nationale ombudsman

Retouradres: Postbus 93122, 2509 AC Den Haag

[redacted]

Geachte [redacted]

Datum
15 augustus 2025

Onderwerp
Woo-besluit informatie Privacy Officer

Ons nummer
2270549

Uw kenmerk

Bijlage(n)

Contactpersoon
[redacted]

Op 14 juli 2025 heeft u een verzoek om informatie ingediend over de functie van de Privacy officer bij de Nationale ombudsman.

Specifiek vraagt u om documenten betreffende:
1. De formele functieomschrijving en het taken- en bevoegdhedenprofiel van de Privacy officer.
2. Protocollen, beleidsdocumenten en procedures die de Privacy officer dient te volgen.
3. Verslagen, memo's, rapportages en evaluaties waarin de rol of het functioneren van de Privacy officer wordt besproken.
4. Documenten over klachten met betrekking tot de uitvoering van de functie van Privacy officer (niet gericht op de persoon).
5. Opleidings- en competentieprofielen voor de functie van Privacy officer;
6. Interne en externe communicatie over de rol, taken of verantwoordelijkheden van de Privacy officer.
7. Alle communicatie (inclusief correspondentie, adviezen en rapportages) tussen de Nationale Ombudsman en de Autoriteit Persoonsgegevens inzake de functie, taken of het functioneren van de Privacy officer.

Uw verzoek wordt aangemerkt als verzoek om openbaarmaking op grond van artikel 4.1 van de Wet open overheid (Woo).

Mijn reactie
Naar aanleiding van uw verzoek is gezocht in ons zaaksysteem en mailboxen op de door u genoemde onderwerpen.
Hieronder ga ik puntsgewijs in op de resultaten van de zoektocht.

1. De formele functieomschrijving en het taken-bevoegdhedenpakket van de Privacy officer.
   Mijn reactie: Er zijn twee documenten aangetroffen die nog niet openbaar zijn.
   - Notitie Rol FG en PO 6 april 2022
   - Privacybeleid 2025-2027

   Deze documenten maak ik deels openbaar. In beide documenten zijn de namen van de medewerkers onleesbaar gemaakt met de kleur zwart. Op grond van artikel 5.1, tweede lid, aanhef en onder e, van de Woo kan ik geen informatie aan u verstrekken als dit de persoonlijke levenssfeer schaadt en dit belang zwaarder weegt dan uw belang bij toegang tot op u betrekking hebbende informatie. Het gaat om persoonsgegevens die (indirect) te herleiden zijn tot een persoon zoals namen, e-mailadressen, telefoonnummers en functienamen. Ik vind het in dit geval belangrijk dat de identiteit van betrokken medewerkers van de Nationale ombudsman

Nationale ombudsman
Bezuidenhoutseweg 151
2594 AG Den Haag

Postbus 93122
2509 AC Den Haag

T 070 356 35 63
post@nationaleombudsman.nl
www.nationaleombudsman.nl

niet bekend wordt omdat dit zijn of haar privacy kan schenden. In het kader van goed werkgeverschap vind ik dat het belang van privacy zwaarder moet wegen dan het belang van openbaarheid. Dit ter bescherming van de privacy van de medewerkers.
De Woo is niet van toepassing op documenten die al openbaar zijn. Naast de gevonden documenten is informatie te vinden op de website van de Rijksoverheid (https://www.functiegebouwrijksoverheid.nl /functiegebouw/functiefamilies/advisering/senior-adviseur).

2. Protocollen, beleidsdocumenten en procedures die de Privacy officer dient te volgen.
   Mijn reactie: Deze informatie is al openbaar. Ik verwijs u naar de website van de Rijksoverheid (https://www.p-direkt.nl/informatie- rijkspersoneel-2020/rechten-en-regels/integriteit/integriteitsbeleid).
   Op onze eigen website is informatie openbaar gemaakt via Woo-besluiten in het jaar 2024:
   - Richtlijnen handelswijze No (AVG-inzageverzoeken)
   - Datalekken periode januari 2020-december 2021 (Protocol datalekken)

3. Verslagen, memo's, rapportages en evaluaties waarin de rol of het functioneren van de Privacy officer wordt besproken.
   Mijn reactie: Dit betreft het personeelsdossier van de medewerker. Deze informatie maak ik in het geheel niet openbaar. Ik verwijs u naar de motivering bij mijn reactie bij punt 1.

4. Documenten over klachten met betrekking tot de uitvoering van de functie van Privacy officer (niet gericht op de persoon).
   Mijn reactie: Deze informatie maak ik niet openbaar. Ik verwijs u naar mijn motivering bij mijn reactie bij punt 1.

5. Opleidings- en competentieprofielen voor de functie van Privacy officer;
   Mijn reactie: Ik verwijs u naar de verstrekte informatie bij mijn reactie bij punt 1.

6. Interne en externe communicatie over de rol, taken of verantwoordelijkheden van de Privacy officer.
   Mijn reactie: Ik verwijs u naar de verstrekte informatie bij mijn reactie bij punt 1.

7. Alle communicatie (inclusief correspondentie, adviezen en rapportages) tussen de Nationale ombudsman en de Autoriteit Persoonsgegevens inzake de functie, taken of het functioneren van de Privacy officer.
   Mijn reactie: Er zijn geen documenten aangetroffen die zien op dit punt.

Wijze van bekendmaking
Naast dat het besluit aan u wordt toegezonden, zal het (geanonimiseerde) besluit worden gepubliceerd op onze website.

Vragen
Als u vragen heeft over de afhandeling van uw verzoek, dan kunt u contact opnemen met de Woo-coördinator. U kunt haar bereiken via telefoonnummer (070) [redacted] Mailen naar woo@nationaleombudsman.nl kan ook. Denk er dan aan om uw dossiernummer (2270549) te vermelden.

Met vriendelijke groet,
namens de Nationale ombudsman,

[redacted]

Hanneke van Essen
Algemeen directeur

Bezwaar
Bent u het niet eens met deze reactie? Neem dan gerust contact met ons op. Doe dit wel ruim binnen de bezwaartermijn van zes weken.
Komt u er daarna nog niet uit? Dan kunt u binnen zes weken na de datum van verzending van het besluit een bezwaarschrift indienen.
Het bezwaarschrift bevat de volgende informatie:
- uw naam en adres;
- de datum waarop u het bezwaarschrift schrijft;
- een omschrijving van het besluit waar u het niet mee eens bent en het bijbehorende dossiernummer;
- de reden van uw bezwaar;
- uw handtekening.

Een bezwaarschrift kunt u indienen via de mail (jz@nationaleombudsman.nl) of per post (Nationale ombudsman, Postbus 93122, 2509 AC Den Haag). Aan het indienen van een bezwaarschrift zijn geen kosten verbonden. Als er naast u nog andere belanghebbenden betrokken zijn bij dit besluit, dan kunnen zij ook bezwaar maken tegen het besluit.

Voorlopige voorziening
Het indienen van een bezwaarschrift schort de werking van het besluit niet op. Dat betekent dat het besluit blijft gelden in de tijd dat uw bezwaarschrift in behandeling is. Meent u dat de betrokken belangen zo zwaar wegen dat u de beslissing op uw bezwaar niet kunt afwachten? Dan kunt u tegelijkertijd met of na indiening van uw bezwaarschrift een verzoek om voorlopige voorziening indienen bij de rechtbank. Hiervoor betaalt u griffiekosten. U kunt ook digitaal een verzoekschrift indienen bij deze rechtbank via https://loket.rechtspraak.nl/bestuursrecht. Daarvoor moet u wel beschikken over een elektronische handtekening (DigiD). Kijk ook op de genoemde website voor de precieze voorwaarden.

