# Beleidskader registerplicht en GEB

Bescherming van persoons- en politiegegevens

VASTGESTELD document

Gegevensautoriteit

Definitief

Versie 2.0

Versie datum 8 november 2019

Rubricering politie intern

« waakzaam en dienstbaar »

# Documentinformatie

**Versiegeschiedenis**

| Versie | Versie datum | Samenvatting van de aanpassing | Gemarkeerde wijzigingen |
|---|---|---|---|
| 0.1 | 26 november 2018 | Eerste opzet door | |
| 0.2 | 11december 2018 | Reacties GA verwerkt . Invulling H4 AVG door | |
| 0.3 | 14 januari 2019 | Reacties Registerwerkgroep ( ) verwerkt. Opzet iets gewijzigd naar verantwoordingsplicht | |
| 0.4 | 5 februari 2019 | Tussenversie met aanpassingen n.a.v. plenaire bespreking registerwerkgroep 24 februari 2019 . | |
| 0.5 | 22 februari | Reacties verwerkt van | |
| 0.6 | 7 maart 2019 | Paragraaf. over GEB uitgebreid en structuur aangepast n.a.v. reacties GA en Verbeterprogramma | |
| 0.7 | 11 maart 2019 | Reacties verwerkt van over uitvoering control-functie, redactieslag van reactie | |
| 1.0 | 14 maart 2019 | Versie voor stuurgroep Verbeterprogramma Wpg en IB en stuurgroep AVG | |
| 1.1 | 28 maart 2019 | Versie goedgekeurd door stuurgroep Verbeterprogramma Wpg en IB, reactie verwerkt | |
| 1.2 | 28 mei 2019 | Enkele reacties nav stuurgroep verwerkt | |
| 1.3 | 1 augustus 2019 | Reactie verwerkt | |
| 1.3 | 3 oktober 2019 | Akkoord Hoofden Bedrijfsvoering Overleg HBVO | |
| 2.0 | 8 november 2019 | Akkoord Breed Bedrijfsvoering Overleg BBVO | |

Is dit het laatst vastgestelde document? Dat is eenvoudig te controleren door binnen de politieomgeving deze link of de QR code te openen.

**Distributie**

| Versie | Verzend datum | Naam | Afdeling / Functie |
|---|---|---|---|
| | | | |
| | | | |

**Review commentaar**

| Versie | Wanneer | Wie | Functie |
|---|---|---|---|
| | | | |
| | | | |

# Inhoudsopgave

# 1. Inleiding

## 1.1 Verantwoordingsplicht

Allerlei technologische ontwikkelingen hebben ertoe geleid dat vanuit de samenleving meer aandacht is gekomen voor privacy en het belang van bescherming van persoonsgegevens. Organisaties die gegevens verwerken moeten daarom veel meer dan vroeger transparant zijn over de gegevens die zij verwerken, en hierover verantwoording afleggen: de verantwoordingsplicht.

De politie staat voor de bescherming van de grondrechten en dus ook het recht dat de privacy beschermt. En ook voor de politie geldt dat het verwerken van persoonlijke gegevens veel meer in de spotlights is komen te staan. De samenleving en de politiek verlangen meer dan vroeger inzicht in en rekenschap over de verwerking van persoonlijke gegevens. De aandacht voor de bescherming van persoonlijke data heeft uiteindelijk geleid tot wijzigingen in de privacyregelgeving, waarin deze verantwoordingsplicht ook wettelijk is vastgelegd. Per 25 mei 2018 is de Algemene verordening gegevensbescherming (hierna: AVG) in werking getreden. Met ingang van 1 januari 2019 is in Nederland de vergelijkbare Europese Richtlijn gegevensbescherming opsporing en vervolging (2016/680) geïmplementeerd in de aldus gewijzigde Wet politiegegevens (hierna: Wpg).

Er zijn diverse instrumenten om uitvoering te geven aan de verantwoordingsplicht. Zo geldt bijvoorbeeld de loggingverplichting, de verplichting om een functionaris voor gegevensbescherming (hierna: FG) aan te stellen, en het verplicht bijhouden van een register van verwerkingen en een register van datalekken. Dit beleidskader gaat over de registerplicht, als onderdeel van de verantwoordingsplicht en de bijkomende verplichting om indien noodzakelijk een gegevensbeschermingseffectbeoordeling (hierna: GEB) uit te voeren. De andere onderdelen van de verantwoordingsplicht vallen buiten scope en zijn elders belegd.

## 1.2 Registerplicht en GEB

De belangrijkste verplichting onder de AVG en aangepaste Wpg is dat verwerkingen van persoons- en politiegegevens voldoen aan belangrijke beginselen zoals rechtmatigheid, transparantie, doelbinding en juistheid. Het register is een manier om verantwoording af te leggen over gegevensverwerkingen. Dat geldt naar de verwerkingsverantwoordelijke, maar ook naar de interne toezichthouder de FG, en de Autoriteit Persoonsgegevens (hierna: AP).Ook kan het register in de toekomst behulpzaam zijn bij het inzichtelijk maken van verwerkingen richting betrokkenen.

De basismaatregel om te voldoen aan de verantwoordingsplicht is het inzichtelijk maken van het effect van een verwerking op de privacy van betrokkene. In het geval er mogelijk een hoog risico is voor de rechten en vrijheden van natuurlijke personen moet er voorafgaande aan de verwerking een GEB worden uitgevoerd. Alle verwerkingen van persoonlijke gegevens zijn beschreven en opgenomen in het register van verwerkingsactiviteiten, oftewel het register. In het register moet worden aangetoond dat er maatregelen zijn genomen ter beveiliging van de persoonsgegevens. Er zijn organisaties die het register of delen daarvan online publiceren, om zo de verwerkingen aan betrokkenen zichtbaar te maken. Dat is voor de politie op dit moment niet aan de orde. Wel kunnen op termijn delen van het register gebruikt worden om betrokkenen en andere stakeholders inzicht te geven in verwerkingen.

