STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 72552
27 december 2018

# Regeling WPG Defensie

*16 december 2018*
*Nr.: BS2018031009*

De Minister van Defensie

Besluit:

*Paragraaf 1 Algemene bepalingen*

**Artikel 1.1 Begrippen en definities**

In deze regeling wordt verstaan onder:
a. *Richtlijn:* Richtlijn (EU) 2016/680 van het Europees parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met 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;
b. *wet:* Wet politiegegevens;
c. *minister:* Minister van Defensie;
d. *ministerie:* Ministerie van Defensie
e. *politiegegeven, persoonsgegeven, gerelateerde gegevens, bestand, verwerken van politiegegevens, verstrekken van politiegegevens, ter beschikking stellen van politiegegevens, afschermen van politiegegevens, verwerkingsverantwoordelijke, betrokkene, verwerker; bevoegde autoriteit, ontvanger, derde land, internationale organisatie, inbreuk op de beveiliging, genetische gegevens, biometrische gegevens, gegevens over gezondheid, profilering:* de definities daarvan, genoemd in artikel 1 van de wet;
f. *bijzondere categorieën van politiegegevens:* de politiegegevens, genoemd in artikel 5 van de wet;
g. *ambtenaar van politie:* de ambtenaar van de Koninklijke Marechaussee voor zover werkzaam in de uitvoering van de politietaak;
h. *politietaak:* de politietaak, genoemd in artikel 4 van de Politiewet 2012, met uitzondering van de bij of krachtens de Vreemdelingenwet 2000 opgedragen taken, bedoeld in artikel 4, onderdeel f, van de Politiewet 2012;
i. *verwerkingsverantwoordelijke:* de minister;
j. *bevoegde autoriteit:* de Koninklijke Marechaussee;
k. *Autoriteit persoonsgegevens:* Autoriteit persoonsgegevens als bedoeld in artikel 35 van de wet;
l. *melding:* de melding, genoemd in artikel 2.2, die is bestemd voor het bereiken van een doel of voor meerdere doelen die met elkaar samenhangen.

**Artikel 1.2 Reikwijdte**

1. Deze regeling is van toepassing op verwerking van politiegegevens door de Koninklijke Marechaussee die in een bestand zijn opgenomen of die bestemd zijn daarin te worden opgenomen en waarvoor de Minister van Defensie de verwerkingsverantwoordelijke is in de zin van de Wet politiegegevens.

2. Deze regeling is niet van toepassing op de verwerking van politiegegevens:
   a. voor activiteiten met uitsluitend persoonlijke doeleinden;
   b. voor de interne bedrijfsvoering.

**Artikel 1.3 Wpg-beheerder en Wpg-onderbeheerder**

1. De Commandant Koninklijke Marechaussee is Wpg-beheerder.

2. De Wpg-beheerder draagt zorg voor naleving van de regelgeving omtrent verwerking van politiegegevens door de Koninklijke Marechaussee. Hij doet dit namens de minister.

3. Ieder jaar rapporteert de Wpg-beheerder zijn bevindingen aan de functionaris voor gegevensbescherming WPG. Hij doet dit uiterlijk op 31 december van dat jaar.

4. De Wpg-beheerder zorgt er voor dat contacten met de Autoriteit persoonsgegevens geschieden

door tussenkomst van de functionaris voor gegevensbescherming WPG.

5. De Wpg-beheerder kan zijn taken geheel of gedeeltelijk opdragen aan een Wpg-onderbeheerder. Hieronder valt het binnen de Koninklijke Marechaussee coördineren van de uitvoering van de regelgeving die van toepassing is op de verwerking van politiegegevens.

6. In uitzondering op het vorige lid kan de Wpg-beheerder het aangaan of beëindigen van een verwerkersovereenkomst, bedoeld in artikel 1.5, niet aan de Wpg-onderbeheerder opdragen.

7. De Wpg-beheerder deelt het opdragen van de taken mee aan de functionaris voor gegevensbescherming WPG.

**Artikel 1.4 Privacyfunctionaris**

1. De Wpg-beheerder wijst binnen de Koninklijke Marechaussee één of meer privacyfunctionarissen aan. Hij deelt dit mee aan de functionaris voor gegevensbescherming WPG.

2. De privacyfunctionaris:
   a. adviseert binnen Defensie over de toepassing van regelgeving die betrekking heeft op de verwerking van politiegegevens;
   b. adviseert binnen Defensie over gecoördineerde uitvoering daarvan;
   c. ziet toe op de verwerking van politiegegevens;
   d. draagt zorg voor melding van een datalek aan de Autoriteit persoonsgegevens.

3. De privacyfunctionaris rapporteert zijn bevindingen jaarlijks aan de Wpg-beheerder.

**Artikel 1.5 Verwerker**

1. De Wpg-beheerder kan politiegegevens laten verwerken door een verwerker, met inachtneming van artikel 6c van de wet en artikel 6:1b van het Besluit politiegegevens.

2. De overeenkomst tot verwerking van de betreffende politiegegevens wordt vastgelegd in een schriftelijke verwerkersovereenkomst tussen de verwerker en de Wpg-beheerder die optreedt namens de minister.

**Artikel 1.6 Functionaris voor gegevensbescherming WPG**

1. Er is een functionaris voor gegevensbescherming WPG. Hij wordt tijdig betrokken bij alle aangelegenheden die verband houden met de bescherming van politiegegevens.

2. De functionaris voor gegevensbescherming WPG vervult binnen het Ministerie van Defensie de taken, genoemd in artikel 36, derde lid, van de wet en ziet toe op de afwikkeling van klachten en het evalueren van incidenten over het verwerken van politiegegevens binnen het ministerie.

3. De functionaris voor gegevensbescherming WPG rapporteert jaarlijks aan de minister over de naleving van de wet en daarop gebaseerde regelgeving binnen het ministerie.

4. Voor de uitoefening van het toezicht beschikt de functionaris voor gegevensbescherming WPG over de bevoegdheden als bedoeld in Titel 5.2 van de Algemene wet bestuursrecht. De functionaris voor gegevensbescherming WPG maakt alleen gebruik van zijn bevoegdheden als dat nodig is voor de vervulling van zijn taak.

5. De functionaris voor gegevensbescherming WPG wordt alle medewerking verleend die hij redelijkerwijs kan vorderen, tenzij een wettelijke geheimhoudingsplicht daar aan in de weg staat.

6. De verwerkingsverantwoordelijke maakt de contactgegevens van de functionaris voor gegevensbescherming WPG openbaar. Hij deelt deze mee aan de Autoriteit persoonsgegevens.

*Paragraaf 2. Weergaven van verwerkingen van politiegegevens*

**Artikel 2.1 Register**

1. Er is een register van verwerkingsactiviteiten, als bedoeld in artikel 31d van de wet, van het ministerie.

2. Het register wordt opgesteld en geactualiseerd door de Wpg-beheerder.

3. Voordat met een nieuwe of gewijzigde verwerking van politiegegevens wordt begonnen, wordt deze verwerking opgenomen in het register.

