specifieke verplichting om de betrokkene schriftelijk in kennis te stellen van de weigering tot inzage (art. 15, derde lid, RI).

Artikel II, onderdeel AM

Artikel 39m

Voor een toelichting op dit artikel over het recht op rectificatie en vernietiging van strafvorderlijke gegevens wordt verwezen naar de toelichting op artikel 28 van de Wpg.

Artikel II, onderdeel AN

Artikel 39n

Voor een toelichting op dit artikel, over bemiddeling of advisering door de AP, wordt verwezen naar de toelichting op de artikel 29 van de Wpg.

Artikel II, onderdeel AP

Artikel 39p

Voor een toelichting op dit artikel, over het kosteloos verstrekken van bepaalde informatie en over de weigering tot verstrekking van die informatie in geval van kennelijk ongegronde of buitensporige verzoeken, wordt verwezen naar de toelichting op artikel 25.

Artikel II, onderdeel AR

Artikel 39r

Voor een toelichting op de inhoud van verscheidene artikelen die van overeenkomstige toepassing worden verklaard, wordt voor het eerste lid verwezen naar de toelichting op de in dat lid aangehaalde artikelen, voor het tweede lid naar de toelichting op de artikelen 35a, 35b en 35d, van de Wpg en voor het vierde tot en met zevende lid naar de toelichting op artikel 35c van die wet, met dien verstande dat:

a. een bestuurlijke boete van ten hoogste de vijfde categorie (€ 83.000.–) kan worden opgelegd voor de overtreding van de artikelen 7 (gegevensbescherming door beveiliging en ontwerp), 7a (gegevensbescherming door standaardinstellingen), 7b, (gegevensbeschermingseffectbeoordeling), 7d (verwerker), 26c (register van de verwerkingsactiviteiten), 26g (melding inbreuk in verband met persoonsgegevens aan toezichthoudende autoriteit en de betrokkene), 26h (voorafgaande raadpleging) en 26f (functionaris voor gegevensbescherming).
b. een bestuurlijke boete van ten hoogste de zesde categorie (€ 830.000.–) kan worden opgelegd voor de overtreding van de artikelen 24, eerste lid (kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens), 7e (geautomatiseerde besluitvorming), 17a en 17b (transparante informatie en te verstrekken informatie aan betrokkene), 18 (recht van inzage), 22 (recht van rectificatie).

Artikel II, onderdeel AS

Artikel 40

In de voorgestelde wijziging worden verscheidene artikelen van overeenkomstige toepassing verklaard die op persoonsgegevens in persoonsdossiers betrekking hebben (zie voor een toelichting op deze artikelen de toelichting op de artikelen 3, 4 en 4a tot en met 4c, van de Wpg). In rapporten van persoonsdossiers kunnen ook bijzondere persoonsgegevens verwerkt zijn, zodat ook artikel 39c, derde tot en met vijfde lid, van overeenkomstige toepassing is.

Artikel II, onderdelen AT en AU

Artikelen 42 en 42a

Voorgesteld wordt de doorgifte van afschriften van de in persoonsdossiers opgenomen rapporten aan andere dan Nederlandse rechterlijke ambtenaren te vervangen door een afzonderlijke regeling die onderscheid maakt tussen de ter beschikkingstelling van deze afschriften aan andere lidstaten van de Europese Unie en de doorgifte van die afschriften aan derde landen. Dit sluit aan op de voor de justitiële en strafvorderlijke gegevens voorgestelde benadering hierin, zie ook de toelichting op artikel 8.

Artikel 42b

Voor een toelichting op de actieve en passieve informatieverplichtingen van de verwerkingsverantwoordelijke wordt verwezen naar de toelichting op de artikelen 17a en 17b. Hieraan wordt nog het volgende toegevoegd. Er is af gezien van de mogelijkheid die de richtlijn biedt om in afzonderlijke gevallen (art. 13, derde lid, RI) of categorisch (art. 13, vierde lid, RI) informatie uit te stellen, te beperken of achterwege te laten vanwege de gronden die in de weg staan aan inzage door de betrokkene. Anders dan bij politiegegevens bestaat onvoldoende aanleiding verdachten van strafbare feiten de betreffende informatie te ontzeggen waar het gaat om justitiële en strafvorderlijke gegevens. Deze gegevens hebben geen betrekking op de opsporingsfase, zodat er geen noodzaak is verstrekking van deze informatie achterwege te laten.

