Omgevingsdienst West-Holland

Privacy Beleid

Omgevingsdienst West-Holland

1. Inleiding

1.1. Visie op gegevensbescherming
De verwerking van persoonsgegevens is inherent aan de uitvoering van de taken van de ODWH als uitvoeringsorganisatie van de provincie Zuid-Holland en dertien gemeenten in het gebied van Holland Rijnland. Voor een goede en zorgvuldige taakuitvoering moet de ODWH de gegevens van inwoners, ondernemers en medewerkers verwerken en soms met andere instanties delen. Informatieverwerking geeft de verantwoordelijkheid om effectieve privacybescherming te bieden.

Het uitgangspunt is dat de ODWH respect heeft voor de persoonlijke levenssfeer van de betrokken inwoners, ondernemers en medewerkers. Daarbij houdt de ODWH zich aan de wettelijke regels op het gebied van de verwerking van de persoonsgegevens.

1.2. Reikwijdte
Dit beleid is van toepassing op alle verwerkingen van persoonsgegevens binnen onze organisatie. De kaders die in dit beleid staan beschreven gelden voor iedereen (ook de bewerkers) die persoonsgegevens verwerken.

1.3. Juridisch kader
Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkenen voorop. Er moet voorkomen worden dat hierop onnodige of te vergaande inbreuken worden gemaakt. De Wet bescherming persoonsgegevens (Wbp) biedt hiervoor het wettelijk kader. Vanaf 1 januari 2016 is de Wbp uitgebreid met de meldplicht datalekken. De uitwerking hiervan wordt verder beschreven in hoofdstuk 4.

Op 25 mei 2018 zal de Algemene Verordening Gegevensbescherming (AVG) in werking treden. De AVG heeft als doel om de privacy van Europese burgers beter te beschermen dan de Wbp nu doet. Wanneer de AVG in werking treedt, zal de Wbp vervallen. Als algemene regel geldt dat persoonsgegevens op behoorlijke en zorgvuldige wijze moeten worden verwerkt. De AVG bepaalt verder dat persoonsgegevens alleen voor een specifiek beschreven doel mogen worden verwerkt, maar ook dat deze gegevens niet langer mogen worden bewaard dan noodzakelijk is om het doel waarvoor ze zijn verzameld, te realiseren. De betrokkene kan altijd inzage of wijziging van de verwerkte persoonsgegevens vragen. Dit wordt in de volgende hoofdstukken nader uitgewerkt.

In aanvulling op de AVG bevat andere wetgeving meer specifieke vereisten.

1.4. Definities
Voordat inhoudelijk op het beleid wordt ingegaan is het van belang om de belangrijkste definities uit de AVG helder te hebben.

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

Verwerking van persoonsgegevens: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending,

verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid.

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.
Voor de verwerking van de persoonsgegevens die bij ons rusten, is het dagelijks bestuur te allen tijde eindverantwoordelijk. Dit geldt ook als we gegevens ter beschikking stellen aan derden of delen in samenwerkingsverbanden.

Beheerder: degene die binnen de organisatie van de verantwoordelijke en binnen de door de verantwoordelijke gegeven instructies en bevoegdheden, belast is met de inrichting en de beveiliging van een bestand binnen een organisatieonderdeel of, in een hiërarchische lijn daarboven, een cluster van bestanden binnen een hoofdgroep en die tevens belast is met de in verband met de verwerking van gegevens geldende procedures.

Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Betrokkene: degene op wie een persoonsgegeven betrekking heeft.

Derde: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.

Toestemming van de betrokkene: elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem/haar betreffende persoonsgegevens worden verwerkt. Deze toestemming moet vrij en ondubbelzinnig zijn. Dat betekent dat betrokkenen in vrijheid hun wil moeten kunnen uiten. Ook mag er geen twijfel zijn of betrokkenen hun toestemming hebben gegeven en voor welke specifieke verwerking zij dit hebben gedaan.

2. Organisatie

2.1. De wettelijke verantwoordelijkheden
De manier waarop dit beleid binnen de ODWH wordt verankerd, is het fundament van de privacy borging. De directeur is verantwoordelijk voor juiste gegevensverwerking en informatiebeveiliging. Echter deze verantwoordelijkheid beperkt zich niet alleen tot de directeur. De afdelingshoofden en teamleiders sturen op het privacy beleid en controleren hun medewerkers op de naleving. De medewerkers zelf zijn verantwoordelijk voor hun gedrag overeenkomstig het privacy beleid en de naleving ervan. Zorgvuldige gegevensverwerking geldt voor iedereen die binnen de ODWH werkzaam is. Het niet in acht nemen van privacy normen of ernstige schending daarvan kan leiden tot het nemen van sanctionele maatregelen.