4. Het register omvat:
   a. de in artikel 31d, eerste lid, van de wet bedoelde gegevens;
   b. indien van toepassing, een afschrift van de afspraken met een verwerker, als bedoeld in artikel 6c, tweede lid, van de wet;
   c. algemene informatie over de locaties en ICT-systemen waar de verwerking plaatsvindt;
   d. informatie over de onderdelen van het proces ten behoeve waarvan het verwerken van persoonsgegevens plaatsvindt;
   e. indien van toepassing een afschrift van de gegevensbeschermingseffectbeoordeling, bedoeld in artikel 4c van de wet.

5. De functionaris voor gegevensbescherming WPG en de Autoriteit persoonsgegevens krijgen op hun verzoek toegang tot het register.

**Artikel 2.2 Documentatie**

De Wpg-beheerder zorgt voor de schriftelijke of elektronische vastlegging van de aangelegenheden, bedoeld in artikel 32, eerste en tweede lid, van de wet.

**Artikel 2.3 Logging**

1. De Wpg-beheerder zorgt voor de elektronische vastlegging van ten minste het verzamelen, wijzigen, raadplegen, verstrekken, doorgeven, combineren of vernietigen van politiegegevens, conform artikel 32a van de wet.

2. De minimale duur van de logging van een politiegegeven is vier jaar.

*Paragraaf 3. Gegevensbeschermingseffectbeoordeling / Privacy Impact Assessment*

**Artikel 3 Gegevensbeschermingseffectbeoordeling**

1. De Wpg-beheerder voert de gegevensbeschermingseffectbeoordeling uit als bedoeld in artikel 4c van de wet, aan de hand van het Model gegevensbeschermingseffectbeoordeling Rijksdienst (PIA).

2. Het projectplan dat op de voorgenomen gegevensbeschermingseffectbeoordeling betrekking heeft, wordt ter advies voorgelegd aan de functionaris voor gegevensbescherming WPG. Het projectplan wordt daarnaast voorgelegd aan de Chief Information Officer als de gegevensverwerking gepaard gaat met de bouw of vergaande aanpassing van een ICT-systeem.

3. Een voltooide PIA bestaat uit:
   a. een algemene beschrijving van de voorgenomen verwerkingen en de verwerkingsdoeleinden;
   b. een beschrijving en beoordeling van de rechtsgrond en de noodzaak van de voorgenomen verwerkingen in relatie tot de verwerkingsdoeleinden;
   c. een beschrijving en beoordeling van risico's van de voorgenomen verwerkingen voor de rechten en vrijheden van de betrokkenen; en
   d. een beschrijving van de voorzorgs- en beveiligingsmaatregelen en mechanismen om de politiegegevens te beschermen en aan te tonen dat is voldaan aan de wet en daarop gebaseerde regelgeving, met inachtneming van de rechten en gerechtvaardigde belangen van betrokkenen.

4. Wanneer uit de gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico als bedoeld in artikel 33b, eerste lid, van de wet oplevert, wordt de Autoriteit persoonsgegevens geraadpleegd, door tussenkomst van de functionaris voor gegevensbescherming, conform art. 33b van de wet.

*Paragraaf 4. Datalek*

**Artikel 4.1 Melding datalek aan de Autoriteit persoonsgegevens**

1. De privacyfunctionaris meldt een inbreuk op de beveiliging, als bedoeld in artikel 33a, eerste lid, van de wet, aan de Autoriteit persoonsgegevens. Hij stuurt een kopie daarvan aan de functionaris voor gegevensbescherming WPG.

2. De melding bevat de in artikel 33a, tweede lid, van de wet genoemde gegevens.

3. De privacyfunctionaris doet de melding binnen 72 uur nadat hij kennis heeft genomen van het datalek.

4. Als het niet waarschijnlijk is dat de inbreuk op de beveiliging een risico voor de rechten en vrijheden van personen met zich meebrengt, doet de privacyfunctionaris de melding zodra hij de informatie kan verstrekken, genoemd in artikel 33a, tweede lid van de wet.

5. Een te late melding gaat vergezeld van een motivering van de vertraging.

**Artikel 4.2 Melding datalek aan de betrokkene**

1. De privacyfunctionaris deelt de inbreuk op de beveiliging mee aan de betrokkene wanneer deze inbreuk waarschijnlijk een hoog risico voor de rechten en vrijheden van personen met zich meebrengt.

2. De mededeling bevat de in artikel 33a, vijfde lid, van de wet genoemde gegevens.

3. De mededeling is niet vereist wanneer:
   a. passende technische en organisatorische maatregelen zijn getroffen en toegepast op de politiegegevens waarop het datalek betrekking heeft;
   b. maatregelen zijn getroffen om er voor te zorgen dat het hoge risico, bedoeld in het eerste lid, zich waarschijnlijk niet meer zal voordoen; of
   c. de mededeling een onevenredige inspanning zou vergen. In dat geval volgt een openbare vergelijkbare maatregel waarmee betrokkene even doeltreffend wordt geïnformeerd.

4. De mededeling kan worden uitgesteld, beperkt of achterwege gelaten:
   a. ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures;
   b. ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen;
   c. ter bescherming van de openbare of de nationale veiligheid;
   d. ter bescherming van de rechten en vrijheden van derden;
   e. in geval van een kennelijk ongegrond of buitensporig verzoek.

*Paragraaf 5. Rechten van betrokkene*

**Artikel 5.1 Informatieverstrekking aan de betrokkene**

1. Op verzoek van betrokkene wordt hem conform artikel 24a van de wet informatie verstrekt over de verwerking van politiegegevens. Dit wordt gedaan in beknopte en toegankelijke vorm en voor zover beveiliging dit toelaat.

2. Op verzoek van betrokkene worden hem conform artikel 24b van de wet de gegevens verstrekt, tenzij ten aanzien van betrokkene het gegronde vermoeden bestaat dat hij een strafbaar feit heeft gepleegd of zal gaan plegen.

**Artikel 5.2 Recht op inzage, rectificatie, aanvulling en vernietiging**

1. Betrokkene richt verzoeken om inzage, rectificatie, aanvulling en vernietiging van politiegegevens, als bedoeld in de artikelen 25 en 28 van de wet, aan de Wpg-beheerder.

2. Het verzoek kan namens betrokkene worden gedaan door de Autoriteit persoonsgegevens of door de advocaat van betrokkene. Betrokkene machtigt zijn advocaat met een bijzondere, daartoe strekkende schriftelijke machtiging.

3. Het verzoek kan namens betrokkene worden gedaan door zijn wettelijk vertegenwoordiger als betrokkene jonger is dan 16 jaar of onder curatele is gesteld.