Notitie

Onderwerp	**FUNCTIONARIS GEGEVENSBESCHERMING NO EN PRIVACY OFFICER**
Dossiernaam	Privacy
Dossiernummer	
Datum	6-4-2022
Van	[redacted]
Aan	BVO / CIO

1. Inleiding

"De Nationale ombudsman (No) verwerkt in het kader van het primair proces en zijn bedrijfsvoering persoonsgegevens en vindt het belangrijk dat met deze persoonsgegevens zorgvuldig wordt omgegaan en dat deze vertrouwelijk worden behandeld. De Nationale ombudsman is krachtens de Algemene Verordening Gegevensbescherming (AVG c.q. Verordening) als overheidsinstantie verplicht om een Functionaris Gegevensbescherming (FG) aan te stellen. Om de onafhankelijkheid van de FG te kunnen borgen en ter operationele ondersteuning is het van belang om ook een Privacy officer (PO) aan te stellen.
Deze notitie beschrijft de rol en de verplichtingen die over en weer gelden tussen de FG, PO en de No"

Uit de AVG vloeit voort dat een FG een sleutelfiguur is bij het waarborgen van gegevensbeheer en worden regels voor zijn/haar aanwijzing, positie en taken vastgelegd. Een FG aanstellen is een eerste stap, maar de FG moet ook voldoende autonomie en middelen krijgen om hun taken doeltreffend te kunnen uitoefenen.[1]

Om de onafhankelijkheid van de FG te kunnen borgen, vindt de operationele uitvoering door de PO plaats. De FG kan zich hierdoor primair richten op zijn toetsende rol en hiermee wordt de kans verkleind dat de FG zijn eigen werk keurt.

De vereisten voor een PO zijn niet vastgelegd in de AVG. Dit geeft de organisatie vrijheid in hoe deze rol ingevuld kan worden. In deze notitie wordt beschreven hoe de No invulling geeft aan beide rollen en wat hun taken en verantwoordelijkheden zijn.

[1] Richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO), WP29.

1. Rol van de Functionaris gegevensbescherming

De Functionaris gegevensbescherming (FG) heeft als intern toezichthouder een onafhankelijke positie en beschikt over toereikende kennis, voldoende middelen en capaciteit om zijn taken in het kader van de AVG naar behoren te kunnen uitvoeren. De belangrijkste taak van de FG is om erop toe te zien dat de AVG nageleefd wordt.[2] Daarnaast fungeert de FG als aanspreekpunt richting de nationale toezichthouder en heeft de FG een adviserende rol.

De FG speelt een fundamentele rol in het creëren van een cultuur van gegevensbescherming binnen de organisatie en helpt ook bij de implementatie van essentiële elementen uit de algemene verordening gegevensbescherming, zoals de beginselen van gegevensverwerking, de rechten van de betrokkenen, privacy by design en privacy by default, register van verwerkingsactiviteiten, beveiliging van de verwerking en melding van en communicatie over inbreuken met betrekking tot gegevens.[3]

Het zijn van FG binnen de No is geen voltijds positie. De andere taken en plichten van de FG binnen de No mogen niet conflicteren met diens taken als FG. Zo mag de FG niet ook een functie vervullen waarbij deze het doel en de middelen voor gegevensverwerkingen vaststelt.

Wordt tegen het advies van de FG in een besluit genomen dat naar zijn oordeel in strijd is met de AVG, dan kan de FG zijn advies voorleggen aan de directeur van de No. Bij verschil van inzicht wordt vastgelegd waarom het advies van de FG niet is gevolgd.

Mensen van wie door de No gegevens worden verwerkt (betrokkenen) moeten contact kunnen opnemen met de FG. De betrokkenen moeten zich kunnen wenden tot de FG voor alle aangelegenheden die verband houden met de AVG, in het bijzonder daar waar het de uitoefening van hun rechten op grond van de AVG betreft.

Taken van de FG

De FG binnen de No is verantwoordelijk voor het uitvoeren van een aantal taken. Deze zijn onder te verdelen in 4 categorieën:

1. Adviseren
2. Toezien op naleving
3. Samenwerking met contactpunt van de AP
4. Optreden als contactpunt voor betrokkenen

1. Adviseren

- De FG informeert en adviseert, gevraagd en ongevraagd aan alle lagen in de organisatie over de verplichtingen op grond van de AVG, de Uitvoeringswet AVG (UAVG) en andere privacywetgeving. De No is verplicht om de FG vooraf te raadplegen bij aangelegenheden over de verwerking van persoonsgegevens.
- De FG legt periodiek verslag af aan het MT over de stand van zaken ten aanzien van privacy compliance in de organisatie.
- Het advies van de FG is niet bindend. De organisatie kan het advies van de FG, gemotiveerd, terzijde leggen en dient het afwijkende besluit vast te leggen.
- De FG geeft advies naar aanleiding van de bevindingen van een DPIA en ziet ook toe op de opvolging van zijn advies. De FG is in principe niet betrokken bij de uitvoering van een DPIA.

[2] Artikel 39(1)(b) AVG
[3] Richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO), WP29, P.14

- Naar aanleiding van een uitgevoerde audit geeft de FG advies over op basis van de bevindingen.
- Bij een datalek dient de FG geraadpleegd te worden om te bepalen of het incident gemeld moet worden bij de AP en de betrokkene(n).

2. **Toezien op naleving**
   De FG moet er op toezien dat binnen de organisatie de regels van de AVG worden nageleefd. Dit betreft voornamelijk een toetsing of controle achteraf.
   - Ad hoc of incident gedreven toetsing naar aanleiding van vragen of klachten van betrokkenen.
   - Structurele toetsing aan de hand van een jaarlijks audit plan waarin onder andere aandacht is voor:
     - PDCA cyclus op processen, middelen en beleid vastgelegd in GRCControl
     - AVG compliance bij externe leveranciers
     - Het register van verwerkingen
     - Behandeling van rechten van betrokkenen
     - Het register van datalekken

3. **Samenwerking met de AP**
   Ten aanzien van de verwerking van persoonsgegevens is de FG voor de AP het eerste aanspreekpunt. De AP beschikt over de contactgegevens van de FG.
   - De FG kan zelf contact opnemen met de AP voor advies of een zogenaamde voorafgaande raadpleging, indien nodig.
   - De AP neemt contact op de met de FG in geval van klachten over de No.

4. **Optreden als contactpunt voor betrokkenen**
   Betrokkenen die hun AVG rechten willen uitoefenen melden zich bij de FG. De FG beoordeelt het verzoek en zet deze door naar de PO voor behandeling.

Deskundigheid en vaardigheden van de FG

Een FG wordt aangewezen op basis van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen om de vereiste taken uit te voeren.[4]

Voor het vereiste niveau van deskundigheid van FG wordt geen definitie gegeven in de AVG. Het Europees Comité voor gegevensbescherming geeft een nadere duiding door aan te geven dat het niveau van deskundigheid in verhouding moet staan tot de gevoeligheid en de complexiteit van de gegevens, alsook de hoeveelheid gegevens die een organisatie verwerkt. Het is aan de verwerkingsverantwoordelijke om hierover een weloverwogen beslissing te maken.

Daarnaast dient de FG enige ervaring te hebben met nationale en Europese wetten en praktijken op het gebied van gegevensbescherming, alsook een grondige kennis van de AVG . Kennis van de bedrijfstak en van de organisatie heeft daarnaast de voorkeur. De FG moet voldoende inzicht hebben in de uitgevoerde verwerkingsactiviteiten, de informatiesystemen en de behoeften van de organisatie op het vlak van gegevensbeveiliging en gegevensbescherming. Wanneer het om een overheidsinstantie of overheidsorgaan gaat, moet de FG ook een gedegen kennis hebben van de administratieve regels en procedures van de organisatie.[5]

[4] Art. 37 lid 5 AVG
[5] Richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO), WP29, p.14;

De FG dient naast de genoemde kennis tevens te beschikken over de persoonlijke vaardigheden en kwaliteiten zoals integriteit en een hoge mate van professionele ethiek.