2.2. Verantwoording
De directeur is verantwoordelijk voor een juiste naleving van de Wbp/AVG en de uitvoering van het beleid op het gebied van gegevensverwerking. Het dagelijks bestuur stelt het privacy beleid vast. De directeur informeert het dagelijks bestuur binnen de jaarlijkse planning en control cyclus over de risico's en over de getroffen privacy beheersmaatregelen, binnen de processen waar de ODWH verantwoordelijk voor is.

2.3. Organisatorische inbedding
De afdelingshoofden en teamleiders zijn verantwoordelijk voor de borging van de uitgangspunten van dit beleid binnen de processen binnen hun bureau. Het borgen van de privacy is onlosmakelijk verbonden met informatiebeveiliging. Zowel de informatiebeveiliging als de privacy is een verantwoordelijkheid van de directeur. Om de processen te ondersteunen zullen experts ingezet worden op het gebied van gegevensverwerking en informatiebeveiliging. Hiervoor zijn de volgende rollen binnen de organisatie aanwezig.

Functionaris gegevensbescherming (FG): De FG rapporteert aan de directeur van de ODWH. Rapportages betreffen o.a. borging van de status van audits, afhandeling van privacyvraagstukken en privacy-incidenten.

Beveiligingsfunctionaris: De Beveiligingsfunctionaris coördineert de informatiebeveiliging en rapporteert aan de directeur van de ODWH. Rapportages betreffen de status van audits.

Binnen de organisatie is een *beveiligingsbeheerder* nodig die verantwoordelijk is voor de technische invulling van informatiebeveiliging. De beveiligingsbeheerder rapporteert aan de beveiligingsfunctionaris.

2.4. Sturing en monitoring
Met een reeks maatregelen kan er gewaarborgd worden dat er binnen de ODWH continu gewerkt wordt aan het optimaliseren en borgen van de kwaliteit van de werkprocessen waarbij privacy een rol speelt. Elke teamleider of afdelingshoofd is verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens die binnen zijn of haar proces plaatsvindt. Het is daarom hun verantwoordelijkheid om te monitoren of persoonsgegevens zorgvuldig verwerkt worden en dit zo nodig bij te sturen. Daarnaast zijn zij verplicht om incidenten te melden bij het loket datalek@ODWH.nl of direct bij de functionaris gegevensbescherming (FG). De FG heeft de verantwoordelijkheid om structureel te toetsen of de wettelijke eisen op het gebied van privacy en informatiebeveiliging zijn geïmplementeerd en worden uitgevoerd.

Juist omdat privacy voor een belangrijk deel mensenwerk is, moet op alle niveaus binnen de ODWH ruime aandacht zijn voor het cyclisch denken. Door privacy vast op de diverse agenda's te plaatsen, ontstaat een continu proces van veranderen en verbeteren. Door vanuit verschillende niveaus en

rollen binnen de ODWH naar de kwaliteit van de uitvoering van privacy te kijken, ontstaat een evenwichtig systeem van checks-and-balances. Hieronder volgen de belangrijkste elementen van deze borging.

Vaststellen beleid
Het dagelijks bestuur stelt het beleid op het gebied van gegevensverwerking vast en draagt zorg dat dit regelmatig wordt geëvalueerd en zo nodig aangepast.

Uitvoering van beleid
De directeur is als verantwoordelijke voor de gegevensverwerking in de zin van de wet verantwoordelijk voor de uitvoering van het privacy beleid en voor de controle op de naleving van afspraken.
De directeur ziet toe op de ontwikkeling en uitvoering van het privacy beleid. Het afdelingshoofd is proceseigenaar van de processen binnen zijn afdeling. Deze krijgt ondersteuning van 'experts' op het gebied van gegevensverwerking en informatiebeveiliging.

Werkoverleggen
Teamleiders en afdelingshoofden maken privacy tot een onderdeel van hun werkoverleg. Zo nodig schuiven de 'experts' op het gebied van gegevensverwerking en informatiebeveiliging bij de overleggen aan. Hiermee werkt de ODWH actief aan een open cultuur, aan het optimaliseren van kennis en een transparante procesuitvoering. Bevindingen of vragen kan iedereen voorleggen aan de functionaris gegevensbescherming.

