AUTORITEIT
PERSOONSGEGEVENS

Privacybeleid Autoriteit Persoonsgegevens

Versie 1.1

Status	definitief
Datum	8 oktober 2019

Inhoud

1. Inleiding

De Autoriteit Persoonsgegevens (AP) is de onafhankelijke Nederlandse toezichthouder op de naleving van de Europese en nationale regels voor de bescherming van persoonsgegevens en draagt hiermee bij aan de bescherming van het grondrecht op bescherming van persoonsgegevens.

In het kader van de uitvoering van haar wettelijk opgedragen taak verwerkt de AP zelf ook persoonsgegevens. Gegevens van en over burgers en medewerkers moeten bij de AP veilig zijn en hun privacy moet zijn gewaarborgd. De Autoriteit is als nationale toezichthouder op het terrein van bescherming van persoonsgegevens een verwerkingsverantwoordelijke die vanuit haar taken en bevoegdheden meer dan de andere verwerkingsverantwoordelijken bekend is met de relevante wet- en regelgeving op het gebied van de bescherming van persoonsgegevens. Om die reden dient de Autoriteit Persoonsgegevens te borgen dat ook zij persoonsgegevens veilig en verantwoord verwerkt bij de uitvoering van haar publiekrechtelijke taak.

Vanaf 25 mei 2018 is in de hele Europese Unie de Algemene verordening gegevensbescherming (AVG) van toepassing.[1] De AP is de toezichthoudende autoriteit als bedoeld in artikel 51 van de AVG en valt ook zelf onder de werkingssfeer van de AVG. Daar waar de AVG ruimte laat om op nationaal niveau bepaalde vraagstukken (aanvullend) te regelen, is dit in Nederland gedaan door middel van de Uitvoeringswet Algemene verordening gegevensbescherming.[2] De Uitvoeringswet is met ingang van 25 mei 2018 in werking getreden.[3] Daarnaast heeft de AP een toezichthoudende taak op de verwerking van persoonsgegevens in het kader van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens. Deze wetten worden aangepast ter implementatie van de EU-Richtlijn 2016/680.[4] [5] Voor zover de AP voornemens is een bestraffende sanctie op te leggen, valt de daarmee samenhangende verwerking van persoonsgegevens naar het oordeel van de AP onder de reikwijdte van de Richtlijn.[6]

[1] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119)
[2] Wet van 16 mei 2018, houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming) (Stb. 2018, 144).
[3] Met uitzondering van artikel 48a (Stb. 2018, 145).
[4] Richtlijn EU 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PbEU 2016, L119).
[5] Wetsvoorstel tot wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen (34 889) (het wetsvoorstel is op 7 juni 2018 als hamerstuk in de Tweede Kamer aanvaard).
[6] Advies AP ten aanzien van wetsvoorstel inzake implementatie van Richtlijn (EU) 2016.680 d.d. 7 april 2017, z2017-01571, p. 6-7 (https://zoek.officielebekendmakingen.nl/blg-833088). Het wetgevingsadvies wordt gepubliceerd op de website van de AP. Na implementatie zullen de Wpg en de Wjsg van toepassing zijn, tenzij de implementatie in strijd is met Richtlijn 2016/680 en de

De AVG legt meer verantwoordelijkheid op organisaties om aan te tonen dat de door hen uitgevoerde verwerkingen aan de regels op het gebied van gegevensbescherming voldoen. Nu de AP zelf ook gegevens verwerkt is ook zij gehouden om aan deze verantwoordelijkheidsplicht (accountability) te voldoen. Zo moet de AP bijvoorbeeld aantonen dat een verwerking aan de belangrijkste beginselen van gegevensverwerking voldoet, zoals rechtmatigheid, transparantie, doelbinding en juistheid. Ook moet de AP kunnen laten zien dat de juiste technische en organisatorische maatregelen zijn genomen om de persoonsgegevens te beschermen. Voor zover de AP voornemens is een bestuurlijke boete op te leggen, dient de daarmee samenhangende gegevensverwerking te voldoen aan de normen van Richtlijn 2016/680.

De AP stelt een externe functionaris gegevensbescherming (FG) aan. Een FG houdt intern toezicht op de toepassing en naleving van de AVG en is in beginsel iemand die binnen de organisatie werkzaam is. De AP is echter zelf de onafhankelijke toezichthouder op de naleving van regels ter bescherming van persoonsgegevens. Om die reden is ervoor gekozen een *externe* FG aan te stellen die meer op afstand staat, om te waarborgen dat ook de FG onafhankelijk van de AP handelt en niet wordt aangestuurd door de AP.[7] De externe FG zal uitsluitend op basis van signalen uit de organisatie acteren en wordt in haar taakuitvoering bijgestaan door privacy contactpersonen binnen de AP, die haar voorzien van de benodigde informatie over bijvoorbeeld nieuwe verwerkingen, DPIA's die uitgevoerd (moeten) worden en over privacyschendingen of signalen hiervan en (andere) relevante zaken op het gebied van gegevensverwerking binnen de AP. De externe FG zal om die reden worden geïnformeerd en ondersteund door een aantal privacy-contactpersonen (per directie één) en een concern privacy contactpersoon. Deze personen zullen tevens de privacy-gerelateerde verzoeken en klachten van burgers en personeel behandelen en de externe FG daarover tijdig informeren. Zo wordt geborgd dat de externe FG over afdoende informatie kan beschikken en haar taak goed kan uitoefenen.

