BELEID BESCHERMING PERSOONSGEGEVENS

Inhoud

Voorwoord

De Nationale ombudsman 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 Algemene Verordening Gegevensbescherming (hierna: AVG) biedt waarborgen voor de bescherming van de persoonlijke levenssfeer van natuurlijke personen met betrekking tot het verwerken van persoonsgegevens. De Nationale ombudsman heeft in lijn met het bepaalde in de AVG beleid opgesteld voor het gebruik van persoonsgegevens.

Het beleid bescherming persoonsgegevens heeft tot doel:

- Regels te stellen voor het verwerken van persoonsgegevens door de Nationale ombudsman.
- Informatie te verschaffen aan personen van wie persoonsgegevens door de Nationale ombudsman verwerkt (zullen) worden.
- Bij te dragen aan de transparantie van de regels die door de Nationale ombudsman worden toegepast bij het verwerken van persoonsgegevens.

Het beleid bescherming persoonsgegevens van de Nationale ombudsman valt onder de verantwoordelijkheid van de directeur van de Nationale ombudsman en wordt door het corporate overleg van de No vastgesteld. Het corporate overleg zorgt dat alle medewerkers op de hoogte zijn van het beleid en het kunnen toepassen op hun dagelijks werkzaamheden. De ambtsdragers van de Nationale ombudsman worden door de directeur op de hoogte gebracht van het beleid.
Ook relevante externe partijen, zoals burgers, bezoekers en leveranciers, worden van het beleid bescherming persoonsgegevens van de Nationale ombudsman op de hoogte gebracht, bijvoorbeeld door korte verklaringen op internet en in overeenkomsten.
In deze notitie wordt uiteengezet wat het beleid bescherming persoonsgegevens van de Nationale ombudsman inhoudt en hoe dit door alle medewerkers van de ombudsman zal worden nageleefd. Zodat betrokkenen er van op aan kunnen dat met persoonsgegevens veilig en verantwoord wordt omgegaan door de Nationale ombudsman.
Wanneer wordt gesproken over Nationale ombudsman wordt hier bedoeld de ambtelijke organisatie van de Nationale ombudsman.

Inleiding

Privacy is een grondrecht dat is verankerd in de Grondwet, verdragen en in wet- en regelgeving, zoals de AVG. Het recht op privacy is geen absoluut recht maar moet worden afgewogen tegen andere rechten, plichten en belangen. De Nationale ombudsman wil (naast het voldoen aan alle wet- en regelgeving) zorgvuldig, veilig en rechtmatig omgaan met persoonsgegevens, waarbij de belangen van betrokkenen centraal staan. Uitgangspunt is steeds dat er een weging moet plaatsvinden tussen de noodzaak voor het verwerken van persoonsgegevens en de gevolgen van deze verwerking voor het individu.

In een bijlage bij deze notitie wordt een aantal in deze notitie gebruikte begrippen nader toegelicht.

1. Wat valt er onder het beleid bescherming persoonsgegevens?

Onder het beleid bescherming persoonsgegevens van de Nationale ombudsman vallen alle verwerkingen van persoonsgegevens. Hieronder worden deze begrippen toegelicht.

1.1 Persoonsgegevens

Een persoonsgegeven is elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Dat het om een natuurlijke persoon moet gaan, houdt in dat gegevens van overleden personen of van organisaties geen persoonsgegevens zijn.
Er zijn vele soorten persoonsgegevens, zoals iemands naam, adres en woonplaats. Maar ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens. En aan een foto is iemand ook te herkennen. Een foto is dus net zo goed een persoonsgegeven. En het houdt niet op bij zulke feitelijke gegevens: gegevens die een waardering over een bepaalde persoon inhouden, bijvoorbeeld een beoordeling van een manager, kan ook een persoonsgegeven zijn.
Gevoelige gegevens als iemands ras, godsdienst of gezondheid worden in de wet bijzondere persoonsgegevens genoemd. Deze zijn door de wetgever extra beschermd en mogen niet zomaar verwerkt worden.
Waar in deze notitie over privacy wordt gesproken wordt bedoeld informationele privacy. Dat wil zeggen dat het gaat om het verwerken en verzamelen van persoonlijke data, zoals financiële gegevens, medische gegevens, contactgegevens etc.