4. De Wpg-beheerder neemt het verzoek in behandeling.

5. Bij het in behandeling nemen van het verzoek stelt de Wpg-beheerder
   a. de identiteit van de verzoeker en van betrokkene vast;
   b. betrokkene, in geval van een verzoek om inzage of rectificatie, schriftelijk in kennis van de ontvangst van het verzoek, de termijn voor uitsluitsel en de mogelijkheid om naar aanleiding daarvan een klacht in te dienen bij de Autoriteit persoonsgegevens.

6. Het verzoek wordt afgewezen:

a. bij een kennelijk ongegrond of buitensporig verzoek; of
b. voor zover dit een noodzakelijke en evenredige maatregel is
   1e. ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures;
   2e. ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen;
   3e. ter bescherming van de openbare of de nationale veiligheid; of
   4e. ter bescherming van de rechten en vrijheden van derden.
7. Op een verzoek om inzage in de gegevens wordt binnen zes weken beslist.
8. Op een verzoek om rectificatie, aanvulling of vernietiging van de politiegegevens, wordt binnen vier weken beslist.
9. Een afwijzing van het verzoek wordt gemotiveerd.

**Artikel 5.3 Bezwaar**

1. Het besluit als bedoeld in artikel 5.2, zevende en achtste lid, bevat de mededeling dat bezwaar gemaakt kan worden en aan wie het bezwaar gericht dient te zijn.

2. Binnen zes weken na de dag van verzending van een besluit als bedoeld in artikel 5.2, zevende en achtste lid, kan een ieder wiens belang rechtstreeks bij dit besluit is betrokken, bezwaar maken.

*Paragraaf 6 Juistheid, volledigheid, beveiliging en beheer*

**Artikel 6.1 Dataminimalisatie, juistheid en volledigheid**

1. Politiegegevens worden slechts verwerkt met inachtneming van artikel 3 van de wet.

2. De Wpg-beheerder treft de nodige maatregelen overeenkomstig artikel 4 van de wet, waaronder:
   a. het vernietigen of rectificeren van politiegegevens zodra blijkt dat deze onjuist zijn;
   b. het vernietigen of verwijderen van politiegegevens zodra deze niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verwerkt;
   c. het vernietigen of verwijderen van politiegegevens zodra een wettelijke bepaling dit vereist;
   d. het onderscheiden tussen feitelijke politiegegevens en politiegegevens die op een persoonlijk oordeel zijn gebaseerd.

**Artikel 6.2 Privacy by design en privacy bij default**

De verwerkingsverantwoordelijke treft technische en organisatorische maatregelen die zorgen voor een passend beveiligingsniveau van politiegegevens overeenkomstig de artikelen 4a en 4b van de wet en artikel 6:1a van het Besluit politiegegevens.

**Artikel 6.3 Autorisatie**

1. Politiegegevens worden alleen verwerkt door ambtenaren, tewerkgesteld of ingedeeld bij de Koninklijke Marechaussee die dit doen in de uitoefening van de politietaak en voorzover zij voor die verwerking zijn geautoriseerd door de Wpg-beheerder.

2. De Wpg-beheerder onderhoudt een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid, conform artikel 6 van de wet.

*Paragraaf 7 Audit*

**Artikel 7 Audit Dienst Rijk**

1. De Audit Dienst Rijk kan, eventueel op verzoek van de functionaris voor gegevensbescherming WPG, een audit uitvoeren naar de naleving van de wet en deze regeling.

2. Wanneer een auditdienst het voornemen heeft een audit te verrichten, wordt de functionaris voor gegevensbescherming WPG hiervan op de hoogte gesteld.

3. De auditdienst rapporteert haar bevindingen aan de minister en aan de functionaris voor gegevensbescherming WPG.

*Paragraaf 8 Aanwijzing*

**Artikel 8**

De Secretaris-Generaal kan nadere aanwijzingen geven ter uitvoering van het bepaalde in deze regeling.

*Paragraaf 9 Slotbepalingen*

**Artikel 9.1 Inwerkingtreding**

Deze regeling treedt in werking met ingang van 1 januari 2019. Indien de Staatscourant waarin deze regeling wordt geplaatst, wordt uitgegeven na 31 december 2018, treedt zij in werking met ingang van de dag na de datum van uitgifte van de Staatscourant waarin zij wordt geplaatst en werkt zij terug tot en met 1 januari 2019.

**Artikel 9.2 Citeertitel**

Deze regeling wordt aangehaald als: Regeling WPG Defensie.

Deze regeling zal met de toelichting worden geplaatst in de Staatscourant.

*'s-Gravenhage, 16 december 2018*

*De Minister van Defensie,*
*A.Th.B. Bijleveld-Schouten*

## TOELICHTING

### Algemeen:

Deze regeling heeft betrekking op de verwerking van politiegegevens. De regeling is een uitwerking van de Wet politiegegevens (Wpg) en het Besluit politiegegevens (Bpg), zoals aangepast aan de *EU-richtlijn 2016/680, L119 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad* (hierna: de richtlijn).

Bescherming van persoonsgegevens valt onder het recht op privacy. In dit kader vereist verwerking van persoonsgegevens een deugdelijke grondslag, een gerechtvaardigd doel en afdoende IT-beveiliging. Men heeft altijd recht op een zorgvuldige omgang met zijn gegevens. Onder bepaalde omstandigheden rechtvaardigen andere belangen een inbreuk op het recht op privacy. Een voorbeeld van zo'n omstandigheid is opsporing van strafbare feiten.

Een persoonsgegeven is een gegeven waarmee men iemand kan identificeren, eventueel in combinatie met andere gegevens. Een verwerking is alles wat er met gegevens gebeurt nadat ze zijn verzameld, dus ook bewaren of vernietigen. Een verwerking kan zich in allerlei gedaanten voordoen. Niet alleen in databases, maar ook in wearables zoals bodycams.

Politiegegevens zijn persoonsgegevens die door bevoegde autoriteiten worden verwerkt met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid (art. 1 van de richtlijn). Bij Defensie is de 'bevoegde autoriteit' de Koninklijke Marechaussee (KMar). Dit krijgsmachtdeel voert meerdere taken uit. De Wpg en het Bpg zijn van toepassing op de taken die staan genoemd in artikel 4 van de Politiewet 2012, met uitzondering van de grensbewakingstaken-zonder-strafrechtelijk-aspect en toezichtstaken. Op die taken is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Zie daarvoor ook de Uitvoeringswet AVG en de Regeling AVG Defensie. De AVG is verder van toepassing op de persoonsgegevens die de Koninklijke Marechaussee in de hoedanigheid van werkgever verwerkt.