Artikel II, onderdelen AV en AW

Artikelen 43 en 44

Voor een toelichting op de voorgestelde wijzigingen in deze artikelen over het recht op inzage door betrokkene in hem betreffende rapporten in een persoonsdossier, en met inbegrip van verstrekkingen daaruit, wordt verwezen naar de toelichting op artikel 18.

Artikel II, onderdeel AX

Artikel 45

De in dit artikel voorgestelde wijziging is van technische aard.

Artikel II, onderdelen AY en AZ

Artikelen 46 en 46a

Voor een toelichting op de voorgestelde wijzigingen over het recht op rectificatie van betrokkene betreffende persoonsgegevens in rapporten uit een persoonsdossier, de vernietiging daarvan of het afschermen, wordt verwezen naar de toelichting op artikel 22. Voor een toelichting op het daarna nieuw toegevoegde artikel over schriftelijke kennisgeving en de afwijzing van een verzoek wordt verwezen naar de toelichting op artikel 21.

Artikel II, onderdelen BA en BB

Artikelen 47 en 48

Voor een toelichting op de voorgestelde wijziging inzake de mogelijkheid tot bemiddeling of advisering door de AP bij een geschil met een verwerkingsverantwoordelijke wordt verwezen naar de toelichting op artikel 29 van de Wpg. Voor een toelichting op de kennisgeving aan ontvangers van onjuiste justitiële gegevens wordt verwezen naar de toelichting op artikel 24.

Artikel II, onderdeel BC

Artikel 49

Voor een toelichting op de voorgestelde verplichting tot het kosteloos verstrekken van bepaalde informatie en over de weigering tot verstrekking van die informatie in geval van kennelijk ongegronde of buitensporige verzoeken, wordt verwezen naar de toelichting op artikel 25.

Artikel II, onderdeel BD

Artikel 51

Dit artikel verklaart ter implementatie van bepaalde onderdelen van de richtlijn in het eerste lid verscheidene artikelen voor justitiële gegevens van overeenkomstige toepassing op persoonsgegevens in persoonsdossiers. Het betreft artikelen die gaan over het klachtrecht en het indienen van een vordering tegen de AP, het bijhouden van een register, over de schriftelijke vastlegging van bepaalde handelingen of voorvallen door de verwerkingsverantwoordelijke, verplichtingen inzake logging, over de functionaris voor gegevensbescherming, over het melden van een datalek bij een inbreuk op de beveiliging en over de verplichte raadpleging van de AP inzake een voorgenomen verwerking van gegevens in een nieuw gegevensbestand. Voor de toelichting op de inhoud van het eerste lid wordt hier verder verwezen naar de toelichting op de artikelen 26a tot en met 26h. In het tweede lid worden verscheidene artikelen over politiegegevens uit de Wpg van overeenkomstige toepassing verklaard. Dit betreft artikelen die gaan over het toezicht door de AP. Voor een toelichting op de inhoud van het tweede lid in verband met controle en toezicht wordt verwezen naar de toelichting op artikel 27. Het derde tot en met vijfde lid bepalen de bevoegdheden waarover de AP beschikt, die in de toelichting op artikel 35c van de Wpg nader worden toegelicht. Die bevoegdheden strekken zich daarmee ook uit tot voorschriften in de Wjsg die op de verwerking van persoonsgegevens in persoonsdossiers betrekking hebben. Voor de toelichting op de hoogte van de bestuurlijke boetes en de betreffende artikelen wordt verwezen naar de toelichting op artikel 39r.