Toezicht
Voor onafhankelijk toezicht op de uitvoering van het privacy beleid wijst de directeur een functionaris voor de gegevensbescherming aan conform artikel 37-39 van de AVG. De FG houdt toezicht op de naleving van de AVG en informeert en adviseert de verwerkingsverantwoordelijke of de verwerker en de werknemers over hun verplichtingen uit hoofde van deze verordening. De FG heeft vrij toegang tot systemen en processen van de ODWH. De FG rapporteert rechtstreeks aan de directeur. De directeur rapporteert aan het dagelijks bestuur. De FG treedt ook op als ombudsman wanneer inwoners klachten hebben over de uitoefening van de privacy rechten en het beleid en doet meldingen van gegevensverwerkingen en datalekken.

Planning en control proces
Privacy vormt een aparte paragraaf binnen het planning en control proces. Jaarlijks legt de directeur verantwoording af aan het dagelijks bestuur over de risico's en beheersmaatregelen met betrekking tot dit beleid.
Daarnaast wordt de privacy een vaste paragraaf binnen alle relevante beleidsplannen van de ODWH en een integraal onderdeel binnen het bedrijfsproces. Hierdoor ontstaat ruimte voor beleidsmatige verbeteringen.

3. Uitgangspunten zorgvuldige gegevensverwerking

3.1 Omgaan met persoonsgegevens
Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt. Dit betekent dat persoonsgegevens alleen worden verwerkt voor het uitvoeren van de in de gemeenschappelijke regeling ODWH opgedragen taken. Zo wordt uitvoering gegeven aan de in de Wbp voorgeschreven doelbinding en proportionaliteit en met ingang van 25 mei 2018 aan de Algemene Verordening Gegevensbescherming. Dit houdt in dat persoonsgegevens alleen voor specifieke, uitdrukkelijke en legitieme doeleinden mogen worden verzameld en dat er niet meer persoonsgegevens worden verwerkt dan voor dat doel noodzakelijk is. Daarbij wordt tenminste rekening gehouden met de verwantschap van doelen, de aard van de gegevens, de gevolgen van de verdere verwerking voor de betrokkene, de wijze waarop de gegevens zijn verkregen en de gestelde waarborgen ter bescherming van de persoonlijke levenssfeer.

3.2 Verkrijging van gegevens
In het merendeel van de gevallen worden persoonsgegevens door de betrokkene zelf verstrekt. Wat er precies met de verzamelde gegevens gebeurt, is afhankelijk van het doel waarvoor ze verzameld worden. Meestal worden ze in een informatiesysteem opgenomen waar ze alleen toegankelijk zijn voor de medewerkers die belast zijn met het uitvoeren van een bepaalde taak. Gegevens worden niet zonder toestemming van de betrokkene of zonder de noodzaak van een goede vervulling van de publiekrechtelijke taak van de ODWH gedeeld.

3.3 Toegang tot en verstrekking van persoonsgegevens
Alle medewerkers, intern en extern zijn verplicht tot geheimhouding van de persoonsgegevens, waarvan zij kennisnemen. Dit wordt gewaarborgd in de ambtseed of belofte dan wel door ondertekening van een geheimhoudingsverklaring. Gegevens uit de gegevensverwerking/bestanden kunnen worden verstrekt aan binnen de ODWH werkzame personen, voor zover dit voor hun taakuitoefening noodzakelijk is.

Aan derden worden de gegevens enkel verstrekt indien dit nodig is voor een goede vervulling van de publiekrechtelijke taak of indien de betrokkene schriftelijk toestemming heeft verleend tot gegevensverstrekking voor een kenbaar specifiek doel.

Daarnaast worden de gegevens verstrekt aan de bewerkers, indien dit voor de uitoefening van publiekrechtelijke taken van de verantwoordelijke noodzakelijk is.

Voor wat betreft instanties ten behoeve van wetenschappelijke of statistische doelen, worden de persoonsgegevens slechts verstrekt onder de voorwaarden dat de uitkomsten waarvoor deze gegevens worden gebruikt, niet meer tot individuele natuurlijke personen herleidbaar zijn.

De ODWH informeert derden, die op vastgestelde wijze bepaalde persoonsgegevens verwerken, over de daaraan gestelde voorwaarden en beperkingen.

De verstrekking van gegevens blijft achterwege voor zover geheimhouding is geboden.