## 1.3 Dit beleidskader

Dit beleidskader beschrijft hoe de politie invulling geeft aan verplichting om verwerkingen te beschrijven en op te nemen in een register en een GEB uit te voeren. Dit beleidskader maakt onderdeel uit van het privacy beleid van de politie.

Dit beleidskader is gericht aan:

- personen die een verantwoordelijkheid hebben in de plan- of ontwerpfase van processen, waaronder werkprocessen, projecten en programma's, proeftuinen, pilots, innovaties en andere verandertrajecten waarin persoons- of politiegegevens worden verwerkt. Dit beleidskader geldt ook wanneer deze plannen gewijzigd worden, bijvoorbeeld wanneer de noodzaak hiertoe blijkt in de uitvoeringsfase.
- personen die de autorisaties verzorgen conform het autorisatiemodel. Tot hun taak behoort het autoriseren van juiste personen voor de tool die de politie ondersteunt bij het uitvoeren van verantwoordingsplicht, zoals het register, de quick scan en de GEB.

- personen die zorgen voor de uitvoering van de control-functie: controllers en auditers. Zij kunnen mede op basis van een (automatische) selectie van gegevens uit het register inzicht krijgen in de stand van zaken met betrekking tot de vulling van het register met verwerkingen en het uitvoeren van GEB's.
- de veranderteams, waaronder de bouwers en beheerders van het verwerkingsregister.

De daadwerkelijke operationele uitvoering van werkprocessen, projecten, programma's, pilots, proeftuinen, innovaties en dergelijke moet in overstemming zijn met dit beleidskader. Voordat met de uitvoering mag worden gestart behoort deze eerst getoetst te worden aan dit beleidskader of aan processen/procedures/uitvoeringskaders die conform dit beleidskader zijn opgesteld.

**Eigenaar**
De Gegevensautoriteit (hierna: GA) is eigenaar van dit beleidsdocument. De GA ziet ook toe op de juiste uitvoering van dit beleid. De FG ziet toe op de rechtmatige uitvoering van de beschreven verwerkingen.

# 2. Verwerkingen, de GEB en het register

Dit hoofdstuk beschrijft de verplichtingen ten aanzien van verwerkingen, de GEB en het register.

## 2.1 Relevante wetgeving

De verplichting om verwerkingen te beschrijven in een register en op hoog risicoverwerkingen een GEB uit te voeren, volgt uit de AVG en de Wpg. De Wpg is van toepassing op de verwerkingen van politiegegevens door een bevoegde autoriteit. Hieronder vallen de verwerkingen in het kader van de politietaak, zoals genoemd in artikel 3 van de Politiewet 2012, uitgezonderd de korpschef-, vreemdelingen, - en burgemeesterstaken. Deze laatst genoemde taken vallen onder het toepassingsbereik van de AVG. De AVG is van toepassing op alle verwerkingen van persoonsgegevens die niet vallen onder het toepassingsbereik van de Wpg.

De vuistregel binnen de politie is dat de AVG geldt voor de bedrijfsvoeringprocessen, korpscheftaken, vreemdelingenzaken en burgemeesterstaken, en een groot deel van de processen van de afdeling Veiligheid, Integriteit en Klachten, en de Wpg voor de operationele politietaak.
De AVG en Wpg sluiten elkaar uit: op een verwerking is óf de Wpg óf de AVG van toepassing.

## 2.2 Verwerkingen en verwerkingsverantwoordelijke

Deze paragraaf beschrijft wat een verwerking is en welke verplichtingen er gelden.

### 2.2.1 Juridisch kader

Alles wat je doet met een persoons- en/of politiegegeven is een verwerking. Het juridisch kader luidt als volgt:

#### 2.2.1.1 Verwerken van persoonsgegevens

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”)[1]

Verwerken van persoonsgegevens: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens[2];

#### 2.2.1.2 Verwerken van politiegegevens

Politiegegeven: elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak, bedoeld in de artikelen 3 en 4 van de Politiewet 2012, met uitzondering van:

- de uitvoering van wettelijke voorschriften anders dan de Wet administratiefrechtelijke handhaving verkeersvoorschriften;
- de bij of krachtens de Vreemdelingenwet 2000 opgedragen taken, bedoeld in artikel 1, eerste lid, onderdeel i, onder 1° en artikel 4, eerste lid, onderdeel f, van de Politiewet 2012[3];

Verwerken van politiegegevens: elke bewerking of elk geheel van bewerkingen met betrekking tot politiegegevens of een geheel van politiegegevens, al dan niet uitgevoerd op geautomatiseerde wijze, zoals het verzamelen, vastleggen,

---

[1] Artikel 4 sub 1 AVG
[2] Artikel 4 sub 2 AVG
[3] Artikel 1 sub a Wpg

ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, afschermen of vernietigen van politiegegevens[4].

Een verwerking omvat dus alle handelingen met betrekking tot een persoons- en/of politiegegeven:

- geautomatiseerde vormen van deze handelingen vallen onder het begrip verwerking
- één verwerking kan bestaan uit een geheel van onderliggende verwerkingen
- een verwerking van persoons- en/of politiegegevensgegevens staat los van de applicatie waarin dit plaatsvindt
- een verwerking kan in één of meerdere systemen plaatsvinden
- één applicatie kan meerdere verwerkingen van gegevens betreffen
- een verwerking die volledig op papier of buiten de kernsystemen- of applicaties (ongestructureerde verwerkingen) wordt uitgevoerd kan onder de reikwijdte van de AVG of Wpg vallen.

Het begrip verwerking is wettelijk gezien ruim gedefinieerd, wat de verwerkingsverantwoordelijke enige speelruimte geeft bij de keuze voor een verwerking in zijn organisatie. Variërend van een zeer abstract niveau tot aan een gedetailleerd inzicht per verwerking. Het gekozen niveau moet aan de verwerkingsverantwoordelijke en de toezichthouders voldoende inzicht bieden in de eventuele risico's van de verwerking.