1.2 Verwerkingen van persoonsgegevens

Verwerken van persoonsgegevens is een ruim begrip. Het is belangrijk te beseffen dat verwerken gaat over alle handelingen die kunnen worden uitgevoerd met persoonsgegevens: van raadplegen, verzamelen tot en met vernietigen.
De medewerkers van de Nationale ombudsman ondersteunt de Nationale ombudsman bij zijn taken en maakt het werk van de Nationale ombudsman toegankelijk en inzichtelijk voor de samenleving. Medewerkers van de Nationale ombudsman zorgen onder meer voor klachtbehandeling, onderzoek, verslaglegging, informatievoorziening, documentatie, archivering, beheer van het gebouw, doelmatig en rechtmatig financieel beheer, personeelszaken en externe voorlichting. Om dit werk te kunnen doen is het vaak noodzakelijk persoonsgegevens te verwerken van medewerkers, burgers en bezoekers. Denk bijvoorbeeld aan persoonsgegevens die gebruikt worden voor de toegangspas, de uitvoering van het personeelsbeleid, facturen en declaraties van medewerkers en uitgifte van IT-middelen.

1.3 Relatie integrale beveiliging, informatiebeveiliging, beleid bescherming persoonsgegevens

Integrale beveiliging is de overkoepelende aanpak van beveiliging en bevat onder andere fysieke beveiliging, informatiebeveiliging en beleid bescherming persoonsgegevens. Informatiebeveiliging is het geheel van preventieve, detectieve, repressieve en correctieve maatregelen alsmede procedures en processen die de beschikbaarheid, exclusiviteit 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 Nationale ombudsman heeft beleid opgesteld voor informatiebeveiliging. Dit beleid is te vinden op het intranet van de Nationale 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 geautoriseerden toegang krijgen en dat informatie niet kan uitlekken.

Het beleid bescherming persoonsgegevens en informatiebeveiliging zijn niet los van elkaar te zien, maar overlappen elkaar ook niet volledig. Het beleid bescherming persoonsgegevens stelt namelijk naast de vraag of de persoonsgegevens goed beveiligd zijn (zie bovenstaande sleutelbegrippen beschikbaarheid, integriteit en vertrouwelijkheid) ook nog aanvullende vragen. Namelijk of de gegevens 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 beleid bescherming persoonsgegevens zich enkel bezig met persoonsgegevens en gaat informatiebeveiliging over veel meer vormen van informatie.

2. Wie zijn de hoofdpersonen?

De hoofdpersonen van de AVG zijn de betrokkenen, de verwerkersverantwoordelijke en de verwerker. Betrokkenen zijn de personen van wie gegevens worden verwerkt. De verwerkingsverantwoordelijke is degene die doel en middelen vaststelt voor de verwerkingen. En de verwerker is degene die persoonsgegevens verwerkt, maar niet onder het rechtstreeks gezag van de verwerkingsverantwoordelijke staat. Daarnaast zijn er voor de naleving van de AVG binnen de Nationale ombudsman nog een aantal taken/rollen belegd, zoals de Functionaris Gegevensbescherming (FG) en de contactpersonen AVG. Hieronder worden de rollen en functies van deze hoofdpersonen nader toegelicht.

2.1 Betrokkenen

Betrokkenen zijn de personen van wie gegevens worden verwerkt. Voor de Nationale ombudsman kunnen dit de volgende categorieën betrokkenen zijn: ambtsdragers, medewerkers, burgers en bezoekers. Voor elke verwerking van persoonsgegevens moet duidelijk zijn wat de rechten en plichten van elk van deze categorieën zijn. In paragraaf AVG-loket wordt nader ingegaan op de rechten van betrokkenen.