3.4 Bescherming van gegevens
De ODWH treft passende technische en organisatorische maatregelen ter bescherming, bevordering van de juistheid en volledigheid van de persoonsgegevens en ter voorkoming van inbreuk, verlies en onrechtmatige verwerking van de persoonsgegevens. Er zijn verschillende instrumenten om gegevensbescherming te waarborgen. Hiervoor is de directeur verantwoordelijk.

Data Privacy Impact Assessment (gegevensbeschermingseffectbeoordeling)
Eén van de instrumenten om gegevensbescherming te waarborgen is de uitvoering van een Data Privacy Impact Assessment (DPIA). Dit is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen. Op basis hiervan kunnen maatregelen worden getroffen om de risico's te verkleinen. Een DPIA is verplicht, als een gegevensverwerking waarschijnlijk een hoog privacy risico oplevert. Of daarvan sprake is, moet worden beoordeeld aan de hand van de criteria die de Europese privacy toezichthouders hebben opgesteld. De FG en de beveiligingsmedewerker adviseren over de noodzaak tot het uitvoeren van een DPIA.

Verwerkingsregister
De AVG noemt verder als verplichte maatregel het bijhouden van een register van verwerkingsactiviteiten om te kunnen laten zien dat wordt voldaan aan de eisen van de AVG. Het verwerkingsregister bevat (onder meer) informatie over de persoonsgegevens die de ODWH verwerkt, in welke systemen dit gebeurt, in welke werkprocessen dit plaats vindt en met welk doel. Tevens worden deze gegevens geclassificeerd naar gevoeligheid van de gegevens.

Dataclassificatie
De maatregelen die getroffen moeten worden om de gegevensbescherming te kunnen borgen, is niet voor elk proces en informatiesysteem hetzelfde. Daarom is het nodig dat alle processen en informatiesystemen die persoonsgegevens verwerken een dataclassificatie ontvangen. Dataclassificatie heeft als doel om de continuïteit, integriteit en vertrouwelijkheid van het proces en het informatiesysteem te benoemen. Dit maakt inzichtelijk welke maatregelen genomen moeten worden om de gegevens die verwerkt worden te beschermen.

Niveau	Vertrouwelijkheid
Geen	**Openbaar** Informatie bevat geen persoonsgegevens en mag door iedereen worden ingezien (bv: algemene informatie op de website van de ODWH)
Laag	**Bedrijfsvertrouwelijk** Persoonsgegevens zijn toegankelijk voor alle medewerkers van de organisatie (bv: informatie op het intranet)
Midden	**Vertrouwelijk** Persoonsgegevens zijn alleen toegankelijk voor een beperkte groep gebruikers (bv: financiële gegevens)
Hoog	**Geheim** Persoonsgegevens zijn gevoelig en alleen toegankelijk voor direct geadresseerde(n) (bv: strafrechtelijke informatie, personeelsgegevens, BSN)

Registratie van gegevensgebruik (logging)
Elk geautomatiseerd systeem dat persoonsgegevens verwerkt, moet een registratie bijhouden van de verwerkingen. In deze logging staat minimaal vermeld welke gebruiker, op welke moment, welke gegevens heeft verwerkt. Logging houdt in:

- chronologische registratie van gegevens over van belang zijnde gebeurtenissen, die zich gedurende een periode in een verwerking voordoen,
- het vastleggen in een log, bijvoorbeeld een systeem log of een security log, van feitelijk uitgevoerde bewerkingen en/of pogingen daartoe.

Verwerkersovereenkomst en convenanten met derden
Bij veel processen binnen de ODWH worden gegevens verwerkt door derden. Het uitbesteden van werkzaamheden aan derden brengt risico's met zich mee op het gebied van gegevensverwerking en informatiebeveiliging. De ODWH blijft verantwoordelijk voor de verwerking van de gegevens. De ODWH moet er daarom op toezien dat gegevens juist verwerkt en beveiligd worden. Met het oog op de omgang met privacy door alle partijen waar de ODWH mee samenwerkt en waarbij persoonsgegevens worden verwerkt, worden verwerkersovereenkomsten afgesloten.
Indien gebruik wordt gemaakt van de diensten van een bewerker, legt de ODWH de wederzijdse verplichtingen met betrekking tot de omgang met persoonsgegevens conform artikel 28 van de AVG schriftelijk in een verwerkersovereenkomst met die verwerker vast. De verwerker verwerkt de persoonsgegevens overeenkomstig de vastgelegde afspraken.
De onderwerpen die in een bewerkersovereenkomst onder andere worden geregeld zijn:

- Instructies van verantwoordelijke: De verwerking mag alleen uitgevoerd worden in overeenstemming met instructies van de verantwoordelijke. De verwerker mag de persoonsgegevens niet voor eigen doeleinden gebruiken, maar alleen om uitvoering te geven aan de instructies van de verantwoordelijke.
- Geheimhouding: In deze bepaling wordt aan de bewerker een geheimhoudingsplicht opgelegd, eventueel gecombineerd met een boetebeding. Overigens is opzettelijke niet-naleving van deze geheimhoudingsplicht strafbaar gesteld in het Wetboek van Strafrecht.
- Beveiligingsmaatregelen: De verantwoordelijke wijst de bewerker op zijn verantwoordelijkheid om passende technische en organisatorische maatregelen te nemen om de persoonsgegevens te beveiligen tegen verlies e.d.
- Locatie van de data: De verantwoordelijke moet weten in welke landen zijn data worden opgeslagen, al dan niet in de cloud. Dit is van belang met het oog op het gegeven dat de data van overheidsdata niet opgeslagen mogen worden, in landen buiten de EU en met name in de Verenigde Staten.
- Audits/verantwoording: De verantwoordelijke moet kunnen controleren of de bewerker zich houdt aan de gemaakte afspraken. Dit gebeurt vaak in de vorm van een audit (onderzoek) door de verantwoordelijke of door een onafhankelijke derde. In de bewerkersovereenkomst kunnen partijen hier nadere afspraken over maken.
- Aansprakelijkheid: De wet bepaalt dat de verantwoordelijke kan worden aangesproken als iemand schade lijdt doordat de Wbp niet wordt nageleefd. Dit geldt zelfs als de schade het gevolg is van nalatigheid van de bewerker, die in dat geval ook zelfstandig aansprakelijk is. In de bewerkersovereenkomst worden heldere afspraken gemaakt over deze verdeling.

De directeur, de teamleider of afdelingshoofd die een uitbesteding, samenwerking of uitwisseling aangaat, ziet toe op de totstandkoming van deze afspraken. De FG wordt bij de totstandkoming betrokken en ziet toe op de naleving daarvan.
Op verwerkersovereenkomsten in kader van de meldplicht datalekken wordt in hoofdstuk 4 nader ingegaan.

Bewaren en vernietigen van gegevens
De AVG schrijft voor dat gegevens niet langer bewaard mogen worden dan het doel waar ze voor nodig zijn. Dit doel wordt beschreven in de wet, daarom lopen de bewaartermijnen van persoonsgegevens uiteen. In diverse wetten zijn minimale en maximale bewaartermijnen opgenomen. Daar waar er geen wettelijke regeling is die voorziet in een verplichte bewaartermijn, kan de ODWH een besluit over de bewaartermijn nemen. Daarnaast geldt de Archiefwet voor het bewaren van papieren en elektronische documenten.
Vernietiging van gegevens gebeurt op basis van de vastgestelde selectielijst. Van iedere vernietiging wordt een verklaring opgesteld. Deze verklaring bevat een specificatie van de bescheiden die zijn vernietigd, op grond waarvan is vernietigd en op welke wijze is vernietigd.

Bij het overbrengen van te bewaren gegevens naar de archiefbewaarplaats van de gemeente is het mogelijk om privacygevoelige gegevens van openbaarheid uit te zonderen voor een periode van maximaal 75 jaar.

3.5. Bewust omgaan met persoonsgegevens

De ODWH streeft naar een cultuur waarbij iedereen elkaar in alle openheid aanspreekt op het eigen gedrag rondom privacy en daarmee van elkaar leert. Communicatie, openheid en toetsing zijn belangrijke randvoorwaarden om een optimaal privacy-beleid te realiseren.

Alle binnen de ODWH werkzame personen behandelen alle informatie over individuele personen die hij/zij ten behoeve van de uitvoering van met opdrachtgevers gesloten overeenkomsten verkrijgt vertrouwelijk en draagt er zorg voor dat deze informatie niet aan derden bekend wordt. Iedereen moet zich bij de uitoefening van hun taken voortdurend bewust zijn van het belang van het waarborgen van de rechten van betrokkenen. Medewerkers moeten persoonsgegevens op een zorgvuldige manier verwerken, zoals omschreven in dit beleid.

Om bewustwording te realiseren is kennisoverdracht nodig. De directeur, FG en de beveiligingsfunctionaris zullen ervoor zorgen dat informatie over gegevensbescherming en informatiebeveiliging herhaaldelijk onder de aandacht wordt gebracht binnen de ODWH.