#### 2.2.1.3 Verwerkingsverantwoordelijke

Alle verwerkingen vinden plaats onder de verantwoordelijkheid van een verwerkingsverantwoordelijke. Dat is degene die alleen of samen met anderen, doel en middelen voor de verwerking vaststelt[5]. De korpschef is verwerkingsverantwoordelijke voor de politie. Deze verantwoordelijkheid is via een mandatenstelsel gemandateerd aan de lijnorganisatie. Overal waar in dit stuk staat 'verwerkingsverantwoordelijke' wordt ook bedoeld de gemandateerd verwerkingsverantwoordelijke.

Wanneer partijen gezamenlijk doel en middelen van de AVG verwerking bepalen zijn zij gezamenlijk verantwoordelijk voor deze verwerking[6]. Bijvoorbeeld in een samenwerkingsverband als het RIEC. Deelnemende partijen hebben een gezamenlijke verwerkingsverantwoordelijkheid voor de verwerking waarvoor gezamenlijk doel en middelen zijn bepaalt. Iedere partij is mede-verantwoordelijke. Partijen blijven wel zelfstandig verantwoordelijk voor hun 'eigen' verwerkingen, waaronder het verstrekken van informatie aan het samenwerkingsverband.

De Wpg kent geen gezamenlijke verwerkingsverantwoordelijkheid, maar wel een gemeenschappelijke verwerking. Wanneer uitsluitend Wpg partijen[7] gezamenlijk een Wpg verwerking uitvoeren wordt altijd één verwerkingsverantwoordelijke aangewezen[8].

### 2.2.2 Keuze verwerking politie

Een bedrijfsfunctiemodel beschrijft de functies (ook wel: doelen) van een organisatie. De politie heeft een bedrijfsfunctiemodel voor de operationele processen en één voor de bedrijfsvoering. Functies worden gerealiseerd door werkprocessen. De relatie tussen functies en werkprocessen is als volgt: functies beschrijven 'wat de politie doet, en de werkprocessen hoe de politie dat doet. Werkprocessen en functies zijn aan elkaar gekoppeld. Een werkproces kan bijdragen aan de realisatie van meerdere functies. Een functie wordt gerealiseerd door meerdere werkprocessen. Het bedrijfsfunctiemodel en de werkprocessen zijn vastgesteld door de Korpsleiding t.b.v. de vorming van de nationale politie. De functies en werkprocessen zijn opgehaald uit de eenheden, het is een beschrijving op tactisch niveau wat alle politie-eenheden doen.

De werkprocessen die de functies in het bedrijfsfunctiemodel realiseren worden gelijkgesteld aan een verwerking in de zin van zowel de AVG als de Wpg[9]. Deze werkprocessen geven inzicht in de huidige verwerkingen van persoons- en politiegegevens. Het bedrijfsfunctiemodel politie omvat echter niet alle verwerkingen, want ook innovaties, een proeftuin of pilot, projecten, nieuwe applicaties, wijzigingen van een bestaande applicatie, een

---

[4] Artikel 1 sub c Wpg
[5] Artikel 4 sub 7 AVG en artikel 1 sub f onder 1 Wpg
[6] Artikel 26 lid 1 AVG
[7] Bevoegde autoriteit die gegevens verwerkt voor de strafrechtspleging: politie, Rijksrecherche en KMAR
[8] Artikel 1 sub f onder 4 Wpg: gemeenschappelijke verwerking
[9] Uiteraard voor zover hier persoons- of politiegegevens in voorkomen.

samenwerkingsverband, een nieuwe werkstroom, en nieuw werkprocessen zijn allemaal verwerkingen waarop de registerplicht en de GEB-verplichting van toepassing zijn.

Voorbeelden van verwerkingen
- het werkproces ‘Aanhouden verdachte’
- de proeftuin ‘ANPR Roermond’
- DNA eliminatie-database politiemedewerkers
- personeelsadministratie
- screening politiesollicitanten

Er bestaat altijd een relatie tussen de werkprocessen en overige verwerkingen, zoals projecten en pilots. Voor alle verwerkingen geldt dat zij één of meerdere relaties met elkaar kunnen hebben. Deze relaties kunnen hiërarchisch zijn, maar dit hoeft niet.

### 2.2.3 Eisen aan verwerkingen

Voor alle verwerkingen geldt dat zij moeten voldoen aan de eisen uit de AVG of de Wpg. Paragraaf 2.6 beschrijft de wat nodig is om specifiek te voldoen aan de wettelijke registerplicht en de verplichting een GEB uit te voeren op hoog risico verwerkingen[10].

## 2.3 GEB

### 2.3.1 Juridisch kader

Wanneer een verwerking van persoon- of politiegegevens een hoog risico oplevert voor de rechten en vrijheden van personen, dan moet voorafgaand aan deze verwerking een beoordeling van het effect van de voorgenomen activiteiten op de bescherming van persoonsgegevens uitgevoerd worden[11]. Het doel van de GEB is om al bij het initiatief van een verwerking waarbij het risico mogelijk hoog is, te beoordelen welk effect de verwerkingsactiviteiten op de betrokkene(n) hebben en hoe de betreffende gegevens het beste kunnen worden beschermd. Aan de hand daarvan kunnen privacy en informatiebeveiligingsrisico’s worden ingeschat en maatregelen worden genomen.

Een GEB moet in ieder geval de volgende elementen bevatten[12]:
- een algemene beschrijving van de beoogde verwerking of verwerkingen
- een beoordeling van de risico’s voor de rechten en vrijheden van betrokkenen
- de beoogde maatregelen ter beperking van de risico’s
- de voorzorgs- en beveiligingsmaatregelen en mechanismen om de persoons- of politiegegevens te beschermen en aan te tonen dat aan het bij of krachtens deze wet bepaalde is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere betrokken personen beoordeling.

