

Praktijkhandboek Wet politiegegevens voor boa's

Goed omgaan met persoonsgegevens



Geactualiseerd,
en met nieuwe
voorbeelden,
februari
2025

Suzanne Franken

Inhoud

Voorwoord	3
Inleiding	6
Hoofdstuk 1 Begrippen	9
Hoofdstuk 2 De Wpg-verwerkingsgrondslagen	14
Hoofdstuk 3 Samenwerken en verstrekken	19
Hoofdstuk 4 Rollen en functionarissen	25
Hoofdstuk 5 Aanpassingen in de werkprocessen en systemen	30
Hoofdstuk 6 De rechten van betrokkenen	34
Hoofdstuk 7 Praktijkvoorbeelden	37
Hoofdstuk 8 Stand van zaken wetgeving en bijbehorende afkortingen	47
Hoofdstuk 9 Ter afsluiting	51
Bijlage A Vuistregels	55
Bijlage B Afkortingenlijst	57
Bijlage C Modelverklaring autorisatie niet-boa	58
Bijlage D Stroomschema verstrekken of ter beschikking stellen	60
Bijlage E Instructie scheidingslijn artikel 8- en 9-verwerking	61
Bijlage F Wet politiegegevens voor boa's	65



Het auteursrecht op dit werk ligt bij Suzanne Franken en is beschermd via een Creative Commons licentie. In hoofdstuk 9 wordt dit nader toegelicht. Neem voor eigen gebruik of voor een gedrukt exemplaar contact op met de auteur via suzanne@sfranken.nl. Deze versie is geactualiseerd in februari 2025.

Voorwoord

Dit praktijkhandboek helpt de buitengewoon opsporingsambtenaar (boa) om correct om te gaan met gegevens die hij verwerkt in het kader van zijn opsporingstaak. Boa's zijn vaak ook toezichthouder. Als in dit boek over boa wordt gesproken, dan gaat het over de uitvoering van de opsporingstaak. Tot 2018 verwerkten boa's alle persoonsgegevens onder het regime van de Wet bescherming persoonsgegevens (Wbp). Tegenwoordig geldt voor toezicht de Algemene Verordening Gegevensbescherming (AVG) en voor opsporing de Wet politiegegevens (Wpg). Als een boa een persoonsgegeven voor toezicht verwerkt en daarna gebruikt voor opsporing, verandert dat gegeven van een persoonsgegeven in een politiegegeven. Daardoor is het van belang dat een boa bekend is met de Wpg. Dit handboek is bedoeld als kennismaking met die wet. Het is zowel bestemd voor de boa als voor beleidsmedewerkers, leidinggevendenden, (privacy)adviseurs en auditors. In de leeswijzer wordt beschreven welk hoofdstuk voor wie het meest relevant is.

Boa's en hun werkgevers moeten zich in de Wpg verdiepen om hun gegevensverwerking rechtmatig uit te kunnen voeren. Er zijn veel verschillende soorten boa's werkzaam bij zowel publieke als private organisaties. Als het gaat om de AVG, dan kun je daar voldoende publicaties en websites over vinden (zie deze handige [kaart](#) van de Autoriteit Persoonsgegevens). Over de Wpg echter niet; daarom dit handboek! Onderstaande voorbeelden maken duidelijk welke soorten gegevens onder welk regime verwerkt dienen te worden:

- Salarisadministratie en andere personeelsgegevens: **AVG**
- Persoonsgegevens over toezicht en bestuursrechtelijke handhaving, zoals bestuurlijke boetes: **AVG**
- Persoonsgegevens over opsporing en vervolging van strafbare feiten: **Wpg**

Disclaimer

Dit handboek is bedoeld als een kennismaking met de Wet politiegegevens, specifiek voor buitengewoon opsporingsambtenaren. In de tekst zijn de consequenties van het Besluit politiegegevens buitengewoon opsporingsambtenaren (**Bpg boa**) verwerkt. De tekst wordt vrijwel jaarlijks geactualiseerd. Er kunnen geen rechten worden ontleend aan de teksten of afbeeldingen. Mocht je onvolkomenheden vinden of andere aanvullingen hebben, neem dan contact op met suzanne@sfranken.nl.

Dit handboek bestaat alleen in digitale vorm, aangezien het jaarlijks wordt geüpdatet. Het is nadrukkelijk ontworpen om op een e-reader of scherm te lezen en niet om te drukken. Denk daaraan voordat je op de print-knop drukt.



Leeswijzer

Zoals in het voorwoord beschreven, is dit boek zowel bestemd voor de boa als voor administratief personeel, beleidsmedewerkers, leidinggevendenden, (privacy)adviseurs en auditors. Voor de boa is hoofdstuk 5 en een groot deel van hoofdstuk 4 minder relevant.

De **inleiding** geeft contextinformatie: wat is de stand van zaken in Europa en in Nederland op het gebied van privacywetgeving, wat is de Wet politiegegevens (Wpg) en waarom is deze wet relevant voor boa's? In **hoofdstuk 1** worden begrippen toegelicht die belangrijk zijn bij privacywetgeving. **Hoofdstuk 2** gaat over de Wpg-verwerkingsgrondslagen: hier worden de verschillende soorten gegevens toegelicht die binnen de Wpg onderscheiden worden. **Hoofdstuk 3** behandelt diverse manieren van gegevensuitwisseling. **Hoofdstuk 4** beschrijft welke instanties en functionarissen de Wpg onderkent. Dit sluit aan bij **hoofdstuk 5**, waarin op hoofdlijnen beschreven wordt wat er moet worden aangepast in de werkprocessen en de systemen.

Hoofdstuk 6 beschrijft welke rechten de burger heeft en wat dit betekent voor de interne organisatie en in **hoofdstuk 7** worden praktijkvoorbeelden uitgewerkt. Als je denkt dat de Wpg niet over jónw werk gaat, lees dan in elk geval dit hoofdstuk. **Hoofdstuk 8** bevat een beschrijving van de wettelijke kaders. **Hoofdstuk 9** bevat verwijzingen naar een aantal handige producten en hulpmiddelen en informatie over de auteur. Tot slot is in de bijlagen een aantal van deze handige hulpmiddelen opgenomen, evenals de wettekst zoals deze geldt voor de boa.

Inleiding

Privacywetgeving in Europa

In 2018 is de Wet bescherming persoonsgegevens (Wbp) vervangen door de Algemene verordening gegevensbescherming (AVG). De AVG geldt echter niet voor gegevens die worden verwerkt voor de opsporing of vervolging van strafbare feiten. Voor dat soort gegevens geldt de Europese Richtlijn gegevensverwerking opsporing en vervolging. Iedere lidstaat moet deze Richtlijn vertalen in eigen, nationale wetgeving. In Nederland is daarom de Wet politiegegevens (Wpg) geschreven. Zo kunnen politie en marechaussee aan deze Richtlijn voldoen. Een andere verandering is dat de Wpg nu ook voor de buitengewoon opsporingsambtenaar geldt, zowel voor de boa werkzaam in de publieke als private sector. Daartoe is op 9 maart 2019 het Besluit politiegegevens voor boa's (Bpg boa) in werking getreden (zie [Staatsblad 2019, 85](#)). De achterliggende reden dat de boa tegenwoordig onder de Wpg werkt, is dat het werkproces lijkt op dat van de politie en het daarom logisch is dat de regels voor gegevensbescherming hetzelfde zijn.

De Wpg, niet alleen voor de politie

Boa's stellen zich steeds meer op als netwerk- en strafrechterketenpartner. Ze moeten wel, want zij zijn samen met de politie en andere organisaties verantwoordelijk voor een veilig en leefbaar Nederland. Daarom is het begrijpelijk dat de gegevensverwerking van de boa, net als die van de politie, onder de Wpg valt. De Wpg geldt sinds 2008 al voor de politie, de marechaussee en de rijksrecherche. En sinds 2009 ook voor de bijzondere opsporingsdiensten, zoals de FIOD. Sinds 2019 is de buitengewoon opsporingsambtenaar met het Bpg boa aan dat lijstje toegevoegd.

Twee regimes voor de boa: de AVG en Wpg

Boa's hebben vaak meerdere taken en verwerken verschillende soorten gegevens. Gegevens die een boa verwerkt in zijn rol als toezichthouder of incidentbestrijder, vallen onder de AVG. De gegevens die de boa als opsporingsambtenaar verwerkt, vallen onder de Wpg. Hij heeft dus een 'twee-petten-uitdaging'. Voor gegevens die hij onder de Wpg verwerkt, gelden andere verwerkingstermijnen en andere regels voor het delen van gegevens. Ook zijn er andere regels over bijvoorbeeld logging en auditing. De gegevenshuishouding, systemen en werkprocessen moeten dus anders worden ingericht dan bij de verwerkingen die in het kader van toezicht worden gedaan.

In ieder boa-domein gelden - vaak landelijke - regels en werkafspraken over wanneer de boa van pet moet wisselen. Voor de sociale recherche (domein 5) geldt bijvoorbeeld dat een vermoed fraudebedrag boven vijftigduizend euro strafrechtelijk wordt onderzocht en afgehandeld. Deze richtlijn bepaalt in dit geval dan de knip wanneer gegevens onder de Wpg vallen.

Leerplichtambtenaren (domein 3) werken volgens de [Methodische Aanpak Schoolverzuim \(MAS\)](#). Deze is ontwikkeld door een aantal instanties en de landelijke vereniging voor leerplichtambtenaren (Ingrado) om schooluitval te voorkomen. Per soort verzuim is in de MAS vastgelegd wanneer er proces-verbaal moet worden opgemaakt. En daarmee ligt dus vast wanneer de overstap van AVG naar Wpg plaatsvindt.

Ook voor domein twee gelden werkafspraken die bepalen wanneer een boa strafrechtelijk optreedt. Deze zijn vastgelegd [Landelijke Handhavingsstrategie Omgevingsrecht](#) (LHSO).

Tot slot geldt dat gemeenten deels keuzevrijheid hebben of ze bepaalde overtredingen strafrechtelijk of bestuursrechtelijk afdoen. Dit is bepaald in het [Besluit bestuurlijke boete overlast in de openbare ruimte](#). Let dus op als een gemeente daar gebruik van maakt. Een overtreding als het verkeerd aanbieden van afval kan daar met een bestuurlijke boete worden afgedaan en zo onder de AVG vallen, terwijl ditzelfde feit bij de meeste gemeenten strafrechtelijk wordt afgedaan en de gegevensverwerking daar dus onder de Wpg valt.



Begrippen

Hoofdstuk 1

Begrippen

Ben je onbekend met privacywetgeving? Dan is het van belang in elk geval de begrippen in dit hoofdstuk door te nemen. In de bijlage is een afkortingenlijst opgenomen en in hoofdstuk 8 wordt een aantal wetten en begrippen toegelicht, vooral bedoeld als achtergrondinformatie.

Persoonsgegevens

Elk gegeven betreffende een identificeerbaar of geïdentificeerde natuurlijke persoon. Het gaat dus om alles dat in verband kan worden gebracht met een natuurlijke persoon: naam, foto, telefoonnummer, personeelsnummer, maar ook een bankrekeningnummer, gps-positie of kenteken. Audio- en video-opnames zijn ook persoonsgegevens. Belangrijk is dat de persoon nog niet geïdentificeerd hoeft te zijn: het is al een persoonsgegeven als het tot identificatie kán leiden.

Politiegegevens

Een persoonsgegeven dat verwerkt wordt in het kader van de opsporingstaak. Hiervoor geldt de Wet politiegegevens. Een politiegegeven is een specifieke versie van een persoonsgegeven.

Betrokkene

De persoon op wie een persoonsgegeven of politiegegeven betrekking heeft. Elke betrokkene heeft een aantal rechten, bijvoorbeeld om de gegevens in te zien die over hem zijn vastgelegd.

Bijzonder persoonsgegevens

Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijkt. Ook genetische en biometrische gegevens en gegevens over gezondheid, seksueel gedrag of seksuele gerichtheid zijn bijzondere persoonsgegevens. Het is verboden bijzondere persoonsgegevens te verwerken, tenzij dit onvermijdelijk is voor het doel van de verwerking en in aanvulling op de verwerking van andere politiegegevens. Wees dus ook terughoudend bij het gebruik van beeldmateriaal. Een foto van een persoon bevat mogelijk informatie over zijn ras en wellicht zijn er meer bijzondere gegevens uit af te leiden, zoals de religie op basis van de gedragen kleding.

Verwerken

Elke handeling met een persoons- of politiegegevens. Dus onder andere opschrijven, registreren, vastleggen, filmen, opnemen, raadplegen, vergelijken, wijzigen, tonen, verstrekken en zelfs wissen van persoonsgegevens zijn allemaal vormen van verwerken.

Verwerkingsgrondslag

De basis waarop persoons- of politiegegevens worden verwerkt. Er zijn verschillende grondslagen voor de verwerking met ieder eigen voorwaarden. Zo kennen artikel 8-gegevens een andere verwerkingstermijn dan artikel 9-gegevens. De verwerkingsgrondslagen zijn opgenomen in paragraaf 2 van de Wpg. De AVG kent zes geheel andere **verwerkingsgrondslagen**.

Verwerkingstermijn

De termijn waarbinnen politiegegevens verwerkt mogen worden. Artikel 8-gegevens hebben een andere verwerkingstermijn dan artikel 9-gegevens. De Wpg kent ook een bewaartermijn; deze volgt op de verwerkingstermijn. In die bewaartermijn zijn gegevens buiten de operationele omgeving geplaatst, maar nog niet fysiek vernietigd.

Ter beschikking stellen

Het delen van politiegegevens binnen het Wpg-domein. Dit is beschreven in artikel 15 van de Wpg. Een synoniem hiervoor is 'free flow of information': in principe dienen politiegegevens gedeeld te worden met ieder die de gegevens nodig heeft voor zijn de uitoefening van zijn taak. Bij dit 'need to know'-principe hoort altijd een noodzakelijkheids-, proportionaliteits- en subsidiariteitsafweging te worden gemaakt. Bijvoorbeeld als een boa van ProRail of Rijkswaterstaat toegang wil tot gegevens van een gemeentelijke boa, moet hij zorgvuldig afwegen of de ProRail-collega deze daadwerkelijk nodig heeft voor zijn werk.

Verstrekken

Het delen van politiegegevens buiten het Wpg-domein. Denk aan Bureau Halt, de burgemeester, Belastingdienst of het Centraal Justitieel Incassobureau. Ook in een samenwerkingsverband kan, onder voorwaarden, verstrekt worden aan partners, zoals een woningbouwvereniging of winkeliers. Elke verstrekking moet worden vastgelegd, zie artikel 32, lid 1 onder b.

Geheimhoudingsplicht

Iedereen die over politiegegevens beschikt, is verplicht tot geheimhouding. Dit geldt zowel voor gegevens die jij hebt verwerkt als gegevens van collega's waar jij toegang toe hebt. De uitzonderingen op deze geheimhoudingsplicht staan beschreven in paragraaf 3 van de Wpg: de verstrekkingen. Als gegevens verstrekt worden, reist de geheimhoudingsplicht mee. Ze vallen na verstrekking vaak onder de AVG. De ontvanger mag de gegevens alleen verwerken voor het doel waarvoor hij ze verkregen heeft en verder geldt nog steeds de geheimhoudingsplicht.

Boa-domein

Elke boa is ingedeeld in één van de zes domeinen:

1. Openbare Ruimte,
2. Milieu, welzijn en infrastructuur,
3. Onderwijs,
4. Openbaar vervoer,
5. Werk, inkomen en zorg,
6. Generieke opsporing.

Elk domein bevat een opsomming van wetten en wetsartikelen. In tegenstelling tot een algemeen opsporingsambtenaar van de politie heeft een boa opsporingsbevoegdheid voor één of meer wetten en wetsartikelen.

Wpg-domein

Alle personen en instanties die gegevens verwerken volgens het regime van de Wpg. In eerste instantie zijn dit de politie, de marechaussee en de rijksrecherche. Sinds 2009 vallen ook de BOD'en onder het Wpg-domein en met de inwerkingtreding van het Bpg boa in 2019 ook de boa, voor zover hij opsporingsgegevens verwerkt.

Proportionaliteit, noodzakelijkheid en subsidiariteit:

Voor alles wat je met (persoons)gegevens doet, geldt dat je moet beoordelen of:

- de verwerking in verhouding staat tot het doel dat je hebt (proportionaliteit);
- alle gegevens daadwerkelijk noodzakelijk zijn (noodzakelijkheid);
- je het doel kunt bereiken op een manier die minder inbreuk maakt op de privacy van betrokkenen (subsidiariteit).

Als je bijvoorbeeld camera's wilt inzetten om een dader van kippenvergiftiging op te sporen, dien je je af te vragen of je er al alles aan gedaan hebt om zonder die camera's de dader te vinden.



De Wpg- verwerkingsgrondslagen

Hoofdstuk 2

De Wpg-verwerkingsgrondslagen

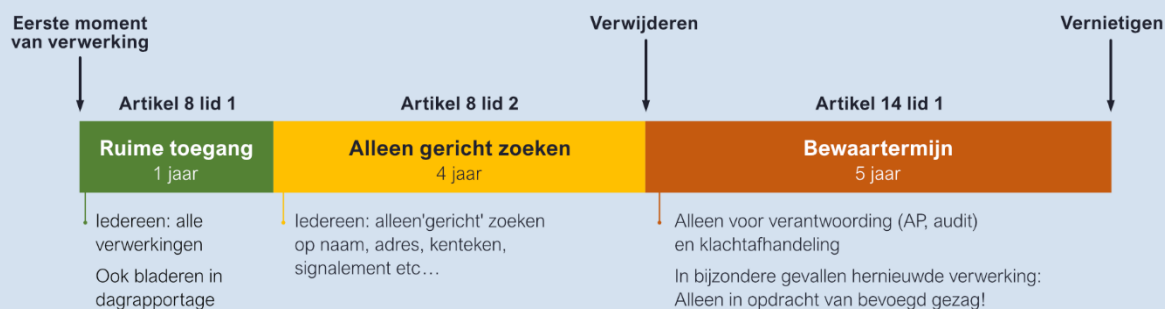
De Wpg onderscheidt verschillende grondslagen waarvoor politiegegevens mogen worden verwerkt. Deze staan in de artikelen 8, 9, 10, 12 en 13. Het Bpg boa beschrijft in artikel 2 dat voor de boa alleen artikel 8, 9 en 13-verwerkingen van toepassing kunnen zijn. Afhankelijk van de grondslag gelden er andere voorwaarden, bijvoorbeeld voor de verwerkings-termijn en toegang voor andere opsporingsambtenaren. Het merendeel van de verwerkingen van een boa valt onder artikel 8.

Artikel 8: Dagelijkse politietaak

Persoonsgegevens die verwerkt worden in het kader van de dagelijkse opsporingstaak, vallen onder artikel 8 van de Wpg. Dit gaat over zaken als wildplassen, foutief aanbieden van afval, alcohol gebruiken op de openbare weg en loslopende honden. Ook proces-verbaal opmaken bij onrechtmatig afgeschoten wild of tuinafvaldump valt hieronder. De gegevens kunnen zowel over verdachten, slachtoffers als andere betrokkenen gaan. Artikel 8-gegevens mogen tot vijf jaar na de eerste verwerkingsdatum met een gerichte zoekvraag worden geraadpleegd en verwerkt. Bijvoorbeeld door te zoeken op een naam, adres of kenteken. Daarna worden ze vijf jaar bewaard (bewaartermijn) en daarna dienen ze te worden vernietigd.

Gedurende de bewaartermijn kunnen de gegevens gebruikt worden voor het afhandelen van klachten en voor audits of een controle door de Autoriteit Persoonsgegevens. Verder geldt dat deze gegevens onder bepaalde omstandigheden ter beschikking kunnen worden gesteld voor hernieuwde verwerking. Ze komen dan als het ware opnieuw tot leven in een actueel opsporingsonderzoek. Gegevens in

de bewaartermijn mogen ook verwerkt worden voor wetenschappelijk onderzoek en statistiek.



Figuur 1: Termijnen artikel 8 gegevens

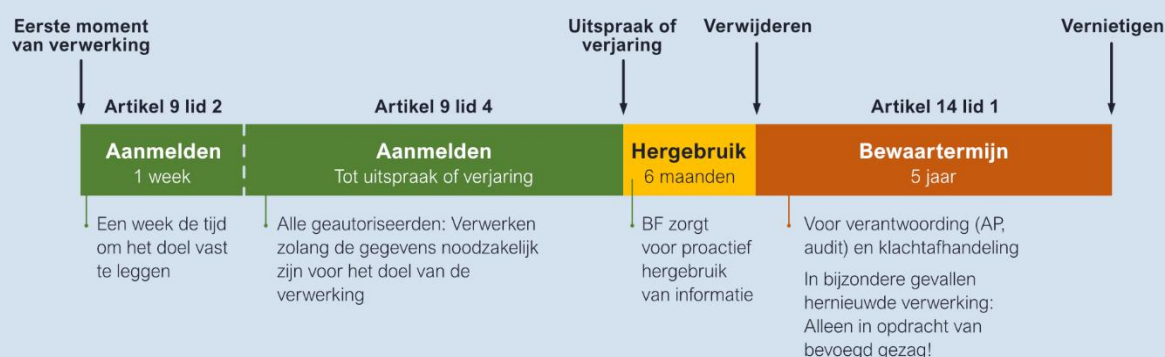
Artikel 9: Opsporingsonderzoek met meer inbreuk

Dit artikel maakt het mogelijk om gegevens te verwerken die specifiek gericht zijn op bepaalde personen of concrete gebeurtenissen. De inbreuk op de privacy is bij deze verwerkingen groter dan bij artikel 8. Het gaat hier bijvoorbeeld om onderzoeken waarbij bijzondere opsporingsbevoegdheden worden ingezet, zoals het plaatsen van een baken onder een auto bij verdenking van stroperij of stelselmatige observatie bij verdenking van een milieudelict. Ook een gericht onderzoek naar het vergiftigen van vossen of dumping van asbest kan onder artikel 9 vallen, bijvoorbeeld als je verwacht dat het onderzoek langer dan veertig uur duurt of als er meerdere opsporingsambtenaren bij betrokken zijn.

Artikel 9-gegevens mogen worden verwerkt tot het doel bereikt is; dat weet je dus niet van tevoren. In de praktijk kun je zeggen: tot er een onherroepelijk vonnis is of tot de verjaringstermijn bereikt is. Daarom moet binnen een week het doel van de verwerking worden aangemeld op een door de boa-werkgever bepaalde werkwijze.

Is het doel bereikt, dan heeft de bevoegd functionaris (BF) nog zes maanden de tijd om informatie uit het onderzoek aan te bieden aan collega's die deze kunnen hergebruiken voor hun eigen onderzoek. Daarna worden ze vijf jaar bewaard en daarna dienen ze te worden vernietigd. Gedurende de bewaartermijn kunnen de gegevens voor dezelfde doeleinden worden gebruikt als de bewaarde gegevens uit artikel 8.

In de bijlage vind je de Instructie scheidingslijn artikel 8- en 9-verwerking. Deze geeft verdere uitleg wanneer je van 8 overgaat in 9.