Verplichtingen van de No bij het aanstellen van een FG

Het is de verantwoordelijkheid van de No om ervoor zorg te dragen dat de FG over voldoende middelen en mandaat beschikt om de rol goed te kunnen vervullen. Om dit te waarborgen dient de No maatregelen te nemen die een correcte uitvoering borgen, hiertoe behoren o.a.:

1. De FG dient onafhankelijk zijn rol te kunnen vervullen. Dit betekent dat de FG geen instructie mag ontvangen ten aanzien van het uitvoeren van de werkzaamheden als FG. De FG dient zich een onafhankelijke visie te kunnen vormen over de uitleg van de AVG.

2. De FG heeft een vorm van ontslagbescherming: de FG kan niet ontslagen of gestraft worden voor de uitvoering van zijn taken.

3. De FG is niet eindverantwoordelijk voor de naleving van de AVG. De verwerkingsverantwoordelijke blijft eindverantwoordelijk voor de goede naleving van de AVG. De FG wordt geraadpleegd en houdt toezicht, maar is niet de degene die uiteindelijk de beslissing neemt over het al dan niet verwerken van persoonsgegevens of het nemen van maatregelen.

4. De FG wordt tijdig en behoorlijk betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. Om te waarborgen dat de FG inderdaad op tijd en in voldoende mate wordt betrokken, wordt de FG:

    - Uitgenodigd om aan vergaderingen van de leiding van de No deel te nemen zodra daar aangelegenheden besproken worden die verband houden met de bescherming van persoonsgegevens.
    - Uitgenodigd wanneer in ander verband beslissingen met gevolgen voor de gegevensbescherming worden genomen.
    - Onmiddellijk geraadpleegd indien zich een datalek of een ander (privacy gerelateerd) incident zich voordoet.

5. De FG heeft zonder beperkingen toegang tot alle persoonsgegevens en verwerkingsactiviteiten zodat de FG zelf kan onderzoeken welke verwerkingsactiviteiten plaatsvinden en of deze voldoen aan de vereisten van de AVG.

6. Verder worden de middelen ter beschikking gesteld die de FG nodig heeft om zijn taken te vervullen. Deze middelen zijn bijvoorbeeld: voldoende tijd om zijn taken uit te voeren, voldoende financiële middelen en de mogelijkheid tot (bij)scholing.

2. Rol van de privacy officer

Het doel van de PO is om op tactisch niveau te adviseren en op operationeel niveau invulling te geven aan de naleving van de AVG en het privacy beleid. Daarmee is de rol van de PO duidelijk anders dan die van de FG.

1. De PO beschikt niet over toezichthoudende bevoegdheden.

2. De PO is ten aanzien van privacy de spin in het web van de organisatie. Waar de FG voornamelijk een toetsende rol heeft ten aanzien van de AVG, geeft de PO juist invulling aan het privacy beleid.

3. De PO heeft een uitvoerende rol en is daarmee verantwoordelijk voor het implementeren en naleven van het privacy beleid van de organisatie. Dit doet de PO in nauwe samenwerking met de FG en Chief Information Security Officer (CISO).

4. Alhoewel de PO verantwoordelijk is voor de implementatie en naleving van het privacy beleid, is hij/zij uiteindelijk niet eindverantwoordelijk. Deze eindverantwoordelijkheid ligt bij het bestuur van de organisatie (de verwerkingsverantwoordelijke).

5. De PO beschikt niet zoals de FG over een onafhankelijke positie en is gepositioneerd binnen het team i-Regie.

Taken van de PO

Hieronder worden de taken van de PO benoemd per aandachtsgebied.

1. Met betrekking tot het privacy beleid
- Het implementeren en naleven van het privacy beleid
- Het opstellen van het privacy plan
- Het coördineren van het privacy plan

2. Met betrekking tot het naleven van AVG verplichtingen
- Adviseren en ondersteunen bij opstellen van verwerkingsovereenkomsten
- Beheren van het verwerkingsregister
- Adviseren en ondersteunen bij de uitvoer van een DPIA
- Coördineren, inventariseren en behandelen van datalekken
- Stimuleren van bewustzijn met betrekking tot privacy in het dagelijks werk binnen de organisatie
- Coördineren van de afhandeling van verzoeken met betrekking tot de rechten van betrokkenen
- Adviseren over privacy en de uitgangspunten van privacy by design en privacy by default bij de start en tijdens de uitvoer van nieuwe projecten
- Het registreren, bijhouden en uitvoeren van privacy maatregelen in een GRC omgeving

3. Informeren en adviseren van de organisatie
- Het adviseren en ondersteunen van de FG en management met betrekking tot privacy compliance
- Advies geven binnen de No over de verwerking van persoonsgegevens en de mogelijk te nemen maatregelen

- Het adviseren van collega's over de verwerking van persoonsgegevens
- Aanspreekpunt voor de organisatie met betrekking tot privacy vraagstukken
- Het samen met de FG zorgdragen voor de compliance-rapportages en risico-rapportages aan de directie

Deskundigheid en vaardigheden van de PO

Een Privacy Officer beschikt over de volgende kennis en ervaring:

- Minimaal een afgeronde hbo-opleiding;
- Minimaal 3 jaar werkervaring in een vergelijkbare functie;
- Actuele kennis van de AVG en aanverwante wet- en regelgeving;
- Erkende certificeringen met betrekking tot privacy is een pré (CIP/E en/of CIP/M);
- Ervaring met Governance, Risk & Compliance systematiek (GRC) en het hanteren van een (werkende) PDCA-Cyclus.

Een Privacy Officer beschikt over de volgende competenties:

- Resultaatgericht en organisatiesensitief;
- Sterk in projectmatig werken en vaardig in het geven van advies;
- Communicatief zeer vaardig en kan goed schakelen tussen verschillende lagen binnen de organisatie;
- Sterk in plan- en projectmatig werken

Privacy beleid

2025-2027

nationale ombudsman

Document classificatie
Vertrouwelijk

Referentie documenten
- Governance beleid IBP 1.0
- Informatiebeveiligingsbeleid
- Procedure AVG inzageverzoeken 1.0
- Protocol datalekken No V1.0
- Informatiebeveiliging en Privacy Bewustzijn Beleid 2024-2026

Versienummer	1.0
Eigenaar	Privacy officer
Opgesteld door	Nationale ombudsman
Status	Definitief
Goedgekeurd door	Algemeen Directeur
Vastgesteld op	9-1-2025
Datum eerste versie	6-6-2024
Laatst bijgewerkt	20-01-2025

Versiebeheer

Datum	Versie	Aangepast door	Wijzigingen
6-6-2024	0.1	[redacted]	Eerste versie
4-7-2024	0.2		Review en aanpassingen
18-7-2024	0.3		Feedback FG verwerkt
29-8-2024	0.4		Feedback CISO en ISO verwerkt
26-9-2024	0.5		Feedback JZ verwerkt + aanpassingen nav vastgestelde verbeteracties GRC
1-10-2024	0.6		Feedback manager O&O verwerkt
10-10-2024	0.7		Toevoeging onder 2.2 & 2.3
7-11-2024	0.8		Feedback CIO-overleg verwerkt
24-12-2024	0.9		verbeteracties interne audit verwerkt
9-1-2025	0.9		Vaststelling in Directeurenoverleg
20-1-2025	1.0		Definitief gemaakt na vaststelling

Definitielijst

Term	Omschrijving
AP	Autoriteit Persoonsgegevens
Audit	Een systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen van bewijsmateriaal en het objectief evalueren daarvan om vast te stellen in welke mate er wordt voldaan aan de door of voor de ombudsman opgestelde criteria ten aanzien van het privacy beleid of wetgeving.
AVG	Algemene Verordening Gegevensbescherming
Betrokkene(n)	De persoon of personen van wie een organisatie persoonsgegevens verwerkt.
Bijzondere persoonsgegevens	Bijzondere persoonsgegevens zijn gegevens die zo gevoelig zijn dat de verwerking ervan iemands privacy ernstig kan beïnvloeden. Voorbeelden zijn gegevens die iets zeggen over iemands gezondheid, ras, godsdienst, politieke voorkeur, strafrechtelijk verleden of seksuele gerichtheid.
Centraal beheerde applicaties	Applicaties waarvan het technisch- en functioneel applicatiebeheer is ondergebracht bij de afdeling Informatieregie.
Datalek	Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is. Waarbij de oorzaak een inbreuk op de beveiliging van deze gegevens is. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens door zo'n inbreuk valt onder een datalek.
DPIA	Data Protection Impact Assessment
E.E.R	Europese Economische Ruimte (EER). Hieronder vallen alle EU-landen en Liechtenstein, Noorwegen en IJsland.
FG	Functionaris voor de Gegevensbescherming
Governance	De toegepaste privacy systematiek binnen de ombudsman
Grondslag	Organisaties mogen alleen persoonsgegevens verwerken als zij daar een goede reden voor hebben. De juridische term hiervoor is 'grondslag'. In de AVG staan 6 mogelijke grondslagen.
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.
PO	Privacy Officer
Uitvoeringswet AVG	Deze nationale wet geeft toelichting en aanvulling over hoe de AVG in Nederland moet worden uitgevoerd.
Verwerkersovereenkomst	Een overeenkomst die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt, en waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven.