Bij het uitvoeren van een GEB op een AVG verwerking ‘wint de verwerkingsverantwoordelijke het advies in van de FG[13]. Deze adviserende taak van de FG is belegd bij de privacyfunctionarissen[14].

Wanneer uit een GEB blijkt dat de verwerking een hoog risico oplevert als de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken, raadpleegt de verwerkingsverantwoordelijke voorafgaand aan de verwerking de toezichthoudende autoriteit[15].

---

[10] Voor een volledig overzicht van alle eisen aan een verwerking i.v.m. privacywet- en regelgeving ontwikkelt de GA een checklist
[11] Artikel 35 lid 1 AVG en artikel 4c lid 1Wpg
[12] Artikel 35 lid 7 AVG en artikel 4c lid 2 Wpg
[13] Artikel 35 lid 2 AVG
[14] Functionaris Gegevensbescherming (kwartiermaken), versie 1.0 definitief van 6 maart 2019
[15] Artikel 36 AVG en artikel 33b lid 1 sub b Wpg

Voor een GEB uitgevoerd op een Wpg verwerking is voorafgaande raadpleging van de AP[16] ook noodzakelijk wanneer de aard van de verwerking, in het bijzonder met gebruikmaking van nieuwe technologieën, mechanismen of procedures, een hoog risico voor de rechten en vrijheden van de betrokkene met zich meebrengt[17].

### 2.3.2 GEB bij politie

De politie maakt gebruik van één centraal verwerkingen registratieproces, waarin twee soorten GEB's zijn opgenomen: één voor de Wpg verwerkingen en één voor AVG verwerkingen. Beide modellen zijn gebaseerd op het rijksmodel Privacy Impact Assessment, maar zijn toepasbaar gemaakt voor de specifieke politiesituatie.

Om na te gaan of er sprake is van een hoog risico voor de privacy is een quick scan ontwikkeld. Er is één quick scan die van toepassing is op zowel AVG als Wpg verwerkingen. Voor de start van een verwerking moet een quick scan worden uitgevoerd op de voorgenomen verwerking. Blijkt hieruit een hoog risico, dan is de volgende stap het uitvoeren van een GEB vóór de start van de voorgenomen verwerking.

Een GEB kan betrekking hebben op een individuele gegevensverwerking, maar kan ook zien op een reeks vergelijkbare verwerkingen die vergelijkbare risico's inhouden. Een GEB hoeft zich dus niet te beperken tot een enkel proces, product of verwerkingsverantwoordelijke, bijvoorbeeld wanneer de politie op meerdere plaatsen een vergelijkbare verwerking uitvoert of met andere instanties een gemeenschappelijke verwerking wil opzetten. Het in kaart brengen van de risico's door middel van een GEB is ook nodig wanneer er nieuwe applicaties of toepassingen worden ontwikkeld.

Het is aan de persoon die verantwoordelijk is voor de verwerking om ervoor te zorgen dat tijdig een quick scan en eventueel een GEB wordt uitgevoerd op de verwerking. Hij zorgt er ook voor dat de juiste expertise aanwezig is om een GEB te kunnen uitvoeren, waaronder deskundigheid op het gebied van privacy en informatiebeveiliging.

Een uitgevoerde GEB geeft inzicht in de risico's voor betrokkene en de informatiebeveiligingsrisico's voor de organisatie. Daar kan de verwerkingsverantwoordelijke op de volgende manieren mee omgaan:

1. aanvullende (informatiebeveiligings-)maatregelen nemen, bijvoorbeeld het anonimiseren of pseudonimiseren van de gegevens, deze maatregelen worden dan beschreven in een actieplan
2. de voorgenomen verwerking aanpassen zodat het risico omlaag gaat, bijvoorbeeld door minder of andere persoons- of politiegegevens te gebruiken
3. de voorgenomen verwerking kan geen doorgang vinden omdat de risico's te hoog zijn in relatie tot het doel van de verwerking, tenzij er een wettelijke uitzonderingsgrond van toepassing is die de verwerking alsnog toestaat.

In principe kan een voorgenomen verwerking niet van start gaan als er nog hoge risico's zijn. Dat betekent dat vóór de start van de verwerking de maatregelen uit het actieplan zijn uitgevoerd. Of de verwerking is zodanig aangepast dat alleen laag- risico's overblijven, waarvan duidelijk is dat deze op een acceptabele manier worden weggewerkt. Er zijn situaties waarin de voorgenomen verwerking toch moet plaatsvinden, ondanks de (hoge) risico's.

Alleen degene die op dat moment verantwoordelijk is voor de verwerking kan besluiten dat deze toch mag starten zonder dat aan alle eisen is voldaan. Voorafgaand aan dit besluit vindt overleg plaats met de FG, GA en de CISO. Welke lijnmanager of portefeuillehouder verantwoordelijk is voor de verwerking volgt uit het mandaatstelsel, zie ook para 5.3 Lijnmanagement.

Een verwerking waar nog een hoog risico van toepassing is moet worden aangemeld bij de AP, dit verloopt altijd via de FG[18].

---

[16] De Gegevensautoriteit is de contactpersoon
[17] Artikel 33b lid 1 sub a Wpg.
[18] Functionaris Gegevensbescherming (kwartiermaken), versie 1.0 definitief van 6 maart 2019

## 2.4 Verwerkingsregister

### 2.4.1 Juridisch kader

Iedere verwerkingsverantwoordelijke is verplicht beschrijvingen van alle verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden in een register bij te houden[19]. De registerplicht dwingt organisaties inzichtelijk te maken hoe met persoonsgegevens en politiegegevens wordt omgaan en dit ook te kunnen verantwoorden.

Het register is ook bedoeld als toezichtinstrument voor zowel de interne toezichthouder, de FG, als de externe toezichthouder, de AP.