Figuur 2: Termijnen artikel 9 gegevens

Artikel 13: Ter ondersteuning van het werk

Dit artikel biedt de mogelijkheid om gegevens die oorspronkelijk zijn verwerkt op basis van artikel 8 of 9, vaak landelijk, verder te verwerken. De verwerkingsverantwoordelijke kan zelf een artikel 13-verwerking starten, nadat hij een bijbehorend artikel 13-protocol heeft opgesteld. De gegevens die onder artikel 13 verwerkt worden, komen voort uit artikel 8- of 9-verwerkingen. Bepaalde gegevens kunnen tegelijkertijd onder artikel 13 als onder 8 of 9 verwerkt worden.

Vooralsnog zijn er geen artikel 13-verwerkingen voor boa's bekend. Het kan bijvoorbeeld gaan om het raadplegen van pv's, boetes, overtredingen van gebiedsverboden of gevarenclassificaties (welke burger is wapen dragend of heeft een gevaarlijke hond?) voor alle opsporingsambtenaren in Nederland. Een goed voorbeeld is het

landelijk delen van informatie over strafbare feiten in verband met hondenbijtincidenten en de muilkorfplicht. Zowel de politie als gemeenten hebben hier een taak in. Indien er een aanlijnplicht geldt of indien er incidenten geweest zijn met een hond, is het relevant om te weten wat zich in een andere gemeente of politie-eenheid heeft voorgedaan. Dit is nodig voor zowel de veiligheid van de opsporingsambtenaar als voor het bepalen van de strafmaat, en mogelijk ook voor een juiste identificatie van de hond en zijn baasje.

Een ander voorbeeld voor een artikel 13-verwerking voor boa's is een register met 'graffiti-tags'. De schade die vervoerders als NS en ProRail lijden als gevolg van graffiti, is enorm. Als zij onderling – en eventueel ook met de politie – de tags of handtekeningen van de plegers met elkaar zouden delen, zou dat in een artikel 13-verwerking kunnen. Dan zouden alle partijen die belast zijn met dergelijke opsporing, toegang kunnen krijgen tot dit register. De diverse verwerkingsverantwoordelijken dienen dit dan onderling met elkaar te organiseren. Zowel het opstellen van het register zelf, als de regels hoe met de gegevens wordt omgegaan: het artikel 13-protocol. Hierin staat wie toegang heeft tot dit register, welke gegevens erin staan en hoe lang ze verwerkt worden.

De nota van toelichting op het Bpg boa geeft aan dat dit artikel met name relevant is voor grote inspectiediensten met een landelijke organisatiestructuur, zoals de Inspectie SZW (Sociale Zaken en Werkgelegenheid) en de ILT (Inspectie Leefomgeving en Transport).

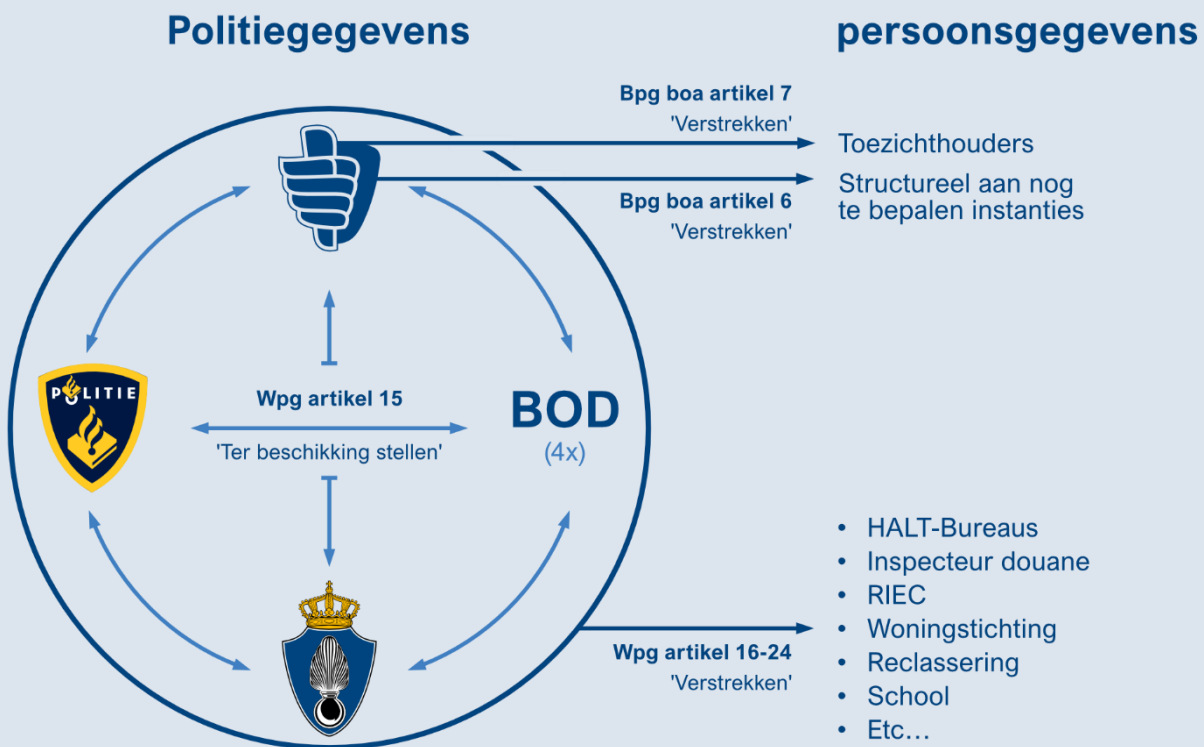
The background is a solid dark blue. On the right side, there is a large, stylized, light blue letter 'S' that is partially cut off by the edge. A horizontal band of a lighter blue checkered pattern runs across the middle of the image, passing behind the text.

Samenwerken
en verstrekken

Hoofdstuk 3

Samenwerken en verstrekken

Er bestaan verschillende mogelijkheden om samen te werken en gegevens uit te wisselen binnen het veiligheidsdomein. De belangrijkste vraag is of de gegevens die verstrekt worden, oorspronkelijk onder de AVG of Wpg verwerkt werden en naar welk domein ze nu toegaan: AVG of Wpg. Verstrekken vanuit AVG naar Wpg (of AVG-AVG) blijft hier buiten beschouwing. Van Wpg naar AVG en van Wpg naar Wpg wordt in onderstaand schema en de rest van dit hoofdstuk toegelicht.



Figuur 3: Ter beschikking stellen voor delen binnen het Wpg-domein, verstrekken voor naar buiten.

Delen in het Wpg-domein: ter beschikking stellen

Als je gegevens deelt binnen het Wpg-domein, heet dat ter beschikking stellen van gegevens. Politiegegevens moeten gedeeld worden met ieder – boa én politie – die deze gegevens nodig heeft voor zijn werk. Kortom: ‘free flow of information’. Daarbij geldt altijd het ‘need-to-know-principe’: de ontvanger moet de gegevens nodig hebben voor zijn taak. De strekking van de wet is dat het breed delen van gegevens de kwaliteit van het werk verbetert. Je weet dan bijvoorbeeld wie bezig is op hetzelfde terrein en welke antecedenten iemand heeft. Zo kun je iemand op de juiste wijze bejegenen, zowel voor jouw eigen veiligheid als om de passende strafmaat te bepalen.

Zowel jouw werkgever als de wetgever vertrouwen op jouw integriteit en professionaliteit: dat je toegang hebt tot gegevens wil niet zeggen dat je ze allemaal mag raadplegen. Daarnaast geldt in de Wpg de plicht tot logging. Dat betekent dat al jouw handelingen worden vastgelegd. Achteraf kan dus gecontroleerd worden of jouw gegevensverwerkingen rechtmatig zijn geweest en nodig zijn geweest voor jouw werk.

Het Bpg (art. 2:13) beschrijft in welke gevallen het ter beschikking stellen geweigerd kan worden. Bijvoorbeeld als er gevaar voor leven of gezondheid van betrokkene is te duchten. De meeste weigeringsgronden zullen voor de boa niet spelen, bijvoorbeeld als het gaat om gegevens over politie-informanten of gegevens verwerkt onder artikel 10 Wpg. Wat wel kan gebeuren, is dat een andere boa, of de politie, contact met je opneemt over een mutatie en dat je bijvoorbeeld eerst nog een getuigenverhoor of zoeking moet verrichten voordat gegevens door een ander gebruikt kunnen worden. Dit is geen weigering van ter beschikking stellen maar eerder het onderling afstemmen welke gegevens wanneer door wie gebruikt kunnen worden.

Samenwerking met politie

Er zijn verschillende manieren waarop boa's en de politie gegevens met elkaar delen. We beschrijven er hier drie: 1) het opvragen van informatie via de meldkamer, de C2000-portofoon of het RTIC, 2)

samen met de politie op pad gaan en 3) het bijwonen van een briefing van de politie. Voor alle situaties geldt free flow of information: zowel de politie als de boa moet gegevens met de ander delen als diegene dat nodig heeft voor zijn werk.

Opvragen van informatie via de meldkamer, de C-2000-portofoon of het RTIC

De politie beschikt over een grote hoeveelheid bronsystemen zoals RDW en BRP. Zo kan een kenteken worden nagetrokken en de identiteit van een burger worden vastgesteld. Het is niet de taak van de politie deze gegevens te delen met andere partijen. Veel boa-werkgevers beschikken eveneens over deze bronnen. Sinds **december 2020** is geregeld dat ook particuliere boa-organisaties over de BRP kunnen beschikken. Dit is nog niet overal in praktijk gebracht en andere bronnen zoals RDW, zijn nog niet voor deze boa's beschikbaar.

Als een boa door de politie vastgelegde gegevens nodig heeft voor zijn werk, kan hij deze opvragen bij de meldkamer, via de C-2000-portofoon of het RTIC, afhankelijk van de lokale afspraken. Het gaat dan vooral om gevaarsindicaties en antecedentgegevens die relevant zijn voor de veiligheid van de boa of om een zaak goed af te handelen, bijvoorbeeld als er sprake is van recidive. Deze gegevens dienen gedeeld te worden. Als je als boa 's nachts bijvoorbeeld een auto in het bos ziet staan en je twijfelt om erop af te stappen, neem dan vooral contact op met de politie. Die dient alle informatie te geven zodat jij veilig en goed jouw werk kunt doen. Tref je een politiemedewerker aan die nog niet weet dat de boa ook onder de werking van de Wpg valt, wijs deze dan op artikel 15 Wpg en het Bpg boa.

Altijd geldt dat er een noodzakelijkheids-, subsidiariteit- en proportionaliteitsafweging gemaakt dient te worden. Dit betekent dat je uit moet kunnen leggen wat je nodig hebt en waar je mee bezig bent. De opsporingsambtenaar die op het punt staat gegevens met jou te delen kan dan inschatten of het nodig is dat jij weet of iemand bijvoorbeeld een geweldpleger, drugsgebruiker of vuurwapengevaarlijk persoon is.

Samen op pad

Boa's werken veel samen met de politie. Bijvoorbeeld bij controles op naleving van de Alcoholwet in de grote steden, controles op afvaldumpingen in het buitengebied, naleving van de scheepvaartwet, en milieuwetgeving in industriële omgevingen. Soms is de boa daar als toezichthouder en neemt de politie het over als er sprake is van een strafbaar feit. In zo'n geval legt de boa zijn gegevens dus niet vast onder de Wpg maar onder de AVG (toezicht), bij voorkeur in een ander systeem als waarin hij zijn opsporingsgegevens verwerkt. Treedt de boa op als opsporingsambtenaar, dan dient hij de gegevens onder de Wpg te verwerken. Vaak muteren politie en boa dan in hun eigen systeem. Een voordeel van samen optrekken is dat noodzakelijke gegevens direct gedeeld kunnen worden. Deze gegevensuitwisseling is een vorm van ter beschikking stellen (artikel 15).

Informatie via een briefing van de politie

Ook het bijwonen van een (deel van een) briefing bij de politie is een vorm van ter beschikking stellen. De plicht tot delen wordt alleen nageleefd na een zorgvuldige noodzakelijkheids-, subsidiariteit- en proportionaliteitsafweging. Deze dient te worden uitgevoerd door de chef die de briefing verzorgt; alleen hij kan bepalen welke gegevens in relatie tot de taak van de boa, noodzakelijk zijn om te delen. Deze free-flow-situatie is nieuw sinds 2019. Voor die tijd mocht een boa alleen een politiebriefing bijwonen als de boa en politie dit met een convenant (artikel 20-samenwerkingsverband) geregeld hadden.

Verstrekken aan partners buiten het Wpg-domein

In de Wpg is vastgelegd aan welke partijen buiten het Wpg-domein je gegevens mag verstrekken. Voor elke verstrekking geldt dat deze moet worden geadministreerd. Als een betrokkene om inzage vraagt, moet hij namelijk kunnen zien met wie zijn gegevens zijn gedeeld. In de Verstrekkingenwijzer voor boa's is in opdracht van de gebruikers van het systeem BRS uitgewerkt aan wie verstrekt mag worden en wat de voorwaarden zijn. Deze wijzer geldt voor alle boa's in Nederland, in alle zes boa-domeinen. Daarom zul je wat betreft jouw werkzaamheden slechts een deel herkennen. Wil je meer weten over verstrekken, lees dan het Naslagwerk Verstrekken. Hierin zijn alle regels en begrippen

rondom verstrekken verder uitgewerkt met praktijkvoorbeelden. Beide documenten zijn te vinden op de [informatiepagina van BRS](#).

In het Bpg boa zijn twee mogelijkheden beschreven om te verstrekken die voor de politie niet gelden. Artikel 6 en 7 van het Bpg boa spreken over het verstrekken van opsporingsgegevens die een boa zelf heeft verzameld. Artikel 6 biedt de mogelijkheid om – als boa-werkgever – structureel verstrekken mogelijk te maken aan een instantie, voor zover deze niet in artikel 18 is opgenomen. De officier van justitie moet met de verstrekking akkoord gaan, er moet een zwaarwegend algemeen belang zijn en er moet een publicatie over in de Staatscourant komen.

Artikel 7 biedt de optie om opsporingsgegevens te verstrekken voor de toezichtstaak, voor zover het toezicht binnen hetzelfde boa-werkveld plaatsvindt. Dit artikel is zowel van toepassing als een boa gegevens wil delen met een partner, als wanneer hij zélf zijn opsporingspet inwisselt voor de toezichtspet. Met de komst van de [beleidsregels](#) van het Openbaar Ministerie van september 2024 is het eenvoudiger geworden om artikel 8-gegevens te verstrekken aan de toezichthouder. Er is namelijk geen toestemming meer nodig van de officier van justitie.



Rollen en functionarissen

Hoofdstuk 4

Rollen en functionarissen

In de AVG en de Wpg passeren verschillende functionarissen de revue. Dit hoofdstuk behandelt de belangrijkste functionarissen en instanties en beschrijft wie wat doet. Het is goed om dit te weten, voordat je leest wat er moet worden aangepast in de werkprocessen en automatisering. Dit hoofdstuk is vooral bedoeld voor beleids- en privacyadviseurs, voor leidinggevend en voor auditors.

Autoriteit persoonsgegevens (AP)

Dit is de autoriteit die in Nederland toezicht houdt op een juiste naleving van privacywetgeving in Nederland. Datalekken moeten bij de AP worden gemeld en betrokkenen kunnen een klacht indienen over een verwerking van hun gegevens waar ze het niet mee eens zijn. De AP kan zowel een boete als last onder dwangsom opleggen, zowel aan private instellingen als aan de overheid. In de Staatscourant van 14 maart 2019 (nr. 14586) is beschreven welk boetebeleid de AP hanteert, zowel voor de Wpg als de AVG: hoever kunnen de boetes oplopen en welke factoren bepalen mede het boetebedrag?

Functionaris gegevensbescherming (FG)

De functionaris voor de gegevensbescherming (FG) is een onafhankelijke functionaris die toezicht houdt op naleving van de AVG en de Wpg. De FG wordt door de verwerkingsverantwoordelijke aangewezen en wordt betrokken bij alle aangelegenheden die gaan over de bescherming van persoonsgegevens. De FG wordt op grond van haar of zijn professionele kwaliteiten en deskundigheid op het gebied van de wetgeving gekozen en is het eerste aanspreekpunt voor de AP.

Overheden zijn verplicht een FG aan te stellen en een grote organisatie als de politie heeft er meerdere. Ook de werkgever van de boa is verplicht een FG aan te stellen. Gezien de grote variatie aan boa-organisaties is het ook mogelijk om één overkoepelende FG aan te wijzen voor meerdere organisaties voor de verwerking van politiegegevens door boa's. Bij sommige gemeenten werken weliswaar meer dan tweehonderd boa's, maar bij kleine instellingen kan het zijn dat er slechts twee boa's werkzaam zijn.

Privacyfunctionaris

De privacyfunctionaris geeft advies en houdt toezicht. Bij de politie – waar bijna 70.000 mensen werken – zijn verschillende van deze functionarissen actief. Voor boa-organisaties is de privacyfunctionaris niet verplicht. In artikel 2, lid 1 van het Bpg boa staat namelijk dat artikel 34 Wpg is uitgezonderd. Een privacyfunctionaris naast een FG is namelijk een nogal zware belasting, zeker voor kleine organisaties. Dit neemt niet weg dat het verstandig kan zijn toch een privacyfunctionaris aan te stellen. Deze persoon kan een adviserende rol innemen bij bijvoorbeeld het inrichten van het verwerkingsregister, het aanwijzen van bevoegd functionarissen en andere Wpg-vraagstukken.

Bevoegd functionaris (BF)

Dit is de 'hoeder' van de gegevens die onder artikel 9 Wpg worden verwerkt. Deze functionaris is beschreven in artikel 2:10, eerste lid, van het Besluit politiegegevens (Bpg). Het moet iemand zijn met voldoende kennis en vaardigheden over dit type gegevens. Hij beslist bijvoorbeeld wie er toegang mag hebben tot deze gegevens en of ze verstrekt kunnen worden aan een samenwerkingspartner. Iedere artikel 9-verwerking dient een bevoegd functionaris (BF) te hebben. De BF wordt aangewezen door de werkgever van de boa. In de bijlage vind je een model voor het aanwijzen van de BF.

De bevoegd functionaris heeft onder andere de volgende taken:

- het doel van de artikel 9-verwerking omschrijven en vastleggen. Zie Wpg art. 32;

- het autoriseren van personen voor de betreffende verwerking;
- bepalen of gegevens voor andere doeleinden mogen worden gebruikt – zie Wpg art. 9, lid 3;
- zorgen dat voor alle gegevens de herkomst en wijze van verkrijgen wordt vastgelegd – zie Wpg art. 3, lid 5;
- bewaken dat gegevens rechtmatig worden verkregen en verwerkt. Hierbij moet vooral worden gelet op de termijnen.

Verwerkingsverantwoordelijke

Dit is de (rechts)persoon die het doel en de middelen bepaalt voor de verwerking van persoonsgegevens (AVG) of politiegegevens (Wpg). Bij de politie is dit de korpschef. Bij de marechaussee is het de Minister van Defensie. Voor de boa is het de werkgever van de boa, zie Bpg boa artikel 1 onder c. Deze moet ervoor zorgen dat de systemen worden aangepast en dat de autorisaties goed geregeld zijn. Ook zorgt hij dat de beveiliging op orde is en dat gegevens verwijderd en gedeeld worden conform de regels uit de Wpg.

Soms worden taken uitbesteed. Bijvoorbeeld aan een regionale uitvoeringsdienst, voor milieu- bodem- en asbesttaken. Of aan een sociale recherche, voor uitkeringen en fraudeonderzoek. Dan moet goed worden nagegaan via welke constructie deze taken zijn overgedragen: zijn ze gedelegeerd? In dat geval oefent de dienst die de taak uitvoert, deze uit onder eigen verantwoordelijkheid. Hij is zelf juridisch verantwoordelijk en daardoor de verwerende partij in bezwaar of beroep. Je kunt stellen dat de verwerkingsverantwoordelijkheid dan ook meereist en dat hij dus voor bijvoorbeeld de audit moet zorgen. In dit [artikel](#) van adviesbureau L2P wordt verder ingegaan op de rol van de verwerkingsverantwoordelijke.

Verwerker

De (rechts)persoon die politiegegevens verwerkt voor een verwerkingsverantwoordelijke. Voorbeelden van verwerkers:

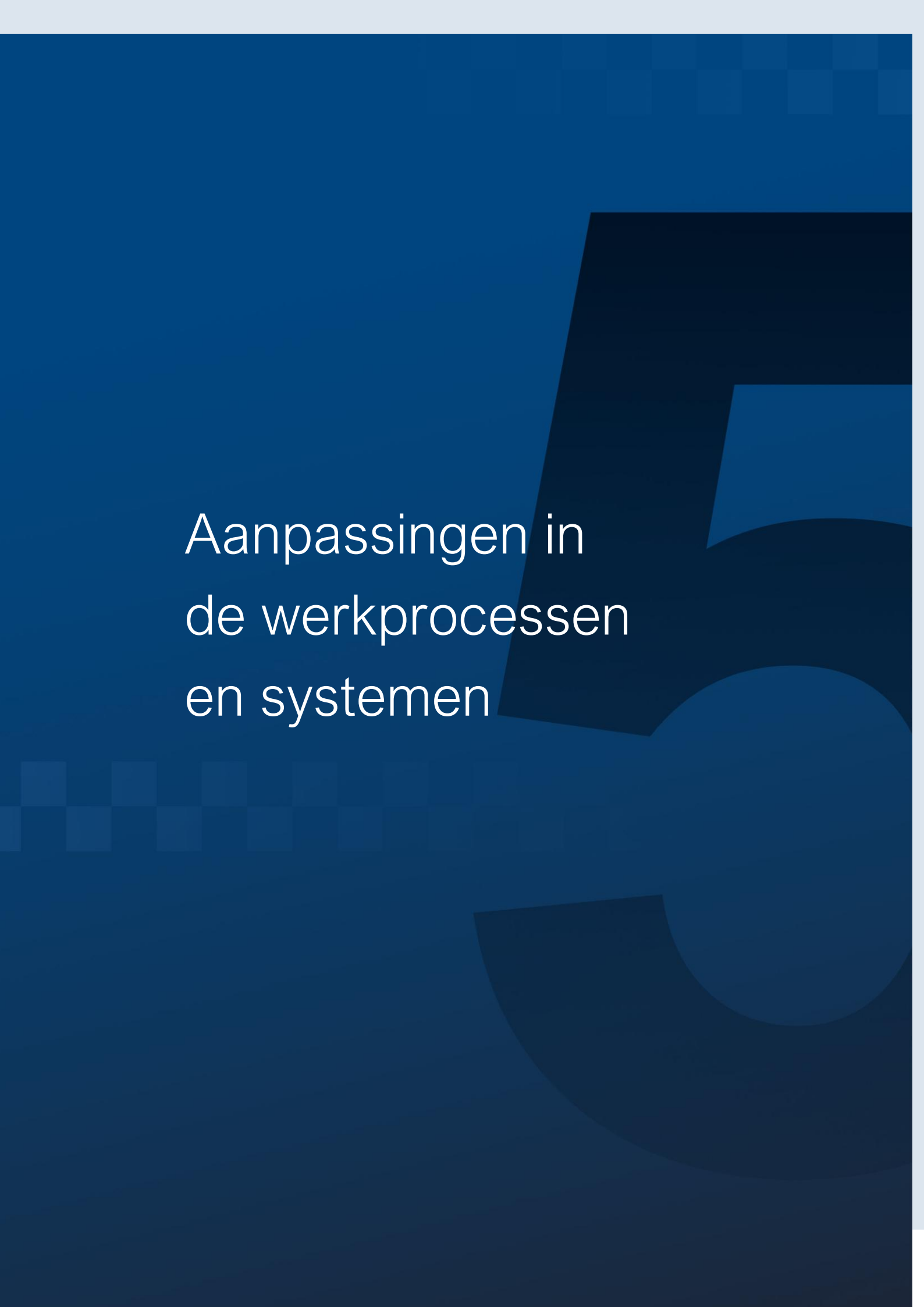
- een particuliere alarmcentrale die beelden van bewakingscamera's ontvangt en bekijkt;
- de leverancier Sigmax als het gaat om gegevens die in het systeem CityControl worden verwerkt;
- de leverancier Eljakim als het gaat om gegevens die in het systeem CAREL worden verwerkt;
- de leverancier Natuurnetwerk als het gaat om gegevens die in het systeem BRS worden verwerkt.