Verwerker	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van en in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.
Verwerking	Een verwerking of een geheel van verwerkingen 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.
Verwerkingsregister	In een verwerkingsregister staat informatie over de persoonsgegevens die een organisatie verwerkt.
Verwerkingsverantwoordelijke	De verwerkingsverantwoordelijke bepaalt de doeleinden waarvoor en de middelen waarmee persoonsgegevens worden verwerkt. De onderneming/organisatie die beslist „waarom” en „hoe” persoonsgegevens moeten worden verwerkt, is de verwerkingsverantwoordelijke. Medewerkers die binnen deze onderneming/organisatie persoonsgegevens verwerken, doen dit om haar taken als verwerkingsverantwoordelijke uit te voeren.

1 Inhoudsopgave

Inleiding

De ombudsman verwerkt voor het uitvoeren van zijn wettelijke taken en zijn bedrijfsvoering persoonsgegevens en vindt het belangrijk dat met deze persoonsgegevens zorgvuldig wordt omgegaan en dat deze vertrouwelijk worden behandeld. De Algemene Verordening Gegevensbescherming (AVG) biedt waarborgen voor de bescherming van de persoonlijke levenssfeer van natuurlijke personen met betrekking tot het verwerken van persoonsgegevens. De ombudsman heeft in lijn met de bepalingen uit de AVG het onderhavig privacy beleid opgesteld voor de verwerking van persoonsgegevens.
Waar in dit document wordt gesproken over de ombudsman wordt hier bedoeld de ambtelijke organisatie van de Nationale ombudsman, Veteranenombudsman en Kinderombudsman.

1.1 Leeswijzer

Hoofdstuk 1 bevat de inleiding waarin het doel en de organisatorische opzet van dit beleidsstuk worden beschreven. In hoofdstuk twee worden enkele begrippen die centraal staan in dit document toegelicht, zoals: *persoonsgegevens*, *verwerking* en *bijzondere persoonsgegevens*. Daarnaast wordt toegelicht welke (bijzondere) persoonsgegevens de ombudsman verwerkt en voor welke doeleinden. Hoofdstuk drie beschrijft vervolgens hoe de rollen en verantwoordelijkheden in de organisatie zijn belegd. In hoofdstuk vier worden de beginselen en uitgangspunten van dit beleid beschreven. Dit hoofdstuk biedt ook de kaders en handvatten voor medewerkers van de ombudsman om op de gewenste wijze te kunnen handelen wanneer het gaat om persoonsgegevens. Hoofdstuk vijf gaat in op de organisatorische en technische maatregelen van het privacy beleid. In hoofdstuk 6 wordt de wijze van controle op dit beleid beschreven.

1.2 Doel en toepassingsbereik

Doel van het privacybeleid is om:

- Regels vast te stellen voor het verwerken van persoonsgegevens door de ombudsman;
- Transparantie te bieden over de wijze waarop bij de verwerking van persoonsgegevens door de ombudsman de regels uit de AVG worden toegepast;
- Aantoonbaar te maken dat de ombudsman voldoet aan de AVG.

Het privacy beleid is van toepassing op de gehele organisatie van de ombudsman. Het beleid valt onder de verantwoordelijkheid van de algemeen directeur. Het privacy beleid is tot stand gekomen volgens het Plan-Do-Check-Act proces. Op het privacy beleid wordt elke drie jaar een evaluatie uitgevoerd door de privacy officer, tenzij aanleiding is om dit eerder te doen. Het beleid en eventuele substantiële wijzigingen hierop worden formeel in het DT-overleg vastgesteld. De privacy officer zorgt dat alle medewerkers op de hoogte zijn van het beleid en het kunnen toepassen binnen hun dagelijks werkzaamheden.
Na vaststelling binnen het DT zijn de respectievelijke managers verantwoordelijk voor de naleving binnen hun afdeling of proces, de managers worden hierbij ondersteund door de AVG-vertegenwoordigers en de privacy officer. Toetsing van naleving van het beleid valt onder de verantwoordelijkheid van de FG.
Het privacy beleid is een document voor intern gebruik. De belangrijkste uitgangspunten van het privacy beleid zijn vertaald naar verschillende korte verklaringen die beschikbaar zijn gesteld voor externe partijen, zoals burgers, bezoekers en leveranciers, bijvoorbeeld op de website van de ombudsman of in overeenkomsten.

1.3 Uitgangspunten bij de verwerking van persoonsgegevens

Transparantie bij het verwerken van persoonsgegevens is een cruciaal onderdeel van de AVG. Het uitgangspunt van dit privacy beleid is dat persoonsgegevens in overeenstemming met de relevante wet- en regelgeving worden verwerkt. Ook wordt rekening gehouden met beginselen zoals behoorlijke en zorgvuldige verwerking, waarbij de belangen van de betrokkenen centraal staan. Per situatie dient een balans te worden gevonden tussen het belang van de ombudsman bij de uitvoering van diens wettelijke taak en het belang van de betrokkene om in vrijheid keuzes te maken met betrekking tot zijn persoonsgegevens. Om aan het bovenstaande te voldoen, gelden de volgende uitgangspunten:

1. De verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen zoals aangeduid in de AVG en de Uitvoeringswet AVG (zie 4.1);
2. Persoonsgegevens worden pas verwerkt indien voorafgaand aan de verwerking een gerechtvaardigd doeleinde is geformuleerd. De doeleinden waarvoor de persoonsgegevens worden verwerkt zijn specifiek en vooraf duidelijk omschreven (zie 4.3);
3. De verwerking van persoonsgegevens is, met het oog op het doel, ter zake dienend. Dit betekent dat de hoeveelheid persoonsgegevens en het soort persoonsgegevens beperkt blijft tot de persoonsgegevens die noodzakelijk worden geacht voor het gespecificeerde doel (zie 4.4);
4. Technische en organisatorische maatregelen zullen worden getroffen zodat de te verwerken persoonsgegevens juist en actueel zijn (zie 4.6);
5. Persoonsgegevens worden zowel technisch als organisatorisch op adequate wijze beschermd, zodat een beveiligingsnorm gehanteerd kan worden dat een passend beveiligingsniveau garandeert (zie 4.7);
6. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze oorspronkelijk zijn verkregen (zie 4.3);
7. Persoonsgegevens worden niet langer verwerkt dan noodzakelijk wordt geacht voor de vastgestelde doeleinden van de verwerking. Hierbij worden de bewaar- en vernietigingstermijnen in acht genomen zoals vastgesteld in de Archiefwet en (de daarop gebaseerde) basisselectielijsten (zie 4.5);
8. De rechten van betrokkenen worden gerespecteerd en in acht genomen (zie 5.2);

1.4 Relatie en overlap met informatiebeveiliging

Informatiebeveiliging is het geheel van preventieve, detective, repressieve en correctieve maatregelen alsmede procedures en processen die de beschikbaarheid, vertrouwelijkheid en integriteit van alle vormen van informatie garanderen, met als doel de continuïteit van de informatie en de informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken. Daarvoor worden organisatorische, technische en personele maatregelen genomen. De ombudsman heeft beleid opgesteld voor informatiebeveiliging. Dit beleid is gepubliceerd op het intranet van de ombudsman.