Dit document is ontwikkeld om structuur en een beleidskader te bieden bij het inrichten van de verplichtingen van de AVG en Richtlijn 2016/680 en om daarover verantwoording te kunnen afleggen. Dit document maakt deel uit van het pakket aan maatregelen en documenten waarmee de AP voldoet aan haar verantwoordingsplicht. Het doel van dit privacybeleid is om de belangen van betrokken van wie de Autoriteit Persoonsgegevens persoonsgegevens verwerkt (burgers en medewerkers) centraal te stellen. Daarnaast helpt het beleid de organisatie zelf om te zien of er voldoende maatregelen zijn genomen om de bij de AP aanwezige persoonsgegevens te beschermen en vormt zij tevens een verantwoording dat de AP voldoet aan de AVG. Het privacybeleid wordt toegepast door de AP en het secretariaat van de AP. Dit stuk is bestemd voor alle medewerkers van de AP en geeft aan waar de AP voor staat en wat zij wil uitdragen.

AP een richtlijnconforme uitleg toepast. Deze uitleg kan op termijn worden aangepast aan de uiteindelijke invulling die in EU-verband moet plaatsvinden.

[7] Dit houdt onder meer in dat de externe FG en aantal klassieke FG-taken niet zelf of niet rechtstreeks vervult. Het gaat onder andere om het informeren en adviseren van (medewerkers van) de AP en haar verwerkers over hun verplichtingen uit hoofde van de AVG en andere gegevensbeschermingsbepalingen, het proactief toezien op naleving van de AVG en het gegevensbeschermingsbeleid van de AP en haar verwerkers en het in dat kader verrichten van audits, taken rondom 'awareness' (bewustmaking en opleiding van personeel van de AP e.d.

Het beleid is vastgesteld en beoordeeld binnen de organisatie om te waarborgen dat gegevensverwerkingen op een rechtmatige wijze plaatsvinden. Het beleid bevat de visie en principes van de organisatie in het kader van privacy en wordt periodiek, of bij grote wijzigingen in de wetgeving of de omgeving van de organisatie, beoordeeld om te controleren of zij nog in voldoende mate aansluit op de realiteit.

De onderwerpen die in dit document aan de orde komen zijn het juridisch kader waarbinnen de AP functioneert, de organisatorische borging van een veilige en rechtmatige verwerking van persoonsgegevens, de soorten gegevens die de AP verwerkt, de beveiligingsmaatregelen en de wijze waarop de AP uitvoering geeft aan de rechten van betrokkenen.

Definitie privacy
In dit document wordt met de term privacy verwezen naar de informationele privacy. Deze gaat over het verwerken en verzamelen van persoonlijke data, zogeheten persoonsgegevens. Hieronder vallen bijvoorbeeld medische gegevens, financiële gegevens en contactgegevens, maar ook alle andere informatie over geïdentificeerde of identificeerbare natuurlijke personen. De AP volgt de definitie van persoonsgegevens zoals die in de AVG en Richtlijn 2016/680 wordt gegeven en uitgelegd.

Afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming
Awb	Algemene wet bestuursrecht
BIR	Baseline Informatiebeveiliging Rijksdienst
BIR_TNK	Baseline Informatiebeveiliging Rijksdienst: Tactisch Normenkader
BVA	Beveiligingsambtenaar
FG	Functionaris gegevensbescherming
UAVG	Uitvoeringswet Algemene verordening gegevensbescherming

2. Juridisch kader

2.1. Wet- en regelgeving

De AP is als de onafhankelijke Nederlandse toezichthouder verantwoordelijk voor het toezicht en de controle op de verwerking van persoonsgegevens door organisaties. Dit kunnen zowel nationale als internationale en zowel private als publieke organisaties zijn. De AP houdt toezicht op de naleving van normen uit internationale verdragen en Europese en nationale wetgeving. Bij een overtreding van één van deze normen kan de AP als toezichthouder optreden.

Bij het functioneren als toezichthoudende autoriteit is de AP in de eerste plaats gebonden aan de normen voor verwerking van persoonsgegevens die uit de AVG, de UAVG en Richtlijn 2016/680 voortvloeien.

Voorts is de AP als bestuursorgaan gebonden aan de algemene regels van bestuursrecht zoals onder meer vastgelegd in de Awb.

Ook neemt de AP voor het bewaren en vernietigen van persoonsgegevens de Archiefwet in acht.

In haar hoedanigheid als verwerkingsverantwoordelijke houdt de AP zich aan alle relevante wet- en regelgeving waaronder:

- Besluit voorschrift informatiebeveiliging rijksdienst 2007;
- Besluit van de Minister-President, Minister van Algemene zaken van 1 juni 2013, nr. 3119942, houdende beveiligingsvoorschrift Rijksdienst 2013;
- Baseline Informatiebeveiliging Rijksdienst (2012).

2.2. Gehanteerde begrippen

Persoonsgegevens (artikel 4, aanhef en onder 1, van de AVG en artikel 3, aanhef en onder 1, van Richtlijn 2016/680)
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Externe natuurlijke personen van wie de AP in het kader van haar toezichthoudende taak persoonsgegevens verzameld alsmede medewerkers in dienst van de AP, worden als betrokkenen aangemerkt. De AP verwerkt bijvoorbeeld de benodigde contactgegevens in het kader van haar taak, alsmede persoonsgegevens in het kader van het dienstverband van haar medewerkers.

Verwerking (artikel 4, aanhef en onder 2, van de AVG en artikel 3, aanhef en onder 2, van Richtlijn 2016/680)
Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

De AP verwerkt bijvoorbeeld gegevens door deze gedurende een bepaalde bewaartermijn op te slaan, waar nodig intern uit te wisselen, te wijzigen of na een beoordeling uit te wisselen met derden.

Verwerkingsverantwoordelijk (artikel 4, aanhef en onder 7, van de AVG)
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.
Verwerkingsverantwoordelijke (artikel 3, aanhef en onder 8, van Richtlijn 2016/680)
De bevoegde autoriteit die, alleen of samen met andere, de doeleinden van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doeleinden van en de middelen voor die verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

De AP is de verwerkingsverantwoordelijke voor de persoonsgegevens die zij in het kader van haar publiekrechtelijke taak verwerkt en die zij als werkgever verwerkt.