2.2 Verwerkingsverantwoordelijke

De Verwerkingsverantwoordelijke is diegene die doel en middelen vaststelt voor de verwerkingen van persoonsgegevens. Voor de organisatie van de Nationale ombudsman is dat de directeur. In de praktijk betekent dit dat elk hoofd van een organisatieonderdeel namens de directeur van de Nationale ombudsman verantwoordelijk is voor alle verwerkingen van persoonsgegevens die binnen het eigen onderdeel plaatsvinden. Wanneer meerdere onderdelen verantwoordelijk zijn voor een verwerking, worden onderling duidelijke afspraken gemaakt wat de respectievelijke verantwoordelijkheden ten aanzien van de AVG zijn en wie als contactpunt voor betrokkenen zal fungeren. Deze afspraken worden opgenomen in het AVG-register.

2.3 Verwerker en intern beheerder

Een verwerker verwerkt persoonsgegevens zonder onder het rechtstreekse gezag van de verwerkingsverantwoordelijke te vallen (iemand of een organisatie buiten de organisatie van de Nationale ombudsman). De verwerker voert slechts een taak uit die de verwerkingsverantwoordelijke heeft uitbesteed.
Wordt de taak uitgevoerd door iemand die wel valt onder rechtstreeks gezag van de verantwoordelijke dan is hij geen verwerker, maar is er sprake van intern beheer. Voordat er persoonsgegevens gedeeld worden met een verwerker moet er een verwerkersovereenkomst worden afgesloten. Dit wordt nader toegelicht in paragraaf 4.6 van deze notitie.

2.4 Functionaris Gegevensbescherming

De Nationale ombudsman heeft sinds ... een functionaris gegevensbescherming (FG) aangesteld. De contactgegevens van de FG zijn te vinden op het intranet en de website van de Nationale ombudsman. 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:

a. Informeren en adviseren van MT en leidinggevenden over hun verplichtingen uit hoofde van wet- en regelgeving in het kader van privacy.
b. Toezien op de naleving van de relevante wetgeving, het beleid bescherming persoonsgegevens en op de inrichting van de interne privacy organisatie.
c. Advies leveren bij een Privacy Impact Assessment (PIA), zowel de inhoudelijke beoordeling als de naleving van de voorgenomen beheermaatregelen.
d. Samenwerken met de centrale toezichthouder, de Autoriteit Persoonsgegevens, in het geval van een onderzoek.
e. Aanspreekpunt voor betrokkenen (medewerkers en burgers) voor alle aangelegenheden bij de verwerking van hun persoonsgegevens.
f. Het afleggen van verantwoording over de verwerkingen van persoonsgegevens in het financieel jaarverslag van de Nationale ombudsman.
g. In geval van incidenten zal de FG (in overleg met de security officer en andere intern betrokkenen) beoordelen of er sprake is van een datalek. Dit wordt zo nodig gemeld bij de Verwerkingsverantwoordelijke en bij de Autoriteit Persoonsgegevens (AP).
h. Opbouwen en onderhouden van nationaal netwerk.

2.5 Contactpersoon AVG

Binnen elke dienst (organisatieonderdeel) wordt minimaal één contactpersoon AVG benoemd, die over voldoende kennis over de AVG beschikt. De contactpersonen AVG zullen hiervoor regelmatig (interne) scholingsactiviteiten krijgen aangeboden. Deze AVG contactpersoon heeft tenminste de volgende taken:

a. Fungeren als ‘adviesloket’ bij vragen binnen de eigen dienst over de AVG.
b. Inventariseren, beoordelen, bijhouden en melden van verwerkingen persoonsgegevens.
c. Aanspreekpunt voor de FG bij incidenten (waaronder datalekken) en privacy verzoeken.
d. 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 Nationale ombudsman.