Artikel II, onderdeel BE

Artikel 51a

Wettelijke taken en wettelijke verplichtingen die de Minister van Justitie en Veiligheid dient te vervullen ten behoeve van de tenuitvoerlegging van vrijheidsbenemende straffen en maatregelen, zijn vastgesteld in de Penitentiaire beginselenwet, de Beginselenwet verpleging ter beschikking gestelden en de Beginselenwet justitiële jeugdinrichtingen. Uit deze zogeheten Beginselenwetten volgt wie het beheer van de inrichtingen voert, zodat in het voorstel voor het beheer over tenuitvoerleggingsgegevens hierbij is aangesloten. Met de tenuitvoerlegging van andere

strafrechtelijke beslissingen is het openbaar ministerie belast, zoals onder meer blijkt uit artikel 553 van het Wetboek van Strafvordering. De verwerking van gegevens hiervoor berust bij het College van procureurs-generaal, waarbij het beheer wordt uitgevoerd door de verschillende parketten.

Artikel 51b

Een deel van de (voorgestelde) voorschriften die van toepassing is op de verwerking van justitiële gegevens, is in het voorgestelde artikel van overeenkomstige toepassing op tenuitvoerleggingsgegevens. Dit betreft voorschriften inzake de juistheid en kwaliteit van gegevens, evenredigheid van en de doeleinden waarvoor verwerking mogelijk is (art. 3), de verplichting tot het treffen van passende en technische organisatorische maatregelen (art. 7), ontwerp en gegevensbescherming door standaardinstellingen (art. 7a), de gevallen waarin een effectbeoordeling dient te worden uitgevoerd (art. 7b), de inschakeling van een verwerker (artikel 7d), geautomatiseerde besluiten (art. 7e), schadevergoeding (art. 7f), verstrekking van gegevens aan lidstaten en aan derde landen (art. 16a en 16b), de verplichting tot actieve informatieverstrekking (art. 17a en 17b), identiteitsvaststelling van een verzoeker (art. 20), het recht op rectificatie van gegevens en de gronden tot afwijzing van een verzoek hierop (art. 22 en 21), de aanmerking als een besluit in de zin van de Awb en de mogelijkheid tot bemiddeling door de AP (art. 23), verbeterde of anderszins aangepaste gegevens in verband met andere instanties die over deze gegevens beschikken (art. 24), de kosteloze verstrekking van gegevens of vergoeding bij kennelijk ongegronde of buitensporige verzoeken (art. 25) en verwerking van bijzondere persoonsgegevens (art. 39c, tweede tot en met vijfde lid).
Het tweede lid beperkt de overeenkomstige toepassing van de voorschriften over het recht op inzage voor een betrokkene. Het recht op inzage, zoals dat in dit wetsvoorstel is geregeld voor justitiële gegevens, is niet van overeenkomstige toepassing indien het recht op kennisneming van gegevens die op de tenuitvoerlegging betrekking hebben bij of krachtens een andere wet specifiek is geregeld. De Beginselenwet verpleging ter beschikking gestelden bevat bijvoorbeeld voorschriften inzake kennisneming gericht op de betrokkene, die verpleegde is (art. 20). Deze voorschriften blijven onverkort van toepassing.

Artikel 51c

De richtlijn vereist dat er passende termijnen voor het wissen van persoonsgegevens worden vastgesteld. De in het eerste lid voorgestelde termijnen komen overeen met de termijnen die voor vernietiging van justitiële gegevens gelden en waarbinnen een onderscheid wordt gemaakt tussen misdrijven en overtredingen. De voorgestelde termijnen zijn niet van toepassing op tenuitvoerleggingsgegevens voor vrijheidsbenemende straffen of maatregelen. Hiervoor zijn in andere regelgeving specifieke bewaartermijnen met daarop volgende vernietiging vastgesteld die onverkort van toepassing blijven, zoals voor het penitentiaire dossier en inrichtingsdossier.
Het voorgestelde tweede en derde lid hebben betrekking op de verstrekking van tenuitvoerleggingsgegevens door de verwerkingsverantwoordelijke. Verstrekkingen in het kader van de tenuitvoerlegging worden veelal overeenkomstig de Wet bescherming persoonsgegevens met een beroep op de goede vervulling van een publiekrechtelijke taak verstrekt. Dit voorstel voorziet in een op deze gegevens toegespitst verstrekkingenregime dat in de plaats komt van het algemene verstrekkingenregime van de Wet bescherming persoonsgegevens. Verstrekkingen zijn in het voorstel uitsluitend mogelijk, indien dit noodzakelijk is met het oog op een