4. Meldplicht datalekken

4.1. Nieuwe wetgeving
Op 1 januari 2016 is de meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp) ingevoerd. Deze meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken moeten melden aan de Autoriteit Persoonsgegevens, en in bepaalde gevallen ook aan de betrokkene van wie persoonsgegevens zijn gelekt.
Elke concreet datalek moet worden beoordeeld en de verantwoordelijke moet een afweging maken of dat concrete datalek onder het bereik van de wettelijke meldplicht valt. In dit hoofdstuk worden handvatten gegeven voor de beoordeling van het datalek en de melding daarvan.
Het niet voldoen aan de meldplicht kan leiden tot handhaving door de Autoriteit Persoonsgegevens. Bij een ernstige schending van de meldplicht kan een boete ter hoogte van € 820.000 worden opgelegd. De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. Nieuw is dat *alle* datalekken moeten worden gedocumenteerd. Met deze documentatie moet de Autoriteit Persoonsgegevens kunnen controleren of aan de meldplicht is voldaan.

4.2. Wat is een datalek
Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is. De ODWH sluit voor de omschrijving van een datalek aan bij de definitie van een datalek in artikel 4 van de AVG. Van een datalek is sprake indien er een inbreuk is op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. Bij een datalek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking - dus aan hetgeen waartegen de beveiligingsmaatregelen bescherming moeten bieden. Er is dus niet alleen sprake van een datalek als een hacker toegang tot persoonsgegevens krijgt. Ook verlies van een laptop geldt als datalek. En zelfs verlies van gegevens door bijvoorbeeld een brand in het datacentrum (waarbij er geen back-up beschikbaar is), ziet de wet als een datalek.

4.3. Melden aan Autoriteit Persoonsgegevens
Op grond van artikel 33 van de AVG moet een datalek meteen, waar mogelijk binnen 72 uur, aan de Autoriteit Persoonsgegevens worden gemeld. Niet elk datalek moet worden gemeld. Voor situaties waarin niet waarschijnlijk is dat de datalek een risico inhoudt voor de rechten en vrijheden van personen, geldt een uitzondering.

4.4. Melden aan de getroffen personen
Indien het datalek waarschijnlijk (een aanzienlijke kans op) een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen wordt - naast de melding aan de Autoriteit Persoonsgegevens - het lek tevens onverwijld gemeld aan de personen waarvan de gegevens zijn gelekt (artikel 34 van de AVG). Dit zullen in de meeste gevallen klanten zijn. Een melding aan betrokkene is niet nodig wanneer er maatregelen conform de AVG zijn getroffen en deze zijn toegepast op de betreffende persoonsgegevens. De gegevens zijn bijvoorbeeld anoniem gemaakt, zodat degene die de gegevens in handen krijgt niet kan achterhalen welke personen de gegevens betreffen. Een melding kan eveneens achterwege gelaten worden als achteraf maatregelen zijn genomen door de verwerkingsverantwoordelijke om te zorgen dat de hoge risico's voor de rechten en vrijheden van betrokkene zich waarschijnlijk niet meer voor zullen doen of de mededeling onevenredige inspanning vergt. In het laatste geval moeten betrokkenen op een andere, even doeltreffende manier, worden geïnformeerd, bijvoorbeeld door een openbare mededeling (artikel 34 AVG).
In de AVG is vastgelegd wat in de melding aan de Autoriteit Persoonsgegevens en aan eventuele betrokkenen in ieder geval omschreven moet worden. Het zou kunnen zijn dat niet alle informatie gelijktijdig verstrekt kan worden. In dat geval is het mogelijk de informatie in stappen te verstrekken (artikel 33 AVG).