2.6 Burgers en bezoekers

De Nationale ombudsman ontvangt dagelijks bezoekers op de website en fysiek in het gebouw van de Nationale ombudsman. Bezoekers van de website en het gebouw van de Nationale ombudsman worden (via een disclaimer en privacy statement) geïnformeerd dat op een veilige en rechtmatige wijze met hun persoonsgegevens wordt omgegaan en worden gewezen op de rechten die zij hebben conform de AVG. In paragraaf 4.9 van deze notitie wordt dit nader toegelicht.
De Nationale ombudsman ontvangt vrijwel dagelijks brieven van derden, die doorgaans binnenkomen bij de Facilitaire Dienst. Dit zijn zowel brieven van burgers als van organisaties, die aandacht vragen voor een veelheid van onderwerpen. Omdat in deze brieven ook persoonsgegevens staan vermeld, worden burgers en organisaties in de ontvangstbevestiging tevens geïnformeerd dat zij bezwaar kunnen maken tegen opname in het uitsluitend intern toegankelijke systeem voor de behandeling van ontvangen brieven. Alle medewerkers hebben toegang tot dit systeem.

2.7 Security Officer

In paragraaf 1.3 van deze notitie is de relatie tussen het beleid bescherming persoonsgegevens en Informatiebeveiligingsbeleid in beeld gebracht.
De security officer is verantwoordelijke voor en coördineert het Informatiebeveiligingsbeleid van de Nationale ombudsman. Vanwege de raakvlakken en overlap zal er regelmatig overleg plaatsvinden tussen de security officer en 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 beleid bescherming persoonsgegevens zal waar mogelijk samen opgetrokken worden.

3. Uitgangspunten beleid bescherming persoonsgegevens Nationale ombudsman

In de AVG zijn deels open normen opgenomen die een nadere vertaling naar het beleid behoeven. Want wat dient te worden verstaan onder ‘passende’ maatregelen, en ‘niet meer persoonsgegevens gebruiken dan noodzakelijk’. Het beleid bescherming persoonsgegevens biedt hierbij de helpende hand. Het vormt als het ware een baseline die het voor de medewerkers inzichtelijk maakt waar elke ambtelijke dienst minimaal aan moet voldoen. Het kan gebruikt worden als normenkader om de AVG te implementeren en handhaven binnen de verschillende onderdelen. Daarnaast kan een baseline door het MT van de Nationale ombudsman gebruikt worden als sturingsmiddel om het beleid bescherming persoonsgegevens binnen de Nationale ombudsman vorm te geven.

Let op: Deze privacy baseline is nadrukkelijk niet gelijk aan het voldoen aan alle privacy- en gegevensbeschermingseisen die de AVG stelt. Het is geen afvinklijstje van noodzakelijke maatregelen. Voor de Nationale ombudsman blijft het uitgangspunt dat er steeds een weging moet plaatsvinden tussen de noodzaak voor het verwerken van persoonsgegevens en de gevolgen van deze verwerking voor het individu.

Volgens de AVG moeten verwerkingen van persoonsgegevens voldoen aan een aantal beginselen. Deze beginselen vormen het fundament voor het beleid bescherming persoonsgegevens van de Nationale ombudsman, zodat alle verwerkingen rechtmatig, veilig en verantwoord plaatsvinden, en worden hieronder toegelicht.

3.1 Rechtmatigheid, behoorlijkheid en transparantie

Deze drie belangrijke begrippen worden hieronder nader toegelicht.