Bij informatiebeveiliging spelen drie begrippen een sleutelrol, namelijk:

- Beschikbaarheid bevat de garanties dat informatie voor gebruikers beschikbaar is op het moment waarop zij de informatie nodig hebben. Kenmerken van beschikbaarheid zijn tijdigheid, continuïteit en robuustheid.
- Integriteit geeft de mate aan waarin de informatie actueel en correct is. Kenmerken zijn juistheid, volledigheid en geautoriseerdheid van de transacties.

- Vertrouwelijkheid of exclusiviteit is het kwaliteitsbegrip waaronder privacybescherming maar ook de exclusiviteit van informatie gevangen kan worden. Het waarborgt dat alleen geautoriseerde toegang krijgen en dat informatie niet kan uitlekken.

Het privacy beleid en informatiebeveiliging zijn niet los van elkaar te zien, maar overlappen elkaar ook niet volledig. Het privacy beleid stelt naast de vraag of de persoonsgegevens goed beveiligd zijn (zie bovenstaande sleutelbegrippen beschikbaarheid, integriteit en vertrouwelijkheid) ook nog aanvullende vragen, namelijk: of de persoonsgegevens wel mogen worden verzameld en verder verwerkt, op welke manier, en in hoeverre dit noodzakelijk is. Deze vragen maken geen deel uit van het informatiebeveiligingsbeleid. Daarnaast houdt het privacy beleid zich enkel bezig met persoonsgegevens en gaat informatiebeveiliging over veel meer vormen van gegevens.

2 Verwerking van persoonsgegevens

Dit privacy beleid omvat alle verwerkingen van persoonsgegevens die door de ombudsman worden uitgevoerd. Hieronder worden de begrippen die centraal staan in dit document nader toegelicht. Daarnaast wordt toegelicht welke (bijzondere) persoonsgegevens de ombudsman verwerkt en voor welke doeleinden.

2.1 Verwerken

Het verwerken van persoonsgegevens is een ruim begrip. Hieronder wordt in ieder geval het volgende verstaan: het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

De medewerkers van de ombudsman ondersteunen de ombudsman bij zijn taken en maken het werk van de ombudsman toegankelijk en inzichtelijk voor de samenleving. Zij zorgen onder meer voor klachtbehandeling, onderzoek, verslaglegging, informatievoorziening, documentatie, archivering, beheer van het gebouw, doelmatig en rechtmatig financieel beheer, personeelszaken en externe voorlichting. Om het voorgaande te kunnen bewerkstelligen is het vaak noodzakelijk om persoonsgegevens te verwerken van medewerkers, burgers en bezoekers. Denk bijvoorbeeld aan persoonsgegevens die gebruikt worden voor het behandelen van klachten, de uitvoering van het personeelsbeleid, facturen en declaraties van medewerkers en uitgifte van IT-middelen.

2.2 Persoonsgegevens

Persoonsgegevens hebben betrekking op een natuurlijk persoon die aan de hand van die gegevens kan worden geïdentificeerd. Identificatie kan geschieden met behulp van de informatie afzonderlijk of in samenhang met andere informatie waarover de ombudsman of een door haar ingeschakelde (sub)verwerker beschikt.

2.2.1 Persoonsgegevens van verzoekers

- NAW-gegevens
- Contactgegevens (telefoonnummer, e-mailadres)
- Alle gegevens die de verzoeker relevant acht voor zijn klacht en aan de ombudsman verstrekt
- Gegevens die de ombudsman tijdens een onderzoek/interventie van overheidsinstanties ontvangt en soms van andere instanties/personen (bijvoorbeeld een gemachtigde)

De ombudsman verwerkt persoonsgegevens van verzoekers in het kader van de hem opgedragen wettelijke taken.

2.2.2 Persoonsgegevens van (oud-)medewerkers van bestuursorganen

- Naam
- Contactgegevens (telefoonnummer, e-mailadres)
- Functie

De ombudsman verwerkt persoonsgegevens van (oud-)medewerkers van bestuursorganen in het kader van de hem opgedragen wettelijke taken.

2.2.3 Persoonsgegevens van bezoekers

- Naam
- Identiteitsbewijs (optioneel)

De ombudsman verwerkt persoonsgegevens van bezoekers om hen te kunnen identificeren.

2.2.4 Persoonsgegevens van (oud-)medewerkers

- NAW-gegevens
- Contactgegevens (telefoonnummer, e-mailadres)
- Financiële gegevens (bankrekeningnummer, loon, vergoedingen, declaraties)
- Beroep en studies (functie, gegevens met betrekking tot gevolgde opleidingen, cursussen en trainingen, behaalde diploma's, certificaten, cijferlijsten)
- BSN
- Kopie ID/Paspoort

De ombudsman verwerkt persoonsgegevens van medewerkers voor tenminste de volgende doeleinden:

- Het berekenen, vaststellen en betalen van salarissen, vergoedingen, belastingen en premies ten behoeve van een personeelslid;
- De evaluatie (functioneren en beoordeling) en ontwikkeling van personeel;
- Vastleggen controle identiteit personeelslid;
- Ziekteverzuim begeleiding en re-integratie ;
- Het uitvoeren van medewerkers tevredenheidsonderzoeken;
- Werving en selectie;
- Op verzoek van de medewerker financieel advies geven & begeleiding van medewerkers m.b.t. inkomsten, salaris voor nu en in de toekomst;
- Bijhouden welke medewerkers een bepaalde training hebben gevolgd;
- Het monitoren van integriteit en integriteitsschendingen;
- Uitgifte IT-middelen.

2.3 Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn gegevens over iemands godsdienst of levensovertuiging, ras, politieke voorkeur, gezondheid, seksuele geaardheid of voorkeur, lidmaatschap van een vakbond, verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon.

In beginsel is het wettelijk verboden om bijzondere persoonsgegevens te verwerken, tenzij er sprake is van een wettelijke grondslag als bedoeld in artikel 9 lid 2 van de AVG. Dit zijn onder andere: uitdrukkelijke toestemming van de betrokkene of een zwaarwegend algemeen belang. Voor de verwerking van bijzondere persoonsgegevens gelden zwaardere eisen ten aanzien van de informatiebeveiliging. In het geval waar de basisbescherming onvoldoende is voor de verwerking van bijzondere persoonsgegevens zal de ombudsman passende technische en organisatorische beveiligingsmaatregelen treffen.

2.3.1 Bijzondere persoonsgegevens van verzoekers

Voor de verwerking door de ombudsman bevat de Uitvoeringswet AVG in artikel 23 onder b een uitzondering. Het verbod om bijzondere persoonsgegevens te verwerken geldt voor de ombudsman niet:

- Voor zover de verwerking noodzakelijk is voor de uitvoering van de hem wettelijk opgedragen taken; en
- onder de voorwaarde dat bij die uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

Dit betekent dat indien de ombudsman bijzondere persoonsgegevens verwerkt in het kader van de aan de ombudsman opgedragen taken en informatie wordt opgevraagd (die noodzakelijk is om die taken uit te voeren) geen toestemming van de verzoeker vereist is om zijn of haar (bijzondere) persoonsgegevens te verwerken. Deze uitzondering geldt volgens art. 32 onder e van de Uitvoeringswet AVG ook voor strafrechtelijke gegevens.

De ombudsman verwerkt bijzondere persoonsgegevens die door verzoekers worden verstuurd. Het gaat dan om gegevens zoals, maar niet beperkt tot, gezondheidsgegevens. Daarnaast verwerkt de ombudsman gegevens van strafrechtelijke aard die door verzoekers of instanties worden verstuurd.