De taken waarop Wpg en Bpg van toepassing zijn, zijn het waken over de veiligheid van de leden van het koninklijk huis; de uitvoering van de politietaak ten behoeve van Nederlandse en andere strijdkrachten; de uitvoering van de politietaak op de luchthaven Schiphol en op andere aangewezen luchtvaartterreinen, en de beveiliging van de burgerluchtvaart; de verlening van bijstand en de samenwerking met de politie; de uitvoering van de politietaak op bepaalde andere plaatsen; de bestrijding van mensensmokkel en van fraude met reis- en identiteitsdocumenten en tot slot het in opdracht van Onze Minister en Onze Minister van Defensie ten behoeve van De Nederlandsche Bank N.V. verrichten van beveiligingswerkzaamheden.

### *Doelbinding: Wpg en AVG*

Een persoonsgegeven kan van het ene privacyregime overgaan in het andere privacyregime. Dit komt met name voor bij de uitvoering van de grensbewakingstaak. De grensbewakingstaak kent strafrechtelijke (Wpg) en vreemdelingrechtelijke aspecten (AVG). Het controleren van een paspoort (AVG) bijvoorbeeld, kan leiden tot inbewaringstelling (Wpg) van de vreemdeling indien de nationale veiligheid dit vordert. De privacyregimes verschillen op een aantal punten van elkaar. Politiegegevens moeten bijvoorbeeld worden gelogd (art. 32a Wpg). De AVG kent deze loggingsplicht niet. Daarom moet men bij de verwerking van een persoonsgegeven altijd in de gaten houden voor welk doel dat persoonsgegeven wordt gebruikt. De doelbinding bepaalt of op het persoonsgegeven de AVG van toepassing is, of de Wpg, of een ander privacyregime. Voor de KMar komt dit op het volgende neer: de verwerking van persoonsgegevens in het kader van asiel en migratie en het houden van toezicht, valt onder het regime van de AVG. 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 verwerking van de persoonsgegevens onder het regime van de Wpg.

Wpg-> Wpg Binnen de opsporingsinstanties politie, KMar en bijzondere opsporingsdiensten (ketenpartners) geldt een 'free flow of information' ten aanzien van politiegegevens (art. 15, eerste lid, Wpg). Politiegegevens kunnen onderling over en weer worden verstrekt en verwerkt zolang het binnen de Wpg-doelen valt. Verstrekking van een politiegegeven voor bepaalde Wpg-doelen aan andere personen of instanties, is mogelijk in bijzondere gevallen en voor zover noodzakelijk met het oog op een zwaarwegend algemeen belang (art. 19 en 20 Wpg).

Wpg-AVG-> Als een politiegegeven binnen de opsporingsinstanties voor een AVG-doel wordt verwerkt, geldt de free flow of information niet. Toch kan er binnen en tussen de opsporingsinstanties snel gegevensuitwisseling plaatsvinden. De gegevensverstrekking gebeurt namelijk geautomatiseerd (art. 3, vierde lid en 23, derde lid, Wpg en art. 4:3, vijfde lid, Bpg). Het politiegegeven kan dan als 'gewoon' persoonsgegeven binnen de politie en KMar verder worden verwerkt op grond van art. 33, eerste lid, onder a, Uitvoeringswet AVG. Een politiegegeven dat de opsporingsinstantie verlaat (bijvoorbeeld naar een ander dienstonderdeel) om voor een AVG-doel te worden verwerkt, kan door de opsporingsinstantie worden verstrekt op basis van art. 3, vierde lid, en 18, eerste lid, Wpg en de artikelen 4:1–4:4, 6a:5 en 6a:6 Bpg). Deze verstrekking kan alleen met het oog op een zwaarwegend algemeen belang, en alleen aan de personen of instanties om de redenen die in het Bpg staan opgesomd. Als de KMar bijstand verleent aan de politie, kan binnen dat bijstands-kader in bijzondere gevallen ook aan andere personen of instanties politiegegevens worden verstrekt, als verstrekking noodzakelijk is met het oog op en zwaarwegend algemeen belang en de verstrekking geschiedt in verband met het verlenen van hulp aan hen die deze behoeven en het uitoefenen van toezicht op het naleven van regelgeving (art. 19 en 20 Wpg).

AVG-> Wpg AVG-gegevens, zoals gegevens die zijn verzameld in de uitvoering van de vreemdelingentaak, kunnen binnen de KMar voor opsporing worden gebruikt op grond van art. 6, eerste lid, onder e, AVG in samenhang met art. 4, eerste lid, Politiewet 2012 en art. 3 Wpg. Dan moet wel zijn voldaan aan alle voorwaarden die in die artikelen staan genoemd. De belangrijkste voorwaarde is dat er een juridische grondslag is voor de verwerking. Dit betekent dat in een wet, een AMvB of ministeriele regeling specifiek moet staan dat die bepaalde AVG-gegevens kunnen worden verstrekt voor dat bepaalde Wpg-doel, door die bepaalde instantie aan een andere bepaalde instantie.

## Artikelsgewijs

### *Artikel 1.1 Definities*

De definities uit de Wpg zijn niet letterlijk overgeschreven in artikel 1, om dubbelingen te voorkomen.

Over de verwerkingsverantwoordelijke wordt nog het volgende opgemerkt. De KMar is een opsporingsinstantie die politiegegevens verwerkt in de uitvoering van zijn politietaak. De KMar is een krijgsmachtdeel, waar de Minister van Defensie hiërarchisch en beheersmatig (art. 4 Politiewet 2012) zeggenschap over heeft. Daarom is de Minister van Defensie in de Wpg aangewezen als verwerkingsverantwoordelijke ter zake (art. 1, onder f, Wpg).

### *Artikel 1.2 Reikwijdte*

De regeling is een interne Defensieregeling. De regeling is van toepassing op verwerking van politiegegevens door de KMar.

### *Artikel 1.3 Wpg-beheerder en Wpg-onderbeheerder*

'Beheerder' in de zin van deze regeling is een functionaris die binnen Defensie verantwoordelijk is voor de naleving van de regelgeving die van toepassing is op de verwerking van politiegegevens, dus de naleving van de Wpg, het Bpg en de AVG. Dit verschilt van 'beheer' in de zin van art. 4 van de Politiewet 2012, dat doelt op de toebedeling van mensen en middelen voor de taakuitvoering van de KMar.

De Wpg-beheerder kan zijn taak geheel of gedeeltelijk opdragen aan een Wgp-onderbeheerder. In dat geval verleent hij de Wpg-onderbeheerder mandaat, machtiging en volmacht tot het doen van alle feitelijke of rechtshandelingen die nodig zijn voor een goede naleving van de Wpg en het Bpg. Het is geen delegatie. Dit betekent dat de Wpg-beheerder zijn bevoegdheden behoudt, ook als hij het mandaat, machtiging en volmacht aan de Wpg-onderbeheerder heeft verleend.

De Wpg-beheerder kan het aangaan of beëindigen van een verwerkersovereenkomst niet aan de Wpg-onderbeheerder overdragen. Dit heeft te maken met het feit dat een verwerkersovereenkomst in feite wordt aangegaan door de minister en het krijgsmachtdeel KMar overstijgt.