Rechtmatigheid

Dat wil zeggen dat elke verwerking van persoonsgegevens gebaseerd moet zijn op één van de zes grondslagen die de AVG noemt. Deze lijst is limitatief, dat wil zeggen dat er geen andere gronden kunnen worden aangevoerd. De grondslagen zijn:

a. Betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden. Let op: deze toestemming moet vrij, specifiek, geïnformeerd en ondubbelzinnig gegeven zijn.
    - ⇨ Deze grondslag bij voorkeur alleen gebruiken als het niet anders kan, zeker in geval er sprake is van een machtsverhouding (werkgever-werknemer, overheid-burger).
b. De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is.
    - ⇨ Denk bijvoorbeeld aan uitvoering van een arbeidsovereenkomst of een bruikleenovereenkomst.
c. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.
    - ⇨ Denk bijvoorbeeld aan de Archiefwet, fiscale bewaarplicht en de Grondwet.
d. De verwerking is noodzakelijk om de vitale belangen van de betrokkene te beschermen. Deze grondslag zal niet vaak gebruikt worden.
    - ⇨ Het gaat hierbij om levensbedreigende situaties. Is een persoon buiten bewustzijn en is medische hulp geboden? Dan kunnen zonder toestemming direct de noodzakelijke persoonsgegevens verwerkt worden om hulp te bieden.
e. 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.
    - ⇨ Het gaat hierbij om relevante taken die in de wet zijn vastgelegd en die nodig zijn om een publieke taak goed te kunnen vervullen. Denk bijvoorbeeld aan de wettelijke taken die de Nationale ombudsman heeft, zoals de behandeling van verzoekschriften. Daarnaast heeft de Nationale ombudsman ook publieke taken, zoals de media informeren over de werkwijze van en de activiteiten van de Nationale ombudsman.
f. De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke. Dat is zo wanneer een verwerking aantoonbaar noodzakelijk is om bedrijfsactiviteiten te verrichten. Bijvoorbeeld het voeren van een personeelsadministratie.
    - ⇨ Denk hierbij bijvoorbeeld aan het belang om het gebouw te beveiligen, het doorsturen van personeelsgegevens tussen diensten of het verwerken van gegevens (inlognamen/wachtwoorden) ten behoeve van netwerkbeveiliging.

Let op:

De grondslagen die hierboven worden genoemd onder b t/m f zorgen ervoor dat het noodzakelijk is dat persoonsgegevens verwerkt worden. Zij zorgen ervoor dat die verwerking aantoonbaar is. De verwerking moet echter behalve aantoonbaar noodzakelijk ook nog proportioneel zijn en voldoen aan de subsidiariteitseis. Dat wil zeggen dat er ook nog nagegaan wordt of de noodzaak om de persoonsgegevens te verwerken in verhouding staat tot de mate van inbreuk in de privacy van de betrokkene. En dat de gekozen verwerking de beste manier is om het doel te bereiken. Wellicht is er een

andere, minder ingrijpende manier, of kan worden volstaan met de verwerking van minder persoonsgegevens. Zie in dit kader ook beginsel 3: dataminimalisatie.

Behoorlijkheid
Dat wil zeggen dat de verwerking van persoonsgegevens netjes en verantwoord is, ook wel genoemd ‘maatschappelijk betamelijk’.

Transparantie
Dat wil zeggen dat de betrokkene op de hoogte wordt gesteld van het feit dat er verwerking van zijn persoonsgegevens plaatsvindt, en wat de doeleinden van deze verwerking zijn, in heldere en begrijpbare taal. Bovendien moet de betrokkene geïnformeerd worden over zijn rechten en hoe hiervan gebruik kan worden gemaakt. De rechten van betrokken worden nader toegelicht in paragraaf 4.4 van deze notitie.

3.2 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.

Het doel bepaalt welk gebruik van de persoonsgegevens is toegestaan en welk gebruik niet. Zo mogen bijvoorbeeld niet méér persoonsgegevens verzameld en gebruikt worden dan nodig is voor het doel en mogen persoonsgegevens niet langer bewaard worden dan nodig is voor het doel. Het doel beperkt ook de mogelijkheid om eenmaal voor een bepaald doel verzamelde persoonsgegevens, voor een ander doel te gebruiken, tenzij het een verenigbaar doel is.