Elke verwerker werkt onder de verantwoordelijkheid van een verwerkingsverantwoordelijke en volgt zijn aanwijzingen op. Ook moet er een verwerkersovereenkomst worden gesloten tussen de verwerker en de verantwoordelijke om de afspraken en verantwoordelijkheden helder vast te leggen.

De verwerkersovereenkomst is iets anders dan een regulier onderhoudscontract met afspraken over het kwaliteitsniveau van geleverde diensten, zoals het maken van back-ups en beschikbaarheid van het systeem. Deze afspraken worden vaak vastgelegd in de vorm van een SLA, Service Level Agreement. Een verwerkersovereenkomst kan gezien worden als aanvulling daarop.

Auditor

In artikel 6:5, lid 1 Bpg is beschreven dat twee jaar na inwerkingtreding van de wet de verwerkingsverantwoordelijke een externe audit moet laten uitvoeren. Dit dient te gebeuren conform de regels uit de **Regeling periodieke audit politiegegevens**. Daarna moet dat elke vier jaar gebeuren. De audit heeft betrekking op de wijze waarop de verwerkingen georganiseerd zijn, de maatregelen en procedures die daarop van toepassing zijn, en de werking van deze maatregelen en procedures ("opzet, bestaan en werking"). Omdat het Bpg boa in 2019 in werking trad, had de eerste externe audit in 2021 moeten worden uitgevoerd; de tweede in 2025. Tevens dient er ieder jaar een interne audit te worden uitgevoerd. Voor de audit zijn diverse hulpmiddelen ontwikkeld. Zie hoofdstuk 9. De auteur verzorgt een tweedaagse **Wpg-audittraining** voor auditors en aankomend auditors.

The background is a solid dark blue. In the top right corner, there is a grid of lighter blue squares. On the right side, there are several overlapping geometric shapes: a large dark blue trapezoid, a medium blue rectangle, and a large dark blue circle. In the bottom left corner, there is a horizontal row of lighter blue squares.

Aanpassingen in de werkprocessen en systemen

Hoofdstuk 5

Aanpassingen in de werkprocessen en systemen

De in dit hoofdstuk beschreven aanpassingen hoeven niet door de boa zelf te worden doorgevoerd. Dit hoofdstuk is vooral van belang voor medewerkers verantwoordelijk voor de automatisering of het humanresourcebeleid.

Labeling en de bevoegd functionaris

In organisaties waar boa's werkzaam zijn, gold vroeger één wet voor de verwerking van persoonsgegevens: de Wet bescherming persoonsgegevens (Wbp). Nu zijn er twee wetten: de AVG en de Wpg. Dat levert meestal twee aparte gegevensverzamelingen op die aan twee aparte werkprocessen gekoppeld zijn: toezicht en opsporing. Het is raadzaam om de opslag van de gegevens in verschillende informatiesystemen te laten plaatsvinden. Als gegevens toch in hetzelfde informatiesysteem staan, moeten ze in elk geval goed 'gelabeld' worden zodat duidelijk is wat het doel van de verwerking is: opsporing of toezicht. Tevens moet – als het om opsporing gaat – zichtbaar zijn welke Wpg-verwerkingsgrondslag van toepassing is: 8, 9 of 13. Er gelden tenslotte andere regels en termijnen. Voor iedere artikel 9-verwerking geldt bovendien dat er een bevoegd functionaris aan gekoppeld moet kunnen worden, dat er selectief geautoriseerd moet kunnen worden, et cetera. Op ICT-gebied moeten er dus wijzigingen worden doorgevoerd.

Privacy by design

Zowel de AVG als de Wpg kent een bepaling over 'Privacy by design'. De verwerkingsverantwoordelijke moet passende technische en organisatorische maatregelen treffen om rechtmatigheid, proportionaliteit en beveiliging van de gegevensverwerking te

garanderen. En dit moet niet achteraf gebeuren, maar al aan de tekentafel waar de verwerking wordt ontworpen ('by design'). Daarnaast kennen beide wetten 'Privacy by default': de standaardinstellingen moeten zo zijn dat de privacy maximaal wordt gewaarborgd. Dat herkennen we allemaal wel met betrekking tot 'aanvinkhokjes' op websites: vroeger stonden ze standaard aan, tegenwoordig moet je ze zelf aanvinken.

Maak bij het inrichten van informatiesystemen en werkprocessen vooral gebruik van reeds bestaande hulpmiddelen en beleidsdocumenten zoals het boekje met **privacyontwerpstrategieën** van Jaap-Henk Hoepman.

Verantwoording afleggen

Op ICT-gebied gelden nog meer regels: er moet onder andere een overzicht worden opgesteld met alle verwerkingen, zoals applicaties en bestanden: een verwerkingsregister. Daarbij moet de volgende informatie worden vastgelegd:

- de verwerkingsgrondslag,
- welke categorieën van betrokkenen en categorieën van gegevens het betreft,
- de verwijdertermijnen,
- wie er toegang hebben,
- welke technische en organisatorische maatregelen zijn genomen voor de beveiliging van de gegevens.

Soms is het verplicht om voorafgaand aan een verwerking een gegevensbeschermingseffectbeoordeling (GEB, vroeger DPIA) op te stellen, bijvoorbeeld als je bodycams of andere technologische hulpmiddelen in gebruik wilt nemen. In zo'n traject beschrijf je systematisch de geplande gegevensverwerking en je onderbouwt waarom deze rechtmatig en noodzakelijk is. Daarna beschrijf je de maatregelen die je neemt om de privacyrisico's te verkleinen of weg te nemen. Ook beschrijf je de resterende risico's en geef je aan wat je doet als het toch een keer mis zou gaan. Bij het opstellen van zo'n GEB is het proces misschien nog belangrijker dan het eindresultaat. Je wilt

dat iedereen meedenkt: de werkvloer, de afdeling communicatie, personeelszaken en de ICT'ers. Raadpleeg voor het uitvoeren van een GEB de **richtlijnen** van de Autoriteit Persoonsgegevens.

Bespreek welke persoonsgegevens verwerkt worden, wat het doel is en wat de gevolgen zijn voor de personen van wie je gegevens verzamelt. Kun je uitleggen waarom het een goed idee is om die gegevens te gaan verwerken? En kun je aantonen dat je aan de wet- en regelgeving voldoet zonder disproportionele privacyrisico's voor de betrokkenen? Dan kan er heel veel.

Een ander element als het gaat om het afleggen van verantwoording en het creëren van transparantie, is de documentatieplicht. Artikel 32 Wpg beschrijft vier gegevensverzamelingen waar de verwerkingsverantwoordelijke voor moet zorgen, namelijk alle

- verstrekkingen,
- artikel 9-doeleinden,
- datalekken en
- weigeringen van inzageverzoeken.

Hoe meer en hoe beter deze werkprocessen geautomatiseerd ondersteund worden (een 'vinkje' om aan te geven dat gegevens verstrekt zijn en aan wie), hoe eenvoudiger het is om aan deze documentatieplicht te voldoen.



De rechten van betrokkenen

Hoofdstuk 6

De rechten van betrokkenen

Een belangrijke aanleiding voor Europa om de privacyregels aan te scherpen, is om de rechten van de personen van wie gegevens worden verwerkt, uit te breiden en het makkelijker voor hen te maken om hun rechten uit te oefenen. Dat is nodig, omdat het technisch gezien steeds eenvoudiger wordt gegevens te verzamelen, te combineren en te bewaren. Niet alleen het bedrijfsleven doet dat, maar ook politie, gemeenten en andere overheidsinstellingen. De risico's zijn niet gering: denk aan het datalek bij de GGD van januari 2021 waarbij informatie uit coronasystemen met adresgegevens, telefoonnummers, burgerservicenummers en medische gegevens zoals testresultaten, in verkeerde handen zijn terecht gekomen.

Privacyverklaring

Personen van wie je gegevens verwerkt, hebben het recht daarvan op de hoogte te worden gebracht voordat de verwerking plaatsvindt. Die informatieplicht wordt niet altijd nageleefd. Vaak hebben organisaties wel een privacyverklaring op hun website waarin de gegevensverwerking onder AVG wordt beschreven, maar ontbreekt de beschrijving van de gegevensverwerking onder de Wpg. Iedere organisatie die boa's in dienst heeft, verwerkt per definitie politiegegevens onder de Wpg. Dit moet dus goed in de privacyverklaring staan.

Recht op inzage

Een ander recht van elke betrokkene is het recht op inzage. Eenieder die wil weten welke persoonsgegevens over hem zijn vastgelegd, kan een kennisnemingsverzoek indienen. Dit geldt zowel voor AVG- als Wpg-gegevens. Hoe dit proces precies verloopt, wordt vastgelegd in lokale afspraken en procedures. Er zijn slechts enkele redenen om een kennisnemingsverzoek te weigeren: bijvoorbeeld als de veiligheid van de staat in gevaar komt, of als het leidt tot schending van de rechten van anderen. Maar in vrijwel alle gevallen zal er inzage moeten worden gegeven. Begin 2018 liet de Directeur Klantenservice van de NS weten dat een paar medewerkers enkele dagen bezig waren geweest om het volledige overzicht op te leveren van slechts één persoon. Hoe beter de organisatie en de werkprocessen zijn ingericht (het verwerkingsregister kan hierbij helpen), hoe sneller aan een verzoek van een burger kan worden voldaan. Als een betrokkene om inzage vraagt, moet ook worden medegedeeld aan welke andere partijen de gegevens zijn verstrekt. Zorg dus dat alle verstrekkingen netjes worden geregistreerd: veilig en afgeschermd voor onbevoegden, maar eenvoudig doorzoekbaar en leverbaar voor inzageverzoeken.

Andere rechten

Het recht op inzage is ook bedoeld om burgers de mogelijkheid te bieden te controleren of de gegevens die over hen verwerkt worden, juist, volledig, ter zake dienend en noodzakelijk zijn. Als dat niet zo is, dan hebben zij nog een aantal rechten. Zo kunnen zij vragen om aanpassing, verwijdering en afscherming van gegevens die op hen betrekking hebben.

The background is a solid blue color. In the top right corner, there is a dark blue rectangular block. A large, dark blue curved shape, resembling a stylized '7' or a swoosh, starts from the right edge and curves downwards towards the bottom right. A horizontal band of a light blue and dark blue checkerboard pattern runs across the middle of the page, behind the text.

Praktijkvoorbeelden

Hoofdstuk 7

Praktijkvoorbeelden

In dit hoofdstuk komen diverse praktijkvoorbeelden aan bod uit alle zes boa-domeinen. Als niet duidelijk is hoe de Wpg jóúw werk raakt, lees dan eerst dit hoofdstuk. Mocht je een fout tegenkomen of een ander idee hebben wat betreft een antwoord, neem dan contact op met de auteur.

- 1 Bij een stroperijzaak blijkt meer aan de hand dan in eerste instantie verwacht. Je verwacht langer dan 40 uur bezig te zijn met het onderzoek en werkt samen met de politie. Wat voor regime is van toepassing op de informatie die je vastlegt: Wpg of AVG? En wat voor verwerkingsgrondslag: artikel 8 of 9?

Dit is een Wpg artikel-9-verwerking. Dat betekent dat er per zaak een bevoegd functionaris moet worden aangewezen en dat de gegevens afgeschermd moeten worden. Als de politie de leiding heeft, is het mogelijk dat zij een BF aanwijst en dat jij als boa meedraait in het onderzoek.

- 2 Mag je een foto van een kenteken of een signalement delen met collega's via Signal of WhatsApp?

Nee, dat is niet toegestaan. Het gaat hier om politiegegevens (mogelijk identificeerbare personen in relatie met een strafbaar feit). Gebruik goed beveiligde systemen, zoals portofoon, telefoon of beveiligde e-mail.

- 3 Kan een stagiair of boa in opleiding geautoriseerd worden voor het verwerken van politiegegevens?

Ja, op grond van artikel 3 van het Bpg boa is het mogelijk dat de werkgever van de boa personen autoriseert die onder zijn beheer werken, maar geen boa zijn. De nota van toelichting bij artikel 3 Bpg boa noemt diverse vormen van verwerking. De werkgever dient vast te leggen om wat voor soort gegevens het gaat, om wat voor soort verwerking het gaat, en voor hoelang ze verwerkt worden. Op de site van BRS is een **modelverklaring** en toelichting te vinden hoe niet-boa's geautoriseerd kunnen worden.

- 4 Een gemeentelijk kwaliteitsadviseur of wethouder is namens de burgemeester belast met het nemen van maatregelen rondom horecaverGUNningen. Hij vraagt de gemeentelijke boa om informatie rondom strafbare feiten in een bar zodat hij kan bepalen of de voor die bar afgegeven vergunning moet worden ingetrokken. Kan de boa deze delen gegevens delen met de kwaliteitsadviseur of wethouder?

Ja, dat is mogelijk. De Wpg biedt de mogelijkheid om te verstrekken aan de burgemeester zodat hij beslissingen kan nemen omtrent verlening, weigering of intrekking vergunning op grond van de Alcoholwet en de Wet op de kansspelen. Indien de burgemeester hier iemand voor gemandateerd heeft, dan mag ook deze persoon de benodigde politiegegevens daarvoor ontvangen. Zowel van de politie als de gemeentelijke boa.

- 5 Een groene boa zet camera's in om zicht te krijgen op wildbewegingen. Nu is op die beelden te zien dat een strafbaar feit wordt gepleegd. Mogen deze beelden door de politie gebruikt worden voor opsporingsberichtgeving?

De camera's zijn oorspronkelijk voor een ander doel in gebruik genomen, dus kunnen de beelden niet direct gebruikt worden. Er zijn twee opties: 1) de opnames worden gevorderd; zo

kunnen ze rechtmatig het Wpg-domein worden binnengehaald. 2) de groene boa die de beelden bekijkt en een vermoeden heeft van een strafbaar feit overhandigt op eigen initiatief de beelden aan de politie. In dat geval is er geen vordering nodig.

- 6 Bij een bedrijventerrein tref je een enorme hoeveelheid grof vuil aan: laminaat, bankstellen, een halve keuken. Je neemt foto's om op zoek te gaan naar de dader. Mag je deze foto's naderhand ook voor een bewustwordingscampagne gebruiken?

Zolang er op deze beelden geen herkenbare personen, voertuigen of locaties staan en er geen goederen op staan die tot identificatie zouden kunnen leiden, mogen de beelden gebruikt worden voor bewustwording of andere campagnes. Gebruik je de beelden in je opsporingsonderzoek? Leg ze dan vast op de juiste plek en behandel ze als politiegegevens. Je doel is het achterhalen van de dader en in combinatie met andere gegevens uit jouw onderzoek, zou je diegene kunnen identificeren. Daarmee worden de beelden politiegegevens.

- 7 Tijdens een aanhouding is een van de verdachten de dans ontsprongen. Er zijn opnames gemaakt met een bodycam. Mogen deze gebruikt worden voor opsporingsberichtgeving?

Dit hangt af van het doel waarvoor de beelden oorspronkelijk vergaard zijn. Voor boa's is het doel van de bodycam vrijwel altijd 'veiliger werken'. De opnames zijn dan vergaard op basis van de grondslag 'gerechtvaardigd belang' in de AVG (artikel 6.1.f) en niet op grond van de opsporingstaak van de boa. Voordat deze opnames mogen worden gebruikt voor opsporing, moeten ze worden overgeheveld van het AVG-domein naar de Wpg. Als een boa slachtoffer is van geweld, kan hij de bodycambeelden aan de politie geven bij zijn aangifte. De politie mag die opnames dan gebruiken voor opsporingsonderzoek bij bijvoorbeeld bedreiging, belediging of mishandeling van de boa.

De politie heeft dat probleem met bodycams niet. Zij mag zelfgemaakte bodycamopnames gebruiken voor opsporing omdat de grondslag van deze bodycams artikel 3 van de Politiewet is. Boa's hebben geen vergelijkbaar wetsartikel om zich op te baseren. Zij hebben geen vergelijkbare wettelijke taak die een inbreuk op grondrechten rechtvaardigt. Er wordt door het Ministerie van Justitie en Veiligheid nagedacht over de vraag of het wenselijk is een specifieke wettelijke grondslag te creëren voor de inzet van bodycams door boa's. Tot die tijd is het raadzaam bodycambeelden die zijn gemaakt in het kader van 'veilig werken' alleen na vordering te gebruiken voor opsporing.

- 8 In een opsporingsonderzoek wordt een tap op een mobieltje gezet. Vallen deze tapgegevens onder artikel 8, 9 of 13 van de Wpg?

Artikel 9. Een tap op een mobieltje is een zogenaamd bijzonder opsporingsmiddel. De inbreuk op de privacy is bij dit soort hulpmiddelen groot en daarom dienen de gegevens verwerkt te worden conform artikel 9 Wpg.

- 9 Een vader belt een OV-bedrijf op: "Ik hoor via-via dat mijn dochter met een boa van jullie in aanraking is geweest. Wat is er gebeurd?" Wat zeg je tegen hem?

Vraag de vader of zijn dochter jonger is dan 16 jaar. Zo ja, dan kan de vader als wettelijke vertegenwoordiger inzage opvragen namens het meisje. Is zij 16 jaar of ouder, dan geef je aan dat zij zelf inzagerecht uit mag oefenen of dat zij een machtiging kan verlenen aan de ouders. Je kunt in dat geval slechts beperkt informatie geven, hoogstens adviseren. De grens van 16 jaar geldt zowel in de Wpg als in de AVG. Daarnaast is het altijd noodzakelijk om de identiteit van de verzoeker goed vast te stellen. Telefonisch informatie geven is sowieso dus niet mogelijk. In december 2020 heeft de **Raad van State** erkend dat gemeenten betrokkenen mogen vragen om zich te identificeren op het gemeentehuis.

- 10 Ook het versturen van gegevens is een vorm van verwerken. Mag een collega – niet zijnde een boa – een door jou opgesteld proces verbaal versturen aan het CJIB?

Het gaat om politiegegevens; de Wpg is dus van toepassing. In vraag 3 van dit hoofdstuk staat een vergelijkbare casus met uitgebreide uitwerking. Ook hier is het antwoord ja.

- 11 Een boa in bus, tram en trein gaat op pad om kaartjes te controleren en scant daarbij ov-chipkaarten. Die kaarten zijn te herleiden tot personen en dus zijn het persoonsgegevens. Valt die gegevensverwerking, het scannen van een ov-chipkaart, onder de AVG of de Wpg?

Deze verwerking valt onder de AVG, omdat de boa bezig is met toezicht houden. Als een zwartrijder een boete krijgt, is dat een voorlopig proces-verbaal dat in eerste instantie onder de AVG valt. Want zwartrijden is geen strafbaar feit uit het Wetboek van Strafrecht, maar een civielrechtelijke overtreding. Pas als de boete na 28 dagen niet is betaald en de vervoerder het proces-verbaal naar het CJIB van het OM stuurt, wordt het anders. Het OM neemt de vordering van de boete op zich en vanaf dat moment is het strafrecht van toepassing. Vanaf dat moment vallen de gegevens onder de Wpg.

- 12 Er is een Woo-verzoek (Wet open overheid) ingediend door een journalist die wil weten wat de toezichtswerkzaamheden van een gemeente zijn wat betreft zwemwaterwetgeving. De journalist wil weten waar en hoe vaak er gecontroleerd is, maar ook of er sancties zijn opgelegd. De gemeente heeft een boete uitgeschreven voor zwemmen in een doorgaande vaarroute waar zwemmen verboden is. De persoonsgegevens van de beboete persoon vallen onder de Wpg. Wat betekent dit voor het Woo-verzoek?

Alle verwerkte gegevens kunnen opgevraagd worden op grond van de Woo – dat geldt voor AVG en Wpg. Maar er kunnen

weigeringsgronden van toepassing zijn – bijvoorbeeld als de veiligheid van de staat in het geding zou komen als de gegevens worden verstrekt. Dat zal bij dit verzoek geen weigeringsgrond zijn, maar het is wel iets om in het achterhoofd te houden. Maar er zijn meer redenen: bijvoorbeeld als de verstrekking het recht op privacy van personen ernstig zou schaden. Daarom moeten alle gegevens die tot personen te herleiden zijn, geanonimiseerd worden. Bij de Woo gaat het om een belangenafweging: het belang van openbaarmaking van de persoonsgegevens zal vaak niet opwegen tegen het belang van de eerbiediging van de persoonlijke levenssfeer van de betrokkene.

- 13 Een gemeentelijke boa heeft foto's gemaakt tijdens een milieuvlucht. Een deel van deze foto's wordt als ondersteunend materiaal gebruikt voor een strafrechtelijk onderzoek. Welk regime is hierop van toepassing?

Als er op de foto's personen te zien zijn, gaat het om persoonsgegevens. Ze vallen onder de AVG zolang ze worden gebruikt voor toezicht. Foto's die gebruikt worden in een strafrechtelijk onderzoek, vallen eveneens onder de Wpg (artikel 8 of 9). Dit betekent dus dat op dezelfde foto's tegelijkertijd zowel de Wpg als de AVG van toepassing is. Het maakt overigens niet uit of de foto's gebruikt worden als bewijsmateriaal of slechts ter ondersteuning van het strafrechtelijk onderzoek; in beide gevallen vallen ze onder de Wpg.

- 14 Een bedrijf heeft asbest verwijderd zonder de juiste vergunning. Uit een gesprek blijkt dat de organisatie niet op de hoogte was van de regels en daarom krijgt zij een waarschuwing; deze wordt vastgelegd in het systeem van de boa. Twee jaar later krijgt hetzelfde bedrijf wederom bezoek van de toezichthouder. Zij blijkt nog steeds asbest te verwijderen zonder vergunning. Nu wordt er een boete uitgeschreven. In het proces-verbaal wordt de controle van twee jaar eerder opgevoerd als een van de verzwarende

omstandigheden om de boete op te leggen. Welk regime (AVG of Wpg) is van toepassing op beide verwerkingen?

De gegevens over de waarschuwing van twee jaar eerder vallen onder de Wpg; het maakt niet uit dat er toen slechts een waarschuwing is gegeven. De gegevens in het proces-verbaal vallen ook onder de Wpg.

- 15 Een groene boa heeft het vermoeden dat er illegaal inheemse vogels worden gevangen door iemand die daar al vaker voor veroordeeld is. Zijn bevindingen leiden ertoe dat de politie een baken plaatst onder het voertuig van de verdachte. Vallen zijn bevindingen en waarnemingen onder artikel 8, 9 of 13 van de Wpg?
-

Artikel 9. In eerste instantie ging het om artikel 8-gegevens. Zodra er een baken wordt geplaatst, een zogenaamd bijzonder opsporingsmiddel, moeten de gegevens onder artikel 9 worden verwerkt. De gegevens worden afgeschermd en de BF bepaalt wie toegang mag hebben tot deze gegevens.