De AVG en de Wpg[20] schrijven voor welke informatie in het register beschreven moet worden:

- contactgegevens van de verwerkingsverantwoordelijke en indien van toepassing de gezamenlijke verwerkingsverantwoordelijken
- het doel van de verwerking
- de categorieën van betrokkenen, dat wil zeggen de personen op wie de gegevens betrekking hebben
- of het persoonsgegevens dan wel politiegegevens betreft
- hoe men aan de gegevens is gekomen; direct van de betrokkene, of anderszins
- aanwijzing van rechtsgrondslag van de verwerking waarvoor de persoons of politiegegevens bedoeld zijn, de verwerkingsgrondslag. Ook bij een eventuele doorgifte moet dit worden geregistreerd
- een algemene beschrijving van technische en organisatorische beveiligingsmaatregelen
- de beoogde termijnen voor verwijdering en vernietiging
- de categorieën van ontvangers aan wie gegevens worden verstrekt, of beschikbaar worden gesteld (zowel intern, als extern)
- toekenning van de juiste autorisaties
- of gebruik wordt gemaakt van (geautomatiseerde) profilering
- de doorgifte van persoonsgegevens (of politiegegevens aan een derde land of internationale organisatie buiten de EU.
- documenten waaruit blijkt dat het derde land passende waarborgen heeft getroffen omtrent de bescherming van de persoonsgegevens.

### 2.4.2 Verwerkingsregister bij politie

Er is één register van verwerkingen, waarin alle Wpg en AGV verwerkingen van de politie staan. Op termijn zal ook de Politieacademie[21] (hierna: PA) gebruik maken van de registertool. De verwerkingen van de PA worden door middel van autorisaties afgescheiden van de politieverwerkingen, want de PA is geen onderdeel van de politie en kent een eigen verwerkingsverantwoordelijke. Het register is de enige authentieke bron voor AVG en Wpg verwerkingen en zal dus moeten voldoen aan kwaliteitseisen[22]. Dat betekent dat wanneer de verwerkingsverantwoordelijke of een toezichthouder op zoek is naar een verwerking, zij daarvoor het register moeten raadplegen.

In het register wordt zoveel mogelijk gebruik gemaakt van referentiegegevens en informatie uit bronbestanden. Het register bevat geen bestanden of documenten maar verwijst hier zoveel mogelijk naar middels een dynamische link. Bijvoorbeeld naar een verwerkersovereenkomst bij de Dienst Verwerving of naar een convenant in het convenantenregister. Dergelijke dynamische verwijzingen kunnen alleen naar interne opslaglocaties binnen de politie verwijzen. Bestanden van externen moeten wél in het register te worden opgenomen.

Het register is een referentie- en toezichtinstrument voor zowel de eigen organisatie als de AP, en kan daarom niet in zijn geheel worden gerubriceerd of geheim worden verklaard. Specifieke onderdelen van het register kunnen wel degelijk vertrouwelijke informatie bevatten. Via autorisaties wordt de inzage op dergelijke vertrouwelijke informatie beperkt.

Van bepaalde verwerkingen is het mogelijk niet wenselijk dat zij in het register worden geregistreerd, omdat informatie hierover te zeer de opsporings- en vervolgingsbelangen van de politie zou schaden. Dit geldt bijvoorbeeld

---

[19] Artikel 30 AVG en Artikel 31d Wpg
[20] Artikel 30 lid 1 AVG en artikel 31d lid 1 Wpg
[21] De Politieacademie is een zelfstandig bestuursorgaan, een ZBO
[22] Dit volgt ook uit §5.7.2 van het Uitvoeringskader Privacy & Security by Design, versie 2.0

voor de verwerking van gegevens over informanten, ook wel ‘artikel 12 Wpg –verwerking’, of de verwerking van gegevens over medewerkers in de bijzondere bedrijfsvoering. De verwerkingsverantwoordelijke beslist hierover in overleg met de FG.

Vanwege het vertrouwelijke karakter van de informatiebeveiliging risicoanalyses binnen de politie worden deze niet centraal in het register opgenomen. Wel wordt aangegeven of een dergelijke analyse is uitgevoerd, wanneer, door wie en waar deze te vinden is. De te nemen privacy- en informatiebeveiligingsmaatregelen worden wel in het register opgenomen.

**Verwerkingen in register**
De hierna volgende verwerkingen worden in het verwerkingsregister opgenomen, waarbij bij iedere verwerking de verwerkingsverantwoordelijke wordt aangegeven:

- verwerkingen waarvoor de korpschef de verwerkingsverantwoordelijke is
- verwerkingen waarvoor de korpschef de mede-verantwoordelijke is in geval van samenwerkingsverbanden. Bijvoorbeeld bij de gemeenschappelijke meldkamer, waar alle partijen gezamenlijk verantwoordelijk zijn. Het gaat dan vaak om een AVG-verwerking.
- verwerkingen die de politie uitvoert als verwerker, bijvoorbeeld de verwerkingen die de politie voor de Koninklijke Marechaussee (KMAR) en de Immigratie- en Naturalisatie Dienst (IND) uitvoert.
- de verwerkingen van de Politieacademie, die als ZBO, ten behoeve van het geven van opleidingen met betrekking tot de uitvoering van de politietaak formeel een zelfstandige verwerkingsverantwoordelijkheid heeft.

Verwerkingen van persoons- of politiegegevens waar de politie geen enkele verantwoordelijkheid heeft, worden niet in het register opgenomen. Zo worden verwerkingen van boa’s die niet werkzaam zijn bij de politie, niet in het register opgenomen.

Door middel van autorisaties wordt de toegang tot de registertool geregeld. Autorisaties worden uitgegeven op basis van functionele noodzaak, conform het vastgestelde autorisatiebeleid. De registertool levert rapportages met betrekking tot de status van alle in het register opgenomen verwerkingen. Rapportages met managementinformatie verlopen via de reguliere rapportagelijnen. Daarbij wordt de cyclus van de 4-, 8- en 12-maandsrapportages gevolgd. De informatie uit het register kan ook worden gebruikt voor het uitvoeren van de control-functie.