Denk bijvoorbeeld aan de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden En het bewaren van persoonsgegevens van afgewezen kandidaten na afronding van een sollicitatieprocedure, Of het bewaren van genodigdenlijsten na afloop van een bijeenkomst.

3.3 Dataminimalisatie

Dataminimalisatie, dat wil zeggen dat niet meer persoonsgegevens worden verwerkt dan nodig is voor het doel waarvoor ze verzameld worden. 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 bijvoorbeeld aan verdere verwerking van persoonsgegevens voor statistische doeleinden. Hierbij worden persoonsgegevens waar mogelijk geanonimiseerd. Zodat de gegevens wel bewaard kunnen blijven voor statistische doeleinden zonder dat ze tot een individueel persoon herleidbaar zijn. De optimale situatie is alleen de strikt noodzakelijke gegevens verzamelen. Als dat niet lukt kies dan voor de optie om alle andere gegevens direct te verwijderen als blijkt dat deze gegevens overbodig zijn.

Denk bijvoorbeeld aan webformulieren. Om te zorgen dat er niet meer gegevens worden verzameld dan noodzakelijk moeten alleen die persoonsgegevens worden gevraagd die nodig zijn voor het leveren van een dienst. Dataminimalisatie moet bij de standaardinstelling van systemen die gebruikt worden en bij het ontwerp van nieuwe systemen meegenomen worden.

3.4 Juistheid

Juistheid, dat wil zeggen dat de persoonsgegevens die verwerkt worden correct zijn en correct blijven. Maar ook het regelmatig controleren van toegang tot systemen en het actueel houden van verleende machtigingen, vallen onder het beginsel juistheid.

Dit betekent dat alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren. Zie verder het recht op rectificatie van betrokkenen in paragraaf 4.4.

3.5 Opslagbeperking

Opslagbeperking (oftewel bewaartermijnen), dat wil zeggen dat een persoonsgegeven alleen mag worden bewaard als identificeerbaar gegeven, voor zolang als het nodig is voor de doeleinden waarvoor het verzameld is.

Het is wel mogelijk om, als de gegevens geanonimiseerd kunnen worden en daarmee dus niet meer direct of indirect identificatie van een persoon mogelijk maken, de gegevens langer te bewaren. Ook hier gelden trouwens weer de uitzonderingen voor archivering, algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Voor sommige gegevens geldt dat deze gedurende een bepaalde periode niet vernietigd mogen worden. Ze moeten worden bewaard in het archief. Verschillende wetten kennen bepalingen waarin een termijn wordt gesteld gedurende welke de persoonsgegevens, na verwijdering uit de actieve administratie, bewaard moeten blijven. Op het intranet van de Nationale ombudsman zijn de regels omtrent archiveren te vinden.

Let op: Verwijderen is niet hetzelfde als vernietigen. Het verwijderen van verzamelde persoonsgegevens houdt in dat deze gegevens buiten het bereik van de actieve administratie worden gebracht en worden ondergebracht in een - al dan niet digitaal - archief. Van vernietigen is pas sprake als de gegevens nergens meer zijn opgeslagen.

3.6 Integriteit en vertrouwelijkheid

Integriteit en vertrouwelijkheid zijn twee begrippen die ook in paragraaf 2.3 aan de orde zijn gekomen bij informatiebeveiliging. Voor het beleid bescherming persoonsgegevens 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 er op kunnen vertrouwen dat er zorgvuldig wordt omgegaan met hun gegevens. De organisatorische en technische maatregelen om dit beginsel binnen de Nationale ombudsman te waarborgen komen in hoofdstuk 4 aan de orde.

3.7 Verantwoordingsplicht/Accountability

De verantwoordingsplicht is één van de belangrijkste verplichtingen van de AVG. Het betekent dat de Nationale ombudsman moet kunnen aantonen dat verwerkingen aan de regels van de AVG voldoen.