- 16 Voor het in kaart brengen van mogelijke hennepplantages wordt een drone ingezet. Zo kan snel worden nagegaan of er verdachte gebieden zijn vrijgemaakt in bosschages of rietvelden. Wat voor gegevens zijn deze drone-beelden en wat zijn de regels?
-

Ervan uitgaande dat op de beelden geen personen of tot personen te herleiden informatie te zien is, gaat het hier in eerste instantie niet om politiegegevens. Toch geldt dat als de beelden aanleiding geven tot verder onderzoek en mogelijk als bewijsmateriaal gebruikt worden, ze behandeld moeten worden als politiegegevens. Als verderop in het onderzoek gegevens gecombineerd worden, bijvoorbeeld met telefoniegegevens, dan kunnen de beelden wel degelijk gekoppeld worden aan een persoon.

- 17 Er is een grasveld vernield doordat er met een quad over geracet is. De boa heeft proces-verbaal opgemaakt. Zijn collega (geen boa) die belast is met het herstellen van de schade, vraagt de boa om de persoonsgegevens van de dader om de schade te verhalen. Mag de boa deze gegevens verstrekken?

Ja, dat mag. De boa-werkgever is benadeelde van een strafbaar feit. In de Verstrekkingenwijzer is beschreven wat de mogelijkheden zijn voor het verstrekken aan benadeelden van strafbare feiten. Deze verstrekkingvorm wordt in het Naslagwerk verstrekken uitgebreid toegelicht.

- 18 Een boa geeft een waarschuwing voor varen met een snelle motorboot zonder dodemansknop. Vallen de gegevens die hij daarbij vastlegt onder de Wpg?

Ja, dit is een strafbaar feit en de boa treedt op in zijn hoedanigheid als boa. Het feit dat hij een waarschuwing geeft en niet direct een proces-verbaal, is niet relevant.

- 19 Een gemeentelijke boa controleert op parkeerplaatsen voor vergunninghouders of de persoon die geparkeerd heeft ook daadwerkelijk een vergunning heeft. Dat blijkt niet het geval en er is sprake van een overtreding. Welke gegevens vallen onder de AVG en welke onder de Wpg?

Als hij gegevens vastlegt omtrent de controle, vallen deze onder de AVG. Zodra er sprake is van een overtreding, zet hij zijn boa-pet op en valt de verdere gegevensverwerking onder de Wpg.

- 20 Is het mogelijk dat gegevens over een boete voor bellen op de fiets bij gemeente A onder de Wpg vallen en bij gemeente B onder de AVG?

Ja, dat is mogelijk. In principe worden deze gegevens onder de Wpg verwerkt; het gaat om een strafbaar feit. Echter, een

gemeente kan tot op zekere hoogte zelf beslissen of bepaalde overtredingen bestuursrechtelijk of strafrechtelijk worden afgedaan. Kiest de gemeente voor bestuursrechtelijk, dan vallen deze gegevens onder de AVG. Dit betekent dus wat voor onder andere het delen van deze informatie met andere opsporingsambtenaren. Het **Besluit bestuurlijke boete overlast in de openbare ruimte** geeft hier meer informatie over.

The background is a solid dark blue. On the right side, there are two large, overlapping circles in a slightly lighter shade of blue. In the top right and bottom left corners, there are small, light blue checkerboard patterns.

Stand van zaken wetgeving en bijbehorende afkortingen

Hoofdstuk 8

Stand van zaken wetgeving en bijbehorende afkortingen

In de bijlagen is een totaaloverzicht van afkortingen opgenomen. Dit hoofdstuk beschrijft welke wetgeving er is en welke afkortingen daarvoor gebruikt worden.

AVG

De Algemene verordening gegevensbescherming heeft per mei 2018 de Wet bescherming persoonsgegevens vervangen en biedt één kader voor het werken met persoonsgegevens in heel Europa. De AVG kent enkele uitzonderingen. Eén daarvan is de verwerking van persoonsgegevens ter voorkoming, opsporing of vervolging van strafbare feiten door bevoegde autoriteiten. Deze persoonsgegevens vallen onder een apart regime: de Wet politiegegevens (Wpg).

UAVG

De AVG werkt rechtstreekse in Nederland én in alle andere EU-lidstaten. De Uitvoeringswet AVG (UAVG) bevat alleen nationale regels om de uitvoering van de AVG goed in Nederland te laten plaatsvinden. Ook deze is op 25 mei 2018 in werking getreden. Het aanstellen van de Autoriteit Persoonsgegevens is hierin bijvoorbeeld geregeld.

Wpg

De Wpg geldt sinds 1 januari 2008 voor politie, marechaussee en Rijksrecherche. Op 1 januari 2019 is de aangepaste Wpg in werking getreden. In deze update zijn de consequenties verwerkt van de Europese wetgeving zoals verwoord in de Europese richtlijn gegevensbescherming opsporing en vervolging.

Bpg

Het Besluit politiegegevens is een algemene maatregel van bestuur (AMvB) die invulling geeft aan een aantal elementen uit de Wpg. In de Wpg staat bijvoorbeeld beschreven dat op structurele basis gegevens verstrekt mogen worden aan een aantal organisaties. In het Bpg is vervolgens uitgewerkt welke organisaties dat zijn. Een praktijkvoorbeeld: Bureau Halt, Stichting Slachtofferhulp Nederland en Jeugdzorg zijn instanties waar regelmatig iets verandert qua naam of takenpakket en met een AMvB kan er makkelijker een aanpassing plaatsvinden dan wanneer zo'n verstrekking in de wet geregeld zou zijn. Het Bpg is sinds 2008 enkele keren aangepast. De laatste aanpassing was van 1 januari 2025, met het **Verzamelbesluit** gegevensverwerking politie en justitie 2024.

Bpg boa

Het Besluit politiegegevens buitengewoon opsporingsambtenaren (Bpg boa) is het besluit waarmee een groot deel van de Wpg van overeenkomstige toepassing is verklaard op gegevensverwerking door boa's. Het besluit lijkt sterk op het Besluit politiegegevens bijzondere opsporingsdiensten. In artikel 2 van het Bpg boa staat precies beschreven welke elementen van de Wpg en de Bpg van toepassing zijn op de gegevensverwerking door de boa. Welke dit zijn, is uitgewerkt in de wettekst in de bijlage.

Bpg BOD

Het Besluit politiegegevens bijzondere opsporingsdiensten is een algemene maatregel van bestuur (een AMvB) waarmee sinds 2009 een groot deel van de artikelen uit de Wpg van overeenkomstige toepassing is verklaard op gegevensverwerking door de BOD'en.

GEB

Een gegevensbeschermingseffectbeoordeling is een document waarin je de verwerking van gegevens systematisch beschrijft en onderbouwt waarom de verwerking noodzakelijk is. Daarna beschrijf je de

maatregelen die je gaat nemen om de privacyrisico's te verkleinen of weg te nemen. In het Engels heet dit een Data Protection Impact Assessment of DPIA. Een GEB is verplicht bij verwerkingen met een hoog risico voor de privacy van betrokkenen, bijvoorbeeld als er nieuwe technologieën worden gebruikt zoals gezichtsherkenning. Raadpleeg daarvoor de **richtlijnen** van de Autoriteit Persoonsgegevens.

Instructie Bpg boa en de rol van de officier van justitie

Met de komst van deze **instructie** op 1 september 2024, is het onder andere mogelijk geworden dat een boa de artikel 8-gegevens die hij verwerkt aan een toezichthouder mag verstrekken, zonder dat tussenkomst door een officier van justitie nodig is.

Ter afsluiting

Hoofdstuk 9

Ter afsluiting

Handige linkjes

In dit Praktijkhandboek wordt geregeld verwezen naar documenten of producten die je nodig hebt om aan de Wpg te voldoen. Hierbij een overzicht, inclusief andere handige linkjes:

- **Besluit politiegegevens boa (Bpg boa)** In dit besluit werd in 2019 de Wet politiegegevens van overeenkomstige toepassing verklaard op de gegevensverwerking door de boa.
- **Besluit politiegegevens bijzondere opsporingsdiensten (Bpg BOD)** In dit besluit werd in 2009 de Wet politiegegevens van overeenkomstige toepassing verklaard op opsporingsambtenaren van bijzondere opsporingsdiensten.
- **Memorie van toelichting Wpg 2008** Toelichting op de Wpg zoals opgesteld in 2008.
- **Memorie van toelichting Wpg 2018** Toelichting op de Wpg zoals opgesteld in 2018, vanwege Europese wijzigingen.
- **Rijkmodel DPIA / GEB** waar alle onderdelen die je moet behandelen zijn opgenomen: rechtsgrond, noodzakelijkheid, risico's en maatregelen.
- Een webinar van februari 2022 voor het **Centrum voor Informatiebeveiliging en Privacy** met 10 praktische tips en praktijkvoorbeelden. En een **podcast** over de Wpg in de dagelijkse praktijk van de boa. Beide met medewerking van Suzanne Franken.
- De Verstrekkingenwijzer Wpg voor boa's bevat alle opties voor de boa om te verstrekken. Er staan tientallen instanties, slachtoffers en benadeelden in. De politie en Kmar hebben een eigen verstrekkingenwijzer. In het Naslagwerk verstrekken voor boa's worden alle verstrekkingsmogelijkheden en begrippen toegelicht die van belang zijn bij het verstrekken van gegevens

naar derden. Beide producten zijn ontwikkeld in opdracht van de gebruikers van het **systeem BRS** en zijn op die site te vinden.

- Ook de Bewaartermijnwijzer, het Naslagwerk Bevoegd Functionaris en de Instructie voor de scheidingslijn tussen artikel 8 en 9 zijn in opdracht van de BRS-gebruikers gemaakt.
- In de bijlagen is de wettekst Wpg opgenomen zoals deze van toepassing is voor het werkveld van de boa. Ook heeft de auteur voor het Besluit politiegegevens een dergelijk document gemaakt.
- NOREA heeft een **Handreiking** Privacy audit Wpg voor boa's ontwikkeld en de VNG heeft specifiek voor gemeenten een **Werkdocument** Audit Wet politiegegevens ontwikkeld.
- De Autoriteit Persoonsgegevens (AP) houdt toezicht op een goede naleving van de regels uit de Wpg. In januari 2023 publiceerde de AP een **nieuwsbericht** waaruit bleek dat vele boa-organisaties niet tijdig hun audit-rapportage hebben ingediend. In juni 2023 heeft de AP een **rapportage** gepubliceerd over hun onderzoek naar de audit-rapportages en in juli 2024 heeft de AP een rapportage gepubliceerd over hun onderzoek naar de hercontroles.

Dankwoord

Ik bedank Hans, Marc, Yvette, Sander, Ramon, Birgit, Stephan, Roswitha, Marjolein, Nicoline, Idith en Jaap-Henk voor hun geduld, tijd en inzet, voor niet moeilijk doen als dat niet nodig is, voor het bieden van inspiratie en voor hun geloof en vertrouwen. Ook dank ik alle lezers van de vorige uitgaven die mij op foutjes hebben gewezen. In het bijzonder dank aan de politie, Gegevensautoriteit voor het lezen van de tekst. Tot slot: Frank, bedankt voor de prachtige en toch praktische opmaak waarmee ik zelf tot op heden elk jaar aanpassingen heb gedaan zodat het handboek actueel blijft.

Over de auteur

Suzanne Franken

Ik werk als trainer, schrijver en business analist. Vanaf 2008 heb ik me verdiept in de Wpg en sinds 2017 in het bijzonder in de Wpg voor boa's. Zowel overheidsorganisaties als commerciële partijen zijn bij mij aan het juiste adres, vooral voor het verzorgen van trainingen aan allerlei doelgroepen: beleidsmedewerkers, boa-coördinatoren, juristen, privacy-officers, FG's en auditors. Mijn trainingen zijn altijd maatwerk en interactief en ik maak veel gebruik van praktijkvoorbeelden.

In opdracht van de gebruikers van het [systeem BRS](#) heb ik diverse hulpmiddelen ontwikkeld waar in dit handboek naar verwezen wordt. Deze zijn grotendeels vrijuit te gebruiken.

Meer informatie op mijn [website](#) en [LinkedIn-profiel](#).



Optreden op de dag van de boa, 7 december 2020

Auteursrecht en commercieel gebruik

Dit boek is uitgebracht onder een Creative Commons Naamsvermelding Niet Commercieel 4.0 Internationaal licentie (CC BY-NC-ND 4.0).



In de praktijk betekent dit dat ik een vergoeding verwacht voor bepaalde vormen van commercieel gebruik. Ik wil graag een eerlijke vergoeding voor de tijd en energie die ik in dit boek heb gestoken, naar rato van de directe inkomsten die jij ontvangt op basis van het gebruik van mijn werk. Als je dit boek gebruikt als onderdeel van een training die je als commerciële dienst aan derden aanbiedt, of als je dit boek gebruikt als onderdeel van een project dat je bij derden uitvoert, dan creëert het gebruik van mijn werk directe inkomsten voor jou. Dit is in het bijzonder het geval als je (een link naar) mijn boek verspreidt als onderdeel van trainingsmateriaal. De omvang van de vergoeding hangt af van hoe significant mijn werk voor je is, en hoeveel omzet je op basis daarvan realiseert. Omdat ik dat niet kan bepalen, ben ik afhankelijk van jouw eerlijkheid om een passende inschatting te maken van hoeveel mijn werk jou waard is. Neem voor meer informatie, spontane donaties en betaalopties, contact met mij op via suzanne@sfranken.nl.

Bijlage A

Vuistregels

In deze bijlage vind je een aantal belangrijke regels bij elkaar. Gebruik deze als checklist nadat je het boek ten minste een keer hebt gelezen.

- 1 Muteer altijd kort, zakelijk en objectief. Leg zoveel mogelijk redenen van wetenschap vast: wie, wanneer, waar, wat, waarom, hoe verkregen, van wie, et cetera.
- 2 Zorg dat de gegevens die je verwerkt juist, volledig en actueel zijn. Leg niet meer vast dan noodzakelijk voor het doel, voor de taak waar je mee bezig bent.
- 3 Zorg dat duidelijk uit jouw mutatie blijkt of er sprake is van een persoonlijk oordeel of interpretatie, of van een feit.
- 4 Werk altijd in de daarvoor bestemde systemen zoals CityControl en BRS; deze helpen je om conform de wet te werken en gegevens bijvoorbeeld tijdig te verwijderen.
- 5 Verwijder gegevens vanaf gegevensdragers zoals je smartphone of zakboekje zo snel als dat kan. Denk ook aan foto's. Voorkom dat deze gesynchroniseerd worden met een Apple- of Google-server. Vermijd sowieso het gebruik van privé-telefoons of tablets.
- 6 Als je vermoedt dat gegevens onder Wpg artikel 9 verwerkt moeten worden, geef dit dan aan en benader een Bevoegd Functionaris.
- 7 Deel gegevens met andere opsporingsambtenaren (ter beschikking stellen); er geldt een free flow of information in combinatie met het need-to-know-principe voor politie, boa, Kmar en de bijzondere opsporingsdiensten.
- 8 Gebruik geen WhatsApp of andere commerciële apps voor onderlinge communicatie, liever ook niet als het 'slechts' om

gewone gegevens gaat. Gebruik een C2000-portofoon, bel je collega op of gebruik beveiligde e-mails vanuit je werk-account.

- 9 Als je gegevens wilt verstrekken, hanteer dan de Verstrekkingswijzer Wpg voor boa's en leg je verstrekking vast.
- 10 Meld een datalek zo snel mogelijk (uiterlijk binnen 24 uur) binnen je organisatie, ook in geval van twijfel.
- 11 Mocht het nodig zijn om gegevens tijdelijk buiten de informatiesystemen op te slaan op bijvoorbeeld je laptop of op papier, zorg dan dat deze achter slot en grendel worden opgeborgen en laat deze zeker nooit in de auto liggen.

Bijlage B

Afkortingenlijst

AP	Autoriteit Persoonsgegevens
AAVG	Aanpassingswet Algemene verordening gegevensbescherming
AMvB	Algemene maatregel van bestuur
AVG	Algemene verordening gegevensbescherming
BF	Bevoegd functionaris
Bjsg	Besluit justitiële en strafvorderlijke gegevens
Bpg	Besluit politiegegevens
Bpg boa	Besluit politiegegevens boa
Bpg BOD	Besluit politiegegevens bijzondere opsporingsdiensten
CJIB	Centraal Justitieel Incassobureau
DPIA	Data Protection Impact Assessment
FIOD	Fiscale inlichtingen- en opsporingsdienst
FG	Functionaris voor de gegevensbescherming
GEB	gegevensbeschermingseffectbeoordeling
OM	Openbaar Ministerie
RTIC	Real Time Intelligence Center
UAVG	Uitvoeringswet Algemene verordening gegevensbescherming
Wbp	Wet bescherming persoonsgegevens
Wpg	Wet politiegegevens
Wjsg	Wet justitiële en strafvorderlijke gegevens
Woo	Wet open overheid

Bijlage C

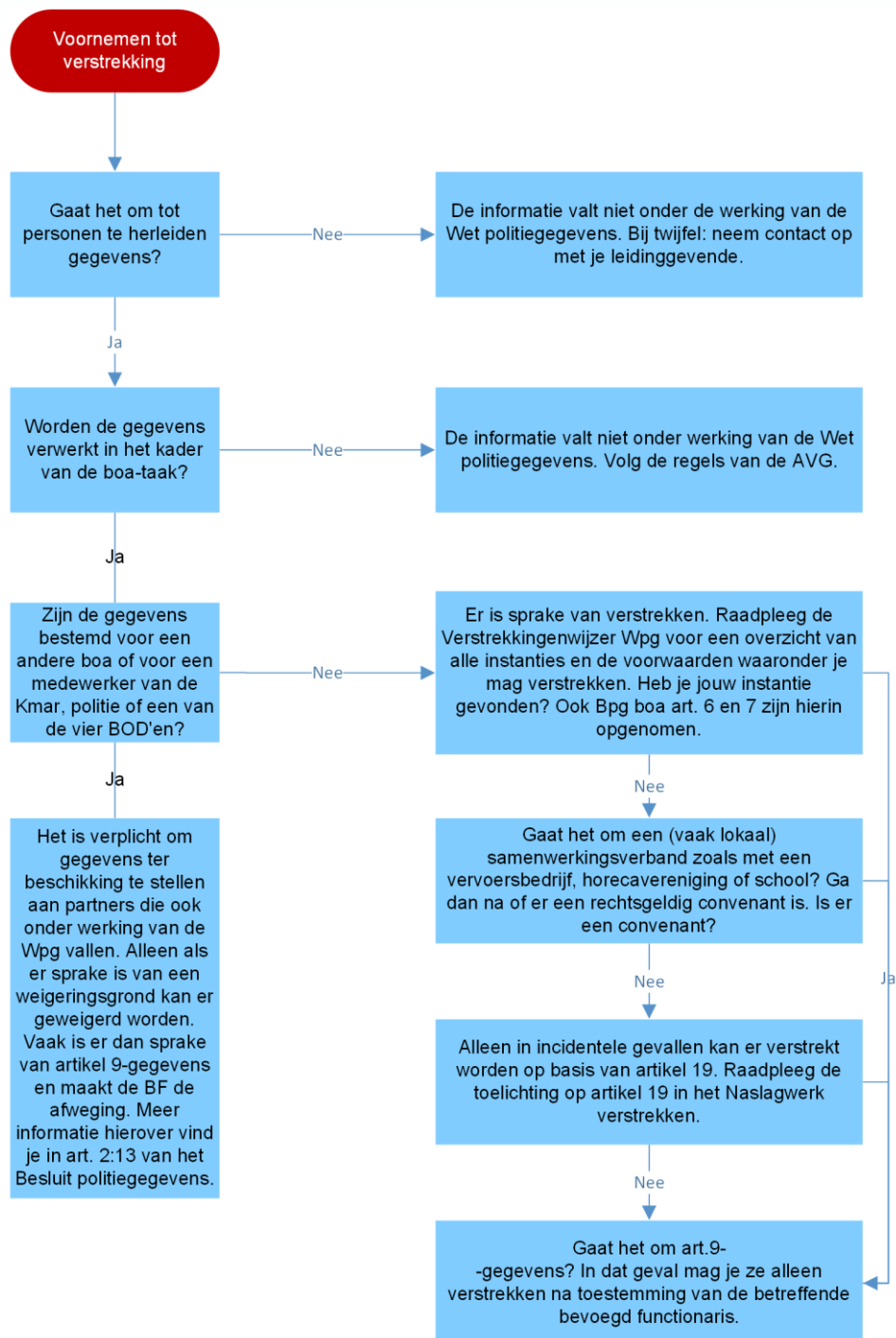
Modelverklaring autorisatie niet-boa

Naam te autoriseren persoon:		
Rol te autoriseren persoon	Stagiair / student / scholier die in het kader van studie of opleiding (bijv. boa opleiding) tijdelijk in een werkproces meedraait of onderzoek verricht	Naam Opleidingsinstituut:
	Uitzendkracht / interim personeel (extern ingehuurd) in dienst bij andere werkgever of zzp'er	Naam werkgever / zzp'er:
	Onderzoeker: iemand van buiten de boa-organisatie die op eigen verzoek of in opdracht politiegegevens nodig heeft voor wetenschappelijk of statistisch onderzoek	Naam werkgever / zzp'er:
	Persoon in dienst van boa-werkgever die ondersteuning biedt bij uitvoering opsporingstaken boa	Naam boa-werkgever
Naam verantwoordelijke boa	Naam en verbalisantennummer van de boa die verantwoordelijk is voor het invoeren en muteren van gegevens door de te autoriseren persoon. Verplicht indien bij soort autorisatie gekozen is voor (onder andere) invoeren of muteren	Naam boa: Verbalisantennummer:
Soort taken / verwerkingen	Het behandelen van bezwaar- of beroepschriften Afhandelen van verzoeken om inzage Verrichten van administratieve werkzaamheden met betrekking tot processen-Verbaal van boa's Verrichten van analyses op opsporingsgegevens Overige administratieve handelingen ter ondersteuning van de boa	
Soort autorisatie	Raadplegen/lezen Invoeren Muteren Verwijderen Verstrekken	
Begindatum autorisatie		
Einddatum autorisatie		
Naam en functie (verwerkingsverantwoordelijke of gemandateerde)		
Datum		

Toelichting: Dit formulier dient te worden ingevuld door de verwerkingsverantwoordelijke (werkgever van de boa) om een niet-boa autorisatie te verlenen voor de verwerking van politiegegevens. In het “Besluit politiegegevens buitengewoon opsporingsambtenaren” (hierna “Bpgboa”, van 6 februari 2019 is een groot deel van de artikelen uit de Wet politiegegevens (“Wpg”) van toepassing verklaard op de gegevensverwerking door een buitengewoon opsporingsambtenaar. Op grond van de Wpg en het Bpgboa onderhoudt de werkgever een systeem van autorisaties voor verwerking van politiegegevens door boa’s voor zover zij politiegegevens nodig hebben voor hun opsporingstaak. Op grond van artikel 6 lid 4 Wpg jo artikel 3 van het Bpg boa is het mogelijk dat de werkgever van de boa personen autoriseert die onder zijn beheer werken, maar geen boa zijn. De nota van toelichting bij artikel 3 Bpg boa noemt de volgende vormen van verwerking: het afhandelen van verzoeken om inzage door de betrokkene, het behandelen van bezwaar- of beroepschriften, het verrichten van administratieve werkzaamheden met betrekking tot processen-verbaal van boa’s – zoals de verzending van gegevens aan het Centraal Justitieel Incasso Bureau (CJIB) – of het verrichten van analyses op opsporingsgegevens. Ook stagiaires van een boa-opleiding kunnen op deze wijze geautoriseerd worden. Zij kunnen bij gesprekken met verdachten en getuigen aanwezig zijn en worden in bepaalde situaties en stages geacht om gegevens te verwerken. Een stagiair zal verwerkingen in het kader van opsporingstaken altijd moeten uitvoeren onder verantwoordelijkheid van de boa, die mutaties (invoeren, muteren, verstrekken) in het systeem moet flatteren. De boa blijft immers verantwoordelijk voor de uitvoering van de opsporingstaken. In het strafproces zal de boa eventueel opgeroepen kunnen worden en de rechter te woord staan, niet de stagiair. Deze boa is in het kader van deze autorisatie de ‘verantwoordelijke boa’.