## 2.5 Samenwerkingsverbanden

Bij deelname aan een verwerking in samenwerkingsverbanden registreert de politie deze in het verwerkingsregister en voert een GEB uit. Daarbij noteert zij de rol ten aanzien van die specifieke verwerking: zelfstandig of mede verantwoordelijk. Voor de gegevens die de politie verstrekt ten behoeve van de gezamenlijke verwerking is de politie zelfstandig verwerkingsverantwoordelijke. Alleen ten aanzien van gezamenlijke verwerkingen[23] is de politie mede-verantwoordelijk.

Bij het uitvoeren van een GEB voor de eigen verwerking in het samenwerkingsverband kan de politie gebruik maken van een al uitgevoerde GEB. Bijvoorbeeld een GEB op een ketenverwerking of een nieuwe wet. Deze moet dan wel naar het oordeel van de politie voldoende inzicht bieden in de risico’s voor de politie-verwerking. In de meeste gevallen zal de politie zelf een (aanvullende) GEB moeten uitvoeren.

## 2.6 Ondersteunende tool

Ter ondersteuning van de uitvoering van de registerplicht en de GEB is een tool aangeschaft. In de tool kan een verwerking worden geregistreerd, en een quick scan en een GEB worden uitgevoerd.

De uitgangspunten voor het gebruik van deze tool zijn als volgt:

- het Politiedienstencentrum (hierna: PDC) zorgt voor het functioneel en technisch beheer van de tool
- de verwerkingsverantwoordelijken zorgen er zelf voor dat verwerkingen in de tool worden geregistreerd, en dat een GEB wordt uitgevoerd en in de tool wordt geregistreerd.
- uit doelmatigheidsoverwegingen worden sommige bedrijfsvoering processen nog geclusterd.

- het Verbeterprogramma Wpg en IB zorgt voor een initiële vulling van het register in de tool met de huidige Wpg verwerkingen, oftewel de werkprocessen uit het BRM politie.
- uit informatiebeveiligingsoverwegingen heeft het MT van het PDC besloten dat de tool in gebruik én beheer wordt genomen binnen het politiedomein. De applicatie wordt lokaal geïnstalleerd op servers van de politie. De applicatie mag niet worden afgenomen als zogenaamde Software as a service (Saas) oplossing, waarbij de applicatie in beheer blijft bij de leverancier en deze door de afnemers benaderbaar is via internet.
- vanuit de tool kunnen naast rapportages ten behoeve van de (status) van de verwerkingen en het toezicht, ook rapportages met management informatie worden gegenereerd. De verwerkingsverantwoordelijke kan deze informatie gebruiken om te sturen op onder andere compliance, voortgang, juistheid en volledigheid van de verwerking die onder zijn verantwoordelijkheid wordt uitgevoerd.
- de tool kan ook gebruikt worden voor het registreren en documenteren van documenten, zoals de toestemming indien een verwerking van persoonsgegevens hierop berust.

## 2.7 Eisen aan verwerkingen

De hiervoor beschreven verplichtingen en uitgangspunten leiden tot de volgende eisen aan een verwerking:

1. Er is sprake van een voornemen tot een nieuwe verwerking, óf een voornemen tot aanpassing van een bestaande verwerking.
2. De voorgenomen verwerking wordt geregistreerd in het register met behulp van de tool.
3. Op de voorgenomen verwerking wordt een quick scan uitgevoerd om een indicatie te krijgen van de risico's voor betrokkenen. Hierbij wordt gebruik gemaakt van de tool.
4. Een informatiebeveiliging specialist voert op de voorgenomen verwerking een informatiebeveiliging analyse uit. In het register wordt geregistreerd of en door wie een dergelijke analyse is uitgevoerd.
5. Wanneer uit de quick scan een hoog risico blijkt, wordt een GEB uitgevoerd en gedocumenteerd vóór de start van de verwerking met behulp van de tool.
6. Voer een GEB uit met een team van deskundigen van de betreffende verwerking, en deskundigen op het gebied van privacy en informatiebeveiliging. Vraag advies aan de PF.
7. Mitigeer de risico's die volgen uit de GEB, en stel daarvoor een actieplan op met per risico de mitigerende maatregelen. Neem dit plan op in de tool.
8. Raadpleeg de AP als blijkt dat alsnog een hoog risico overblijft. Dit moet vóór de start van de verwerking en verloopt altijd via de FG.
9. De FG en de GA hebben een rol in het toezicht op registratie van verwerkingen in het register en het uitvoeren van een GEB. De GA vanuit een systeemverantwoordelijkheid, de FG vanuit zijn verantwoordelijkheid als wettelijke toezichthouder en adviseur. Desgevraagd geeft de FG advies over de GEB.

Iedere voorgenomen verwerking moet voldoen aan bovenstaande vereisten. Wanneer dat niet het geval is mag de verwerking (het project, de proeftuin, de pilot, de innovatie) niet starten. Alleen de verwerkingsverantwoordelijke kan besluiten dat deze toch mag starten zonder dat aan alle eisen is voldaan. Voorafgaand aan dit besluit vindt overleg plaats met de FG, GA en de CISO.

# 3. Rollen en verantwoordelijkheden

De korpsbrede taken, rollen en verantwoordelijkheden met betrekking tot privacy in de politie organisatie worden beschreven in het privacy beleid. In dit hoofdstuk worden specifieke rollen, taken en verantwoordelijkheden in relatie tot het verwerkingsregister en de GEB verder uitgewerkt.

## 5.1 De korpschef

De korpschef is als verwerkingsverantwoordelijke eindverantwoordelijk voor het wetsconform gebruik van persoonsgegevens.

Via een stelsel van mandaten en ondermandaten is deze verantwoordelijkheid gemandateerd. Iedere verwerking heeft daardoor altijd een verwerkingsverantwoordelijke namens de korpschef.