2.3.2 Bijzondere persoonsgegevens van medewerkers

De ombudsman verwerkt in ieder geval de volgende bijzondere persoonsgegevens van medewerkers:

- Melding ziekteverzuim, arbeidsongeschiktheid en re-integratiegegevens (geen medische gegevens) in het kader van de Wet Verbetering Poortwachter;
- Registratie fiscale verrekening lidmaatschap vakorganisaties;
- Registratiegegevens medewerkers met afstand tot de arbeidsmarkt;
- Nevenwerkzaamheden, ook onbezoldigd, welke ook werkzaamheden kunnen bevatten voor politieke partijen, kerk of anderszins.

3 Rollen en verantwoordelijkheden

Om naleving van de bescherming van persoonsgegevens binnen de ombudsman te waarborgen en daarmee ook naleving aan de AVG zijn verschillende rollen belegd, zoals de Functionaris Gegevensbescherming, de Privacy Officer, de Chief Information Security Officer, de Information Security Officer, de AVG-vertegenwoordigers en de manager informatieregie. Daarnaast vervult de ombudsman als organisatie vanuit de AVG ook een rol. In dit hoofdstuk worden deze rollen nader toegelicht.

3.1 Verwerkingsverantwoordelijke

De Nationale ombudsman is de verwerkingsverantwoordelijke en als zodanig verantwoordelijk voor de naleving van de AVG, omdat het doel en de middelen voor de verwerkingen van persoonsgegevens worden vastgesteld door de ombudsman. Binnen de organisatie ligt de eindverantwoordelijkheid bij de algemeen directeur. In de praktijk betekent dit dat elke directeur van een organisatieonderdeel namens de algemeen directeur van de ombudsman verantwoordelijk is voor alle verwerkingen van persoonsgegevens die binnen het eigen onderdeel plaatsvinden.

3.2 Verwerker

Een verwerker verwerkt persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke, zonder onder het rechtstreekse gezag van de verwerkingsverantwoordelijke te vallen (iemand of een organisatie buiten de organisatie van de ombudsman). De verwerker voert slechts een taak uit die de verwerkingsverantwoordelijke heeft uitbesteed.

3.3 Functionaris gegevensbescherming

De ombudsman heeft een Functionaris Gegevensbescherming (FG) aangesteld sinds mei 2018. De contactgegevens van de FG zijn te vinden op het intranet en op de website van de ombudsman. De FG is aangemeld bij de Autoriteit Persoonsgegevens.

De FG heeft als intern toezichthouder een onafhankelijke positie en beschikt over toereikende kennis, voldoende middelen en capaciteit om zijn taken in het kader van de AVG naar behoren te kunnen uitvoeren. Onder deze taken vallen onder andere:

- Informeren en adviseren binnen de ombudsman over de verplichtingen uit hoofde van de AVG, de Uitvoeringswet en andere relevante wet- en regelgeving met betrekking tot de bescherming van persoonsgegevens;
- Toezien op de naleving van de AVG en andere relevante wet- en regelgeving m.b.t. de bescherming van persoonsgegevens en van het door de ombudsman vastgestelde beleid voor de bescherming van persoonsgegevens;
- Adviseren over de Data Protection Impact Assessment (DPIA) bij nieuwe of gewijzigde verwerkingen, zowel de inhoudelijke beoordeling als de naleving van de voorgenomen beheersmaatregelen;
- Schakel tussen de ombudsman en de Autoriteit Persoonsgegevens voor wat betreft het vragen van advies omtrent de uitleg van bepaalde onderdelen van de AVG;
- Fungeren als contactpunt voor de Autoriteit Persoonsgegevens over kwesties in verband met de verwerking van persoonsgegevens;
- Onafhankelijk aanspreekpunt voor betrokkenen (bijv. medewerkers en burgers) voor alle aangelegenheden bij de verwerking van hun persoonsgegevens;

- Het afleggen van verantwoording over de verwerkingen van persoonsgegevens in het jaarverslag van de ombudsman;
- In geval van incidenten zal de FG desgevraagd adviseren bij de beoordeling of er sprake is van een datalek en de afhandeling daarvan;
- Het verzorgen van compliance-rapportages en risico-rapportages aan de directie en portefeuillehouder(s).

3.4 Privacy Officer

De Privacy Officer is uitvoerend voor het opstellen, implementeren en naleven van het privacy beleid van de organisatie. De PO zorgt ervoor dat de organisatie het privacy beleid naleeft en dat de organisatie voldoet aan toepasselijke wet- en regelgeving ten aanzien van privacy (waaronder de AVG). De taken van de PO staan hieronder beschreven:

- Het opstellen van het privacy beleid;
- Het mee opstellen van het Informatiebeveiliging en privacy jaarplan;
- Het mee coördineren van de implementatie van het IB&P jaarplan;
- Het adviseren van de FG en lijnmanagement met betrekking tot privacy compliance;
- Bewustmaking en opleiding van personeel dat betrokken is bij de verwerking van persoonsgegevens;
- Het adviseren van collega's over de verwerking van persoonsgegevens;
- Het ondersteunen bij het uitvoeren van Data Protection Impact Assessments (DPIA's);
- Het bijwerken en actueel houden van het register van verwerkingsactiviteiten binnen het eigen proces;
- Het coördineren, inventariseren en registreren van datalekken, in nauwe samenwerking met de FG;
- Het beoordelen van de impact van wijzigingen in wetgeving die gevolgen hebben voor privacy;
- Het coördineren van de afhandeling van verzoeken met betrekking tot de rechten van betrokkenen, in nauwe samenwerking met de FG die de controle op de afhandeling doet;
- Adviseren over verwerkersovereenkomsten en/of samenwerkingsovereenkomsten;
- Het ontwikkelen, evalueren en beoordelen van periodieke rapportages m.b.t. privacy-compliance en privacy-risico's;
- Het adviseren over privacy en de uitgangspunten van privacy-by-design bij de start en tijdens de uitvoering van nieuwe projecten;
- Het verzorgen met de FG van compliance-rapportages en risico-rapportages aan de directie en portefeuillehouder(s).

3.5 AVG-vertegenwoordigers

De AVG-vertegenwoordiger brengt het privacy beleid - in samenwerking met het management - onder de aandacht van de medewerkers van de eigen directie, met als doel om het privacy bewustzijn te vergroten binnen de ombudsman en daarnaast te ondersteunen met het borgen van het privacy beleid.
Binnen elke directie (organisatieonderdeel) van de ombudsman wordt minimaal één AVG-vertegenwoordiger benoemd. De AVG-vertegenwoordigers ontvangen periodiek (interne) scholingsactiviteiten om hun kennisniveau op peil te houden.
De AVG-vertegenwoordiger heeft de volgende taken:

- Fungeren als 'adviesloket' bij vragen binnen de eigen dienst over de AVG. De AVG-vertegenwoordiger fungeert als eerste aanspreekpunt binnen de eigen dienst voor vragen over de AVG.
- Inventariseren, beoordelen, bijhouden en melden van verwerkingen persoonsgegevens in het AVG-register.

- Fungeren als aanspreekpunt voor de Privacy Officer bij incidenten (waaronder datalekken) en privacy verzoeken.
- Zorgen dat de AVG blijvend onder de aandacht is van de medewerkers van de eigen dienst en draagt zo bij aan het privacy bewustzijn van de medewerkers van de ombudsman.
- Deelname aan het maandelijkse AVG-overleg en vervolgens relevante onderwerpen binnen de eigen dienst onder de aandacht brengen.

3.6 Chief Information Security Officer (CISO)

De CISO is verantwoordelijke voor en houdt toezicht op het naleven van het Informatiebeveiligingsbeleid van de ombudsman. Vanwege de raakvlakken en overlap zal er regelmatig overleg plaatsvinden tussen de CISO, ISO, Privacy Officer en/of FG, bijvoorbeeld wanneer er sprake is van incidenten, zoals datalekken of de invoering van nieuwe (technische) maatregelen. Ook met betrekking tot voorlichting, bewustwording en borging van zowel het informatiebeveiligingsbeleid als het privacy beleid zal waar mogelijk samen opgetrokken worden. Een uitgebreide rolbeschrijving van de CISO is opgenomen in het IB&P Governance beleid.