Bijlage D

Stroomschema verstrekken of ter beschikking stellen



Bijlage E

Instructie scheidingslijn artikel 8- en 9-verwerking

Inleiding

Deze instructie is een hulpmiddel om te kunnen bepalen onder welk doel, artikel 8 of 9 Wpg, gegevens verwerkt moeten worden. De scheidingslijn tussen beide verwerkingsdoelen is niet eenduidig en biedt de boa interpretatieruimte. Om die reden zijn deze richtlijnen opgesteld. Een juiste beoordeling is van belang om te weten welke voorwaarden en verwerkingstermijnen van toepassing zijn op een gegevensverwerking of registratie. Wanneer je een registratie onterecht als art. 8 aanmerkt, dan geldt een verwerkingstermijn van 5 jaar voor deze gegevens. Als je als medewerker een onderzoek te snel als art. 9 aanmerkt, dan levert dat extra administratieve last op. Zo moet er een bevoegd functionaris worden toegekend, het onderzoek moet worden aangemeld en het schonen verloopt anders dan bij een art. 8-verwerking. Tevens geldt dat in BRS artikel 9-verwerkingen grotendeels zijn afgeschermd. Hieronder volgt een algemene omschrijving wat verstaan wordt onder artikel 8 en artikel 9 Wpg.

Richtlijnen artikel 9-verwerking

Hieronder volgen richtlijnen die je kunnen helpen beoordelen of er een artikel 9-verwerking ingesteld moet worden. De richtlijnen zijn weergegeven in volgorde van invloed op de beslissing. Zo is het toepassen van een bijzonder opsporingsbevoegdheid altijd een reden om een onderzoek als artikel 9 te labelen en zal de verwerkingstermijn niet vaak rechtvaardiging zijn, mede omdat er alternatieven zijn die de termijnen verlengen (Art 13, lid 1 onder b Wpg). De richtlijnen zijn mede gebaseerd op de richtlijnen zoals deze bij de politie gelden.

- 1 Als er bijzondere opsporingsmiddelen worden toegepast zoals tappen, gebruik van een (wild) camera (126g SV), of een baken plaatsen.
- 2 Als de verwachting is dat er meer dan 40 uur onderzoek nodig is én het om een strafbaar feit gaat waarvoor voorlopige hechtenis is toegestaan.
- 3 Als er een verkennend onderzoek als bedoeld in artikel 126gg WSV wordt gestart.
- 4 Als er gericht grote hoeveelheden gegevens worden verwerkt over personen of locaties.
- 5 Als er met meerdere opsporingsambtenaren aan een onderzoek gewerkt wordt, bijvoorbeeld samen met de politie.
- 6 Als afscherming van de gegevens gewenst is.
- 7 Als een langere verwerkingstermijn van de gegevens gewenst of te voorzien is. Bijvoorbeeld bij ernstige misdrijven met een onbekende dader.

Toelichting op punt 2

Hier worden twee criteria samen genomen, aangezien een feit waar voorlopige hechtenis op is toegelaten op zichzelf onvoldoende is om de overstap naar artikel 9 te maken. De keuze voor artikel 9 is altijd de keuze van de opsporingsambtenaar zelf; hij kan ook beslissen om pas bij 60 of 80 uur onderzoek de overstap naar 9 te maken. Bij milieuzaken kun je stellen dat als een zaak met een BSBm, een SAM of een verkort misdrijf pv wordt afgedaan, dat je deze dan onder artikel 8 kunt afhandelen. Dit heeft te maken met de criteria waaronder het mogelijk is om voor een dergelijk instrument te kiezen.

Toelichting op punt 4

Een voorbeeld van gericht en omvangrijk gegevens verwerken is wanneer gegevens, die in eerste instantie vanuit de dagelijkse opsporingstaak (art.8) zijn verwerkt, aanleiding geven om een dossier op te bouwen en een persoon als veelpleger te identificeren. Vanaf dat moment worden over die veelpleger gericht allerlei gegevens verzameld en opgenomen in het dossier. Dat betekent het begin van een art.9-verwerking. Een ander voorbeeld is wanneer een analyse wordt gestart omdat er meldingen zijn geweest over ernstige overlast in een woonwijk of afvaldump in een buitengebied. Deze meldingen

komen in eerste instantie voort uit de dagelijkse opsporingstaak (art.8) maar geven nu voldoende aanleiding om gericht allerlei informatie te verzamelen en de probleemsituatie te analyseren.

Toelichting op punt 5

Als er samengewerkt wordt, bijvoorbeeld bij een horeca- of brandweercontrole, en is sprake van strafbare feiten waar meerdere opsporingsambtenaren bij betrokken zijn, dan is het mogelijk om de verwerking als artikel 9 aan te wijzen. Let wel op dat een boa bij dergelijke samenwerkingen vaak als toezichthouder optreedt en een partner zoals de politie de strafbare feiten afhandelt. In dat geval vallen de gegevens die door de toezichthouder worden vastgelegd onder de AVG en niet onder de Wpg. Als er samengewerkt wordt in een grote stroperijzaak of bij een milieudelict op een bedrijventerrein, en de boa levert daadwerkelijk input als boa, dan kan de verwerking als artikel 9 worden aangemerkt.

Toelichting op punt 6

Afschermen van gegevens is niet zonder meer toegestaan. Er wordt te vaak gegrepen naar het middel van afschermen uit angst dat collega's onzorgvuldig omgaan met door de boa vastgelegde gegevens. De Wpg stelt het delen van gegevens verplicht met ieder die onder de Wpg werkt en die gegevens nodig heeft voor zijn werk (artikel 15 Wpg). In lid 2 wordt beschreven dat er een aantal weigeringsgronden zijn die in Bpg Artikel 2:13 verder zijn uitgewerkt. De weigeringsgronden zijn beperkt en limitatief, bijvoorbeeld als er sprake is van een embargo-onderzoek aangewezen door het College van procureurs-generaal, als het gegevens betreft omtrent informanten of als gevaar voor leven of gezondheid van betrokkene te duchten is. Indien er publieke personen betrokken zijn, zou deze laatste als weigeringsgrond aangemerkt kunnen worden. Bijvoorbeeld indien de partner van de burgemeester verdachte is bij een milieudelict of indien een multinational verdachte is en je weet dat de pers er direct op zou duiken indien dit naar bekend wordt. Echter, angst van een boa dat gegevens door collega's geraadpleegd worden voor eigen belang (waar wordt er gecontroleerd op visakten?), of uit sensatiezucht (welke bekende Nederlander is geverbaliseerd voor wildplassen?), is geen reden om de gegevens af te schermen. Het uitgangspunt is dat iedere boa-organisatie een

zorgvuldig integriteitsbeleid hanteert dat voorkomt dat uit nieuwsgierigheid gegevens geraadpleegd worden. Afschermen is daar niet het juiste instrument voor. Daarnaast geldt dat alle verwerkingen gelogd worden, dus jouw handelingen zijn altijd traceerbaar.

Artikel 9, en dan?

Vrijwel elk onderzoek begint als een 8-verwerking. Als een boa zijn onderzoek als artikel 9 aanmerkt, dan dient hij een bevoegd functionaris te benaderen. Elk artikel 9-onderzoek heeft een bevoegd functionaris. Onder diens verantwoordelijkheid worden de gegevens vervolgens verwerkt. Hij bepaalt wie voor dat onderzoek geautoriseerd wordt, hoe de gegevens verwerkt worden en of deze (tijdelijk) worden afgeschermd voor andere gebruikers die in hetzelfde informatiesysteem werken. De taken van de bevoegd functionaris zijn uitgewerkt in het Naslagwerk Bevoegd Functionaris.

Bijlage F

Wet politiegegevens voor boa's

Wet politiegegevens boa's

Onderstaande tekst is een bewerking van de wettekst Wpg, waarbij alleen die artikelen zijn opgenomen die van overeenkomstige toepassing zijn verklaard op de gegevensverwerking door de boa. Vandaar de titel: het is niet de Wpg zoals deze voor de politie en de Kmar geldt, maar een aangepaste versie zoals die voor de boa geldt. Welke artikelen voor de boa gelden, is uitgewerkt in artikel 2 lid 1 van het Bpg boa. Daarnaast gelden voor de boa de extra artikelen zoals beschreven in het Bpg boa.

§1 Algemene bepalingen

Artikel 1. (definities)

In deze wet en de daarop berustende bepalingen wordt verstaan onder:

- a. *politiegegevens*: 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;
- b. *persoonsgegeven*: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon;
- c. *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, 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;
- d. *verstrekken van politiegegevens*: het bekend maken of ter beschikking stellen van politiegegevens;

- e. *ter beschikking stellen van politiegegevens*: het verstrekken van politiegegevens aan personen die overeenkomstig deze wet zijn geautoriseerd voor het verwerken van politiegegevens;
- f. *verwerkingsverantwoordelijke*: dit is bij:
 - 1°. de politie: de korpschef, bedoeld in artikel 27 van de Politiewet 2012;
 - 2°. de rijksrecherche: het College van procureurs-generaal;
 - 3°. de Koninklijke marechaussee: Onze Minister van Defensie;
 - 4°. een gemeenschappelijke verwerking van politiegegevens met het oog op een gemeenschappelijk doel door twee of meer organisaties als bedoeld in dit onderdeel: de verwerkingsverantwoordelijke die door de betrokken verwerkingsverantwoordelijken is belast met de feitelijke zorg voor de verwerking en het treffen van de maatregelen, bedoeld in de artikelen 4 en 4a;
- g. *betrokkene*: degene op wie een politiegegeven betrekking heeft;
- h. *Autoriteit persoonsgegevens*: de autoriteit, bedoeld in artikel 6 van de Uitvoeringswet Algemene verordening gegevensbescherming;
- i. *verwerker*: de natuurlijke persoon of rechtspersoon, overheidsinstantie, dienst of enig ander orgaan die of dat ten behoeve van de verwerkingsverantwoordelijke politiegegevens verwerkt. Indien een verwerker in strijd met het bij of krachtens deze wet bepaalde de doeleinden en middelen van de verwerking bepaalt, wordt die verwerker met betrekking tot die verwerking als verwerkingsverantwoordelijke aangemerkt;
- j. *Onze Ministers*: Onze Ministers van Veiligheid en Justitie en van Defensie gezamenlijk;
- k. *ambtenaar van politie*: de ambtenaar, bedoeld in artikel 2 van de Politiewet 2012, alsmede de ambtenaar van de Koninklijke marechaussee voor zover werkzaam ter uitvoering van de politietaak, bedoeld in onderdeel a, en indien artikel 46 wordt toegepast, de ambtenaar, werkzaam bij de in dat artikel genoemde dienst en de ambtenaar, bedoeld in artikel 142, eerste lid, van het Wetboek van Strafvordering;
- l. *bevoegde autoriteit*: iedere overheidsinstantie die bevoegd is voor de taken, bedoeld in onderdeel a, of ieder ander orgaan dat of iedere andere entiteit die is gemachtigd openbaar gezag en openbare bevoegdheden uit te oefenen met het oog op de taken, bedoeld in onderdeel a;
- m. *gerelateerde gegevens*: de politiegegevens die bij de vergelijking van gegevens, bedoeld in de artikelen 8, tweede lid, 11, eerste en tweede lid, 12, vierde lid en 24, eerste en tweede lid, overeenkomen en de erbij behorende gegevens alsmede de politiegegevens waarmee bij het in combinatie met elkaar verwerken van politiegegevens, bedoeld in de artikelen 8, derde lid, en 11, vierde lid, verband blijkt te bestaan;
- n. *afschermen*: het markeren van opgeslagen politiegegevens met als doel de verwerking ervan in de toekomst te beperken;
- o. *bestand*: elk gestructureerd geheel van politiegegevens dat volgens bepaalde

criteria toegankelijk is, ongeacht of dit geheel van gegevens gecentraliseerd of gedecentraliseerd is, dan wel verspreid op een functioneel of geografisch bepaalde wijze;

- p. *ontvanger*: de natuurlijke persoon aan wie of de rechtspersoon of overheidsinstantie waaraan politiegegevens worden verstrekt;
- q. *inbreuk op de beveiliging*: 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;
- r. *genetische gegevens*: persoonsgegevens met betrekking tot de overgeërfd of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die persoon en die met name voortkomen uit een analyse van een biologisch monster van die persoon;
- s. *biometrische gegevens*: persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische, of gedragskenmerken van een natuurlijke persoon op grond waarvan de eenduidige identificatie van die persoon mogelijk is of bevestigd wordt, zoals afbeeldingen van het gezicht of dactyloscopische gegevens;
- t. *gegevens over gezondheid*: persoonsgegevens met betrekking tot de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten, waarmee informatie over zijn gezondheid wordt gegeven;
- u. *profilering*: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van die gegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met de bedoeling met name aspecten betreffende zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;
- v. *derde land*: ieder land of gebied dat geen lidstaat is of daarvan geen onderdeel uitmaakt;
- w. *internationale organisatie*: een organisatie en de daaronder ressorterende internationaalpubliekrechtelijke organen of andere organen die zijn opgericht bij of op grond van een overeenkomst tussen twee of meer landen;
- x. *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 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 het Kaderbesluit 2008/977/JBZ van de Raad;
- y. *lidstaat*: lidstaat van de Europese Unie die de richtlijn heeft geïmplementeerd.

Artikel 2. (reikwijdte)

1. Deze wet is van toepassing op de verwerking van politiegegevens door een bevoegde autoriteit die in een bestand zijn opgenomen of die bestemd zijn daarin te worden opgenomen.
2. Deze wet is niet van toepassing op de verwerking van politiegegevens:
 - a. ten behoeve van activiteiten met uitsluitend persoonlijke doeleinden;
 - b. ten behoeve van de interne bedrijfsvoering.

Artikel 3. (noodzakelijkheid, rechtmatigheid en doelbinding)

1. Politiegegevens worden slechts verwerkt voor zover dit noodzakelijk is voor de bij of krachtens deze wet geformuleerde doeleinden.
2. Politiegegevens worden slechts verwerkt voor zover dit behoorlijk en rechtmatig is, de gegevens rechtmatig zijn verkregen en de gegevens, gelet op de doeleinden waarvoor zij worden verwerkt, toereikend, terzake dienend en niet bovenmatig zijn.
3. Politiegegevens die zijn verkregen voor een doel, als bedoeld in artikel 1, onderdeel a, kunnen worden verwerkt voor een ander doel, bedoeld in artikel 1, onderdeel a, voor zover deze wet of Unierecht uitdrukkelijk daarin voorziet en de verwerking voor dat andere doel noodzakelijk is en in verhouding staat tot dat doel.
4. Politiegegevens kunnen voor een ander doel dan die, bedoeld in artikel 1, onderdeel a, worden verwerkt door personen en instanties die bij of krachtens de wet met het oog op een zwaarwegend algemeen belang of wetgeving van de Europese Unie zijn aangewezen.
5. Bij de verwerking van politiegegevens op grond van de artikelen 9, 10 en 12 worden de herkomst van deze gegevens en de wijze van verkrijging vermeld.

Artikel 4. (juistheid en volledigheid politiegegevens)

1. De verwerkingsverantwoordelijke treft de nodige maatregelen opdat politiegegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn. Hij zorgt voor het onverwijld vernietigen of rectificeren van politiegegevens als blijkt dat deze, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn. De bevoegde autoriteit controleert, voor zover praktisch uitvoerbaar, de kwaliteit van politiegegevens voordat de gegevens worden verstrekt. Voor zover mogelijk wordt bij de doorzending van politiegegevens de noodzakelijke informatie toegevoegd aan de hand waarvan de ontvangende bevoegde autoriteit de mate van juistheid, volledigheid en betrouwbaarheid van politiegegevens kan beoordelen, alsmede de mate waarin zij actueel zijn.
2. De verwerkingsverantwoordelijke treft de nodige maatregelen opdat politiegegevens worden verwijderd of vernietigd zodra zij niet langer noodzakelijk zijn voor het doel waarvoor zij zijn verwerkt of dit door enige

wettelijke bepaling wordt vereist.

3. Voor zover mogelijk worden politiegegevens die op feiten zijn gebaseerd onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd.
4. Indien wordt vastgesteld dat onjuiste politiegegevens zijn verstrekt, of dat de politiegegevens op onrechtmatige wijze zijn verstrekt, wordt de ontvanger daarvan onverwijld in kennis gesteld. In dat geval dienen de gegevens te worden gerectificeerd of vernietigd, of wordt de verwerking beperkt, als bedoeld in artikel 28, tweede lid.

Artikel 4a. (gegevensbescherming door beveiliging en ontwerp)

1. De verwerkingsverantwoordelijke en de verwerker treffen passende technische en organisatorische maatregelen om:
 - a. te waarborgen en te kunnen aantonen dat de verwerking van politiegegevens wordt verricht in overeenstemming met hetgeen bij of krachtens deze wet is bepaald;
 - b. het gegevensbeschermingsbeleid en de gegevensbeschermingsbeginselen op een doeltreffende manier uit te voeren respectievelijk toe te passen;
 - c. bij de bepaling van de verwerkingsmiddelen en de verwerking zelf de nodige waarborgen, zoals pseudonimisering, in de verwerking in te bouwen ter naleving van hetgeen bij of krachtens deze wet is bepaald en ter bescherming van de rechten van de betrokkenen.
2. De verwerkingsverantwoordelijke en de verwerker treffen passende technische en organisatorische maatregelen om een beveiligingsniveau te waarborgen dat op het risico is afgestemd, met name met betrekking tot de verwerking van de bijzondere categorieën van politiegegevens, bedoeld in artikel 5, en op een zodanige manier dat de politiegegevens beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging.
3. Bij het treffen van de maatregelen, bedoeld in het eerste en tweede lid, houden de verwerkingsverantwoordelijke en de verwerker rekening met de aard, de reikwijdte, de context en de doeleinden van de verwerking, alsmede met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen.
4. In aanvulling op het derde lid houden de verwerkingsverantwoordelijke en de verwerker ten aanzien van het eerste lid, onder c, en het tweede lid, rekening met de stand van de techniek en de uitvoeringskosten.
5. De maatregelen, bedoeld in het eerste en tweede lid, worden periodiek geëvalueerd en zo nodig geactualiseerd.
6. Bij of krachtens algemene maatregel van bestuur worden nadere regels gesteld over de maatregelen, bedoeld in het eerste en tweede lid.

Artikel 4b. (gegevensbescherming door standaardinstellingen)

1. De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard:
 - a. alleen die politiegegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking; en
 - b. politiegegevens niet zonder tussenkomst van een natuurlijke persoon voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.
2. De in het eerste lid, onder a, bedoelde maatregelen betreffen in ieder geval de hoeveelheid verzamelde politiegegevens, de mate waarin zij worden verwerkt, de periode van opslag en de toegankelijkheid van de politiegegevens.

Artikel 4c. (gegevensbeschermingseffectbeoordeling)

1. Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context of doelen ervan, waarschijnlijk een hoog risico voor de rechten en vrijheden van personen oplevert, voert de verwerkingsverantwoordelijke voorafgaande aan de verwerking een beoordeling uit van het effect van de voorgenomen verwerkingsactiviteiten op de bescherming van persoonsgegevens.
2. De beoordeling bevat tenminste:
 - a. een algemene beschrijving van de beoogde verwerkingen;
 - b. een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
 - c. de beoogde maatregelen ter beperking van de risico's;
 - d. de voorzorgs- en beveiligingsmaatregelen en mechanismen om de 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.
3. Indien nodig verricht de verwerkingsverantwoordelijke een toetsing om te beoordelen of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling wordt uitgevoerd, zulks ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden.

Artikel 5. (bijzondere categorieën van politiegegevens)

De verwerking van politiegegevens waaruit ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakbond blijkt, en de verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, of gegevens over gezondheid, seksuele leven en seksuele gerichtheid vindt slechts plaats wanneer dit onvermijdelijk is voor het doel van de verwerking, in aanvulling op de verwerking van andere politiegegevens betreffende de persoon en de gegevens afdoende zijn beveiligd.

Artikel 6. (autorisaties)

1. De verwerkingsverantwoordelijke onderhoudt een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid.
2. Politiegegevens worden slechts verwerkt door ambtenaren van politie die zijn belast met de taken bedoeld in artikel 1, onderdeel a die daartoe door de verwerkingsverantwoordelijke zijn geautoriseerd en voor zover de autorisatie strekt.
3. De verwerkingsverantwoordelijke autoriseert de ambtenaren van politie die onder zijn beheer vallen voor de verwerking van politiegegevens ter uitvoering van de onderdelen van de politietaak waarmee zij zijn belast. De autorisatie bevat een duidelijke omschrijving van de verwerkingen waartoe de betreffende ambtenaar wordt geautoriseerd en de onderdelen van de politietaak ter uitvoering waarvan de verwerkingen worden gedaan.
4. In bijzondere gevallen kan de verwerkingsverantwoordelijke personen die geen ambtenaar van politie zijn en die onder zijn beheer vallen, autoriseren voor de verwerking van politiegegevens ter uitvoering van de onderdelen van de politietaak waarmee zij zijn belast.
5. In bijzondere gevallen kan de verwerkingsverantwoordelijke de ambtenaar van politie die onder het beheer van een andere verwerkingsverantwoordelijke valt, autoriseren voor de verwerking van politiegegevens ter uitvoering van in de autorisatie omschreven onderdelen van de politietaak. De verwerking van politiegegevens vindt in dat geval plaats onder het beheer van de verwerkingsverantwoordelijke die de autorisatie heeft verleend.
6. Bij of krachtens algemene maatregel van bestuur worden nadere regels gesteld over de categorieën van personen die voor bepaalde gegevensverwerkingen geautoriseerd kunnen worden en de deskundigheidseisen die aan hen kunnen worden gesteld.
7. De verwerkingsverantwoordelijke wijst de functionaris aan, bedoeld in artikel 9, derde lid, 10, vijfde lid, 11, eerste, tweede en vierde lid, 12, vierde en vijfde lid, en 13, derde lid. Bij algemene maatregel van bestuur kunnen regels worden gesteld over de ambtenaren van politie die kunnen worden aangewezen als functionaris.