Verwerker (artikel 4, aanhef en onder 8, van de AVG en artikel 3, aanhef en onder 9, van Richtlijn 2016/680)
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt

Als verwerker voor de AP worden onder meer aangemerkt partijen die in het kader beveiliging of de verwerking van meldingen inzake datalekken persoonsgegevens voor de AP verwerken.

Derde (artikel 4, aanhef en onder 10, van de AVG)
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.

Als derde worden onder meer aangemerkt toezichthoudende autoriteiten als bedoeld in artikel 51, eerste lid, van de AVG, van andere lidstaten, waaraan de AP in het kader van een onderzoek persoonsgegevens overdraagt.

3. Soorten verwerkingen

3.1. Aard en omvang persoonsgegevens

Tijdens de uitvoering van haar toezichthoudende taken verwerkt de AP verschillende soorten persoonsgegevens. Hierbij valt te denken aan verwerkingen in het kader van het inspecteren van het bedrijfsleven en publieke organisaties, het behandelen van tips, meldingen, klachten en (handhavings)verzoeken, bezwaar- en beroepsprocedures of het aannemen van nieuw personeel. In bepaalde gevallen kan het voorkomen dat de AP persoonsgegevens moet delen met derden. Dit kan bijvoorbeeld het geval zijn als er sprake is van een beroepsprocedure of als een verzoek om gegevensdeling door de leidende toezichthoudende autoriteit wordt gedaan.

De AP verwerkt bij haar werkzaamheden alle mogelijke categorieën van persoonsgegevens, waaronder naam, adres, woonplaats, telefoonnummer, geboortedatum, emailadressen, financiële persoonsgegevens, bankrekeningnummers, paspoortkopieën, foto's, bijzondere persoonsgegevens zoals medische gegevens, strafrechtelijke persoonsgegevens en bij wet voorgeschreven identificatienummers (BSN).

De AP heeft in het verwerkingenregister een overzicht gemaakt van de verschillende verwerkingsactiviteiten die onder haar verantwoordelijkheid plaatsvinden. Het verwerkingenregister bevat van iedere afzonderlijk verwerking nadere informatie over onder meer:

- de herkomst van de persoonsgegevens;
- de verwerkingsdoeleinden;
- de grondslag van de verwerking;
- de categorieën van persoonsgegevens;
- de categorieën van betrokkenen;
- de categorieën van ontvangers;
- de beveiligingsmaatregelen;
- de bewaartermijn van de gegevens.

Het verwerkingenregister bevat een extra categorie van een verwerking van persoonsgegevens bij boetebesluiten, die naar het oordeel van de AP onder de Richtlijn 2016/680 vallen.

Voor meer informatie over de aard en omvang van de persoonsgegevens die de AP verwerkt wordt verwezen naar het verwerkingenregister.

3.2. Doeleinden verwerking persoonsgegevens

Het doel waarvoor de AP persoonsgegevens verwerkt is het houden van toezicht op de naleving van de AVG, Richtlijn 2016/680, de UAVG, de Wet politiegegevens, Wet justitiële en strafvorderlijke gegevens, de Telecommunicatiewet, de Kieswet, de Wet raadgevend referendum en de Wet basisregistratie personen. De diverse werkzaamheden van de AP, zoals het behandelen van signalen van inbreuken op het persoonsgegevensbeschermingsrecht, het doen van onderzoek daarnaar, het geven van voorlichting, het

behandelen van verzoeken om handhaving, de registratie van datalekken, handhaving van de bij of krachtens de AVG of UAVG gestelde verplichtingen (waaronder het opleggen van bestuurlijke boetes), het behandelen van bezwaar- en beroepsprocedures, en de met deze werkzaamheden gepaard gaande verzameling, vastlegging, opslag en gebruik van persoonsgegevens, vinden met dit doel plaats. Daarnaast vindt verwerking van persoonsgegevens plaats in het kader van de beheersmatige activiteiten van de AP.

Voor meer informatie over de doeleinden van de verwerking van persoonsgegevens door de AP wordt verwezen naar het verwerkingenregister.

3.3. Grondslagen verwerking

De belangrijkste grondslag voor de verwerking van persoonsgegevens door de AP is gelegen in artikel 6, eerste lid, onder e, van de AVG. De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. De taken van de AP staan onder meer opgesomd in artikel 57 van de AVG, artikel 35 van de Wet politiegegevens en artikel 27 van de Wet justitiële en strafvorderlijke gegevens.[8]

Het verbod om bijzondere categorieën van persoonsgegevens te verwerken is niet van toepassing op grond van artikel 23, aanhef en onder b, van de UAVG, voor zover de verwerking noodzakelijk is voor de uitvoering van de aan de AP wettelijk opgedragen taken, onder voorwaarde dat bij die uitvoering is voorzien in zodanig waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

3.4. Bewaartermijnen persoonsgegevens

Op grond van artikel 3 van de Archiefwet is de AP verplicht de onder haar berustende archiefbescheiden in goede, geordende en toegankelijke staat te brengen en te bewaren, alsmede zorg te dragen voor de vernietiging van de daarvoor in aanmerking komende archiefbescheiden. In een selectielijst is vastgelegd welke bescheiden worden bewaard. Tevens is aangegeven welke bescheiden voor vernietiging in aanmerking komen en binnen welke termijn vernietiging moet plaatsvinden.[9] Archiefbescheiden die niet voor vernietiging in aanmerking komen en ouder zijn dan twintig jaar worden overgebracht naar een archiefbewaarplaats (artikel 12 van de Archiefwet).

Voor zover in de archiefbescheiden persoonsgegevens voorkomen is daarop de AVG van toepassing. Voor de archiveringstaak zijn diverse uitzonderingen in de AVG opgenomen.