zwaarwegend algemeen belang dat moet voldoen aan een van de in het tweede lid limitatief opgesomde doeleinden. Hierbij kan worden gedacht aan de verstrekking van persoonsgegevens van een gedetineerde met het oog op schuldhulpverlening of reclassering, aan de verstrekking van die gegevens met het oog op een besluit door het UWV, een verstrekking met het oog op controle van een woonadres in de basisregistratie voor personen, of een verstrekking aan het slachtofferloket. Het derde lid stelt aan de toelaatbaarheid van verstrekking aanvullende eisen.

Artikel 51d

Voor een toelichting op de inhoud van het eerste en tweede lid wordt verwezen naar de toelichting op de artikelen over het recht een klacht in te dienen bij of een vordering in te stellen tegen de AP, het bijhouden van een register, schriftelijke vastlegging en logging, de functionaris voor gegevensbescherming, melding van veiligheidsinbreuken, raadpleging door de verwerkingsverantwoordelijke van de AP over voorgenomen verwerkingen, alsmede het toezicht door de AP en taakbestanddelen van deze autoriteit. Dit betreft de toelichting op de artikelen 26a tot en met 26g en artikel 27. Het derde tot en met vijfde lid bepalen de bevoegdheden waarover de AP beschikt, die in de toelichting op artikel 35c van de Wpg nader worden toegelicht. Die bevoegdheden strekken zich daarmee ook uit tot voorschriften in de Wjsg die op de verwerking van tenuitvoerleggingsgegevens betrekking hebben. Voor de toelichting op de hoogte van de bestuurlijke boetes en de betreffende artikelen wordt verwezen naar de toelichting op artikel 39r.

Artikel 51e

De richtlijn bepaalt dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en legitieme doeleinden worden verzameld en niet op een met die doeleinden onverenigbare wijze worden verwerkt (art. 4, eerste lid, onder b, van de richtlijn). Deze verplichting wordt voor gerechtelijke strafgegevens in het voorgestelde artikel vastgesteld.

Artikel 51f

De richtlijn bevat een samenhangend geheel aan verplichtingen dat ook van toepassing is op de verwerking van gerechtelijke strafgegevens. Voor zover dit noodzakelijk is voor een volledige en juiste implementatie worden die verplichtingen geïmplementeerd door eerdere artikelen over de verwerking van justitiële en strafvorderlijke gegevens van overeenkomstige toepassing te verklaren. In dit artikel worden de bepalingen van overeenkomstige toepassing verklaard die betrekking op onderwerpen als de juistheid en kwaliteit van gegevens, evenredigheid van en de doeleinden waarvoor verwerking mogelijk is, de verplichting tot het treffen van passende en technische organisatorische maatregelen, ontwerp en gegevensbescherming door standaardinstellingen en de gevallen waarin een gegevensbeschermingseffectbeoordeling dient te worden uitgevoerd, de inschakeling van een verwerker, geautomatiseerde besluitvorming, schadevergoeding, het ter beschikking stellen van gerechtelijke strafgegevens aan andere lidstaten van de Europese Unie en doorgifte daarvan aan derde landen, informatieverplichtingen, het recht op inzage op gerechtelijke strafgegevens, identiteitsvaststelling bij verzoeken, het recht op rectificatie van gerechtelijke strafgegevens op verzoek, de schriftelijke kennisgeving omtrent verzoeken, de afwijzing van een verzoek tot inzage of rectificatie, bemiddeling door de AP, het aanmerken van een beslissing op een verzoek tot inzage of rectificatie als een besluit in de zin van de Awb, onjuiste persoonsgegevens en kosteloze

verstrekking en weigering bij kennelijk ongegronde of buitensporige verzoeken.