3.7 Information Security Officer (ISO)

De ISO houdt zicht bezig met het verbeteren van informatiebeveiligingsbeleid en risicomanagement. Daarnaast kan de ISO gevraagd worden om het lijnmanagement te ondersteunen en adviseren, toezien op naleving en realisatie van het beleid. Een uitgebreide rolbeschrijving van de ISO is terug te vinden in het IB&P Governance beleid.

3.8 Manager Informatieregie

De Manager informatieregie draagt er zorg voor dat de beheerde ICT-faciliteiten in overeenstemming worden gebracht met het privacy beleid, voor zover dat technisch mogelijk is. In het verlengde hiervan zorgt de Manager informatieregie ervoor dat toekomstige beheerde ICT-faciliteiten getoetst worden aan het privacy beleid. Inhoudelijke afwijkingen worden voorafgaand aan een implementatie aan de FG voorgelegd.
Bij de verwerving, ontwikkeling en onderhoud van beheerde ICT-faciliteiten worden vanaf het begin privacyoverwegingen meegenomen in het ontwerp van (nieuwe) verwerkingen van persoonsgegevens.

4 Uitgangspunten gegevensverwerking

Volgens de AVG moeten verwerkingen van persoonsgegevens voldoen aan een aantal beginselen. Deze vormen het fundament voor het privacy beleid van de ombudsman, zodat alle verwerkingen rechtmatig, veilig en verantwoord plaatsvinden. In de volgende paragrafen worden deze uitgangspunten nader toegelicht.

4.1 Rechtmatige verwerking van persoonsgegevens

Het verwerken van (bijzondere) persoonsgegevens door de ombudsman is gebaseerd op één van de grondslagen zoals beschreven in artikel 6 (of artikel 9) van de AVG.

4.2 Transparantie

De ombudsman houdt zich aan de regels omtrent het transparant maken van de door haar verrichte verwerkingen door:

1. de informatie of communicatie beknopt, transparant, begrijpelijk en gemakkelijk toegankelijk te maken, o.a. door haar privacyverklaring op de website (artikel 12, lid 1 AVG);
2. in duidelijke en eenvoudige taal worden aan te bieden (artikel 12, lid 1 AVG). Dit vereiste is extra belangrijk wanneer de informatie specifiek voor een kind bestemd is (artikel 12, lid 1 AVG);
3. de informatie schriftelijk “of met andere middelen, met inbegrip van, indien dit passend is, elektronische middelen” te verstrekken (artikel 12, lid 1 AVG);
4. indien betrokkene daarom verzoekt, de mogelijkheid om informatie mondeling mee te delen (artikel 12, lid 1 AVG); en
5. als uitgangspunt te hanteren dat informatie over het algemeen kosteloos wordt verstrekt (artikel 12, lid 5 AVG).

De ombudsman informeert betrokkenen, waaronder verzoekers, bezoekers (van de website) en medewerkers via privacyverklaringen. In het kader van transparantie wordt door de ombudsman specifiek en aantoonbaar rekening gehouden met de bescherming van kinderen.

4.3 Doelbinding

Doelbinding, dat wil zeggen dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en vervolgens alleen op met dat doel verenigbare wijze worden verwerkt. De ombudsman verwerkt persoonsgegevens voor de volgende doeleinden:

- Nakomen contractuele verplichtingen;
- Nakomen wettelijke taken;
- Relatiebeheer;
- Nakomen van administratieve verplichtingen;
- Andere noodzakelijke doeleinden voor het uitvoeren van werkzaamheden.

Het verwerkingsregister beschrijft per verwerking het doeleinde. De verwerking zal niet plaatsvinden als blijkt dat de verwerking van persoonsgegevens onverenigbaar is met het doel.

4.4 Dataminimalisatie

Dataminimalisatie houdt in dat niet meer persoonsgegevens worden verwerkt dan nodig zijn om het doel waarvoor ze verzameld worden te bereiken. Bij het ontwikkelen van nieuwe diensten en producten wordt nagedacht over welke persoonsgegevens nodig zijn om de dienst te kunnen leveren, maar ook in bestaande processen moet aandacht zijn voor dataminimalisatie.
Denk in het kader van dataminimalisatie aan de verdere verwerking van persoonsgegevens voor statistische doeleinden. Persoonsgegevens worden in dat geval (en waar mogelijk) geanonimiseerd zodat de gegevens wel bewaard kunnen blijven voor statische doeleinden zonder dat deze tot een individueel persoon herleidbaar zijn. De optimale situatie is alleen de strikt noodzakelijke persoonsgegevens te verzamelen. Indien dat niet lukt, dient ervoor gekozen te worden om alle andere gegevens direct te verwijderen als blijkt dat deze gegevens niet noodzakelijk zijn.
Dataminimalisatie moet bij de standaardinstelling van systemen die gebruikt worden en bij het ontwerp van nieuwe systemen meegenomen worden.

4.5 Opslagbeperking

De ombudsman bewaart persoonsgegevens niet langer dan redelijkerwijs noodzakelijk en in lijn met de vereisten zoals deze zijn neergelegd in de basisselectiedocumenten en de Archiefwet. De ombudsman voert daarvoor een dataretentie beleid waarmee in lijn gehandeld kan worden met deze vereisten.
Na het verlopen van de vastgestelde bewaartermijn worden persoonsgegevens (digitaal) gearchiveerd en overgedragen aan het Nationaal archief. Indien er geen wettelijke bewaartermijn bestaat voor het bewaren van de persoonsgegevens en de gegevens niet bestemd zijn voor historische, statistische of wetenschappelijke doeleinden dan worden ze op passende wijze vernietigd na het verstrijken van de relevante bewaartermijn.

4.6 Juistheid

De ombudsman neemt alle redelijke maatregelen om de persoonsgegevens die door de organisatie worden verwerkt, juist zijn en worden geactualiseerd als dat nodig is.

4.7 Integriteit en vertrouwelijkheid

Integriteit en vertrouwelijkheid zijn twee begrippen die ook in paragraaf 1.4 aan de orde zijn gekomen bij informatiebeveiliging. Voor het privacy beleid wordt onder deze begrippen verstaan dat persoonsgegevens door passende technische of organisatorische maatregelen op een dusdanige manier verwerkt worden dat een passende beveiliging is gewaarborgd zodat betrokkenen erop kunnen vertrouwen dat er zorgvuldig wordt omgegaan met hun gegevens. De organisatorische en technische maatregelen om dit beginsel binnen de ombudsman te waarborgen komen in hoofdstuk 5 aan de orde.

4.8 Verantwoordingsplicht

De verantwoordingsplicht is één van de belangrijkste verplichtingen van de AVG. Het betekent dat de ombudsman moet kunnen aantonen dat aan de regels van de AVG wordt voldaan. Het privacybeleid draagt bij aan deze verantwoordingsplicht. Daarnaast beschikt de ombudsman over een informatiebeveiliging en privacy Governance systematiek welke beschreven staat in het IB&P governance beleid. De uitgangspunten in deze beide documenten maken aantoonbaar dat er passende en effectieve interne processen en instrumenten aanwezig zijn om de bescherming van de rechten en vrijheden van alle betrokkenen te waarborgen. Daarnaast kan de ombudsman dit aantonen met het AVG-register.

5 Maatregelen voor de bescherming van persoonsgegevens

Passende technische en organisatorische maatregelen komen voort uit de principes van privacy-by-design, privacy by default en het uitvoeren van DPIA's.

5.1 Verwerkingsregister

De ombudsman verzamelt informatie over de verwerkte persoonsgegevens in een register over alle verwerkingen van persoonsgegevens. Het register wordt actueel gehouden. Het register bevat in ieder geval de volgende informatie:

- Naam en contactgegevens van de ombudsman;
- Doelen van de verwerking;
- Beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- Beschrijving van de ontvangers van de persoonsgegevens;
- Beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie en de eventueel maatregelen die zijn genomen om de gegevens te beschermen;
- De termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- Algemene beschrijving van de beveiligingsmaatregelen.