## 5.2 Landelijke portefeuillehouders

De portefeuilles zijn gericht op planvorming en monitoring van de uitvoering. De landelijke portefeuillehouder is verantwoordelijk voor de beleidsvorming op zijn portefeuille, en voorbereiding van besluitvorming inclusief impactanalyse op de eenheden en het PDC. Hierbij zorgt de portefeuillehouder er voor dat het beleid voldoet aan de eisen uit dit beleidskader.

### 5.2.1 Portefeuillehouder AVG

De portefeuillehouder AVG is verantwoordelijk voor de beleidsontwikkeling op het gebied van de AVG. Dat betreft verwerkingen inzake de bedrijfsvoering, vreemdelingenzaken en korpscheftaken. Hij ziet erop toe dat de voor de uitvoering verantwoordelijken (resp. directeur PDC, portefeuillehouder vreemdelingenzaken en portefeuillehouder korpscheftaken) zijn beleid implementeren met inachtneming van de verplichtingen uit dit beleidskader.

De portefeuillehouder is daarnaast eigenaar van de ondersteunende tool. Hij zorgt ervoor dat de organisatie gebruik kan maken van de tool voor het uitvoeren van de verplichtingen in dit beleidskader. Ook zorgt de portefeuillehouder voor technische en functionele ondersteuning bij het gebruik van de tool.

### 5.2.2 Portefeuillehouder Wpg

De portefeuillehouder Wpg is verantwoordelijk voor de beleidsontwikkeling op het gebied van de Wpg. Dat zijn verwerkingen in het kader van de politietaak, zoals genoemd in artikel 3 van de Politiewet 2012, uitgezonderd de korpschef-, vreemdelingen, - en burgemeesterstaken. Hij ziet erop toe dat de voor de uitvoering verantwoordelijken zijn beleid implementeren met inachtneming van de verplichtingen uit dit beleidskader.

## 5.3 Lijnmanagement

Het lijnmanagement is verantwoordelijk voor de implementatie en uitvoering van privacybeleid, waaronder dit beleidskader. Het lijnmanagement voor de operationele taakuitvoering bestaat uit de korpschef, eenheidschef, sectorhoofd (waaronder een districtschef) en teamchef (waaronder een basisteamchef). Voor de bedrijfsvoering zijn dit korpschef, directeur van het PDC, diensthoofd en afdelingshoofd. Het lijnmanagement besluit over de start van een verwerking, en is ervoor verantwoordelijk dat deze voldoet aan de verplichtingen uit dit beleidskader. Besluit het lijnmanagement te starten met een verwerking die niet voldoet, dan is daarover vóóraf overleg met de FG, GA en CISO.

## 5.4 FG

De FG houdt onafhankelijk toezicht op de toepassing en naleving van de verplichtingen in dit beleidskader. De FG rapporteert rechtstreeks aan de korpschef. Daarnaast heeft de FG een wettelijke adviesrol. De advisering aangaande de uitvoering van een GEB is door de FG belegd bij de privacyfunctionaris. Op grond van de Wpg heeft de privacyfunctionaris een zelfstandige adviseringsrol

## 5.5 Team informatiebeveiliging

Het team Informatiebeveiliging voert op verzoek van de verwerkingsverantwoordelijke een informatiebeveiligingsanalyse uit op voorgenomen verwerking en adviseert over te nemen beveiligingsmaatregelen.

## 5.6 Privacyfunctionarissen

De privacyfunctionarissen adviseren over de verplichtingen in dit beleidskader. Naast advisering hebben privacyfunctionarissen ook een toezichthoudende taak. Dat is een wettelijk omschreven taak voor wat betreft Wpg verwerkingen. Voor AVG verwerkingen is deze taak ontleend aan de bevoegdheden van de FG, dat geldt ook t.a.v. het verwerkingsregister.

## 5.7 Gegevensautoriteit

De GA is verantwoordelijk voor de ontwikkeling van privacybeleid. Vanuit een systeemverantwoordelijkheid monitort de GA de uitvoering van dit beleid.

## 5.8 Directie Operatiën

De directie en het PDC zijn gezamenlijk verantwoordelijk voor het bedrijfsreferentiemodel. De bedrijfsarchitect van deze directie toetst periodiek of de in het register opgevoerde verwerkingen leiden tot een wijziging in de werkprocessen. De bedrijfsarchitect van de Staf PDC doet het zelfde met betrekking tot de verwerkingen ten behoeve van de bedrijfsvoering.

## 5.9 Directeur PDC

De directeur van het PDC is verantwoordelijk voor de uitvoering van verwerkingen ten behoeve van de bedrijfsvoering. Een deel daarvan vindt plaats in de eenheden, maar altijd onder verantwoordelijkheid van het PDC.

## 5.10 De Centrale Ondernemingsraad

Instemming of advies van de COR is nodig voor het uitvoeren van verwerkingen van persoonsgegevens op bepaalde onderwerpen. Welke dit zijn staat in artikel 27 van de Wet op de ondernemingsraden. Periodiek bespreekt de GA dergelijke verwerkingen met de COR commissie AVG.

## 5.11 AP

De AP is de externe toezichthouder met de bijbehorende wettelijke toezicht bevoegdheden. Zo is de AP bevoegd tot inzage in het verwerkingsregister en kunnen zij documenten en informatie opvragen. De AP kan boetes en een last onder dwangsom opleggen. De AP moet voor de start van een verwerking worden geraadpleegd als daaraan risico's zijn verbonden die niet gemitigeerd kunnen worden.