[8] Na inwerkingtreding implementatiewet richtlijn worden dit artikel 35b, eerste lid, onder a, van de Wpg resp. artikel 27, derde lid, van de Wjsg jo. Artikel 35b, eerste lid, onder a, van de Wpg.
[9] Vaststellingsbesluit selectielijst neerslag handelingen College Bescherming Persoonsgegevens beleidsterrein Persoonsregistraties vanaf 1989 (Stcrt. 2006, 99).

3.5. Werkprocessen

In de werkprocessen van de diverse afdelingen binnen de AP wordt concreet aangegeven hoe medewerkers voor een specifiek werkproces, bijvoorbeeld een verzoek om handhaving, de behandeling van een bezwaarschrift of een verzoek om gegevensdeling van een andere Europese toezichthouder, met persoonsgegevens omgaan. De afdelingshoofden zijn primair verantwoordelijk voor het vastleggen van deze werkprocessen. Het kader wordt hierbij gevormd door de elf basisregels die in paragraaf 4.1 worden beschreven.

In bepaalde gevallen kan het voorkomen dat de AP gegevens moet delen met derden. Dit kan bijvoorbeeld het geval zijn als sprake is van een beroepsprocedure of als er een samenwerking plaatsvindt met een toezichthouder van een andere lidstaat. Uitgangspunt is dat de AP alleen gegevens deelt als dat noodzakelijk is voor zo'n procedure. Per geval wordt beoordeeld of het delen van gegevens noodzakelijk is. De beoordeling en het eindoordeel worden in het dossier vastgelegd door de primaire behandelaar.

4. Governance en organisatorische borging gegevensverwerking

De AP zorgt ervoor – naast de benodigde technische maatregelen –dat alle medewerkers op een rechtmatige wijze persoonsgegevens verwerken. Hoe dit binnen de AP organisatorisch wordt geborgd, wordt in dit hoofdstuk beschreven. Zo wijst de AP personen aan bij wie gegevensverwerkingen door de AP op de agenda staan en zorgt de AP ervoor dat de verwerking van gegevens door verschillende afdelingen regelmatig wordt gecontroleerd.

4.1. Functies

In deze paragraaf wordt beschreven welke functies binnen de AP een taak en verantwoordelijkheid hebben in de borging van een rechtmatige verwerking van persoonsgegevens binnen de organisatie.

Functies in verschillende lagen

Alle medewerkers binnen de AP zijn verantwoordelijk voor een rechtmatige omgang met persoonsgegevens. Daartoe zijn de volgende elf basisregels opgesteld:

1. Verwerk persoonsgegevens alléén als dit nodig is in het kader van de toezichthoudende taak van de AP
2. Gebruik alleen die persoonsgegevens die je nodig hebt voor je doel/activiteit
3. Zorg dat de persoonsgegevens die je verwerkt juist en actueel zijn
4. Sla persoonsgegevens op zo min mogelijk plekken op
5. Deel de persoonsgegevens alleen met collega's die direct betrokken zijn
6. Laat persoonsgegevens niet onbeheerd achter
7. Neem de grootste zorgvuldigheid in acht wanneer je persoonsgegevens verwerkt over iemands ras, religie, gezondheid, strafverleden etc.
8. Verwijder de persoonsgegevens na het verstrijken van de bewaartermijn
9. Neem de grootste zorgvuldigheid en terughoudendheid in acht als het gaat om het verstrekken van persoonsgegevens aan derden
10. Raadpleeg de privacy coördinator van jouw directie bij bijzondere situaties of voor advies
11. Denk je dat je persoonsgegevens hebt gelekt? Meld dit direct aan je direct leidinggevende. Bel buiten kantooruren, in het weekend of tijdens verlof direct met 070-8888508.

Deze basisregels vormen ook het kader bij het vaststellen of aanpassen van de diverse werkprocessen binnen de organisatie.

Iedere medewerker heeft zijn of haar eigen verantwoordelijkheid voor een rechtmatige omgang met persoonsgegevens. Om dit te controleren en te coördineren, houden een aantal daartoe aangewezen personen zich naast hun reguliere werkzaamheden bezig met de borging van de rechtmatige verwerking van persoonsgegevens door de AP, in de volgende lagen:

1. Per directie een aangewezen privacy coördinator;
2. Eén concern privacy coördinator;
3. De afdelingshoofden;
4. De directeuren;
5. De Algemeen directeur;
6. Een van de leden van de AP.

Functionaris gegevensbescherming
Naast de verschillende medewerkers van de AP stelt de AP een FG aan. De FG handelt onafhankelijk van de AP, en wordt niet aangestuurd door de AP. Om dit te waarborgen is de FG niet in dienst van de AP, maar is een externe FG aangewezen. Dit is een advocaat werkzaam bij Pels Rijcken, de Landsadvocaat. De AP oefent geen invloed uit op hetgeen de FG doet. Alle leden en medewerkers van de AP werken volledig mee aan alle verzoeken van de FG.

Beveiligingsambtenaar
De beveiligingsambtenaar (BVA) is verantwoordelijk voor de beveiliging van de persoonsgegevens die worden verwerkt door de AP.

Afdelingshoofd Bedrijfsvoering
Het hoofd van de afdeling Bedrijfsvoering is verantwoordelijk voor de periodieke evaluatie en eventuele aanpassing van het privacybeleid en voor het verwerkingenregister.