Artikel 6a. (toegang tot politiegegevens)

1. De verwerkingsverantwoordelijke heeft toegang tot de politiegegevens die onder zijn beheer worden verwerkt ten behoeve van het toezicht op de naleving van het bij of krachtens deze wet bepaalde.
2. De verwerkingsverantwoordelijke verleent de ambtenaren van politie die onder zijn beheer vallen en die zijn belast met de taken, bedoeld in artikel 1, onderdeel a, toegang tot de politiegegevens die onder zijn beheer worden verwerkt, voor zover nodig voor de uitvoering van hun taak.

3. De verwerkingsverantwoordelijke verleent de verwerker, bedoeld in artikel 6c, eerste lid, alsmede degenen die belast zijn met de controle en het toezicht, bedoeld in de artikelen 33, 34, 35 en 36, alsmede degenen die in zijn opdracht technische werkzaamheden verrichten, toegang tot de politiegegevens die onder zijn beheer worden verwerkt, voor zover zij deze behoeven voor de uitvoering van hun taak.

Artikel 6b. (onderscheid tussen verschillende categorieën van betrokkenen)

De verwerkingsverantwoordelijke maakt in voorkomend geval en voor zover mogelijk een duidelijk onderscheid tussen politiegegevens betreffende verschillende categorieën van betrokkenen, zoals:

- a. personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen gaan plegen;
- b. slachtoffers van een strafbaar feit, of personen ten aanzien van wie op basis van bepaalde feiten wordt vermoed dat zij slachtoffer kunnen worden van een strafbaar feit;
- c. derden, zoals getuigen of personen die anderszins informatie kunnen verstrekken over strafbare feiten, of personen die contact hebben of banden onderhouden met één van de personen, bedoeld onder a of d;
- d. personen die voor een strafbaar feit zijn veroordeeld.

Artikel 6c. (verwerker)

1. Indien de verwerkingsverantwoordelijke politiegegevens te zijnen behoeve laat verwerken door een verwerker maakt hij uitsluitend gebruik van een verwerker die afdoende garandeert dat de passende technische en organisatorische maatregelen en procedures zodanig worden geïmplementeerd dat bij de verwerking wordt voldaan aan het bij of krachtens deze wet bepaalde en de rechten van de betrokkene worden gewaarborgd.
2. De uitvoering van verwerkingen door een verwerker wordt geregeld in een schriftelijke overeenkomst of andere rechtshandeling die de verwerker aan de verwerkingsverantwoordelijke bindt. Bij of krachtens algemene maatregel van bestuur worden nadere regels gesteld over de inhoud van de overeenkomst of rechtshandeling.
3. De verwerker en eenieder die handelt onder het beheer van de verwerkingsverantwoordelijke of van de verwerker verwerkt de politiegegevens uitsluitend volgens de instructies van de verwerkingsverantwoordelijke, tenzij hij op grond van de nationale wetgeving of Unierecht tot die verwerking verplicht is.
4. De verwerker neemt geen andere verwerker in dienst dan na voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke. In het geval van een algemene schriftelijke toestemming informeert de verwerker de

verwerkingsverantwoordelijke over de toevoeging of vervanging van andere verwerkers, met de mogelijkheid van bezwaar door de verwerkingsverantwoordelijke.

5. De verwerker stelt de verwerkingsverantwoordelijke zonder onnodige vertraging in kennis van een inbreuk op de beveiliging.

Artikel 7. (geheimhoudingsplicht)

1. De ambtenaar van politie of de persoon aan wie politiegegevens ter beschikking zijn gesteld is verplicht tot geheimhouding daarvan behoudens voor zover een bij of krachtens de wet gegeven voorschrift tot verstrekking verplicht, de bepalingen van paragraaf 3 verstrekking toelaten of de taak, bedoeld in artikel 1, onderdeel a in bijzondere gevallen tot verstrekking noodzaakt.
2. De persoon aan wie politiegegevens zijn verstrekt is verplicht tot geheimhouding daarvan behoudens voor zover een bij of krachtens de wet gegeven voorschrift tot verstrekking verplicht of zijn taak daartoe noodzaakt.
3. Artikel 272, tweede lid, van het Wetboek van Strafrecht is niet van toepassing.

Artikel 7a (geautomatiseerde individuele besluitvorming)

1. Een besluit dat uitsluitend op geautomatiseerde verwerking is gebaseerd, met inbegrip van profilering, dat voor de betrokkene nadelige rechtsgevolgen heeft of hem in aanmerkelijke mate treft, is verboden, tenzij wordt voorzien in voorafgaande menselijke tussenkomst door of namens de verwerkingsverantwoordelijke en in specifieke voorlichting aan de betrokkene.
2. Een besluit, bedoeld in het eerste lid, wordt niet gebaseerd op de categorieën van politiegegevens, bedoeld in artikel 5, tenzij de Autoriteit persoonsgegevens over de voorgenomen verwerking is geraadpleegd, overeenkomstig artikel 33b, eerste lid.
3. Profilering die leidt tot discriminatie van personen op grond van de in artikel 5 bedoelde categorieën van politiegegevens is verboden.

§2 De verwerking van politiegegevens met het oog op de uitvoering van de politietaak

Artikel 8. (uitvoering van de dagelijkse politietaak)

1. Politiegegevens kunnen worden verwerkt met het oog op de uitvoering van de dagelijkse politietaak gedurende een periode van één jaar na de datum van de eerste verwerking.
2. Voor zover dat noodzakelijk is met het oog op de uitvoering van de dagelijkse politietaak kunnen politiegegevens ten aanzien waarvan de in het eerste lid genoemde termijn is verstreken geautomatiseerd worden vergeleken met

politiegegevens die worden verwerkt op grond van het eerste lid teneinde vast te stellen of verbanden bestaan tussen de betreffende gegevens. De gerelateerde gegevens kunnen verder worden verwerkt met het oog op de uitvoering van de dagelijkse politietaak.

3. Voor zover dat noodzakelijk is met het oog op de uitvoering van de dagelijkse politietaak kunnen politiegegevens ten aanzien waarvan de in het eerste lid genoemde termijn is verstreken in combinatie met elkaar worden verwerkt teneinde vast te stellen of verbanden bestaan tussen de betreffende gegevens. Indien zulke verbanden bestaan kunnen de gerelateerde gegevens verder worden verwerkt met het oog op de uitvoering van de politietaak.
4. Politiegegevens, die worden verwerkt op grond van het eerste, tweede en derde lid, kunnen ter beschikking worden gesteld voor verdere verwerking op grond van de artikelen 9, 10 en 12.
5. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld over de categorieën van gegevens op basis waarvan politiegegevens vergeleken kunnen worden.
6. De politiegegevens, die zijn verwerkt op grond van het eerste, tweede en derde lid, worden vernietigd zodra zij niet langer noodzakelijk zijn voor de uitvoering van de dagelijkse politietaak en worden in ieder geval uiterlijk vijf jaar na de datum van eerste verwerking verwijderd.

Artikel 9. (onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval)

1. Politiegegevens kunnen gericht worden verwerkt ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval.
2. Het doel van het onderzoek wordt binnen een week, nadat is begonnen met de verwerking, bedoeld in het eerste lid, schriftelijk vastgelegd.
3. Politiegegevens die worden verwerkt overeenkomstig het eerste lid, kunnen, na instemming van een daartoe bevoegde functionaris, ter beschikking worden gesteld voor verdere verwerking voor zover dat noodzakelijk is voor een ander onderzoek als bedoeld in het eerste lid, de verwerking, bedoeld in de artikelen 10 en 12, of de uitvoering van de dagelijkse politietaak, bedoeld in artikel 8.
4. De politiegegevens die zijn verwerkt op grond van het eerste lid en niet langer noodzakelijk zijn voor het doel van het onderzoek, worden verwijderd, of gedurende een periode van maximaal een half jaar verwerkt teneinde te bezien of zij aanleiding geven tot een nieuw onderzoek als bedoeld in het eerste lid of een nieuwe verwerking als bedoeld in artikel 10, en na verloop van deze termijn verwijderd.

Artikel 11. (geautomatiseerd vergelijken en in combinatie zoeken, art. 11 lid 2 n.v.t. Bpg boa)

1. Voor zover dat noodzakelijk is voor een onderzoek als bedoeld in artikel 9, eerste lid, kunnen politiegegevens die voor dat onderzoek zijn verwerkt, geautomatiseerd worden vergeleken met andere politiegegevens die worden verwerkt op grond van artikel 8 of 9 teneinde vast te stellen of verbanden bestaan tussen de betreffende gegevens. De gerelateerde gegevens kunnen, na instemming van een daartoe bevoegde functionaris, voor dat onderzoek verder worden verwerkt.
3. Bij of krachtens algemene maatregel van bestuur worden regels gesteld over de uitvoering van de gegevensvergelijking. Deze regels kunnen betrekking hebben op:
 - a. de categorieën van gegevens op basis waarvan politiegegevens vergeleken kunnen worden;
 - b. het coderen van politiegegevens door deze te voorzien van een indicatie over betrouwbaarheid en vertrouwelijkheid en de mogelijkheid deze verder te verwerken voor een onderzoek als bedoeld in artikel 9 of een verwerking als bedoeld in artikel 10;
 - c. de wijze waarop de verbanden zichtbaar gemaakt worden.
4. Voor zover dat noodzakelijk is voor een onderzoek als bedoeld in artikel 9, eerste lid, of een verwerking als omschreven in artikel 10, eerste lid, kunnen in bijzondere gevallen in opdracht van het bevoegd gezag, bedoeld in de artikelen 11, 12 en 14 van de Politiewet 2012, politiegegevens die worden verwerkt op grond van artikel 8, 9 of 10 in combinatie met elkaar worden verwerkt teneinde vast te stellen of verbanden bestaan tussen de gegevens. Indien zulke verbanden bestaan kunnen de gerelateerde gegevens, na instemming van een daartoe bevoegde functionaris, voor dat onderzoek of die verwerking verder worden verwerkt.
5. Voor zover dat noodzakelijk is voor een onderzoek als bedoeld in artikel 9, eerste lid, of een verwerking als omschreven in artikel 10, eerste lid, kunnen politiegegevens die worden verwerkt op grond van artikel 8, 9 of 10 geautomatiseerd worden vergeleken met andere dan politiegegevens.

Artikel 13. (ondersteunende taken)

1. Ten behoeve van de ondersteuning van de taak, bedoeld in artikel 1, onder a kunnen de politiegegevens die worden verwerkt overeenkomstig artikel 8, 9 en 10, verder worden verwerkt voor zover zij relevant zijn voor:
 - a. het vaststellen van eerdere verwerkingen ten aanzien van eenzelfde persoon of zaak, onder meer ter bepaling van eerdere betrokkenheid bij strafbare feiten;
 - b. het ophelderen van strafbare feiten die nog niet herleid konden worden tot een verdachte;
 - c. identificatie van personen of zaken;
 - d. het onder de aandacht brengen van personen of zaken met het oog op het uitvoeren van een gevraagde handeling danwel met het oog op een juiste bejegening van personen;
 - e. het uitvoeren van taken ten dienste van de justitie.
2. Ten behoeve van de ondersteuning van de taak, bedoeld in artikel 1, onderdeel a kunnen de politiegegevens die worden verwerkt overeenkomstig artikel 8, 9 of 10 door een verwerkingsverantwoordelijke centraal verder worden verwerkt voor zover zij relevant zijn voor het verkrijgen van landelijk inzicht in specialistische onderwerpen. De verder verwerkte gegevens worden ter beschikking gesteld aan door een verwerkingsverantwoordelijke geautoriseerde personen voor zover zij deze behoeven voor de uitvoering van de taak bedoeld in artikel 1, onder a.
3. Ten behoeve van de ondersteuning van de taak bedoeld in artikel 1, onderdeel a, worden de politiegegevens die overeenkomstig artikel 8, 9 en 10 worden verwerkt, voor zover zij relevant zijn voor geautomatiseerde vergelijking met het oog op de melding van verschillende verwerkingen jegens eenzelfde persoon, daarvoor ter beschikking gesteld en verder verwerkt. De gerelateerde gegevens kunnen, na instemming van een daartoe bevoegde functionaris, verder worden verwerkt op grond van artikel 8, 9 of 10.
4. Bij algemene maatregel van bestuur worden regels gesteld over hetgeen met het oog op de in het eerste, tweede en derde lid bedoelde verwerkingen tevoren schriftelijk wordt vastgelegd en ter inzage gelegd. In ieder geval worden regels gesteld over de schriftelijke vastlegging van:
 - a. het specifieke doel ten behoeve waarvan de gegevens ter ondersteuning van de taak, bedoeld in artikel 1, onderdeel a, verder worden verwerkt;
 - b. de categorieën van personen over wie gegevens ten behoeve van het betreffende doel verder worden verwerkt en de soorten van de over hen op te nemen gegevens;
 - c. de gevallen waarin of de termijnen waarbinnen het verder verwerken van de betreffende gegevens wordt beëindigd.

Artikel 14. (bewaartermijnen)

1. De op grond van de artikelen 8, zesde lid, 9, vierde lid, en artikel 10, zesde lid, verwijderde politiegegevens worden gedurende een termijn van vijf jaar bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen en vervolgens vernietigd.
2. De artikelen 16 tot en met 20 alsmede de artikelen 23 en 24 zijn op de overeenkomstig het eerste lid bewaarde politiegegevens niet van toepassing.
3. In bijzondere gevallen en voor zover dat noodzakelijk is voor een doel als bedoeld in artikel 9 of 10, kunnen politiegegevens die overeenkomstig het eerste lid worden bewaard, in opdracht van het bevoegd gezag, bedoeld in de artikelen 11, 12 en 14 van de Politiewet 2012, ter beschikking worden gesteld voor hernieuwde verwerking op grond van artikel 9 of 10.
4. Van de vernietiging, bedoeld in het eerste lid, wordt afgezien voor zover de waarde van de archiefbescheiden als bestanddeel van het cultureel erfgoed of voor historisch onderzoek zich daartegen verzet. De betreffende gegevens worden zo spoedig mogelijk overgebracht naar een archiefbewaarplaats. Daarbij worden met toepassing van artikel 15 van de Archiefwet 1995 beperkingen aan de openbaarheid gesteld. Onze Ministers kunnen over het in de eerste en derde volzin bepaalde beleidsregels vaststellen.

Artikel 15. (ter beschikking stellen van politiegegevens)

1. De verwerkingsverantwoordelijke stelt politiegegevens ter beschikking aan personen die door hemzelf dan wel door een andere verwerkingsverantwoordelijke overeenkomstig artikel 6, tweede lid, zijn geautoriseerd voor de verwerking van politiegegevens, voor zover zij deze behoeven voor de uitvoering van hun taak.
2. In bijzondere gevallen kan, indien dit noodzakelijk is voor een goede uitvoering van de taak, bedoeld in artikel 1, onderdeel a, de terbeschikkingstelling van politiegegevens door de verwerkingsverantwoordelijke worden geweigerd dan wel kan de verwerkingsverantwoordelijke beperkende voorwaarden stellen aan de verdere verwerking. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld over de gronden waarop de terbeschikkingstelling kan worden geweigerd en over de beperkende voorwaarden die kunnen worden gesteld.

Artikel 15a. (ter beschikkingstelling binnen Europese Unie)

1. Politiegegevens worden of kunnen worden ter beschikking gesteld aan de bevoegde autoriteiten in andere lidstaten van de Europese Unie of aan organen en instanties die zijn opgericht krachtens de hoofdstukken 4 en 5 van Titel V van het verdrag betreffende de werking van de Europese Unie, die zijn belast met de taken, bedoeld in artikel 1, onderdeel a, voor zover dat voortvloeit uit een rechtsinstrument op grond van het verdrag betreffende de werking van de Europese Unie.

2. Bij algemene maatregel van bestuur worden nadere regels gesteld over de ter beschikkingstelling van politiegegevens, bedoeld in het eerste lid, alsmede over de verdere verwerking en de daarbij te stellen voorwaarden aan het gebruik daarvan door ontvangstgerechtigde autoriteiten of internationale organen en instanties, en over de ontvangst van politiegegevens vanuit andere lidstaten van de Europese Unie. Onverminderd specifieke voorzieningen in een rechtsinstrument, bedoeld in het eerste lid, mogen de voorwaarden niet afwijken van de voorwaarden voor vergelijkbare doorzendingen van politiegegevens binnen het Europese deel van Nederland.

§3 De doorgifte of verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee

Artikel 16. (verstrekking aan gezagsdragers)

1. De verwerkingsverantwoordelijke verstrekt politiegegevens aan:
 - a. leden van het openbaar ministerie voor zover zij deze behoeven:
 - 1°. in verband met hun gezag of zeggenschap over de politie of over andere personen of instanties die met de opsporing van strafbare feiten zijn belast, of
 - 2°. voor de uitvoering van andere hun bij of krachtens de wet opgedragen taken;
 - b. de burgemeesters voor zover zij deze behoeven:
 - 2°. in het kader van de handhaving van de openbare orde.
 - c. de verwerkingsverantwoordelijke voor zover hij deze behoeft in verband met:
 - 1°. het verrichten van een onderzoek naar aanleiding van klachten, als bedoeld in artikel 70 van de Politiewet 2012 en artikel 14 van de Wet op de bijzondere opsporingsdiensten, of
 - 2°. disciplinaire bestraffing vanwege niet-nakoming van verplichtingen of plichtsverzuim, als geregeld bij of krachtens artikel 47 van de Politiewet 2012 en de regelgeving die van toepassing is op de aanstelling of arbeidsovereenkomst van de opsporingsambtenaar, bedoeld in artikel 141, onderdeel d, van het Wetboek van Strafvordering, of
 - 3°. schorsing of ontslag van de ambtenaar van de Koninklijke marechaussee voor zover werkzaam ter uitvoering van de politietaken, bedoeld in artikel 4, eerste lid, onderdelen a, b, c, d, e, g en h van de Politiewet 2012 vanwege niet nakoming van verplichtingen of plichtsverzuim als geregeld bij of krachtens artikel 12 van de Wet ambtenaren defensie, of
 - 4°. het verrichten van een onderzoek naar de betrouwbaarheid als bedoeld in artikel 48q, eerste lid, 48s, tweede lid, of 48x, eerste en tweede lid, van de Politiewet 2012.
2. Op de verstrekkingen, bedoeld in het eerste lid, onderdeel c, is artikel 15, tweede lid, van overeenkomstige toepassing.

Artikel 17. (verstrekking aan inlichtingendiensten)

Politiegegevens kunnen worden verstrekt voor zover dit voortvloeit uit de Wet op de inlichtingen- en veiligheidsdiensten 2017.

Artikel 17a. (doorgiften aan derde landen)

1. Politiegegevens kunnen met inachtneming van het bij of krachtens deze wet bepaalde worden doorgegeven aan een verwerkingsverantwoordelijke in een derde land of aan een internationale organisatie, voor zover dit noodzakelijk is voor de doeleinden, bedoeld in artikel 1, onderdeel a, en indien de Commissie van de Europese Unie heeft besloten dat het derde land of de internationale organisatie een toereikend beschermingsniveau voor de voorgenomen gegevensverwerking verzekert.
2. Bij ontstentenis van een besluit van de Commissie, bedoeld in het eerste lid, kunnen politiegegevens worden verstrekt of doorgegeven indien:
 - a. in een juridisch bindend instrument passende waarborgen voor de bescherming van persoonsgegevens zijn geboden; of
 - b. de verwerkingsverantwoordelijke na beoordeling van alle omstandigheden heeft geconcludeerd dat het derde land of de internationale organisatie passende waarborgen biedt voor de bescherming van persoonsgegevens. De verantwoordelijke informeert de Autoriteit persoonsgegevens over de categorieën van doorgifte op grond van dit onderdeel.
3. Bij ontstentenis van een besluit van de Commissie, bedoeld in het eerste lid, of van passende waarborgen, bedoeld in het tweede lid, is een doorgifte of een categorie van doorgiften van politiegegevens aan een derde land of internationale organisatie slechts toegelaten indien de doorgifte noodzakelijk is:
 - a. om een vitaal belang van de betrokkene of van een andere persoon te beschermen;
 - b. is om de gerechtvaardigde belangen van de betrokkene te beschermen, wanneer het recht van de lidstaat van waaruit de doorgifte van politiegegevens plaatsvindt aldus bepaalt;
 - c. is om een onmiddellijk en ernstig gevaar voor de openbare veiligheid van een lidstaat of derde land te voorkomen;
 - d. in afzonderlijke gevallen met het oog op de uitvoering van de taak, bedoeld in artikel 1, onderdeel a;
 - e. in afzonderlijke gevallen met het oog op het instellen, uitoefenen of verdedigen van rechtsvorderingen in verband met de uitvoering van de taak, bedoeld in artikel 1, onderdeel a, en de grondrechten en fundamentele vrijheden van de betrokkene niet prevaleren boven het algemeen belang van de doorgifte, bedoeld in de onderdelen d en e.
4. In het geval de doorgifte, bedoeld in het eerste, tweede en derde lid en onverminderd een internationale overeenkomst tussen lidstaten en derde landen, politiegegevens betreft die van een andere lidstaat afkomstig zijn, is onverminderd deze leden toestemming van de bevoegde autoriteit uit die lidstaat vereist voor doorgifte, tenzij de doorgifte noodzakelijk is met het oog op het voorkomen van een onmiddellijk en ernstig gevaar voor de openbare

veiligheid van een lidstaat of een derde land of voor de fundamentele belangen van een lidstaat, en voorafgaande toestemming niet tijdig kan worden verkregen. De voor het geven van voorafgaande toestemming verantwoordelijke autoriteit wordt onverwijld in kennis gesteld.

5. In afwijking van het eerste, tweede en derde lid, en onverminderd een van kracht zijnde bilaterale of multilaterale internationale overeenkomst tussen lidstaten en derde landen op het gebied van justitiële samenwerking in strafzaken en politieke samenwerking kunnen in afzonderlijke en specifieke gevallen politiegegevens worden doorgegeven aan een ontvanger in een derde land, zonder tussenkomst van een bevoegde autoriteit in dat land, indien de doorgifte strikt noodzakelijk is voor de uitvoering van de taak, bedoeld in artikel 1, onderdeel a, en indien aan de volgende voorwaarden is voldaan:
 - a. de doorgifte is strikt noodzakelijk voor de uitvoering van een in het Unierecht of het lidstatelijke recht omschreven taak van de bevoegde autoriteit die de doorgifte doet, ter verwezenlijking van de doeleinden van artikel 1, eerste lid, van de richtlijn;
 - b. de bevoegde autoriteit die de doorgifte doet, bepaalt dat er geen grondrechten en fundamentele vrijheden van de betrokkene zijn die zwaarder wegen dan het openbaar belang dat de doorgifte in dat specifieke geval noodzakelijk maakt;
 - c. de bevoegde autoriteit die de doorgifte doet, is van mening dat de doorgifte aan een autoriteit die in het derde land bevoegd is voor de in artikel 1, eerste lid, van de richtlijn, bedoelde doeleinden, ondoeltreffend of ongeschikt is, met name omdat de doorgifte niet tijdig kan worden bewerkstelligd;
 - d. de autoriteit die in het derde land bevoegd is voor de in artikel 1, eerste lid, bedoelde doeleinden wordt zonder onnodige vertraging op de hoogte gebracht, tenzij dit ondoeltreffend of ongeschikt is;
 - e. de bevoegde autoriteit die de doorgifte doet, licht de ontvanger in over het nader bepaalde doel of de nader bepaalde doeleinden waarvoor de persoonsgegevens bij uitsluiting door laatstgenoemde mogen worden verwerkt, op voorwaarde dat een dergelijke verwerking noodzakelijk is.
6. Politiegegevens kunnen door een derde land of internationale organisatie verder worden doorgegeven aan een ander derde land of een andere internationale organisatie, indien de bevoegde autoriteit toestemming verleent voor die verdere doorgifte, na alle relevante factoren naar behoren in aanmerking te hebben genomen, waaronder de ernst van het strafbare feit, het doel waarvoor de gegevens oorspronkelijk waren doorgegeven en het niveau van gegevensbescherming in het derde land of de internationale organisatie waaraan de persoonsgegevens verder worden doorgegeven.
7. Bij algemene maatregel van bestuur worden nadere regels gesteld over de doorgifte van politiegegevens, bedoeld in het eerste, tweede, derde en zesde lid, alsmede over de verdere verwerking en de daarbij te stellen voorwaarden aan het gebruik daarvan door ontvangstgerechtigde autoriteiten of internationale organen, en over de ontvangst van politiegegevens vanuit derde landen.