Artikel 51g

Gegevens die voor onderzoek en beoordeling van strafzaken door gerechten worden verwerkt, dienen op grond van het eerste lid te worden verwijderd indien de verwerking hiervan niet langer noodzakelijk is voor de uitoefening van hun rechterlijke taken. Indien de strafrechter tot een strafrechtelijke beslissing komt, hangt het van het vervolg van de desbetreffende zaak af of de gerechtelijke strafgegevens verwijderd dienen te worden uit een gegevensbestand. Het kan zijn dat er hoger beroep open staat tegen een strafrechtelijke beslissing en als van die mogelijkheid gebruik wordt gemaakt, zal toegang tot de processtukken en de daarin voorkomende gegevens van personen noodzakelijk blijven voor de uitoefening van rechtspraak. In dat geval is verwijdering van gegevens niet vereist. Verwijdering van gegevens is te onderscheiden van de vernietiging daarvan. Bij verwijdering zijn gegevens niet langer in een gegevensbestand aanwezig voor operationele doeleinden, maar zijn die nog beschikbaar ter uitvoering van de verplichtingen op grond van de Archiefwet. Evenals thans het geval is zijn op grond van artikel 41 van de Archiefwet de besturen van de gerechten belast met de zorg van archiefbescheiden. Het tweede lid heeft betrekking op de verstrekking van gerechtelijke strafgegevens door gerechten. Dit is uitsluitend toegestaan voor zover dit ten behoeve van de behandeling van strafzaken plaatsvindt in overeenstemming met het hierover bepaalde bij of krachtens het Wetboek van Strafvordering. Hiervoor kan worden gewezen op de Wet herziening regels betreffende de processtukken in strafzaken (Stb. 2011, 601) en het Besluit processtukken in strafzaken (Stb. 2011, 602). Verstrekkingen door gerechten dienen daarmee te passen binnen het strafprocesrecht. Het door de rechtspraak ter beschikking stellen van processtukken aan de raadsman van een verdachte met gebruikmaking van een digitaal strafdossier («Mijn Strafdossier») voldoet hieraan.