4.6. Melden van een datalek aan FG
De medewerker die direct of indirect kennis draagt of krijgt van een incident inzake het lekken van privacygegevens meldt dit rechtstreeks aan de FG. De FG beoordeelt samen met het datalekteam of deze onder de meldingsplicht valt. Zo ja, dan adviseert het datalekteam aan het verantwoordelijke afdelingshoofd of het datalek te melden bij de Autoriteit Persoonsgegevens. De directeur beslist of de melding wordt gedaan.
Het datalek wordt conform artikel 33 van de AVG onverwijld gemeld aan de Autoriteit Persoonsgegevens. De termijn voor het melden van het datalek begint te lopen op het moment dat de verantwoordelijke, of een bewerker, op de hoogte is geraakt van een incident dat mogelijk onder de meldplicht valt. Wat in een concreet geval als 'onverwijld' wordt aangemerkt zal afhangen van de omstandigheden van het geval. De melding wordt in ieder geval zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking, gedaan, tenzij op dat moment inmiddels uit onderzoek is gebleken dat het incident niet onder de meldplicht datalekken valt. Indien het incident later dan 72 uur na ontdekking wordt gemeld, dan wordt er gemotiveerd waarom de melding later is gedaan.
Mocht er binnen 72 uur na de ontdekking van het incident nog niet volledig zicht zijn op wat er is gebeurd en om welke persoonsgegevens het gaat, wordt alsnog een melding gedaan op basis van de gegevens op dat moment. Eventueel wordt de melding naderhand aangevuld of ingetrokken.

4.7. Bewaren van informatie over datalek
Alle datalekken worden gedocumenteerd in een overzicht. Dit overzicht bevat de feiten en gegevens van het lek, zoals de oorzaak van het lek, de soort gegevens die gelekt zijn, het moment dat het lek is ontdekt en op welke wijze het lek gedicht is. Als het datalek ook aan de getroffen personen is gemeld, wordt de communicatie hierover bewaard.

De AVG schrijft niet voor hoe lang het overzicht moet worden bewaard. In eerste instantie wordt er uitgegaan van een bewaartermijn van minimaal één jaar. In bepaalde gevallen kan het nodig zijn om een langere bewaartermijn te hanteren. Zo moeten de gegevens minimaal drie jaar worden bewaard als er geen melding aan de betrokkene is gedaan omdat er zwaarwegende redenen waren of omdat er voldoende technische beschermingsmaatregelen zijn genomen, waardoor er geen ongunstige gevolgen voor de betrokkene zijn.

4.8. Afspraken met bewerkers
In veel gevallen wordt het verwerken van persoonsgegevens uitbesteed aan een derde partij. Deze derde partij noemt de AVG een verwerker. Data kunnen bijvoorbeeld toegankelijk zijn voor een clouddienstverlener die updates uitvoert op software, opgeslagen staan bij een hostingprovider, of beschikbaar zijn voor het marketingbedrijf dat e-mails in opdracht van klanten verzendt.
Voordat de persoonsgegevens voor de verwerking worden uitbesteed aan een bewerker, wordt eerst nagegaan of deze voldoende waarborgen biedt ten aanzien van de naleving van de meldplicht voor datalekken.

In de verwerkersovereenkomst worden afspraken vastgelegd over de maatregelen die de verwerker moet nemen zodat de ODWH aan de meldplicht voor datalekken kan voldoen.
In veel gevallen is de verwerker de eerste die kennisneemt van een opgetreden datalek. Om aan onze eindverantwoordelijkheid te voldoen moet de verwerker ons tijdig en adequaat informeren over de datalekken waarvan hij kennis krijgt. In elke verwerkersovereenkomst worden daar afspraken over gemaakt.

5. Rechten van betrokkene

5.1. Algemeen
De ODWH neemt passende maatregelen zodat de betrokkene zijn rechten op grond van de wet kan uitoefenen.

Bij een verzoek aan de ODWH kan de ODWH de identiteit controleren van een verzoeker, voordat het inzageverzoek in behandeling wordt genomen. Dit kan door te vragen een identiteitsbewijs te laten zien of om een kopie daarvan op te sturen.

De ODWH stelt iedere ontvanger aan wie persoonsgegevens zijn verstrekt in kennis van iedere rectificatie, wissing van persoonsgegevens of beperking van de verwerking, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. De ODWH verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.

5.2. Recht van inzage (15 AVG)
Iedere betrokkene heeft het recht om te vragen welke persoonsgegevens van hem of haar voor welke doeleinden verwerkt worden. Dit wordt het recht van inzage genoemd. Dit recht geldt alleen voor de eigen gegevens en niet voor de gegevens van anderen. Dit verzoek kan schriftelijk per brief of per e-mail aan de ODWH worden gedaan. Wanneer de ODWH veel informatie over iemand heeft kan de ODWH aan verzoeker vragen om aan te geven welke gegevens hij precies wil hebben.