### *Artikel 1.4 Privacy-functionaris*

De privacyfunctionaris (art. 34 Wpg) heeft bijzondere deskundigheid op het gebied van privacyrecht. Hij heeft een adviesrol, ziet inhoudelijk toe op de verwerking van politiegegevens en meldt datalekken aan de Autoriteit persoonsgegevens (AP). De AP is de nationale toezichthouder op het gebied van

gegevensbescherming. De privacyfunctionaris rapporteert jaarlijks zijn bevindingen aan de Wpg-beheerder.

### *Artikel 1.5 Verwerker*

Een verwerker is de persoon of instantie die politiegegevens verwerkt ten behoeve van de verwerkingsverantwoordelijke (art. 1, onder i, Wpg). Bij Defensie doet de verwerker dat volgens de instructies van de Wpg-beheerder, die de instructies namens de minister geeft. De Wpg-beheerder behoudt de regie en bepaalt doel en middelen van de verwerking.

In artikel 6c, tweede lid van de Wpg en artikel 6:1b Bpg staan de eisen waaraan de verwerkingsovereenkomst moet voldoen. De verwerkingsovereenkomst bevat het onderwerp, duur, aard en doel van de verwerking, het soort politiegegevens, de categorieën van betrokkenen en de rechten en verplichtingen van de pg-beheerder die namens de minister optreedt. Daarnaast staat in de verwerkersovereenkomst dat de verwerker uitsluitend handelt volgens instructies, gegeven van of namens de Wpg-beheerder. Ook staat in de overeenkomst dat de tot verwerking gemachtigde personen zich verplichten tot vertrouwelijkheid, dat de verwerker de Wpg-beheerder bijstaat om naleving van de rechten van betrokkenen te verzekeren en dat de verwerker na afloop van de diensten naar keus van de Wpg-beheerder de gegevens wist of ter beschikking stelt en kopieën verwijdert – tenzij opslag van de gegevens verplicht is. Voorts staat in de verwerkersovereenkomst dat de verwerker aan de Wpg-beheerder alle informatie ter beschikking stelt die nodig is om de nakoming van art. 6:1b Bpg aan te tonen. Tot slot staat in de overeenkomst dat de verwerker eventuele inschakeling van een ‘onder-verwerker’ afstemt met de Wpg-beheerder en dat de verwerker daarbij aan alle wettelijke vereisten voldoet.

Niet alleen de verwerkingsovereenkomst, maar ook de verwerker zelf moet aan bepaalde wettelijke vereisten voldoen. Zo mag bijvoorbeeld uitsluitend gebruik worden gemaakt van een verwerker die afdoende garandeert dat de passende technische en organisatorische maatregelen en procedures zodanig worden geïmplementeerd dat wordt voldaan aan de Wpg. Voor de eisen wordt met name verwezen naar de artikelen 4a, 6a, derde lid, 6c, 31c, derde en vierde lid, 31d, tweede lid, 32a en 33b Wpg. Ook de andere bepalingen van de wet zijn relevant. Volgens de wetgever moet worden aangenomen dat een verplichting die die geldt voor de verwerkingsverantwoordelijke, tevens geldt voor de verwerker. Dit kan in de overeenkomst worden vastgelegd.

### *Artikel 1.6 Functionaris voor gegevensbescherming WPG*

De functionaris voor gegevensbescherming (FG-WPG) is een van de twee privacy-toezichthouders op het gebied van bescherming van persoonsgegevens binnen Defensie. Er is een FG-AVG die zich richt op verwerkingen van persoonsgegevens binnen het AVG-regime, en er is een FG-WPG die verwerkingen van politiegegevens tot zijn voornaamste aandachtsgebied heeft. Omdat een persoonsgegeven kan overgaan van het AVG-regime naar het Wpg-regime en vice versa, werken de FG’s nauw samen.

In artikel 36, derde lid van de Wpg staan de taken van de FG-WPG opgesomd. De eerste taak is het toezien op naleving van de wet en het beleid over het verwerken van politiegegevens. Hieronder valt ook toezicht op de toewijzing van autorisaties, en toezicht op de opleiding van degenen die de politiegegevens verwerken. De tweede taak is het informeren en adviseren van de minister en de gegevensverwerkers over de Wpg. De derde taak is het adviseren over de gegevensbeschermings-effectbeoordeling (GEB[1]) en het toezien op de uitvoering ervan. De vierde taak is het optreden als contactpunt voor de AP en het daar mee samenwerken. De FG-WPG moet zijn taken en verplichtingen onafhankelijk kunnen uitvoeren (overweging 63 bij de Richtlijn).

Het jaarlijks rapporteren, genoemd in het derde lid, volgt uit art. 36, vierde lid, Wpg.

In het vierde lid wordt verwezen naar Titel 5.2 van de Algemene wet bestuursrecht. Deze Titel gaat over de algemene plichten en bevoegdheden van een toezichthouder. De toezichthouder mag inlichtingen en inzage vorderen. Ook mag hij zakelijke gegevens en bescheiden inzien en die kopiëren.

Om het toezicht daadwerkelijk te effectueren is in het vijfde lid de verplichting opgenomen om medewerking te verlenen aan de FG-WPG, tenzij een geheimhoudingsplicht daar aan in de weg staat.

### *Artikel 2.1 Register*

Het register bevat algemene omschrijvingen van de verwerkingen van politiegegevens. Het register

[1] Voorheen de privacy Impact Assessment (PIA).

heeft geen betrekking op afzonderlijke verwerkingsactiviteiten in een specifiek geval. Het register dient ter controle en toezicht op de gegevensverwerking. Voordat met een verwerking wordt begonnen, meldt de Wpg-beheerder de verwerking in het register. Op het moment van het opstellen van deze regeling staat nog niet vast in welke IT-applicatie het register wordt opgenomen.

Gelet op art. 31d Wpg wordt In het register opgenomen: de contactgegevens van de verwerkingsverantwoordelijke en van de FG-WPG, de verwerkingsdoeleinden, een beschrijving van de categorieën ontvangers, betrokkenen, doorgiften en van persoonsgegevens, eventueel gebruik van profilering, de rechtsgrondslag van de verwerking, de verwijder- of vernietigingstermijnen, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen en de toekenning van autorisaties.

Op hun verzoek krijgen de FG-WPG en de AP toegang tot het register, ten behoeve van hun toezichthoudende taak.

***Artikel 2.2 Documentatie***

De Wpg-(onder)beheerder draagt zorg voor de schriftelijke vastlegging van (1) de doelen van onderzoeken, gericht op handhaving van de rechtsorde in een bepaald geval, conform art. 9, tweede lid, Wpg; (2) de verstrekking of doorgifte van politiegegevens aan anderen dan politie en Koninklijke Marechaussee – met uitzondering van verstrekking of doorgifte aan inlichtingen- en veiligheidsdiensten als dit zich niet verdraagt met de staatsveiligheid; (3) de feitelijke of juridische redenen die ten grondslag liggen aan afwijzing van betrokkenes verzoek om inzage, rectificatie of vernietiging van politiegegevens; (4) datalekken, de gevolgen daarvan en de getroffen correctiemaatregelen.