4.2. Taken en verantwoordelijkheden

Medewerkers
De medewerkers zorgen ervoor dat zij volgens de basisregels en de daarvoor vastgestelde werkprocessen omgaan met de persoonsgegevens. Bij problemen bij het volgen van de werkprocessen informeren zij daarover hun afdelingshoofd en de privacy coördinator. Eventuele vragen over de verwerking van persoonsgegevens en over het werkproces voor datalekken, waaronder de vraag of sprake is van een datalek, kunnen de medewerkers stellen aan de privacy coördinator van de betreffende directie. Als sprake is van een nieuwe verwerking van persoonsgegevens, meldt de medewerker die verantwoordelijk is voor het project of proces waarin persoonsgegevens worden verwerkt, dit aan de privacy coördinator.
Als er sprake is van een datalek, meldt de medewerker dit aan zijn of haar leidinggevende en de beveiligingsambtenaar.

Concern privacy coördinator en overige privacy coördinatoren
De concern privacy coördinator heeft als taak om ervoor te zorgen dat medewerkers binnen de organisatie zich bewust blijven van de rechtmatige omgang met persoonsgegevens, door hen daarover periodiek te informeren, onder meer over de hiervoor beschreven basisregels. Daarbij volgt de concern privacy

coördinator een communicatieplan, dat de concern privacy coördinator samen met privacy coördinatoren van alle directies opstellen.
Daarnaast beantwoorden de concern en de overige privacy coördinatoren eventuele vragen van medewerkers over specifieke gegevensverwerkingen. Indien een medewerker een nieuwe verwerking bij de (concern) privacy coördinator meldt die nog niet in het verwerkingsregister is opgenomen, meldt de (concern) privacy coördinator dit aan de directeur met het voorstel dit toe te voegen aan het register. De (concern) privacy coördinator beantwoordt vragen van medewerkers over mogelijke datalekken.
Tevens bestudeert de privacy coördinator het rapport over de naleving van geldende privacywet- en regelgeving binnen zijn/haar directie en informeert de concern privacy coördinator hierover.. De concern privacy coördinator treedt in contact met de directeur over eventuele knelpunten of moeilijkheden die daaruit blijken, teneinde deze op te lossen. Tevens informeert hij de directeur direct in geval van dringende zaken, waaronder datalekken.

Directeur
De directeuren van de verschillende directies binnen de Autoriteit Persoonsgegevens zijn binnen hun directie verantwoordelijk voor een juiste naleving van de geldende wet- en regelgeving inzake de bescherming van persoonsgegevens. Ieder kwartaal informeert de concern privacy coördinator op basis van de informatie die hij/zij heeft verkregen van de overige privacy coördinatoren de Algemeen directeur over de verwerking van persoonsgegevens binnen de organisatie. De directeuren kunnen deze taken toebedelen aan een van de afdelingshoofden.
Elke directie brengt (met behulp van het verwerkingenregister) in kaart welke persoonsgegevens er op zijn of haar directie worden verwerkt. Indien sprake is van een nieuwe verwerking die nog niet in het verwerkingsregister is opgenomen, meldt de directeur dit aan de Algemeen directeur met het voorstel dit toe te voegen aan het register. De directeur ziet erop toe dat de gegevens verwerkt worden volgens de daarvoor ingerichte werkprocessen. Steekproefsgewijs controleert de directeur of deze werkprocessen gevolgd worden. Eens in de drie maanden stelt de directeur een rapport op, waarin wordt omschreven of deze werkprocessen worden gevolgd en of er bepaalde moeilijkheden of incidenten zijn (die door de medewerkers van de directie zijn geconstateerd).

Algemeen directeur
Tenminste eens in de drie maanden wordt aan de Algemeen directeur gerapporteerd over de omgang met persoonsgegevens binnen de verschillende directies. Daartoe stellen de directeuren per directie een rapport op, waarin zowel de knelpunten worden besproken die wel alsmede de knelpunten die niet door de directeuren zelf kunnen worden opgelost. Indien sprake is van een nieuwe verwerking die nog niet in het verwerkingsregister is opgenomen, beslist de Algemeen directeur of deze verwerking wordt toegevoegd aan het register. Indien de verwerking wordt toegevoegd aan het register, stelt de Algemeen directeur het hoofd van de afdeling Bedrijfsvoering hiervan in kennis. Daarnaast informeren de directeuren de Algemeen directeur direct in het geval van dringende zaken, waaronder datalekken. Tot slot informeert de Algemeen directeur ieder kwartaal het daartoe aangewezen lid van de AP over de verwerking van persoonsgegevens binnen de directies.

Lid van de AP
De AP is als verwerkingsverantwoordelijke eindverantwoordelijke voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens door de medewerkers binnen de AP. Om deze verantwoordelijkheid te kunnen dragen informeert de Algemeen directeur ieder kwartaal het daartoe aangewezen lid van het college van de AP, (ter bespreking ieder kwartaal tijdens de vergadering van de AP). Dit geschiedt mede op basis van de rapporten die door de directeuren zijn opgesteld. Daarnaast informeert de Algemeen directeur het daartoe aangewezen lid van de AP direct in het geval van dringende zaken, waaronder datalekken.

Beveiligingsambtenaar
De BVA zorgt ervoor dat de juiste personen toegang hebben tot de juiste gegevens en draagt er zorg voor dat de systemen zijn ingericht zodat gegevens niet langer worden bewaard dan de bewaartermijn die daarvoor staat. De beveiligingsambtenaar zorgt ervoor dat na een melding daarvan door een medewerker het werkproces voor datalekken in werking wordt gezet.

Afdelingshoofd Bedrijfsvoering
Dit document wordt beheerd door de afdeling Bedrijfsvoering. Deze afdeling zorgt ten minste eens per drie jaar voor een evaluatie en eventuele bijstelling van het privacybeleid. Indien er eerder aanleiding is om het document tussentijds aan te passen kan dit ook door een addendum aan het document toe te voegen. Voorts is het afdelingshoofd ervoor verantwoordelijk dat een nieuwe verwerkingsactiviteit in het verwerkingenregister wordt opgenomen, na een besluit daartoe van de Algemeen directeur.