Artikel 51h

In het eerste lid worden verscheidene artikelen van overeenkomstige toepassing verklaard op gerechtelijke strafgegevens. Deze artikelen hebben achtereenvolgens betrekking op het recht van betrokkene een klacht in te dienen bij de AP, de verplichtingen betreffende schriftelijke vastlegging, het door de verwerkingsverantwoordelijke of de verwerker raadplegen van de AP over voorgenomen verwerkingen, het toezicht door de AP op de verwerking van justitiële gegevens overeenkomstig het bij en krachtens deze wet en enkele taakbestanddelen en de verwerking van bijzondere persoonsgegevens. In het tweede lid worden artikelen, waar passend, van overeenkomstige toepassing verklaard uit paragraaf 5 van de Wpg. Het betreft achtereenvolgens de artikelen die betrekking hebben op het door de verwerkingsverantwoordelijke bijhouden van een schriftelijk register, de logging van bepaalde gegevens, de melding van datalekken, de positie en toezichtstaken van de AP en de samenwerking met toezichthoudende autoriteiten in andere lidstaten van de Europese Unie. Voor een toelichting hierop wordt verwezen naar de toelichting op de artikelen 31d, 32a, 33a, en 35a, 35b en 35d van de Wpg. Het derde tot en met vijfde lid bepalen de bevoegdheden waarover de AP beschikt, die in de toelichting op artikel 35c van de Wpg nader worden toegelicht. Voor de toelichting op de hoogte van de bestuurlijke boetes en de betreffende artikelen wordt verwezen naar de toelichting op artikel 39r. Hoewel de 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 rechterlijke taken, teneinde de onafhankelijkheid van rechters bij de uitvoering van die taken te vrijwaren. De 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 (overweging 80 RI). Dit is in artikel 45, tweede lid, van de richtlijn vastgelegd, waarbij in de Nederlandstalige versie van de richtlijn abusievelijk in de zin «Elke lidstaat schrijft voor dat elke toezichthoudende autoriteit belast is met het toezicht op verwerking door gerechten in het kader van hun gerechtelijke taken» het woord «niet» is weggevallen na de woorden «toezichthoudende autoriteit». Uit anderstalige versies van de richtlijn blijkt eenduidig dat dit een kennelijke vergissing betreft. In overeenstemming met de richtlijn is in het zesde lid bepaald dat de AP niet is belast met het toezicht op de verwerking van gerechtelijke strafgegevens door de gerechten, bedoeld in artikel 2 van de Wet op de rechterlijke organisatie in het kader van de uitoefening van hun rechterlijke taken. Enkel in gevallen waarin duidelijk is dat toezicht door de AP op geen enkele wijze van invloed kan zijn op de rechterlijke oordeelsvorming in de strafzaak die bij een gerecht in behandeling is, bestaat er bevoegdheid dit toezicht uit te oefenen. Over het algemeen zullen gerechtelijke strafgegevens zodanig verweven zijn met een specifieke strafzaak die in behandeling is dat de bevoegdheid van de AP tot het houden van toezicht, al dan niet op basis van een handhavingsverzoek, ontbreekt. Die bevoegdheid is wel aanwezig indien de uitoefening daarvan geen relatie heeft met de oordeelsvorming van de rechter in een specifieke strafzaak, zoals het toezicht op de feitelijke juistheid van gerechtelijke strafgegevens, de naleving van bewaartermijnen, de verstrekking van gerechtelijke strafgegevens aan derden of de naleving van voorschriften over het treffen van passende technische en organisatorische maatregelen ten aanzien van de verwerking van gerechtelijke strafgegevens in een gegevensbestand.

ARTIKEL III

Artikel 27b, vierde en vijfde lid (nieuw)

Het Wetboek van Strafvordering bevat voorschriften over de toekenning van een strafrechtsketennummer. De strafrechtketendatabank bevat onder meer identificerende persoonsgegevens die noodzakelijk zijn voor de vaststelling van de identiteit van verdachten en veroordeelden. De gegevens in deze databank worden niet gezien als politiegegevens in de zin van de Wpg of als justitiële of strafvorderlijke gegevens in de zin van de Wet justitiële en strafvorderlijke gegevens. De gegevens in deze databank worden geraadpleegd ten behoeve van de toepassing van het strafrecht binnen de strafrechtketen. Om aan de implementatieverplichtingen uit de richtlijn te voldoen, worden waar dit passend is artikelen uit de Wjsg van overeenkomstige toepassing verklaard op de verwerking van deze gegevens. Daarnaast is in het Besluit identiteitsvaststelling verdachten en veroordeelden ter concretisering en in aanvulling daarop voorzien in specifieke voorschriften, zoals over de vernietiging van gegevens (art. 5 tot en met 8).

Artikel IV

Artikel 12, derde lid

Op basis van de Wwft is een eenheid opgericht, de Financiële inlichtingen eenheid, die is belast met het verzamelen en analyseren van meldingen rond zogenoemde ongebruikelijke transacties door financiële instellingen. Hierboven is, bij de toelichting op artikel 1a, reeds opgemerkt dat de Wpg,