***Artikel 2.3 Logging***

Logging is een geautomatiseerd proces, dat standaard in een ICT-systeem is ingebouwd. De vastgelegde gegevens worden uitsluitend gebruikt voor de externe en interne controle van de rechtmatigheid van de verwerking, voor interne controles, ter waarborging van integriteit en de beveiliging van politiegegevens en voor strafrechtelijke procedures (art. 32a, tweede lid, Wpg).

De minimale duur van logging van een politiegegeven is op vier jaar gesteld, conform de MvT van de Wet tot wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen. Daarbij is aangesloten bij de bewaartermijn van een politiegegeven ten behoeve van het inzagerecht van betrokkene (art. 25, eerst lid, onder c, Wpg). Als niet aan de loggingplicht wordt voldaan, kan de AP een last onder bestuursdwang opleggen (art. 35c, eerste lid, onder b, Wpg). ICT-systemen die werkzaam waren op 5 mei 2016, moeten uiterlijk op 6 mei 2023 aan deze loggingsverplichting zijn aangepast. De maximale duur van logging van een politiegegeven hangt af van de maximale bewaartermijn van dat gegeven. Deze vloeit voort uit de artikelen 8, 9 en 10 Wpg.

***Artikel 3.1 Gegevensbeschermingseffectbeoordeling / Privacy Impact Assessment***

Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, waarschijnlijk een hoog risico voor de rechten en vrijheden van personen oplevert, voert de Wpg-beheerder voorafgaand aan de verwerking een beoordeling uit van het effect van de voorgenomen verwerkingsactiviteiten op de bescherming van persoonsgegevens, conform artikel 4c Wpg.

De GEB/PIA is een instrument om op een gestructureerde en gestandaardiseerde wijze in kaart te brengen en te beoordelen wat de effecten voor betrokkene zijn van voorgenomen regelgeving, beleid of projecten waarbij politiegegevens worden verwerkt. Op basis van de GEB/PIA worden maatregelen getroffen om deze effecten voor betrokkenen te voorkomen of verkleinen. De regelgeving, het beleid, de projecten en daarmee samenhangende systemen worden grondig doorgelicht met het idee ‘een goed begin is het halve werk’. Een GEB/PIA moet dus in een vroeg stadium worden uitgevoerd. Dit voorkomt latere, kostbare aanpassingen in processen, herontwerp van systemen of zelfs stopzetten van een project. Hiermee wordt ook voldaan aan de verplichting om bij het ontwerp rekening te houden met gegevensbescherming (privacy by design).

Een GEB/PIA bestrijkt relevante systemen en procedures van verwerkingsactiviteiten, maar geen individuele gevallen. Een GEB/PIA kan wel betrekking hebben op een enkele soort gegevensverwerking (bijvoorbeeld alleen vernietigen van gegevens). Een GEB/PIA kan ook zien op een reeks vergelijkbare verwerkingen die vergelijkbare risico’s inhouden. Een GEB/PIA kan betrekking hebben op nieuw(e) regelgeving, beleid of projecten. Een GEB/PIA kan daarnaast wijzigingen betreffen in bestaande regelgeving, beleid of projecten.

Hoe je een GEB/PIA uitvoert, staat in het 'Model gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)'. Dit Model staat op internet en is opgenomen in het Handboek Portfoliomanagement Rijk. Het Model is gericht op de gegevensbeschermingseffectbeoordeling die wordt uitgevoerd bij AVG-persoonsgegevens (art. 36 AVG), maar is ook op de Wpg-GEB toepasbaar. De Wpg-GEB/PIA verschilt op een aantal punten van de GEB/PIA die op AVG-gegevens betrekking heeft. (1) De Wpg vereist niet dat de GEB een systematische beschrijving bevat van de verwerkingsdoeleinden. Toch is het raadzaam om de verwerkingsdoeleinden ook in de Wpg-GEB/PIA te noemen. Dat maakt het geheel compleet. (2) De Wpg vereist niet om een beoordeling van de noodzaak en evenredigheid van de verwerkingsdoeleinden met betrekking tot de doeleinden, op te noemen. Toch is het raadzaam om dit ook in de Wpg-GEB/PIA te noemen. Het is niet onwaarschijnlijk dat de AP hier om vraagt in het kader van dataminimalisatie. Dataminimalisatie is de in art. 3 Wpg opgenomen verplichting om politiegegevens slechts te verwerken voor zover dit noodzakelijk is opdat zo min mogelijk politiegegevens worden verwerkt.

Het projectplan dat op de voorgenomen GEB/PIA betrekking heeft, wordt ter advies voorgelegd aan de FG- WPG. Het projectplan wordt daarnaast voorgelegd aan de Chief Information Officer als de gegevensverwerking gepaard gaat met de bouw of vergaande aanpassing van een ICT-systeem. Als Chief Information Officer is de Hoofddirecteur Bedrijfsvoering aangewezen.

***Artikel 4.1 Melding datalek aan de Autoriteit persoonsgegevens.***

Een datalek is 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 tot gevolg (art. 1, onder q, Wpg).

Politiegegevens moeten beveiligd zijn tegen verlies en tegen onrechtmatige verwerkingen zoals diefstal. Een datalek is een inbreuk op de beveiliging waardoor de politiegegevens (tijdelijk) onbeschermd zijn. Een inbreuk op de beveiliging kan ontstaan door technisch of organisatorisch falen (waaronder menselijke fouten), zoals slordig beheer van wachtwoorden die toegang geven tot informatiebestanden, het verkeerd adresseren van een brief of e-mail die politiegegevens bevat, het als oud papier aanbieden van gevoelige stukken, of het zoekraken van een geheugenstick. Een inbreuk kan ook ontstaan door bewust menselijk gedrag (inbraak, diefstal of hack).

De privacyfunctionaris meldt het datalek aan de AP. In het kader van de afweging of een bepaald voorval aan de AP moet worden gemeld, overlegt hij met de FG-WPG.

De melding aan de AP blijft achterwege als de inbreuk op de beveiliging niet een kans op ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens oplevert. De kans op nadelige gevolgen is vaak groot bij grote aantallen gegevens of bij bijzondere gegevens. Bijzondere gegevens zijn persoonsgegevens die iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, het lidmaatschap van een vakvereniging, etnische afkomst, genetische gegevens en biometrische gegevens betreffen (art. 5 van de wet).

Een te late melding gaat vergezeld van een motivering van de vertraging (artikel 33a, eerste lid, Wet politiegegevens).