4.3. P&C-cyclus

Er zijn drie formele momenten in het jaar waarin de AP zich moet verantwoorden, te weten:

- Beleids-/jaarplan (jaarlijks voor 1 december);
- Halfjaarrapportage (jaarlijks uiterlijk 30 juli);
- Jaarverslag (jaarlijks uiterlijk 15 maart).

In het beleids-/jaarplan geeft de AP aan wat de doelen/ambities voor het komende jaar zijn. Hierin wordt de implementatie en naleving van de AVG door de AP als verwerkingsverantwoordelijke een vast element. In respectievelijk de halfjaarrapportage en het jaarverslag wordt gerapporteerd over de voortgang en eventuele maatregelen die getroffen worden om daadwerkelijk AVG-proof te zijn en te blijven.

De interne controlecyclus, zoals in de vorige paragrafen is beschreven, heeft een frequentie van viermaal per jaar. Elk kwartaal informeren de directeuren de Algemeen directeur. De Algemeen directeur informeert vervolgens ook ieder kwartaal het lid van de AP dat intern verantwoordelijk is voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens door de medewerkers van de AP. Twee van deze interne controlemomenten lopen synchroon met de halfjaarrapportage en het jaarverslag.

5. Informatiebeveiliging

In het kader van de uitvoering van haar taak als toezichthouder vertrouwen burgers, marktpartijen en overheidsorganisaties gevoelige informatie aangaande zichzelf en hun bedrijfsvoering toe aan de AP, die deze verwerkt in haar organisatie en informatiesystemen. De AP is verantwoordelijk voor het inrichten, onderhouden en continue verbeteren van een passende beveiliging van deze informatie. De AP draagt daarom zorg voor een passende beveiliging van informatie, in lijn met de wettelijke verplichtingen, haar eigen organisatierisico's en het vertrouwen en de belangen van haar medewerkers alsmede van de organisaties wiens informatie zij onder haar beheer heeft in het kader van haar taak als toezichthouder.

Omdat de informatie die de AP verwerkt ook persoonsgegevens betreft, worden in dit hoofdstuk van het privacybeleid de hoofdlijnen van het informatiebeveiligingsbeleid besproken.

De doelstelling van de AP voor informatiebeveiliging is het treffen en onderhouden van passende maatregelen ter beveiliging van informatie om zo te voldoen aan de wettelijke verplichtingen en om schade voor medewerkers, marktpartijen en overheidsinstanties te voorkomen.

5.1. Baseline Informatiebeveiliging Rijksdienst

Ter invulling van haar wettelijke verplichtingen heeft de AP onder meer de beheersmaatregelen in de Baseline Informatiebeveiliging Rijksdienst: Tactisch Normenkader[10] (BIR_TNK) op passende wijze geïmplementeerd. De BIR is geheel gestructureerd volgens NEN/ISO 27001, bijlage A en NEN/ISO 27002 en beschrijft de invulling van deze normen voor de Rijksoverheid. Daarnaast zijn in de BIR_TNK specifieke aanvullende rijksnormen gegeven.

In de BIR worden normen gegeven voor de volgende onderwerpen:

- Het beveiligingsbeleid;
- Organisatie van de informatiebeveiliging;
- Beheer van bedrijfsmiddelen;
- Personele beveiliging;
- Fysieke beveiliging en beveiliging van de omgeving;
- Beheer van communicatie- en bedieningsprocessen;
- Toegangsbeveiliging;
- Verwerving, ontwikkeling en onderheid van informatiesystemen;
- Beheer van informatiebeveiligingsincidenten;
- Bedrijfscontinuïteitsbeheer;
- Naleving.

[10] Baseline Informatiebeveiliging Rijksdienst, Tactisch Normenkader (2012) (BIR_TNK2012).

5.2. Het beleid voor informatiebeveiliging

Hoe de AP invulling geeft aan de normen voor informatiebeveiliging zoals die volgen uit de BIR_TNK is neergelegd in het beleid voor informatiebeveiliging. Dit beleid voor informatiebeveiliging wordt formeel vastgesteld door het directieberaad van de AP en is uitgewerkt in de volgende documenten:

1. Beleidskader voor Informatiebeveiliging
2. Beleid voor Informatiebeveiliging
3. Handboek Managementsysteem Informatiebeveiliging
4. Handboek voor Medewerkers

Het document *Beleidskader voor Informatiebeveiliging* beschrijft de door de directie van de AP vastgestelde uitgangspunten en kaders voor informatiebeveiliging.

Het document *Beleid voor Informatiebeveiliging* beschrijft de voorzieningen van administratieve, technische of beheersmatige aard, die gericht zijn op het beheersen van de beveiligingsrisico's en het handhaven van een passend beveiligingsniveau. Onderwerpen die hierin worden behandeld zijn bijvoorbeeld omgang met derde partijen, het beheer van bedrijfsmiddelen, de personele en fysieke beveiliging, het beheer van ICT systemen, de toegangsbeveiliging, autorisaties, de werking, ontwikkeling, onderhoud en het beheer van het informatiesysteem, informatiebeveiligingsincidenten, bedrijfscontinuïteitenbeheer en de naleving van het beleid.

Het *Handboek Managementsysteem voor informatiebeveiliging* beschrijft de procesmatige aanpak voor het inrichten, onderhouden en verbeteren van het gewenste niveau van informatiebeveiliging. Daarnaast worden hierin de organisatie, coördinatie, functionele taken en verantwoordelijkheden in het kader van het informatiebeveiligingsbeleid gedefinieerd.

Het *Handboek voor Medewerkers* geeft handvatten voor een praktische invulling van het Beleid in de dagelijkse werkzaamheden van alle managers en medewerkers.