De AVG-vertegenwoordigers zijn verantwoordelijk voor de inrichting en inhoud van het verwerkingsregister.

5.2 Rechten van betrokkenen

De AVG geeft een betrokkene de volgende rechten ten aanzien van zijn/haar persoonsgegevens.

- Recht op inzage (art. 15 AVG): Het recht om onder meer een kopie te ontvangen van de verwerkte persoonsgegevens;
- Recht op vergetelheid (art. 17 AVG): het recht om ‘vergeten’ te worden, ofwel het wissen van de persoonsgegevens;
- Recht op rectificatie (art. 16 AVG): Het recht om de persoonsgegevens te laten wijzigen.
- Het recht op dataportabiliteit (art. 20 AVG). Het recht om persoonsgegevens over te laten dragen aan een andere partij.
- Het recht op beperking van de verwerking (art. 18 AVG): Het recht om minder gegevens te laten verwerken.
- Het recht om niet te worden te worden onderworpen aan geautomatiseerde individuele besluitvorming en profilering (art. 22 AVG). Oftewel: het recht op een menselijke blik bij besluiten.
- Het recht om bezwaar te maken tegen de gegevensverwerking (art. 21 AVG).
- Het recht op informatie (art. 13 en 14 AVG): Het recht op heldere informatie over wat een organisatie met persoonsgegevens gaat doen en waarom. Duidelijk gemaakt moet worden welke persoonsgegevens er worden verwerkt, waarom dat gebeurd (welk doel) en met wie gegevens worden gedeeld of doorverkocht aan andere organisaties en welke organisaties dat precies zijn.

De ombudsman waarborgt de rechten van betrokkenen en houdt persoonsgegevens juist en actueel. Er is een procedure ingericht om te zorgen dat betrokkenen hun rechten kunnen uitoefenen, welke staat beschreven in de Procedure AVG verzoeken. De inhoud van de procedure wordt duidelijk en transparant gecommuniceerd, zowel op het intranet als op het internet. In het kader van rechten van betrokkenen, wordt door de ombudsman specifiek en aantoonbaar rekening gehouden met de bescherming van kinderen. Er wordt op een voor kinderen duidelijke en eenvoudige taal gecommuniceerd. De privacy officer is verantwoordelijk voor de afhandeling van verzoeken van betrokkenen. De FG kan daarbij om advies worden gevraagd. Daarnaast voert de FG steekproefsgewijs controles uit op de juiste en tijdige afhandeling van verzoeken van betrokkenen.

5.3 Verwerkersovereenkomst

Met alle door de ombudsman ingeschakelde verwerkers wordt een verwerkersovereenkomst afgesloten zoals bepaald in art. 28 AVG. Een referentie naar de verwerkersovereenkomst wordt opgenomen in het verwerkingsregister.

5.4 Data Protection Impact Assessment (DPIA) en pre-DPIA

De ombudsman heeft een proces waarmee een gegevensbeschermingseffectbeoordeling (GEB)/ Data Protection Impact Assessment (DPIA), wordt uitgevoerd indien een verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen (de betrokkenen). Bij het uitvoeren van een DPIA wordt inzichtelijk gemaakt wat de impact van de verwerking is op de persoonlijke levenssfeer van betrokkenen, zodat de ombudsman indien benodigd aanvullende maatregelen kan treffen om eventuele samenhangende risico's te mitigeren.
Bij elk nieuw project of product waarbij persoonsgegevens worden verwerkt, wordt door de ombudsman een pre-DPIA afgenomen. De privacy officer is verantwoordelijk voor het uitvoeren van een pre-DPIA en wordt zodanig tijdig betrokken bij een nieuw project of product. De pre-DPIA toets is een snelle manier om te bepalen of de verwerking van persoonsgegevens dusdanig risicovol is dat er een DPIA moet worden uitgevoerd.
De ombudsman hanteert hiervoor een DPIA beleid waarin onder meer staat beschreven wanneer een DPIA moet worden uitgevoerd, op welke moment het advies van de FG wordt ingewonnen bij het uitvoeren van een DPIA en in welke gevallen een toetsing wordt uitgevoerd om te beoordelen of een gewijzigde verwerking conform de DPIA wordt uitgevoerd.

5.5 Procedure datalekken

5.5.1 Datalekken

Binnen de Nationale ombudsman wordt een datalek geclassificeerd als een inbreuk op de beveiliging van persoonsgegevens. Het kan hierbij gaan op een inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit.
Om de gevolgen van datalekken voor betrokkenen te beperken, toezicht te kunnen houden op de juiste afhandeling van datalekken en te waarborgen dat de AP en betrokkenen worden geïnformeerd indien nodig, is een Protocol Datalekken opgesteld. Het Protocol Datalekken staat op NoHow.

Daarnaast houdt de Nationale ombudsman een register bij van datelekken waarmee lering getrokken kan worden uit datalekken en waarmee herhaling in de toekomst voorkomen kan worden. Indien hier aanleiding toe is kan met het register tevens aan de Autoriteit Persoonsgegevens aangetoond worden dat de ombudsman in lijn met de wettelijke verplichtingen hiertoe datalekken monitort en opvolgt.

5.5.2 Melding en afhandeling

Iedere medewerker bij de ombudsman die een datalek constateert of het vermoeden heeft dat er zich een datalek heeft voorgedaan of nog kan voordoen, moet dit direct melden. Het proces omtrent het melden van datalekken staat beschreven in het Protocol Datalekken.

5.6 Delen van persoonsgegevens

Verstrekking van persoonsgegevens aan derde partijen zal alleen plaatsvinden indien dit verenigbaar is met het doel waarvoor de gegevens zijn verzameld, of wanneer toestemming is gegeven door de betrokkenen, dan wel een wettelijke bepaling voorschrijft dat de gegevens moeten worden verstrekt. Bij het bepalen of de verstrekking verenigbaar is worden

verschillende factoren in acht genomen, waaronder of er een verband bestaat met het doel waarvoor de gegevens zijn verzameld, de verhouding met de betrokkenen, de aard van de gegevens, de (mogelijke) gevolgen van de verstrekking, of er passende waarborgen zijn genomen en de verwachtingen van de betrokkenen. Dit wordt altijd voorafgaande aan het delen van de persoonsgegevens nagegaan.

5.7 Bewustzijn

De ombudsman draagt zorgt voor een passend bewustzijnsniveau van medewerkers omtrent de bescherming van persoonsgegevens. De wijze waarop dit wordt gedaan is beschreven in het Informatiebeveiliging & Privacy Bewustwording beleid.

6 Controle beleid

De FG is verantwoordelijk voor de controle op de naleving van dit beleid. De FG voert jaarlijks een controle uit, o.a. door middel van:

- PDCA cyclus in het Privacy Management Systeem. De FG is verantwoordelijk voor het uitzetten van de periodieke controle middels het Privacy Management Systeem. Op basis van de bevindingen worden verbeterpunten vastgesteld om de naleving van de AVG te verbeteren. De FG houdt toezicht op het doorvoeren van de verbeterpunten.
- Controle op en toetsing van verwerkingen op basis van het register van verwerkingsactiviteiten. De FG is hiervoor verantwoordelijk.
- Interne audit. De CISO en FG zijn verantwoordelijk voor het uitzetten van de periodieke interne audit ten aanzien van informatiebeveiliging en privacy.

De FG rapporteert elk kwartaal aan de directie over de naleving van de AVG en andere relevant wet- en regelgeving betreffende de bescherming van persoonsgegevens, over de naleving van het door de ombudsman vastgestelde privacy beleid en over eventuele risico's die daarmee verband houden. Indien de FG constateert dat dit privacy beleid niet wordt nageleefd, zal de FG de directie hierover informeren en adviseren welke acties nodig zijn om het privacy beleid na te komen. Zodanig dat de directie kan sturen op naleving van dit beleid.