De melding aan de AP beschrijft (1) de aard en omvang van de inbreuk, waaronder het aantal en de categorieën van betrokkenen en gegevensbestanden; (2) de naam en contactgegevens van de FG-WPG; (3) de waarschijnlijke gevolgen van de inbreuk; (4) de voorgestelde of uitgevoerde maatregelen om de inbreuk te beëindigen of de nadelige gevolgen te beperken. Als het niet mogelijk is de informatie gelijktijdig, in een keer te verstrekken, kan de informatie in stappen worden verstrekt (art. 33a, derde lid, Wpg). Dit voorkomt onnodige vertraging.

Wat te doen bij een datalek?
- direct telefonisch melden bij het Defensie Operatie Centrum: 070-3188550;
- binnen 24 uur digitaal melden via de IV applicatie Melden van Voorvallen (MVV). Intranetportaal > selfservice > app Inspraak > melden voorval. Dan kiezen voor: bijzondere gebeurtenis > schending privacy.
- informeer de privacyfunctionaris. Dat gebeurt automatisch als de MVV-melding is geautoriseerd;
- de privacyfunctionaris meldt het datalek aan de AP als daar aanleiding toe is;
- als het verlies of stelen van de persoonsgegevens gevolgen waarschijnlijk een hoog risico met zich meebrengt voor de rechten en vrijheden van natuurlijke personen, krijgen diegenen bericht van de inbreuk op de beveiliging. Dit gebeurt zonder onnodige vertraging.

### *Artikel 4.2 Melding datalek aan de betrokkene*

Het datalek wordt door de privacyfunctionaris ook aan betrokkene meegedeeld wanneer dat waarschijnlijk een hoog risico voor de rechten en vrijheden van personen met zich meebrengt. Daarbij kan worden gedacht aan onrechtmatige publicatie, aantasting in eer en goede naam, identiteitsfraude of discriminatie.

De mededeling van het datalek aan de betrokkene bevat een omschrijving van de aard van het datalek, de naam en de contactgegevens van de FG-WPG, een beschrijving van de waarschijnlijke gevolgen van het datalek op de beveiliging en een beschrijving van de voorgestelde of uitgevoerde maatregelen om het datalek te beëindigen of de gevolgen ervan te beperken (art. 33a, vijfde lid, Wpg).

Onder omstandigheden is een mededeling aan betrokkene niet vereist of kan de mededeling worden uitgesteld, beperkt of achterwege worden gelaten. Dit volgt uit de art. 33a, zesde lid, en 27, eerste lid, van de wet.

### *Artikel 5.1 Informatieverstrekking aan de betrokkene*

Op diens verzoek wordt betrokkene informatie over de verwerking van politiegegevens verstrekt in beknopte en toegankelijke vorm en conform artikel 24a van de wet. De informatie wordt verstrekt met passende middelen, bij voorkeur in dezelfde vorm als waarin het verzoek is gedaan, tenzij dit op (beveiligings-)bezwaren stuit. De verstrekking is kosteloos. In bepaalde gevallen wordt de informatie in de vorm van strafrechtelijk processtuk gegoten.

Op verzoek van betrokkene worden hem de gegevens verstrekt, conform artikel 24b van de wet, tenzij ten aanzien van betrokkene het gegronde vermoeden bestaat dat hij een strafbaar feit heeft gepleegd of zal gaan plegen (art. 6b, onder a, Wpg).

Het gaat om informatie over: (1) contactgegevens van de privacyfunctionaris en de FG-WPG; (2) verwerkingsdoelen van de politiegegevens; (3) de rechten van betrokkene op inzage, rectificatie, aanvulling en vernietiging; (3) het recht een klacht in te dienen bij de AP. In specifieke gevallen kan betrokkene ook andere informatie worden verstrekt. Dat betreft informatie over de rechtsgrondslag van de verwerking, de bewaartermijn van de politiegegevens, het bestaan van geautomatiseerde besluitvorming, de categorieën van de ontvangers van de gegevens en eventueel extra informatie, in het bijzonder wanneer de politiegegevens zonder medeweten van betrokkene worden verzameld (art. 24b, Wpg).

### *Artikel 5.2 Recht op inzage, rectificatie, aanvulling en vernietiging*

Betrokkene heeft recht op inzage in politiegegevens die over hem gaan (art. 25 Wpg). Daarnaast heeft hij recht op rectificatie en aanvulling van politiegegevens die hem betreffen. Daarbij wordt rekening gehouden met het doel van de verwerking (art. 28, eerste lid, Wpg). Het ligt bijvoorbeeld niet voor de hand om een politiegegeven te rectificeren als het deel uitmaakt van een opsporingsonderzoek dat tot doel heeft te bepalen of het politiegegeven wel klopt.

Ook heeft betrokkene recht op vernietiging van de politiegegevens als de verwerking ervan strijdt met de wet of om te voldoen aan een wettelijke verplichting. De Wpg-beheerder kan in plaats van vernietiging kiezen voor afscherming indien betrokkene de juistheid van de gegevens betwist, maar de (on)juistheid ervan niet kan worden geverifieerd of als de gegevens moeten worden bewaard als bewijsmateriaal (art. 28, tweede lid, Wpg).

Het verzoek kan ook worden ingediend door de advocaat van betrokkene, door de AP of door zijn wettelijk vertegenwoordigers (art. 26, tweede lid, Wpg). In die gevallen moet niet alleen de identiteit van betrokkene worden vastgesteld, maar ook de identiteit van de verzoeker.

Een voorbeeld van een kennelijk buitensporig verzoek is bijvoorbeeld een verzoek dat deel uitmaakt van een hele reeks van verzoeken die elkaar snel opvolgen.

Dat onder omstandigheden een verzoek kan worden afgewezen, volgt uit art. 27, eerste lid, Wpg. Dat op een verzoek om inzage in de gegevens binnen zes wordt weken beslist, volgt uit art. 25, zesde lid, Wpg. Dat op een verzoek om rectificatie, aanvulling of vernietiging van de politiegegevens, binnen vier weken wordt beslist, volgt uit art. 28, vijfde lid, Wpg.

### *Artikel 5.3 Bezwaar*

Een beslissing op een verzoek van betrokkene tot inzage, rectificatie of vernietiging van hem betref-

fende politiegegevens, is een besluit in de zin van art. 1: 3 van de Algemene wet bestuursrecht (art. 29, eerste lid, Wpg). Onderaan dat besluit is de bezwaarclausule opgenomen, waarin staat op welke manier betrokkene bezwaar kan indienen bij de Afdeling Juridische Dienstverlening. Na de bezwaarfase gelden de reguliere beroepsfasen uit de Algemene wet bestuursrecht, tenzij betrokkene in de beroepstermijn de AP heeft verzocht om bemiddeling of advies. In dat geval kan betrokkene na afronding van die bemiddeling of dat advies, nog gedurende zes weken beroep instellen (art. 29, tweede lid, Wpg).