5.3. Organisatie van het informatiebeveiligingsbeleid

Maandelijks wordt het onderwerp informatiebeveiliging geagendeerd voor het directieberaad en jaarlijks wordt door het directieberaad een managementreview uitgevoerd ter beoordeling van het document *Beleid voor Informatiebeveiliging*, het beveiligingsniveau en de efficiëntie en effectiviteit van de getroffen beheersmaatregelen.

Eens per drie jaar wordt het beveiligingsbeleid en het beveiligingsniveau geëvalueerd door een onafhankelijke externe deskundige die hierover rapporteert aan het directieberaad . De verdere organisatie en coördinatie en de functionele taken en verantwoordelijkheden in het kader van informatiebeveiliging zijn gedefinieerd in het *Handboek Managementsysteem Informatiebeveiliging*.

5.4. Beveiligingsincidenten

De verantwoordelijkheden en procedures voor het beheer van beveiligingsincidenten en zwakheden in de beveiliging zijn gedocumenteerd in het *Handboek Managementsysteem Informatiebeveiliging.* Tevens zijn hier de procedures voor het rapporteren van beveiligingsgebeurtenissen en zwakheden in de beveiliging, alsmede de reactie- en escalatieprocedure vastgelegd teneinde een tijdige, doeltreffende en ordelijke reactie te bewerkstelligen.

Medewerkers zijn van de procedures voor het rapporteren van beveiligingsgebeurtenissen en zwakheden op de hoogte gebracht middels het *Handboek voor Medewerkers* en in het kader van communicaties ter bevordering van het informatiebeveiligingsbewustzijn. Vastgestelde of vermoede beveiligingsincidenten, alsmede waargenomen of verdachte zwakke plekken in systemen of diensten, worden door alle medewerkers, ingehuurd personeel en externe gebruikers, per direct gemeld bij de direct leidinggevende. De leidinggevende informeert de BVA die het incident administreert, classificeert en behandelt. Buiten kantooruren kunnen dringende zaken gemeld worden op het MT piket nummer, volgens de procedure *"Beveiligingsincidenten en zwakheden in de beveiliging melden"*, in het *Handboek voor Medewerkers*. Verlies, vermissing of diefstal van apparatuur of media die gegevens van de organisatie kunnen bevatten worden altijd aangemerkt als beveiligingsincident.

De BVA beheert de aangemelde incidenten en zwakheden, onderneemt conform de vastgestelde reactie- en escalatieprocedure in het *Handboek Managementsysteem, bijlage B*, actie en rapporteert de status en voortgang aan het directieberaad en aan de melder. Van afgehandelde incidenten en zwakheden worden aard, omvang en kosten geregistreerd en onderdeel gemaakt van maandelijkse rapportage aan het directieberaad. Het directieberaad evalueert de gerapporteerde incidenten en zwakheden periodiek met als doel de getroffen beheersmaatregelen voor informatiebeveiliging te verbeteren.

5.5. Naleving

Jaarlijks wordt vastgesteld, gedocumenteerd en geactualiseerd welke wettelijke en regelgevende eisen en contractuele verplichtingen op de AP rusten en wat de benadering van de organisatie in de naleving van deze eisen is. Het lijnmanagement houdt actief toezicht op de naleving van het beleid door medewerkers en inhuurkrachten binnen hun verantwoordelijkheidsgebied en corrigeert waar nodig.

Middels interne en/of externe audits wordt aangetoond dat de beveiligingsdoelstellingen worden gehaald en dat de benodigde beheersmaatregelen getroffen en effectief zijn. Informatiesystemen worden jaarlijks getoetst tegen de geldende eisen en de effectiviteit van geïmplementeerde technische maatregelen wordt hierbij gecontroleerd.

6. Rechten van betrokkenen

Onder de AVG[11] hebben betrokkenen de volgende rechten waarop zij zich kunnen beroepen tegenover de verwerkingsverantwoordelijke:

1. Het recht op dataportabiliteit (recht om persoonsgegevens over te dragen);
2. Het recht op vergetelheid (recht op wissing);
3. Het recht op inzage in de persoonsgegevens van betrokkene die de verwerkingsverantwoordelijke verwerkt;
4. Het recht op rectificatie en aanvulling;
5. Het recht op beperking van de verwerking (recht om minder gegevens te laten verwerken);
6. Het recht met betrekking tot geautomatiseerde besluitvorming en profilering;
7. Het recht om bezwaar te maken tegen de gegevensverwerking.

Voorts hebben betrokkenen recht op:

8. duidelijke informatie over wat de verwerkingsverantwoordelijke met hun gegevens doet;
9. indiening van een klacht bij de toezichthoudende autoriteit, indien zij van mening zijn dat de verwerking inbreuk maakt op de AVG;
10. intrekking van eerder gegeven toestemming voor de verwerking van bepaalde persoonsgegevens.

De AP is zelf ook een verwerkingsverantwoordelijke en betrokkenen kunnen zich dus ook tegenover de AP op deze rechten beroepen. Het beroepen op sommige rechten ligt in de situatie dat de AP verwerkingsverantwoordelijke is meer voor de hand dan op andere rechten. Zo is goed denkbaar dat betrokkenen zich beroepen op hun recht op inzage, rectificatie, verwijdering of beperking of dat zij hun eerder gegeven toestemming intrekken of een klacht indienen. Een beroep op het recht om niet te worden onderworpen aan geautomatiseerde besluitvorming lijkt minder waarschijnlijk in situaties waarin de AP de verwerkingsverantwoordelijke is.