Artikel 18. (verstrekking aan derden structureel)

1. Bij of krachtens algemene maatregel van bestuur kunnen personen en instanties worden aangewezen aan wie of waaraan, met het oog op een zwaarwegend algemeen belang, politiegegevens worden of kunnen worden verstrekt ter uitvoering van de bij of krachtens die algemene maatregel van bestuur aan te geven taak.
2. In bijzondere gevallen kan Onze Minister van Veiligheid en Justitie toestemming of opdracht geven tot het verstrekken van daarbij door hem te omschrijven politiegegevens voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang. Van de desbetreffende beschikking wordt mededeling gedaan aan de Autoriteit persoonsgegevens.

Artikel 19. (verstrekking aan derden incidenteel)

In bijzondere gevallen kan de verwerkingsverantwoordelijke, voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, in overeenstemming met het bevoegd gezag, bedoeld in de artikelen 11, 12 en 14 van de Politiewet 2012, beslissen tot het verstrekken van politiegegevens aan personen of instanties voor de volgende doeleinden:

- a. het voorkomen en opsporen van strafbare feiten;
- b. het handhaven van de openbare orde;
- c. het verlenen van hulp aan hen die deze behoeven;
- d. het uitoefenen van toezicht op het naleven van regelgeving.

Artikel 20. (verstrekking aan derden structureel voor samenwerkingsverbanden)

1. De verwerkingsverantwoordelijke kan, voor zover dit met het oog op een zwaarwegend algemeen belang noodzakelijk is ten behoeve van een samenwerkingsverband van de bevoegde autoriteiten met personen of instanties, in overeenstemming met het bevoegd gezag, bedoeld in de artikelen 11, 12 en 14 van de Politiewet 2012, beslissen tot het verstrekken van politiegegevens aan die personen en instanties voor de volgende doeleinden:
 - a. het voorkomen en opsporen van strafbare feiten;
 - b. het handhaven van de openbare orde;
 - c. het verlenen van hulp aan hen die deze behoeven;
 - d. het uitoefenen van toezicht op het naleven van regelgeving.
2. In de beslissing, bedoeld in het eerste lid, wordt vastgelegd ten behoeve van welk zwaarwegend algemeen belang de verstrekking noodzakelijk is, ten behoeve van welk samenwerkingsverband de politiegegevens worden verstrekt, alsmede het doel waartoe dit is opgericht, welke gegevens worden verstrekt, de voorwaarden onder welke de gegevens worden verstrekt en aan welke personen of instanties de gegevens worden verstrekt.

Artikel 21. (nadere regels bij algemene maatregel van bestuur)

Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld over de categorieën van politiegegevens die worden of kunnen worden verstrekt op grond van de artikelen 18, 19 en 20.

Artikel 22. (verwerking voor wetenschappelijk onderzoek en statistiek)

1. Politiegegevens kunnen worden verwerkt ten behoeve van beleidsinformatie, wetenschappelijk onderzoek of statistiek met het oog op de taak, bedoeld in artikel 1, onderdeel a, onder de voorwaarde dat de resultaten daarvan geen persoonsgegevens mogen bevatten.
2. Bij algemene maatregel van bestuur worden nadere regels gesteld over de verstrekking van politiegegevens ten behoeve van het bepaalde in het eerste lid.

Artikel 23. (rechtstreekse verstrekking)

1. Verstrekking van politiegegevens aan de leden van het openbaar ministerie als bedoeld in artikel 16, eerste lid, onderdeel a, kan rechtstreeks plaatsvinden voor zover noodzakelijk met het oog op:
 - a. strafvorderlijke beslissingen omtrent opsporing en vervolging en de hulp aan slachtoffers van strafbare feiten;
 - b. bij algemene maatregel van bestuur aan te wijzen beslissingen.
2. Verstrekking van politiegegevens als bedoeld in artikel 18 vindt alleen rechtstreeks plaats aan bij algemene maatregel van bestuur aangewezen personen of instanties met een publiekrechtelijke taak door middel van geautomatiseerde vergelijking van persoonsgegevens met bij algemene maatregel van bestuur aan te wijzen categorieën van politiegegevens.
3. Aan de korpschef, bedoeld in artikel 27 van de Politiewet 2012 en aan de Minister van Defensie kan verstrekking van politiegegevens als bedoeld in artikel 18 rechtstreeks plaatsvinden voor zover noodzakelijk met het oog op het uitvoeren van hun bij algemene maatregel van bestuur aangewezen wettelijke taken.
4. De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen teneinde te waarborgen dat rechtstreekse verstrekking uitsluitend plaatsvindt voor zover noodzakelijk op grond van het bepaalde bij of krachtens het eerste, tweede en derde lid. Bij algemene maatregel van bestuur kunnen hierover nadere regels worden gesteld

Artikel 23a

1. Verstrekking van politiegegevens aan de verwerkingsverantwoordelijke als bedoeld in artikel 16, eerste lid, onderdeel c, kan rechtstreeks plaatsvinden.
2. Verstrekking van politiegegevens aan de verwerkingsverantwoordelijke ten behoeve van de uitvoering van de artikelen 91 en 94 van de Wet op de

inlichtingen- en veiligheidsdiensten 2017 kan rechtstreeks plaatsvinden.

3. Artikel 23, vierde lid, is van overeenkomstige toepassing.

Artikel 24. (rechtstreekse verstrekking aan inlichtingen- en veiligheidsdiensten)

1. Voor zover dat noodzakelijk is voor de uitvoering van de taak, bedoeld in artikel 8, tweede lid, van de Wet op de inlichtingen- en veiligheidsdiensten 2017 *[wijziging als gevolg van Stb. 2017, 317 – Wiv 2017]*, kunnen door de Algemene Inlichtingen- en Veiligheidsdienst verwerkte gegevens rechtstreeks geautomatiseerd worden vergeleken met bij algemene maatregel van bestuur, op voordracht van Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties en Onze Minister van Veiligheid en Justitie gezamenlijk, te bepalen categorieën van politiegegevens teneinde vast te stellen of verbanden bestaan tussen de betreffende gegevens. De gerelateerde gegevens kunnen daarvoor rechtstreeks worden verstrekt aan ambtenaren werkzaam bij de Algemene Inlichtingen- en Veiligheidsdienst waarbij in bepaalde, door een lid van het College van procureurs-generaal en de Directeur-Generaal van de Algemene Inlichtingen- en Veiligheidsdienst gezamenlijk vast te stellen gevallen, op een gezamenlijk vast te stellen wijze, daarvan kennis wordt gegeven aan het lid van het openbaar ministerie als bedoeld in artikel 66 van de Wet op de inlichtingen- en veiligheidsdiensten 2017.
2. Voor zover dat noodzakelijk is voor de uitvoering van de taak, bedoeld in artikel 10, tweede lid, van de Wet op de inlichtingen- en veiligheidsdiensten 2017 *[wijziging als gevolg van Stb. 2017, 317 – Wiv 2017]*, kunnen door de Militaire Inlichtingen- en Veiligheidsdienst verwerkte gegevens rechtstreeks geautomatiseerd worden vergeleken met bij algemene maatregel van bestuur, op voordracht van Onze Minister van Defensie en Onze Minister van Veiligheid en Justitie gezamenlijk, te bepalen categorieën van politiegegevens teneinde vast te stellen of verbanden bestaan tussen de betreffende gegevens. De gerelateerde gegevens kunnen daarvoor rechtstreeks worden verstrekt aan ambtenaren werkzaam bij de Militaire Inlichtingen- en Veiligheidsdienst waarbij in bepaalde, door een lid van het College van procureurs-generaal en het hoofd van de Militaire Inlichtingen- en Veiligheidsdienst gezamenlijk vast te stellen gevallen, op een gezamenlijk vast te stellen wijze, daarvan kennis wordt gegeven aan het lid van het openbaar ministerie als bedoeld in artikel 66 van de Wet op de inlichtingen- en veiligheidsdiensten 2017.
3. Artikel 23, vierde lid, is van overeenkomstige toepassing.

§ 4. Rechten van de betrokkene

Artikel 24a. (informatie aan de betrokkene)

1. De verwerkingsverantwoordelijke verstrekt aan de betrokkene informatie over de verwerking van politiegegevens in een beknopte en toegankelijke vorm en in duidelijke en eenvoudige taal. De informatie wordt met passende middelen, waaronder elektronische, verstrekt en in het algemeen in dezelfde vorm als de vorm van het verzoek.
2. Indien de betrokkene verzoekt om inzage, op grond van artikel 25, eerste lid, of rectificatie, bedoeld in artikel 28, eerste lid, wordt hij schriftelijk en zonder onnodige vertraging in kennis gesteld van de ontvangst van het verzoek, de termijn voor uitsluitel en de mogelijkheid om naar aanleiding daarvan een klacht in te dienen bij de Autoriteit persoonsgegevens.
3. De verstrekking van de informatie, bedoeld in de artikelen 7a, 24b, 25, eerste lid, 28, 33a, vijfde lid, geschiedt kosteloos.
4. In het geval van een kennelijk ongegrond of buitensporig verzoek, met name vanwege de geringe tussenpozen tussen opeenvolgende verzoeken, kan de verwerkingsverantwoordelijke weigeren gevolg te geven aan het verzoek.
5. De verstrekking van informatie, bedoeld in de artikelen 24b, 25, eerste lid, en 28, vindt plaats overeenkomstig de artikelen 30 tot en met 34 van het Wetboek van Strafvordering als de gegevens in een processtuk worden verwerkt.

Artikel 24b. (verstrekking van informatie aan de betrokkene)

1. De verwerkingsverantwoordelijke verstrekt in elk geval de volgende informatie aan de betrokkene:
 - a. de identiteit en contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de functionaris voor gegevensbescherming;
 - b. de verwerkingsdoelen van de politiegegevens;
 - c. de rechten van de betrokkene, bedoeld in de artikelen 25, eerste lid, en 28, eerste en tweede lid;
 - d. het recht een klacht in te dienen bij de Autoriteit persoonsgegevens, en de contactgegevens van die autoriteit.
2. In specifieke gevallen verstrekt de verwerkingsverantwoordelijke de volgende informatie aan de betrokkene:
 - a. de rechtsgrondslag van de verwerking;
 - b. de bewaartermijn van de politiegegevens;
 - c. in voorkomend geval, de categorieën van de ontvangers van de politiegegevens;
 - d. indien noodzakelijk, extra informatie, in het bijzonder wanneer de politiegegevens zonder medeweten van de betrokkene worden verzameld;
 - e. het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 7a, eerste lid, bedoelde profilering, en nuttige informatie over de

onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

3. De verwerkingsverantwoordelijke kan de verstrekking van informatie, als bedoeld in het tweede lid, uitstellen, beperken of achterwege laten voor zover dit een noodzakelijke en evenredige maatregel is in verband met een belang, bedoeld in artikel 27, eerste lid, onderdelen a tot en met e.
4. Het tweede lid is niet van toepassing ten aanzien van de verwerking van gegevens van personen, bedoeld in artikel 6b, onder a.

Artikel 25. (recht op inzage)

1. De betrokkene heeft het recht om op diens schriftelijke verzoek van de verwerkingsverantwoordelijke binnen zes weken uitsluitend te verkrijgen over de verwerking van hem betreffende persoonsgegevens en, wanneer dat het geval is, om die persoonsgegevens in te zien en om informatie te verkrijgen over:
 - a. de doelen en de rechtsgrond van de verwerking;
 - b. de betrokken categorieën van politiegegevens;
 - c. de vraag of de deze persoon betreffende politiegegevens gedurende een periode van vier jaar voorafgaande aan het verzoek zijn verstrekt en over de ontvangers of categorieën van ontvangers aan wie de gegevens zijn verstrekt, met name ontvangers in derde landen of internationale organisaties;
 - d. de voorziene periode van opslag of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
 - e. het recht te verzoeken om rectificatie, vernietiging of afscherming van de verwerking van hem betreffende politiegegevens;
 - f. het recht een klacht in te dienen bij de Autoriteit persoonsgegevens, en de contactgegevens van die autoriteit;
 - g. de herkomst, voor zover beschikbaar, van de verwerking van hem betreffende politiegegevens.
2. De verwerkingsverantwoordelijke kan zijn beslissing voor ten hoogste vier weken verdagen, dan wel voor ten hoogste zes weken indien blijkt dat bij verschillende regionale eenheden of bij de landelijke eenheid van de politie politiegegevens over de verzoeker worden verwerkt. Van de verdaging wordt schriftelijk mededeling gedaan.

Artikel 26. (formaliteiten)

1. Bij de behandeling van verzoeken als bedoeld in de artikelen 25 en 28 draagt de verwerkingsverantwoordelijke zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker. Wanneer de verwerkingsverantwoordelijke redenen heeft om te twifelen aan de identiteit van de persoon die het verzoek doet, kan hij de nodige aanvullende informatie vragen ter bevestiging van de identiteit van de betrokkene.
2. De verzoeken ten aanzien van minderjarigen die de leeftijd van zestien jaren nog niet hebben bereikt, en ten aanzien van onder curatele gestelden worden

gedaan door hun wettelijk vertegenwoordigers. De betrokken mededeling geschiedt eveneens aan de wettelijk vertegenwoordigers.

3. De verzoeken kunnen tevens worden gedaan door een advocaat aan wie de betrokkene een bijzondere machtiging heeft verleend met het oog op de uitoefening van zijn rechten krachtens deze wet en die het verzoek uitsluitend doet met de bedoeling de belangen van zijn cliënt te behartigen. De betrokken mededeling geschiedt aan de advocaat. De verwerkingsverantwoordelijke kan aan de bijzondere machtiging eisen stellen.

Artikel 27. (uitzonderingen)

1. Een verzoek als bedoeld in de artikelen 25, eerste lid, en 28, eerste en tweede lid, wordt afgewezen voor zover dit een noodzakelijke en evenredige maatregel is:
 - 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 veiligheid;
 - d. ter bescherming van de rechten en vrijheden van derden;
 - e. ter bescherming van de nationale veiligheid;
 - f. ingeval van een kennelijk ongegrond of buitensporig verzoek, als bedoeld in artikel 24a, vierde lid.
2. Een gehele of gedeeltelijke afwijzing van een verzoek als bedoeld in het eerste lid is schriftelijk en bevat de redenen voor de afwijzing.
3. Een verzoek als bedoeld in de artikelen 25, eerste lid, en 28, eerste lid, wordt afgewezen als het verzoek de gegevens betreft, die worden verwerkt bij of krachtens artikel 12.

Artikel 28. (recht op rectificatie en vernietiging van politiegegevens)

1. De betrokkene heeft het recht op diens schriftelijke verzoek van de verwerkingsverantwoordelijke rectificatie van de hem betreffende onjuiste politiegegevens te verkrijgen en, rekening houdend met het doel van de verwerking, het recht om onvolledige politiegegevens te laten aanvullen, onder meer door middel van een aanvullende verklaring. Het verzoek bevat de aan te brengen wijzigingen.
2. De betrokkene heeft het recht op diens schriftelijke verzoek van de verwerkingsverantwoordelijke zonder onnodige vertraging vernietiging van de hem betreffende politiegegevens te verkrijgen indien de gegevens in strijd met een wettelijk voorschrift worden verwerkt of om te voldoen aan een wettelijke verplichting. In plaats van vernietiging draagt de verwerkingsverantwoordelijke zorg voor afscherming als:
 - a. de juistheid van de gegevens door de betrokkene wordt betwist en de juistheid of onjuistheid niet kan worden geverifieerd, in welk geval de

- verwerkingsverantwoordelijke de betrokkene informeert voordat de afscherming wordt opgeheven, of
- b. de gegevens moeten worden bewaard als bewijsmateriaal.
3. De verwerkingsverantwoordelijke stelt de betrokkene binnen vier weken schriftelijk in kennis met betrekking tot de opvolging van zijn verzoek.
 4. De verwerkingsverantwoordelijke geeft de rectificatie van de onjuiste politiegegevens door aan de bevoegde autoriteit van wie de gegevens afkomstig zijn.
 5. Indien de verwerkingsverantwoordelijke politiegegevens heeft gerectificeerd, vernietigd of afgeschermd, stelt hij de ontvangers daarvan in kennis.

§ 4a. Rechtsbescherming

Artikel 29. (toepasselijkheid Awb)

1. Een beslissing op een verzoek als bedoeld in artikel 25 of 28 geldt als een besluit in de zin van de Algemene wet bestuursrecht.
2. De belanghebbende kan zich binnen de termijn bepaald voor het beroep op grond van de Algemene wet bestuursrecht tot de Autoriteit persoonsgegevens wenden met het verzoek te bemiddelen of te adviseren in zijn geschil met de verwerkingsverantwoordelijke. In dat geval kan in afwijking van artikel 6:7 van de Algemene wet bestuursrecht het beroep nog worden ingesteld nadat de belanghebbende van de Autoriteit persoonsgegevens bericht heeft ontvangen dat de behandeling van de zaak is beëindigd, doch uiterlijk zes weken na dat tijdstip.
3. In klachtprocedures waarbij de verwerkingsverantwoordelijke of onder zijn verantwoordelijkheid werkzame personen ingevolge artikel 9:31 van de Algemene wet bestuursrecht worden verplicht tot het verstrekken van inlichtingen of het overleggen van stukken aan de Nationale ombudsman met betrekking tot politiegegevens die zijn te herleiden tot een informant als bedoeld in artikel 12, zevende lid, kan Onze Minister van Veiligheid en Justitie beslissen dat artikel 9:31, vijfde en zesde lid, van die wet buiten toepassing blijft.
4. Indien Onze Minister van Veiligheid en Justitie heeft beslist dat artikel 9:31, vijfde en zesde lid, van de Algemene wet bestuursrecht buiten toepassing blijft en de verwerkingsverantwoordelijke of onder zijn verantwoordelijkheid werkzame personen worden verplicht tot het overleggen van stukken, wordt volstaan met het ter inzage geven van de desbetreffende stukken. Van de desbetreffende stukken wordt op generlei wijze een afschrift vervaardigd.
5. In procedures inzake beslissingen als bedoeld in het eerste lid waarbij de verwerkingsverantwoordelijke of onder zijn verantwoordelijkheid werkzame personen ingevolge artikel 8:27, 8:28 of 8:45 van de Algemene wet bestuursrecht worden verplicht tot het verstrekken van inlichtingen of het overleggen van stukken met betrekking tot politiegegevens die zijn te herleiden

tot een informant als bedoeld in artikel 12, zevende lid, kan Onze Minister van Veiligheid en Justitie beslissen dat artikel 8:29, derde tot en met vijfde lid, van die wet buiten toepassing blijft. Indien aan de rechtbank stukken dienen te worden overgelegd, wordt alsdan met het ter inzage geven van de desbetreffende stukken volstaan. Van de desbetreffende stukken wordt op generlei wijze een afschrift vervaardigd. Indien Onze Minister van Veiligheid en Justitie de rechtbank mededeelt dat uitsluitend zij kennis zal mogen nemen van de inlichtingen onderscheidenlijk de stukken, kan de rechtbank slechts met toestemming van de andere partijen mede op grondslag van die inlichtingen of stukken uitspraak doen.

Artikel 31a. (klacht bij Autoriteit persoonsgegevens)

1. Onverminderd bestaande rechtsmiddelen heeft iedere betrokkene het recht een klacht in te dienen bij de Autoriteit persoonsgegevens indien de betrokkene van mening is dat de verwerking van hem betreffende persoonsgegevens niet in overeenstemming is met het bij of krachtens deze wet bepaalde.
2. Indien de Autoriteit persoonsgegevens niet bevoegd is op grond van artikel 35, eerste lid, zendt zij de klacht zonder onnodige vertraging door aan de autoriteit in een andere lidstaat van de Europese Unie die bevoegd is tot het uitoefenen van het toezicht, bedoeld in artikel 35, eerste lid. De betrokkene wordt van de doorzending in kennis gesteld.
3. Op verzoek van de betrokkene verleent de Autoriteit persoonsgegevens verdere bijstand.
4. De Autoriteit persoonsgegevens faciliteert het indienen van klachten door maatregelen te nemen, zoals het ter beschikking stellen van een klachtformulier dat ook elektronisch kan worden ingevuld, zonder dat andere communicatiemiddelen worden uitgesloten.
5. De Autoriteit persoonsgegevens neemt binnen drie maanden een beslissing op een klacht als bedoeld in het eerste lid. Een beslissing op een klacht geldt als een besluit in de zin van de Algemene wet bestuursrecht.
6. In het geval van een kennelijk ongegronde of buitensporige klacht, met name vanwege de geringe tussenpozen tussen klachten, kan de Autoriteit persoonsgegevens weigeren gevolg te geven aan de klacht.

Artikel 31b. (rechtsvordering tegen Autoriteit persoonsgegevens)

Een vordering tegen de Autoriteit persoonsgegevens wordt ingesteld bij een gerecht, bedoeld in artikel 2 van de Wet op de rechterlijke organisatie, in Nederland.

Artikel 31c (schadevergoeding)

1. Indien iemand schade lijdt doordat ten opzichte van hem in strijd wordt gehandeld met de bij of krachtens deze wet gegeven voorschriften zijn de volgende leden van toepassing, onverminderd de aanspraken op grond van

andere wettelijke regels.

2. Voor nadeel dat niet in vermogensschade bestaat, heeft de benadeelde recht op een naar billijkheid vast te stellen schadevergoeding.
3. De verwerkingsverantwoordelijke is aansprakelijk voor de schade of het nadeel, voortvloeiende uit het niet-nakomen van de in het eerste lid bedoelde voorschriften. De verwerker is aansprakelijk voor die schade of dat nadeel, voor zover ontstaan door zijn werkzaamheid.
4. De verwerkingsverantwoordelijke of de verwerker kan geheel of gedeeltelijk worden ontheven van deze aansprakelijkheid, indien hij bewijst dat de schade hem niet kan worden toegerekend.