# Bijlage 1

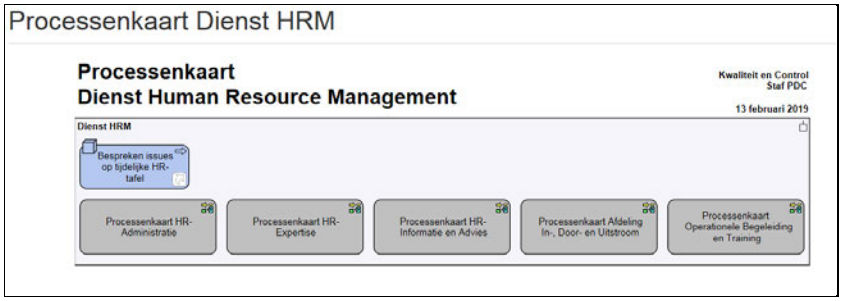
## Processen en werkstromen Bedrijfsvoering (AVG)

Hierin zijn beschreven de processenkaarten per dienst van het PDC, de integrale werkstromen én de werkstromen van de diensten. Op een processenkaart staan per organisatieonderdeel (afdeling, sector of team) de processen welke binnen dit organisatieonderdeel worden uitgevoerd. Van deze processen zijn een definitie, de beschrijving en de versie weergegeven.

Ten aanzien van de bedrijfsvoering is dit gelaagd ingericht:

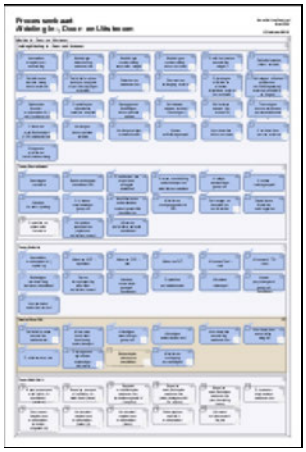
Hoofdniveau (PDC)


Sub niveau: Dienst HRM




Detail niveaus: Sector: HR-Administratie

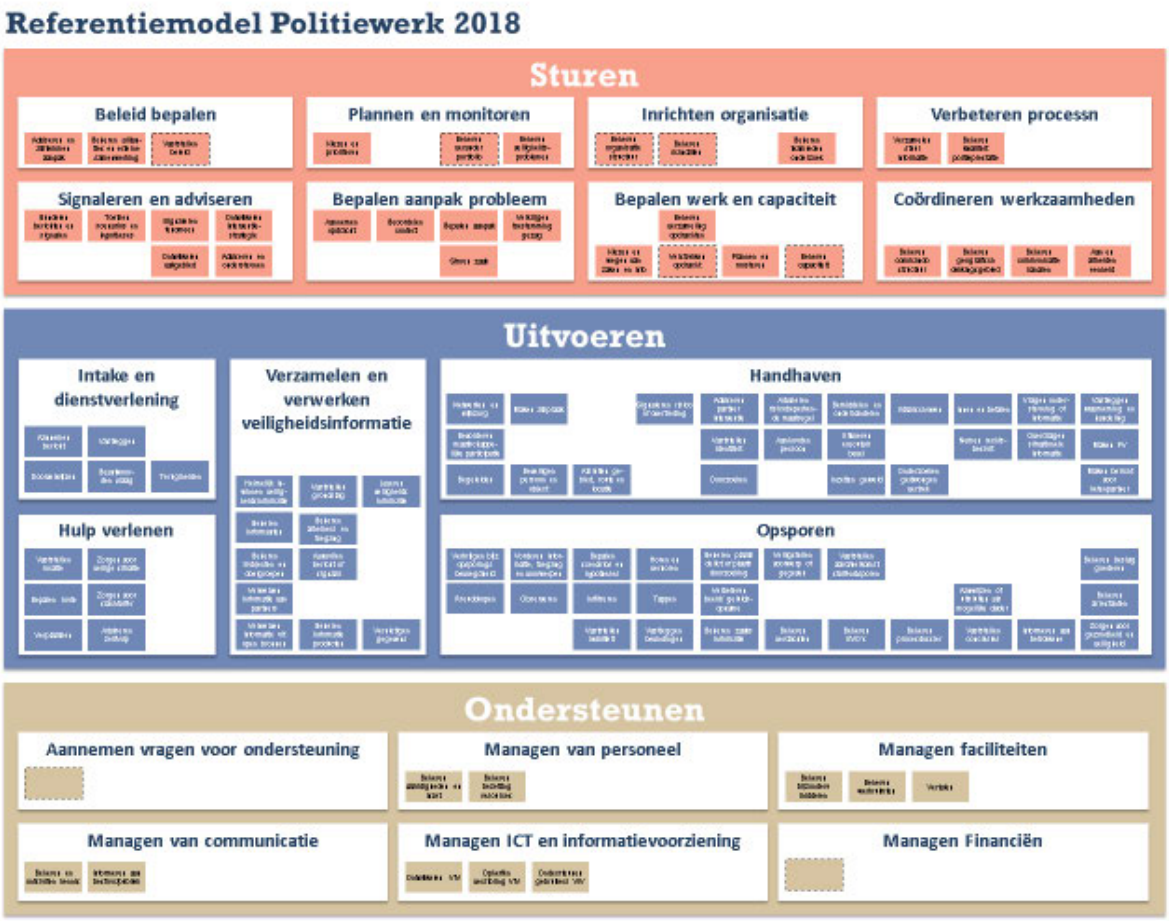
Sector In- Door en Uitstroom (IDU)



Bron: Staf PDC, Kwaliteit en Control, 13 februari 2019

- Relevante artikelen uit de AVG en de gewijzigde Wpg
- Het BRM 2018, inclusief de werkprocessen en de toelichting

# Bijlage 2


Referentiemodel Politiewerk 2018
Sturen
Beleid bepalen
Plannen en monitoren
Inrichten organisatie
Verbeteren processn
Signaleren en adviseren
Bepalen aanpak probleem
Bepalen werk en capaciteit
Coördineren werkzaamheden
Uitvoeren
Intake en dienstverlening
Verzamelen en verwerken veiligheidsinformatie
Handhaven
Hulp verlenen
Opsporen
Ondersteunen
Aannemen vragen voor ondersteuning
Managen van personeel
Managen faciliteiten
Managen van communicatie
Managen ICT en informatievoorziening
Managen Financiën