Het beleid bescherming persoonsgegevens draagt bij aan deze verantwoordingsplicht. Hiermee toont de Nationale ombudsman aan dat er passende en effectieve interne processen en instrumenten aanwezig zijn. Zodat de principes en verplichtingen van gegevensbescherming kunnen worden nageleefd zodat betrokkenen voldoende beschermd zijn.

Daarnaast kan de Nationale ombudsman dit aantonen met het AVG-register.

De organisatorische en technische maatregelen om dit beginsel binnen de Nationale ombudsman te waarborgen komen in hoofdstuk 4 van deze notitie aan de orde.

4. Organisatorische en technische maatregelen beleid bescherming persoonsgegevens

Ter waarborging van het beleid bescherming persoonsgegevens treft de Nationale ombudsman verschillende organisatorische, technische en fysieke maatregelen die hieronder worden toegelicht. Deze maatregelen bieden de kaders en handvatten aan medewerkers van de Nationale ombudsman om op de gewenste wijze te kunnen handelen wanneer het gaat om persoonsgegevens. In deze paragraaf worden deze organisatorische en technische maatregelen nader toegelicht.

4.1 Aanstelling FG

In de AVG is het een verplichting geworden voor alle overheidsinstanties en publieke organisaties om een FG aan te stellen. De FG zorgt er voor dat het MT gevraagd en ongevraagd op de hoogte wordt gesteld van de naleving van het beleid bescherming persoonsgegevens binnen de diensten van de Nationale ombudsman, en zorgt dat het MT op de hoogte is van risico’s en misstanden. Voor uitgebreide omschrijving van de rol en taken van de FG wordt verwezen naar paragraaf 2.4.

4.2 Contactpersoon AVG per dienst

De AVG contactpersoon brengt het beleid bescherming persoonsgegevens, in samenwerking met het diensthoofd, onder de aandacht van de medewerkers van de eigen dienst zodat het privacybewustzijn wordt vergroot en het beleid bescherming persoonsgegevens geborgd is binnen alle diensten. Voor omschrijving van de rol en taken van de AVG contactpersoon wordt verwezen naar paragraaf 2.5.

4.3 AVG-register

Alle verwerkingen van persoonsgegevens worden opgenomen in het digitale AVG register. De gedachte hierachter is dat wanneer de documentatie niet op orde is, niet aangetoond kan worden dat zorgvuldig wordt omgegaan met de bescherming van persoonsgegevens. Bovendien kan in geval van incidenten (datalekken), een bezoek van de toezichthouder (Autoriteit Persoonsgegevens) of verzoeken van betrokkenen adequaat worden gehandeld. Het AVG-register wordt door elke onderdeel zelf gevuld, door de AVG-contactpersoon. De verantwoordelijke leidinggevende geeft per verwerking een definitief akkoord.

4.4 AVG-loket

De Nationale 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. Dit wordt duidelijk en transparant gecommuniceerd, zowel op het intranet als op het internet.

4.5 Procedure datalekken

Er kan sprake zijn van een datalek wanneer belangrijke documenten, gegevensbestanden of gegevensdragers als een telefoon of usb-stick zijn kwijtgeraakt of bijvoorbeeld onbedoeld zijn gepubliceerd. Om de gevolgen van datalekken voor betrokkenen te beperken en toezicht te kunnen houden op de juiste afhandeling van datalekken is een procedure datalekken opgesteld. Deze is te vinden op het intranet. Bovendien wordt een register bijgehouden van de (potentiële) datalekken en beveiligingsincidenten. Het doel van deze registratie is dat ervan kan worden geleerd, zodat datalekken in de toekomst zoveel mogelijk worden voorkomen. Een ander doel is dat daarmee aan de Autoriteit Persoonsgegevens kan worden aangetoond dat datalekken daadwerkelijk worden gemonitord en opgevolgd.