### *Artikel 6.1 Dataminimalisatie, juistheid en volledigheid*

In artikel 3 Wpg is kort gezegd bepaald dat verwerking van politiegegevens alleen aan de orde is voor zover behoorlijk, rechtmatig, noodzakelijk, toereikend, ter zake dienend en niet bovenmatig is voor de uitoefening van de politietaken (dataminimalisatie).

Verwerking voor een ander doel – bijvoorbeeld een AVG-doel – kan (1) als daar een wettelijke grondslag voor is en het noodzakelijk is en in verhouding staat tot dat doel en de verwerking voor dat andere doel; of (2) bij of krachtens de Wpg aangewezen personen of instanties die politiegegevens verwerken met het oog op een zwaarwegend algemeen belang. Een voorbeeld van (2) is de verstrekking van politiegegevens aan de Stichting Comensha, ten behoeve van de coördinatie van de opvang en verzorging van slachtoffers van mensenhandel en de registratie van gegevens over mensenhandel (art. 4:3, eerste lid, onder b, ten 3e Bpg).

In artikel 4 Wpg is kort gezegd bepaald dat de verwerkingsverantwoordelijke de nodige maatregelen moet treffen om te zorgen dat politiegegevens juist en nauwkeurig zijn voor het doel waarvoor ze worden verwerkt. In dit kader controleert de Wpg-beheerder de kwaliteit van de politiegegevens voordat de KMar deze verstrekt, als dat praktisch uitvoerbaar is. Als dat kan, wordt nadere informatie verstrekt bij doorzending van de politiegegevens, zodat de ontvanger de juistheid, volledigheid en betrouwbaarheid daarvan kan controleren, en kan nagaan of de gegevens nog actueel zijn (art. 4, eerste lid, Wpg).

### *Artikel 6.2 Beveiliging en beheer*

De Wpg-beheerder treft passende technische en organisatorische maatregelen op het gebied van beleid, procedures en ICT, om de rechtmatigheid, proportionaliteit en beveiliging van de politiegegevens zoveel mogelijk te garanderen. Hij houdt daarbij rekening met o.a. de aard en het doel van de verwerking, de stand der techniek en de mogelijke privacyrisico's voor betrokkenen. De beveiliging is gericht op dataminimalisatie en pseudonimisering, waar mogelijk. De beveiligingseisen zijn met name voor bijzondere categorieën van persoonsgegevens van belang.

De vereiste beveiliging kan worden bereikt door privacy by design (ontwerp) en privacy by default (standaardinstellingen). Privacy by design houdt in dat al tijdens de inrichting en ontwikkeling van organisatie, beleid, procedures en ICT-systemen, aandacht wordt besteed aan privacyverhogende maatregelen, zoals autorisaties en dataminimalisatie. Privacy by default houdt in dat er technische en organisatorische maatregelen worden genomen om er voor te zorgen dat als standaard, alléén persoonsgegevens worden verwerkt die noodzakelijk zijn voor het specifieke te bereiken doel, bijvoorbeeld door niet meer gegevens te vragen dan nodig is.

In de artikelen 4a en 4b Wpg staan de eisen waaraan de maatregelen moeten voldoen. Dit is nader uitgewerkt in artikel 6:1a van het Besluit politiegegevens. De maatregelen dienen daarnaast te voldoen aan het Besluit voorschrift informatiebeveiliging rijksdienst 2007 en aan het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013). Tot slot kunnen ook besluiten over beveiligingsbeleid van de AP richtinggevend zijn.

Gelet op artikel 6:1a Besluit politiegegevens wordt eerst een beoordeling van de risico's uitgevoerd en worden vervolgens maatregelen getroffen om

a. te verhinderen dat onbevoegde personen toegang krijgen tot apparatuur voor de verwerking van persoonsgegevens (controle op toegang tot de apparatuur);
b. te verhinderen dat onbevoegden gegevensdragers lezen, kopiëren, wijzigen of verwijderen (controle op de gegevensdragers);
c. te verhinderen dat onbevoegden gegevens invoeren of opgeslagen persoonsgegevens inzien, wijzigen of verwijderen (controle op opslag);
d. te verhinderen dat onbevoegden systemen voor geautomatiseerde gegevensverwerking gebruiken met behulp van datatransmissieapparatuur (controle op gebruiker);
e. er voor te zorgen dat personen die geautoriseerd zijn om een systeem voor geautomatiseerde gegevensverwerking te gebruiken, uitsluitend toegang hebben tot de gegevens waarop hun autorisatie betrekking heeft (controle op toegang tot de gegevens);

f. er voor te zorgen dat kan worden nagegaan en vastgesteld aan welke organen persoonsgegevens zijn of kunnen worden verstrekt of beschikbaar gesteld met behulp van datatransmissieapparatuur (controle op transmissie);
g. er voor te zorgen dat later kan worden nagegaan en vastgesteld welke persoonsgegevens wanneer en door wie in een systeem voor geautomatiseerde gegevensverwerking zijn ingevoerd (controle op invoer);
h. te verhinderen dat onbevoegden persoonsgegevens lezen, kopiëren, wijzigen of verwijderen tijdens het de doorgifte van persoonsgegevens of het vervoer van gegevensdragers (controle op transport);
i. er voor te zorgen dat de geïnstalleerde systemen in geval van storing opnieuw kunnen worden ingezet (controle op herstel);
j. er voor te zorgen dat de functies van het systeem werken, dat eventuele functionele storingen worden gesignaleerd en dat opgeslagen persoonsgegevens niet kunnen worden beschadigd door het verkeerd functioneren van het systeem (controle op betrouwbaarheid en integriteit).

Bij de ontwikkeling van maatregelen, procedures en ICT-systemen, kan ook worden gekeken naar de resultaten van de GEB/PIA's.

### *Artikel 7 Audit*

De Audit Dienst Rijk verricht externe audits. De Audit Dienst Defensie verricht interne audits. De auditdiensten kunnen, al dan niet op verzoek van de FG-WPG en al dan niet periodiek, een audit uitvoeren naar de naleving van de regeling en van het bij of krachtens de wet bepaalde. De auditdienst stemt dit af met de FG-WPG, door hem vooraf te informeren over het voornemen een audit te verrichten.

### *Artikel 8 Aanwijzing*

De Secretaris-Generaal kan op basis van dit artikel aanwijzingen geven over de vorm en de manier waarop de Wpg(onder)-beheerder uitvoering moet geven aan deze regeling. De aanwijzingen zijn een aanvulling op de wet en het Bpg en hebben betrekking op de manier waarop politiegegevens juist, nauwkeurigheid en accuraat worden verwerkt, zoals de manier waarop met een datalek wordt omgegaan.

### *Artikel 9 Inwerkingtreding*

Met de inwerkingtredingsdatum is aangesloten bij de datum waarop de Richtlijn gegevensbescherming opsporing en vervolging is geïmplementeerd in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens.

*De Minister van Defensie,*
*A.Th.B. Bijleveld-Schouten*