op basis van de Wwft, van toepassing blijft op de verwerking van persoonsgegevens door de Financiële inlichtingen eenheid. Op de verwerking van persoonsgegevens door de Financiële inlichtingen eenheid zijn een aantal artikelen van de Wpg overeenkomstige toepassing. Dit betreft de artikelen 1, 2, 3, eerste en tweede lid, 4, 5, 6, 7, 15, 16, eerste lid, onderdelen a, b en c, 17, 18, 22 en 23, 25 tot en met 31, alsmede artikel 33 van de Wpg.
Om de verwerking van persoonsgegevens door de Financiële inlichtingen eenheid in overeenstemming te brengen met de richtlijn gegevensbescherming opsporing en vervolging is aanpassing van artikel 12, derde lid, van de Wwft noodzakelijk. Daartoe wordt voorgesteld (1) de naar aanleiding van de implementatie van de richtlijn gewijzigde bepalingen van de Wpg ook van toepassing te doen zijn op de verwerking van persoonsgegevens door de Financiële inlichtingen eenheid, en (2) de naar aanleiding van die implementatie voorgestelde opneming van nieuwe bepalingen in de Wpg tevens van toepassing te doen zijn op de verwerking van persoonsgegevens door de Financiële inlichtingen eenheid.
De gewijzigde bepalingen van de Wpg betreffen de artikelen 1, 2, 3, eerste en tweede lid, 4, 5, 6, 15, 16, eerste lid, 17, 22, 25, 26, 27, 28, 29 en 32 Wpg.
De nieuwe bepalingen van de Wpg betreffen de artikelen 4a (gegevensbescherming door ontwerp), 4b (gegevensbescherming door standaardinstellingen), 4c (gegevensbeschermingseffectbeoordeling), 6a (toegang tot politiegegevens), 6b (onderscheid tussen verschillende categorieën van betrokkenen), 6c (verwerker), 7a (geautomatiseerde individuele besluitvorming), 15a (ter beschikkingstelling binnen Europese Unie), 17a (doorgiften aan derde landen), 24a (informatie aan de betrokkene), 24b (verstrekking van informatie aan de betrokkene), 31a (klacht bij AP), 31d (register), 32a (logging), 33a (melding datalekken), 33b (voorafgaand consulteren AP), 35 (toezicht AP), 35a (positie AP), 35b (taken AP), 35c (bevoegdheden AP), 35d (samenwerking met toezichthoudende autoriteiten in andere lidstaten) en 36 Wpg (functionaris gegevensbescherming).

Artikel V

Als het wetsvoorstel herziening tenuitvoerlegging strafrechtelijke beslissingen (Kamerstukken 34 086) tot wet wordt verheven en in werking treedt, wordt de Minister van Justitie en Veiligheid direct verantwoordelijk voor de tenuitvoerlegging van alle straffen en maatregelen (art. 6:1:1 Sv). Met de in deze samenloopbepaling voorgestelde wijziging van artikel 1, onderdeel k, van de Wjsg wordt voorop gesteld dat de Minister verwerkingsverantwoordelijke is voor de verwerking tenuitvoerleggingsgegevens (en niet alleen voor vrijheidsbenemende straffen en maatregelen). Aangezien het openbaar ministerie tijdens de tenuitvoerlegging van strafrechtelijke beslissingen specifieke wettelijke taken en bevoegdheden in de uitvoering houdt, en in dat kader zelfstandig persoonsgegevens over de tenuitvoerlegging blijft verwerken, wordt de verwerkingsverantwoordelijkheid van het College van procureurs-generaal hiervoor eveneens in de definitie benoemd. Bij deze taken en bevoegdheden kan onder meer worden gedacht aan het aanbrengen van zaken bij de rechter indien tijdens de tenuitvoerlegging een vervolgbeslissing moet worden genomen op basis van het verloop van de tenuitvoerlegging (art. 6:6:1 Sv), aan beslissingen over de toepassing van vervangende hechtenis (art. 6:3:3 Sv) of van het dwangmiddel gijzeling (art. 6:4:20 Sv), aan het stellen van bijzondere voorwaarden bij een voorwaardelijke invrijheidsstelling (art. 6:2:11 Sv) en aan het toezicht houden op de naleving van opgelegde vrijheidsbeperkingen (art. 6:3:14 Sv).