6.1. Ontvangst verzoek

Als betrokkenen zich tegenover de AP willen beroepen op hun rechten onder de AVG genoemd in de punten 1 tot en met 7, dan kunnen zij hierover een brief sturen. Het indienen van een klacht als bedoeld in punt 9, niet zijnde een verzoek om handhaving, kan via een webformulier worden ingediend. Of het intrekken van eerder gegeven toestemming (punt 10) via de elektronische weg mogelijk is, hangt af van de manier waarop die eerdere toestemming is gegeven. Heeft dit via de elektronische weg plaatsgevonden, dan kan dit ook op dezelfde manier weer worden ingetrokken.

Als de AP een brief ontvangt waarin een betrokkene zich op zijn of haar rechten beroept als bedoeld onder punt 1 tot en met 7, dan wordt deze naar de afdeling Staftaken en Wetgevingsadvisering van de directie Juridische Zaken & Wetgevingsadvisering toegestuurd voor een inhoudelijke beoordeling van het verzoek.

[11] Richtlijn 2016/680 bevat het recht op inzage (artikel 14) en het recht op rectificatie of wissing van persoonsgegevens en verwerkingsbeperking (artikel 16).

De afdeling Staftaken en Wetgevingsadvies is verantwoordelijk voor de verdere afhandeling van het verzoek. Hierbij wordt de afdeling Stafzaken en Wetgevingsadvisering waar mogelijk bijgestaan door de privacy coördinator van de betreffende directie waarop het verzoek betrekking heeft, of in geval van diens afwezigheid door de concern privacy coördinator.

6.2. Inhoudelijke beoordeling van het verzoek

Na ontvangst op de afdeling Staftaken en Wetgevingsadvisering vindt een inhoudelijke beoordeling van het verzoek plaats, waarbij wordt gekeken of de AP aan het verzoek van de betrokkene kan voldoen. Hoewel het in principe de bedoeling is dat aan de rechten van betrokkenen wordt voldaan, kan het zijn dat de AP een uitzondering moet maken. Dit kan bijvoorbeeld het geval zijn als op grond van Unie- of lidstaatrechtelijke bepalingen een bepaalde verantwoordelijkheid rust op de verwerkingsverantwoordelijke om de rechten van betrokkenen te beperken. Daarnaast wordt gekeken of een van de uitzonderingen van de AVG of UAVG van toepassing is.

In het geval van de AP zal bijvoorbeeld gekeken moeten worden of voldaan kan worden aan de rechten van betrokkenen zonder dat dit de wettelijke taak van de AP in de weg staat. Ook zal gekeken moeten worden of er geen andere wettelijke plichten zijn die aan voldoening in de weg staan. Zo kan een wettelijke plicht om gegevens te bewaren bijvoorbeeld betekenen dat niet altijd voldaan kan worden aan een verzoek van een betrokkene om de op hem of haar betrekking hebbende persoonsgegevens te wissen. En als een betrokkene bijvoorbeeld bezwaar maakt tegen de verwerking van zijn persoonsgegevens in het kader van een onderzoek dan zal de AP moeten beoordelen of zij aan dit verzoek kan voldoen.

6.3. Afhandeling van het verzoek

Indien de afdeling Staftaken en Wetgevingsadvisering na beoordeling tot de conclusie komt dat het verzoek moet worden afgewezen, deelt zij de betrokkene schriftelijk gemotiveerd mede waarom niet aan het verzoek kan worden voldaan. De privacy coördinator van de betreffende directie en de concern privacy coördinator ontvangen eveneens een afschrift.

Als de afdeling Staftaken en Wetgevingsadvisering tot het oordeel komt dat een verzoek om inzage moet worden toegewezen, wordt een kopie verstrekt van de persoonsgegevens die worden verwerkt en wordt de informatie verstrekt als bedoeld in artikel 15, eerste lid, van de AVG. Deze afdeling is verantwoordelijk voor de verdere afhandeling van het verzoek, maar schakelt voor de uitvoering daarvan de afdeling(en) en/of medewerker(s) in die toegang hebben tot de desbetreffende persoonsgegevens. Zij zijn gehouden de benodigde gegevens en informatie per ommegaande aan de afdeling Staftaken en Wetgevingsadvisering te verstrekken. De direct leidinggevende draagt hiervoor de verantwoordelijkheid.

Bij toewijzing van het verzoek om gegevenswissing, dataportabiliteit, wijziging, beperking van de verwerking en bezwaar, zijn nadere handelingen binnen de organisatie noodzakelijk. De afdeling Staftaken en Wetgevingsadvisering schakelt daarvoor de concern privacy coördinator resp. de privacy coördinatoren van de betreffende directie(s) en/of afdeling(en) in en/of medewerker(s) die toegang hebben tot de

desbetreffende persoonsgegevens, teneinde ze te wissen, over te dragen, te wijzigen of aan te vullen, de verwerking te beperken of de verwerking te staken. Deze afdelingen en/of medewerkers zijn gehouden deze handelingen per ommegaande uit te voeren. De direct leidinggevende is hiervoor verantwoordelijk. De afdeling Staftaken en Wetgevingsadvisering is verantwoordelijk voor de verdere afhandeling van het verzoek en deelt de uitkomst van het verzoek schriftelijk mede aan de betrokkene. Waar nodig wordt duidelijk gemaakt hoe aan het verzoek is voldaan.

6.4. Termijn voor afhandeling

De afdeling Staftaken en Wetgevingsadvisering zorgt dat zij in binnen een maand na binnenkomst reageert op het verzoek van de betrokkenen. In deze eerste reactie kan de AP aan het verzoek voldoen of duidelijk maken waarom zij niet aan het verzoek zal voldoen. In uitzonderlijke gevallen, bijvoorbeeld als verzoek bijzonder complex is of als één betrokkene bijzonder veel verzoeken heeft gedaan, zal de AP binnen drie maanden antwoorden op het verzoek. Als de AP niet binnen een maand aan het verzoek kan voldoen zal zij de betrokkene in ieder geval binnen een maand laten weten dat zij meer tijd nodig heeft om aan het verzoek te voldoen.