4.6 Verwerkersovereenkomsten via Bestuursbureau (Inkoop)

Wanneer externe partijen (verwerkers) toegang hebben tot de persoonsgegevens moeten met deze externe partij onder andere afspraken gemaakt worden over de organisatorische en technische beveiliging van persoonsgegevens, de rechtmatigheid van de gegevensverwerking en het melden van datalekken bij de verwerkingsverantwoordelijke van de Nationale ombudsman. Deze afspraken worden opgenomen in een verwerkingsovereenkomst. Het Bestuursbureau beschikt over een standaard verwerkingsovereenkomst en kan hierbij adviseren.

4.7 Privacy Impact Assessment

De verwerkingsverantwoordelijke is verplicht een gegevensbeschermingseffectbeoordeling (GEB), ook wel genoemd een Privacy Impact Assessment (PIA), uit te voeren voor verwerkingen die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen (de betrokkenen). Er moet dan inzichtelijk worden gemaakt wat de impact van de verwerking is op de persoonlijke levenssfeer van betrokkenen, zodat door het treffen van maatregelen de risico's kunnen worden teruggebracht naar acceptabele grenzen. Bij elk nieuw project of systeem waarbij mogelijk risicovolle verwerkingen van persoonsgegevens zijn betrokken, zal een GEB/PIA worden afgenomen.

4.8 Interne/externe scholing

- FG moet voldoende kennis opbouwen en bijhouden
- FG zorgt dat AVG-contactpersonen voldoende kennis opbouwen en bijhouden
- FG zorgt dat medewerkers Nationale ombudsman voldoende kennis opbouwen en bijhouden

4.9 Interne en externe communicatie

Een transparante interne en externe communicatie door het Bestuursbureau van de Nationale ombudsman zorgt er voor dat alle betrokkenen op de hoogte zijn van het beleid bescherming persoonsgegevens van de Nationale ombudsman en geïnformeerd zijn over hoe ze gebruik kunnen maken van hun rechten. Daarbij is het beleid bescherming persoonsgegevens van de Nationale ombudsman vooral bedoeld om de interne organisatie te informeren. En zijn de privacyverklaringen en disclaimers vooral bedoeld om de buitenwereld te informeren. Zij zijn meer het visitekaartje naar buiten toe en informeren betrokken hoe zij gebruik kunnen maken van hun rechten en plichten.

Bijlage: verklaring van begrippen

- Integrale beveiliging: beveiliging van personen, gebouwen, terreinen, (gerubriceerde) informatie, privacy en integriteit.
- Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (‘de betrokkene’). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
- We kennen vier vormen van privacy:
    - Informationele privacy: gaat over het verwerken en verzamelen van persoonlijke data, bijvoorbeeld financiële gegevens, medische gegevens, contactgegevens etc.
    - Territoriale privacy: gaat over de persoonlijke omgeving van een individu en de grenzen die hierbij horen, bijvoorbeeld op werk, thuis en publieke ruimtes.
    - Lichamelijke privacy: gaat over de fysieke privacy van een persoon bijvoorbeeld genetische onderzoeken, drugstests, abortus etc.
    - Communicatieve privacy: gaat over de vrijheden rondom correspondentie via post, telefoongesprekken, e-mail etc.
- Privacy Enhancing Technologies: de term Privacy Enhancing Technologies (PET) wordt gehanteerd om alle ICT-middelen aan te duiden die gebruikt kunnen worden om persoonsgegevens te beschermen.
- Gegevensbeschermingseffectbeoordeling (GEB/PIA): een GEB/PIA is een risicoanalyse die een organisatie helpt om bij een nieuw project, proces of systeem in een vroeg stadium inzicht te krijgen in de privacyrisico’s.
- Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, maar niet onder diens rechtstreekse gezag valt.
- Verwerking: 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.
- Verwerkingsverantwoordelijke: 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