§ 5. Controle en toezicht op de gegevensverwerking

Artikel 31d. (register)

1. De verwerkingsverantwoordelijke houdt een register bij dat de volgende gegevens bevat:
 - a. de naam en de contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de functionaris voor gegevensbescherming;
 - b. de doelen van de verwerking;
 - c. de categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties;
 - d. een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
 - e. in voorkomend geval, het gebruik van profilering;
 - f. in voorkomend geval, de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie;
 - g. een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de politiegegevens bedoeld zijn;
 - h. zo mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd;
 - i. zo mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging, bedoeld in artikel 4a;
 - j. de toekenning van de autorisaties, bedoeld in artikel 6.
2. De verwerker houdt een register bij dat de volgende gegevens bevat:
 - a. de naam en de contactgegevens van de verwerker of verwerkers en van iedere verwerkingsverantwoordelijke ten behoeve van wie de verwerker handelt en, in voorkomend geval, van de functionaris voor gegevensbescherming;
 - b. de categorieën van verwerkingen die namens iedere verwerkingsverantwoordelijke zijn uitgevoerd;
 - c. indien van toepassing, doorgiften van politiegegevens aan een derde land

- of een internationale organisatie, onder vermelding van dat derde land of die internationale organisatie, indien door de verwerkingsverantwoordelijke uitdrukkelijk daartoe geïnstrueerd;
- d. indien mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen, bedoeld in artikel 4a.

Artikel 32. (documentatie)

1. De verwerkingsverantwoordelijke draagt zorg voor de schriftelijke vastlegging van:
 - a. de doelen van de onderzoeken, bedoeld in artikel 9, tweede lid;
 - b. de verstrekking of doorgifte van politiegegevens op grond van paragraaf 3, met uitzondering van de verstrekking, bedoeld in artikel 17 en artikel 24, eerste en tweede lid, indien dit zich niet verdraagt met het belang van de veiligheid van de staat;
 - c. de feitelijke of juridische redenen die ten grondslag liggen aan een afwijzing, bedoeld in artikel 27, eerste lid;
 - d. een inbreuk op de beveiliging van persoonsgegevens, bedoeld in artikel 33a, inclusief de feiten omtrent de inbreuk, de gevolgen ervan en de maatregelen die zijn getroffen ter correctie.
2. Bij de doorgifte van politiegegevens aan een verwerkingsverantwoordelijke in een derde land of aan een internationale organisatie, bedoeld in artikel 17a, tweede lid, onderdeel b, en derde lid, omvat de schriftelijke vastlegging de datum en tijd van doorgifte, informatie over de ontvangende bevoegde autoriteit, de reden van doorgifte en de doorgegeven gegevens zelf.
3. De verantwoordelijke draagt zorg voor de schriftelijke melding van een gemeenschappelijke verwerking van politiegegevens aan de Autoriteit persoonsgegevens.
4. De politiegegevens, bedoeld in het eerste lid, worden bewaard tenminste tot de datum waarop de laatste controle, bedoeld in artikel 33, is verricht.
5. Bij of krachtens algemene maatregel van bestuur worden nadere regels gesteld over de wijze van vastlegging.

Artikel 32a. (logging)

1. De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de vastlegging langs elektronische weg (logging) van ten minste de volgende verwerkingen van politiegegevens in geautomatiseerde systemen: het verzamelen, wijzigen, raadplegen, verstrekken onder meer in de vorm van doorgiften, combineren of vernietigen van politiegegevens.
2. De vastgelegde gegevens, bedoeld in het eerste lid, worden uitsluitend gebruikt voor de controle van de rechtmatigheid van de gegevensverwerking, voor interne controles, ter waarborging van de integriteit en de beveiliging van de politiegegevens en voor strafrechtelijke procedures.

Artikel 33. (audits)

1. De verwerkingsverantwoordelijke doet de uitvoering van de bij of krachtens deze wet gegeven regels controleren door middel van het periodiek doen verrichten van privacy audits.
2. De verwerkingsverantwoordelijke zendt een afschrift van de controleresultaten van de privacy audits aan de Autoriteit persoonsgegevens.
3. Indien uit de controleresultaten blijkt dat niet wordt voldaan aan het bij of krachtens deze wet bepaalde, laat de verwerkingsverantwoordelijke binnen een jaar een hercontrole uitvoeren op die onderdelen die niet voldeden aan de gestelde voorwaarden. Het tweede lid is van overeenkomstige toepassing.
4. Een ieder die betrokken is bij een controle als bedoeld in het eerste of derde lid is verplicht tot geheimhouding van de persoonsgegevens waarover hij de beschikking heeft gekregen, behoudens voor zover enig wettelijk voorschrift hem tot mededeling verplicht of zijn taak daartoe noodzaakt.
5. Bij of krachtens algemene maatregel van bestuur worden nadere regels gesteld betreffende de inhoud en wijze van uitvoering van de controles, bedoeld in het eerste en derde lid.

Artikel 33a. (melding datalekken)

1. De verwerkingsverantwoordelijke meldt een inbreuk op de beveiliging onverwijld en uiterlijk binnen 72 uur nadat hij ervan heeft kennis genomen aan de Autoriteit persoonsgegevens, tenzij het niet waarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van personen met zich meebrengt. In het geval de melding na 72 uur wordt gedaan, gaat deze vergezeld van een motivering voor de vertraging.
2. De melding, bedoeld in het eerste lid, bevat ten minste de volgende informatie:
 - a. een beschrijving van de aard en omvang van de inbreuk, bedoeld in het eerste lid, waaronder begrepen, waar mogelijk, de categorieën van betrokkenen en van gegevensbestanden en, bij benadering, het aantal betrokkenen en gegevensbestanden;
 - b. de mededeling van de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
 - c. een beschrijving van de waarschijnlijke gevolgen van de inbreuk, bedoeld in het eerste lid;
 - d. een beschrijving van de voorgestelde of uitgevoerde maatregelen om de inbreuk, bedoeld in het eerste lid, te beëindigen en, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen ervan.
3. Voor zover het niet mogelijk is de informatie, bedoeld in het tweede lid, gelijktijdig te verstrekken, kan deze zonder onnodige vertraging in stappen worden verstrekt.
4. De verwerkingsverantwoordelijke deelt een inbreuk op de beveiliging van politiegegevens, die zijn doorgezonden door of aan een

verwerkingsverantwoordelijke van een andere lidstaat, zonder onnodige vertraging mee aan de verwerkingsverantwoordelijke van deze lidstaat.

5. De verwerkingsverantwoordelijke deelt een inbreuk op de beveiliging mede aan de betrokkenen als deze inbreuk waarschijnlijk een hoog risico voor de rechten en vrijheden van personen met zich meebrengt. De mededeling bevat een omschrijving van de aard van de inbreuk op de beveiliging en ten minste de informatie, bedoeld in het tweede lid, onderdelen b, c en d.
6. De mededeling aan de betrokkenen, bedoeld in het vijfde lid, is niet vereist wanneer:
 - a. de verwerkingsverantwoordelijke passende technische en organisatorische beschermingsmaatregelen heeft getroffen en deze maatregelen zijn toegepast op de politiegegevens waarop de inbreuk, bedoeld in het eerste lid, betrekking heeft;
 - b. de verwerkingsverantwoordelijke maatregelen heeft getroffen om ervoor te zorgen dat het hoge risico, bedoeld in het vijfde lid, zich waarschijnlijk niet meer zal voordoen, of
 - c. de mededeling een onevenredige inspanning zou vergen. In dat geval volgt een openbare mededeling of vergelijkbare maatregel waarmee de betrokkenen even doeltreffend worden geïnformeerd.
7. De mededeling aan de betrokkene kan worden uitgesteld, beperkt of achterwege gelaten op de gronden, bedoeld in artikel 27, tweede lid.

Artikel 33b. (voorafgaand raadplegen Autoriteit persoonsgegevens)

1. De Autoriteit persoonsgegevens wordt door de verwerkingsverantwoordelijke of de verwerker geraadpleegd over de voorgenomen verwerking van politiegegevens die in een nieuw bestand zullen worden opgenomen, wanneer:
 - a. 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;
 - b. uit een gegevensbeschermingseffectbeoordeling, bedoeld in artikel 4c, eerste lid, blijkt dat de verwerking een hoog risico zou opleveren als de verwerkingsverantwoordelijke geen maatregelen treft om het risico te beperken.
2. De Autoriteit persoonsgegevens kan een lijst opstellen van de verwerkingen waarvoor raadpleging, overeenkomstig het eerste lid, vereist is.
3. De verwerkingsverantwoordelijke verstrekt de Autoriteit persoonsgegevens de gegevensbeschermingseffectbeoordeling, bedoeld in artikel 4c, en, desgevraagd, alle andere informatie op grond waarvan de Autoriteit persoonsgegevens de conformiteit van de verwerking en met name de risico's voor de bescherming van persoonsgegevens van de betrokkene en de betrokken waarborgen kan beoordelen.

4. Wanneer de Autoriteit persoonsgegevens van oordeel is dat de voorgenomen verwerking van politiegegevens, bedoeld in het eerste lid, niet voldoet aan het bij of krachtens deze wet bepaalde, geeft zij binnen een termijn van ten hoogste zes weken schriftelijk advies aan de verwerkingsverantwoordelijke en, in voorkomend geval, aan de verwerker.
5. De termijn, bedoeld in het vierde lid, kan, rekening houdend met de complexiteit van de voorgenomen verwerking, worden verlengd met een maand. In dit geval wordt de verwerkingsverantwoordelijke en, in voorkomend geval, de verwerker, binnen een maand na de ontvangst van het verzoek in kennis gesteld van de verlenging en de redenen daarvoor.

Artikel 35. (toezicht Autoriteit persoonsgegevens)

1. De Autoriteit persoonsgegevens, bedoeld in artikel 6, eerste lid, van de Uitvoeringswet Algemene verordening gegevensbescherming, ziet in het Europese deel van Nederland toe op de verwerking van politiegegevens overeenkomstig het bij en krachtens deze wet bepaalde.
2. Artikel 16 van de Uitvoeringswet Algemene verordening gegevensbescherming is van overeenkomstige toepassing.

Artikel 35a. (positie Autoriteit persoonsgegevens)

1. De Autoriteit persoonsgegevens treedt bij de uitvoering van haar taken en de uitoefening van haar bevoegdheden volledig onafhankelijk op.
2. Ieder lid van de Autoriteit persoonsgegevens beschikt over de nodige kwalificaties, ervaring en vaardigheden, met name op het gebied van de bescherming van persoonsgegevens, voor het uitvoeren van zijn taken en het uitoefenen van zijn bevoegdheden.
3. De leden van de Autoriteit persoonsgegevens blijven vrij van al dan niet rechtstreekse externe invloed en vragen noch aanvaarden instructies van wie dan ook bij de uitvoering van hun taken en de uitoefening van hun bevoegdheden overeenkomstig deze paragraaf.
4. De leden van de Autoriteit persoonsgegevens onthouden zich van alle handelingen die onverenigbaar zijn met hun taken en verrichten gedurende hun ambtstermijn geen al dan niet bezoldigde beroepswerkzaamheden die onverenigbaar zijn met hun taken.

Artikel 35b. (taken Autoriteit persoonsgegevens)

1. De Autoriteit persoonsgegevens heeft tot taak:
 - a. het toezien op de verwerking van persoonsgegevens overeenkomstig het bij of krachtens deze wet bepaalde en het handhaven daarvan;
 - b. het geven van advies over voorstellen van wet en ontwerpen van algemene maatregelen van bestuur die geheel of voor een belangrijk deel betrekking hebben op de verwerking van persoonsgegevens;

- c. het beter bekend maken van het brede publiek met, en verschaffen van meer inzicht in de risico's, de regels, de waarborgen en de rechten in verband met de verwerking van persoonsgegevens;
 - d. het beter bekend maken van de verwerkingsverantwoordelijken en de verwerkers met hun verplichtingen uit hoofde van het bij of krachtens deze wet bepaalde;
 - e. het desgevraagd verstrekken van informatie aan iedere betrokkene over de uitoefening van zijn rechten uit hoofde van het bij of krachtens deze wet bepaalde en het, in voorkomend geval, daartoe samenwerken met de autoriteiten in andere lidstaten, bedoeld in artikel 35d, eerste lid, die zijn belast met het toezicht;
 - f. het behandelen van klachten van betrokkenen, of van organen, organisaties of verenigingen die de betrokkene vertegenwoordigen, het onderzoeken van de inhoud van de klacht en de klager binnen een redelijke termijn in kennis stellen van de voortgang en het resultaat van het onderzoek, met name indien verder onderzoek of coördinatie met een andere toezichthoudende autoriteit nodig is;
 - g. het naar aanleiding van een klacht, bedoeld in artikel 31a, eerste lid, controleren van de rechtmatigheid van de verwerking en de betrokkene binnen een redelijke termijn informeren over het resultaat van de controle of van de redenen waarom de controle niet is verricht;
 - h. het samenwerken met andere autoriteiten die zijn belast met het toezicht, bedoeld in artikel 35d, eerste lid, teneinde voor de samenhang in de toepassing en de handhaving van het bij of krachtens deze wet bepaalde te zorgen, onder meer door informatie te delen en wederzijdse bijstand aan te bieden;
 - i. het verrichten van onderzoeken naar de naleving van het bij of krachtens deze wet bepaalde, ook op basis van informatie die de Autoriteit persoonsgegevens ontvangt van een andere autoriteit die is belast met het toezicht, bedoeld in artikel 35, eerste lid, of een andere overheidsinstantie;
 - j. het volgen van de relevante ontwikkelingen voor zover deze de bescherming van persoonsgegevens beïnvloeden, met name de ontwikkeling van de informatie- en communicatietechnologieën;
 - k. het verstrekken van advies naar aanleiding van een voorafgaande raadpleging, bedoeld in artikel 33b, eerste lid, en
 - l. het leveren van een bijdrage aan de activiteiten van het Comité, opgericht bij Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.
2. De Autoriteit persoonsgegevens verricht haar taken kosteloos voor de betrokkene en voor de functionaris voor gegevensbescherming.

Artikel 35c. (bevoegdheden Autoriteit persoonsgegevens)

1. De Autoriteit persoonsgegevens is bevoegd:
 - a. de verwerkingsverantwoordelijke of de verwerker te waarschuwen dat met de voorgenomen verwerkingen waarschijnlijk een inbreuk wordt gemaakt op het bij of krachtens deze wet bepaalde;
 - b. een last onder bestuursdwang op te leggen ter handhaving van het bij of krachtens deze wet bepaalde;
 - c. een bestuurlijke boete op te leggen indien de verwerkingsverantwoordelijke handelt in strijd met hetgeen is bepaald bij of krachtens:
 - de artikelen 4a, 4b, 4c, 6c, 31d, 32, 33a, 33b en 36 van ten hoogste het bedrag van de geldboete van de vijfde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht;
 - de artikelen 5, 7a, 24a, 24b, 25 en 28 van ten hoogste het bedrag van de geldboete van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht;
 - d. een advies te verstrekken aan de verwerkingsverantwoordelijke naar aanleiding van een voorafgaande raadpleging, bedoeld in artikel 33b, eerste lid;
 - e. de verwerkingsverantwoordelijke te verplichten een inbreuk in verband met persoonsgegevens te melden aan de betrokkene.
2. Bij het besluit over het opleggen van een bestuurlijke boete, bedoeld in het vierde lid, en over de hoogte daarvan wordt voor elk concreet geval naar behoren rekening gehouden met:
 - a. de aard, de ernst en de duur van de inbreuk, rekening houdend met de aard, de omvang of het doel van de verwerking in kwestie alsmede het aantal getroffen betrokkenen en de omvang van de door hen geleden schade;
 - b. de opzettelijke of nalatige aard van de inbreuk;
 - c. de door de verwerkingsverantwoordelijke of de verwerker genomen maatregelen om de door betrokkenen geleden schade te beperken;
 - d. de mate waarin de verwerkingsverantwoordelijke of de verwerker verantwoordelijk is gezien de technische en organisatorische maatregelen die hij heeft uitgevoerd overeenkomstig de artikelen 4a en 4b;
 - e. eerdere relevante inbreuken door de verwerkingsverantwoordelijke of de verwerker;
 - f. de mate waarin er met de Autoriteit persoonsgegevens is samengewerkt om de inbreuk te verhelpen en de mogelijke negatieve gevolgen daarvan te beperken;
 - g. de categorieën van persoonsgegevens waarop de inbreuk betrekking heeft;
 - h. de wijze waarop de Autoriteit persoonsgegevens kennis heeft gekregen van de inbreuk, met name of, en zo ja in hoeverre, de verwerkingsverantwoordelijke of de verwerker de inbreuk heeft gemeld;
 - i. de naleving van de in het eerste lid genoemde maatregelen, voor zover die eerder ten aanzien van de verwerkingsverantwoordelijke of de verwerker in kwestie met betrekking tot dezelfde aangelegenheid zijn genomen.

3. De werking van de beschikking tot oplegging van de bestuurlijke boete, bedoeld in het eerste lid, onder c, wordt opgeschort totdat de bezwaar- of beroepstermijn is verstreken of, indien bezwaar is gemaakt respectievelijk beroep is ingesteld, op het bezwaar respectievelijk het beroep is beslist.
4. De bevoegdheden, bedoeld in het eerste lid, onderdelen d en e, gelden als een besluit in de zin van de Algemene wet bestuursrecht.

Artikel 35d. (samenwerking met toezichthoudende autoriteiten in andere lidstaten)

1. De Autoriteit persoonsgegevens verstrekt aan een autoriteit in een andere lidstaat die is belast met het toezicht, bedoeld in artikel 35, eerste lid, relevante informatie en wederzijdse bijstand om deze richtlijn op een consequente manier ten uitvoer te leggen en toe te passen, en neemt maatregelen om doeltreffend met elkaar samen te werken.
2. De Autoriteit persoonsgegevens neemt alle passende maatregelen die nodig zijn om een verzoek om informatie of wederzijdse bijstand van een andere autoriteit, bedoeld in het eerste lid, zonder onnodige vertraging en in ieder geval binnen één maand na de ontvangst ervan te beantwoorden. De verzoekende autoriteit wordt geïnformeerd over de resultaten of, in voorkomend geval, de voortgang van de maatregelen die naar aanleiding van het verzoek zijn genomen.
3. Een verzoek om bijstand van de Autoriteit persoonsgegevens bevat alle nodige informatie, waaronder het doel van en de redenen voor het verzoek. De uitgewisselde informatie wordt alleen gebruikt voor het doel waarvoor om die informatie is verzocht.
4. De Autoriteit persoonsgegevens kan een verzoek om bijstand van een andere autoriteit, bedoeld in het eerste lid, gemotiveerd afwijzen indien:
 - a. zij niet bevoegd is voor het onderwerp van het verzoek of voor de maatregelen die zij wordt verzocht uit te voeren, of
 - b. inwilliging van het verzoek indruist tegen de richtlijn of het Unierecht of het Nederlandse recht dat op de Autoriteit persoonsgegevens van toepassing is.
5. Behoudens regels voor vergoeding voor specifieke uitgaven die voortvloeien uit het verstrekken van wederzijdse bijstand in uitzonderlijke omstandigheden geschiedt de wederzijdse bijstand, bedoeld in het tweede lid, kosteloos.
6. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld over de wijze van verstrekking van de informatie, bedoeld in het eerste lid.

Artikel 36. (functionaris voor gegevensbescherming)

1. De verwerkingsverantwoordelijke benoemt een functionaris voor gegevensbescherming. Voor verschillende bevoegde autoriteiten kan, rekening houdend met hun organisatiestructuur en omvang, één functionaris voor gegevensbescherming worden aangewezen. De functionaris voor

gegevensbescherming wordt door de verwerkingsverantwoordelijke tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van politiegegevens.

2. De functionaris voor gegevensbescherming wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de taken, bedoeld in het derde lid, te vervullen.
3. De functionaris voor gegevensbescherming is tenminste belast met de volgende taken:
 - a. het toezien op de naleving van het bepaalde bij of krachtens deze wet en op het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van de autorisaties, bedoeld in artikel 6, de bewustmaking en opleiding van de ambtenaren van politie die zijn betrokken bij de verwerking van politiegegevens en de audits, bedoeld in artikel 33;
 - b. het informeren en adviseren van de verwerkingsverantwoordelijke en de ambtenaren van politie die politiegegevens verwerken over hun verplichtingen op grond van het bepaalde bij of krachtens deze wet en andere gegevensbeschermingsbepalingen op grond van het Unierecht of het Nederlandse recht;
 - c. het desgevraagd verstrekken van advies over de gegevensbeschermingseffectbeoordeling, bedoeld in artikel 4c, en het toezien op de uitvoering ervan;
 - d. het samenwerken met de Autoriteit persoonsgegevens;
 - e. het optreden als contactpunt voor de Autoriteit persoonsgegevens inzake aangelegenheden in verband met de verwerking van persoonsgegevens en, voor zover dienstig, het plegen van overleg over enige andere aangelegenheid.
4. De functionaris voor gegevensbescherming stelt jaarlijks een verslag op van zijn bevindingen.
5. De verwerkingsverantwoordelijke maakt de contactgegevens van de functionaris voor gegevensbescherming openbaar en meldt de functionaris voor gegevensbescherming aan bij de Autoriteit persoonsgegevens.
6. De verwerkingsverantwoordelijke stelt de functionaris voor gegevensbescherming de benodigde middelen ter beschikking voor het vervullen van de taken, bedoeld in het derde lid, en voor het in standhouden van zijn deskundigheid.

§ 7. Slotbepalingen

Artikel 46. (toepassing op gegevensverwerking door bijzondere opsporingsdiensten)

1. Het bij of krachtens de Wet politiegegevens bepaalde met betrekking tot de gegevensverwerking, bedoeld in de artikelen 10, eerste lid onder a, en 12, is van overeenkomstige toepassing op de verwerking van persoonsgegevens door een ambtenaar, werkzaam bij een bijzondere opsporingsdienst, bedoeld in artikel 2 van de Wet op de bijzondere opsporingsdiensten. Op voordracht van Onze Ministers en Onze Minister wie het mede aangaat worden bij algemene maatregel van bestuur ook andere onderdelen van het bij of krachtens deze wet bepaalde van overeenkomstige toepassing verklaard op de verwerking van persoonsgegevens door een ambtenaar, werkzaam bij een bijzondere opsporingsdienst, bedoeld in artikel 2 van de Wet op de bijzondere opsporingsdiensten, of een buitengewoon opsporingsambtenaar, bedoeld in artikel 142, eerste lid, van het Wetboek van Strafvordering.
2. Voor zover toepassing is gegeven aan het eerste lid:
 - a. stelt de verwerkingsverantwoordelijke politiegegevens voor verdere verwerking ter beschikking aan opsporingsambtenaren, als bedoeld in de artikelen 141, onderdeel d, en 142, eerste lid, van het Wetboek van Strafvordering, voor zover zij deze behoeven voor de vervulling van hun taak;
 - b. stelt de verwerkingsverantwoordelijke van de bijzondere opsporingsdienst of van de buitengewoon opsporingsambtenaar, bedoeld in artikel 142, eerste lid, van het Wetboek van Strafvordering, de gegevens waarop het bepaalde bij of krachtens deze wet van toepassing of van overeenkomstige toepassing is ter beschikking aan personen die overeenkomstig artikel 6, tweede lid, zijn geautoriseerd voor de verwerking van politiegegevens, voor zover zij deze behoeven voor de vervulling van hun taak.
Artikel 15, tweede lid, is van overeenkomstige toepassing.
3. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld over de ambtenaren die werkzaam zijn bij een bijzondere opsporingsdienst, die tot het verwerken van politiegegevens als bedoeld in het eerste lid kunnen worden geautoriseerd, alsmede over het beheer en de organisatie van de bijzondere opsporingsdienst waar zij werkzaam zijn.