ARTIKEL VI

Het voorstel van wet houdende regels voor het kunnen verlenen van verplichte zorg aan een persoon met een psychische stoornis (Wet verplichte geestelijke gezondheidszorg) (Kamerstukken 32 399) bevat in artikel 14:17 een wijziging van de artikelen 8a en 39e van de Wet justitiële en strafvorderlijke gegevens. Ook het voorliggende wetsvoorstel wijzigt laatstgenoemde artikelen, zodat zich tussen beide wetsvoorstellen samenloop voordoet. Ten tijde van de totstandkoming van deze memorie van toelichting staat nog niet vast welk wetsvoorstel met wijziging van deze artikelen als eerste tot wet wordt verheven en in werking zal treden. Dit artikel regelt de samenloop voor het geval de Wet verplichte geestelijke gezondheidszorg eerder of later in werking treedt nadat het tot wet is verheven. Het eerste lid regelt de samenloop indien dat wetsvoorstel tot wet is verheven en eerder in werking treedt dan deze wet. En het tweede lid indien dit wetsvoorstel nadat het tot wet is verheven eerder in werking treedt dan de Wet verplichte geestelijke gezondheidszorg.

Artikel VII

Naar aanleiding van het advies van de Afdeling advisering van de Raad van State is een evaluatiebepaling opgenomen. Hiervoor is aangesloten bij het model van de Aanwijzingen voor de regelgeving (Ar 164). In het licht van de voorgenomen herziening van de privacywetgeving voor opsporing en vervolging en rekening houdend met het verslag van de Commissie over de evaluatie en herziening van de richtlijn, uiterlijk op 6 mei 2022 (art. 62, eerste lid, RI), wordt voorgesteld de termijn voor de eerste evaluatie te stellen op drie jaar, zodat de bevindingen en uitkomsten van die evaluatie kunnen worden betrokken in de herziening van de privacywetgeving en tevens ter kennis van de Commissie kunnen worden ingebracht ten behoeve van de evaluatie van de richtlijn (art. 62, derde lid, RI).

Artikel VIII

Eerste lid

De richtlijn gegevensbescherming opsporing en vervolging dient op 6 mei 2018 te zijn geïmplementeerd. Zoals in het algemeen deel aan de orde is gekomen, bevat de richtlijn echter de mogelijkheid de geautomatiseerde systemen uiterlijk in 2023 in overeenstemming te brengen met de verplichting tot geautomatiseerde vastlegging van gegevens over de gegevensverwerking (logging). In uitzonderlijke omstandigheden is verder uitstel mogelijk, tot uiterlijk 6 mei 2026. Rekening houdend met deze afwijkende termijnen is in dit lid voorzien in de mogelijkheid om voor de verschillende artikelen of onderdelen van dit wetsvoorstel een verschillend tijdstip van inwerkingtreding vast te stellen.

Tweede lid

Het uitgangspunt is dat dit wetsvoorstel uitsluitend strekt tot implementatie van de richtlijn. Op enkele specifieke punten is evenwel gebleken dat dit uitgangspunt tot een onbevredigende uitkomst zou leiden. Dit betreft in de eerste plaats de verruiming van de implementatie in de Wjsg tot de gegevens van rechtspersonen. Dit betreft in de tweede plaats de uitvoering van toezeggingen van het kabinet rond het rapport van de «Big Data in een vrije en veilige samenleving» (zie paragraaf 5.2.2). Als gevolg hiervan is de uitzondering die artikel 5, onderdeel e, van de Wet raadgevend referendum maakt voor wetten die uitsluitend strekken tot implementatie, bij dit wetsvoorstel niet van toepassing. Het bieden van de

mogelijkheid tot het houden van een referendum voorafgaand aan inwerkingtreding zou de uiterste implementatiedatum van 6 mei 2018 in gevaar brengen. Gelet hierop voorziet dit artikel, onder verwijzing naar artikel 12 van de Wet raadgevend referendum, in een grondslag tot eerdere inwerkingtreding van het wetsvoorstel.

De Minister voor Rechtsbescherming,
S. Dekker