De ODWH reageert binnen vier weken schriftelijk per brief of e-mail op een verzoek om inzage. Afhankelijk van de complexiteit van het verzoek en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De ODWH stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van een dergelijke verlenging.
De inzage kan gegeven worden door een volledig overzicht van de gegevens, kopieën/afdrukken of inzage ter plekke. De ODWH kan er zelf voor kiezen om, in plaats van een overzicht, kopieën of afdrukken te geven van de documenten. De ODWH is daartoe niet verplicht.

De ODWH mag een vergoeding vragen voor het verstrekken van kopieën. Deze vergoeding is € 0,23 per pagina met een maximum van € 5,00.
Er mag een redelijke vergoeding gevraagd worden van hoogstens € 22,50 als het gaat om:
- meer dan 100 pagina's;
- een moeilijk toegankelijke gegevensverwerking;
- afdrukken van een of meer foto’s.

Deze vergoedingen zijn wettelijk geregeld in het Besluit kostenvergoeding rechten betrokkene Wbp.

5.3. Recht op rectificatie (art. 16 AVG)
De betrokkene heeft het recht om de gegevens over hem of haar te laten verbeteren of aan te vullen.
Iemand kan om correctie vragen als zijn persoonsgegevens:
- feitelijk onjuist zijn;
- onvolledig zijn of niet ter zake doen voor het doel waarvoor ze zijn verzameld;
- op een andere manier in strijd met een wet worden gebruikt.

De ODWH is verplicht binnen 4 weken schriftelijk of per e-mail te reageren op uw correctieverzoek. Besluit de ODWH de gegevens te corrigeren, dan moet dit zo snel mogelijk gebeuren. Indien het technisch gezien niet mogelijk is om gegevens te verbeteren, bijvoorbeeld doordat deze zijn opgeslagen op een cd-rom, dan kan de ODWH een bestand met aanvullingen en verbeteringen aanleggen.

Indien de ODWH in het voorafgaande jaar de (onjuiste) gegevens aan andere organisaties doorgegeven dan zal de ODWH ook zo snel mogelijk deze andere organisaties van de wijzigingen op de hoogte stellen, tenzij het onmogelijk is om die organisaties op te sporen of wanneer dit een onevenredige inspanning van de ODWH zou vergen.

5.4. Recht op gegevenswissing ('vergetelheid') (art. 17 AVG)
Een betrokkene heeft het recht op het wissen van zijn persoonsgegevens en kan hiertoe een verzoek doen. De ODWH heeft de verplichting deze gegevens te wissen zonder onredelijke vertraging in een aantal gevallen. Dit kan bijvoorbeeld het geval zijn wanneer de persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of verwerkt of wanneer de persoonsgegevens onrechtmatig zijn verwerkt. De ODWH heeft, indien hij de persoonsgegevens openbaar heeft gemaakt, ook de verplichting om andere organisaties die deze persoonsgegevens verwerken ervan op de hoogte te stellen dat de betrokken heeft verzocht om het wissen van links naar, of kopieën of reproducties van die persoonsgegevens. De ODWH dient daarbij, met inachtneming van de beschikbare technologie en de middelen waarover hij beschikt, redelijke maatregelen te nemen, waaronder technische maatregelen, in de organisaties die de persoonsgegevens verwerken over het verzoek van betrokkene te informeren.
De ODWH is niet verplicht persoonsgegevens te wissen wanneer de verwerking van persoonsgegevens nodig is voor de vervulling van zijn publieke taak.

5.5. Recht op beperking van de verwerking (art. 18 AVG)
Het recht op beperking van een verwerking houdt in dat, op verzoek van de betrokkene, de verwerking van bepaalde persoonsgegevens tijdelijk gestopt moet worden. Dit kan bijvoorbeeld zijn om de juistheid van de persoonsgegevens te controleren. Of wanneer de persoonsgegevens niet meer nodig zijn voor de doelen van de verwerking, maar de betrokkene ze nodig heeft voor de instelling, uitoefening of verdediging van een rechtsvordering. Ook wanneer de betrokkene bezwaar heeft gemaakt tegen de verwerking en in afwachting is van het antwoord op de vraag of de gronden voor de verwerking van de ODWH zwaarder wegen dan de belangen van de betrokkene, kan van het recht op beperking gebruikt gemaakt worden.

5.6. Recht op overdraagbaarheid
Het recht op dataportabiliteit, oftewel overdraagbaarheid van persoonsgegevens houdt in dat betrokkenen het recht hebben om de persoonsgegevens te ontvangen die een organisatie van hen heeft. Vervolgens kunnen betrokkenen deze gegevens zelf opslaan voor persoonlijk (her)gebruik. Ook kunnen ze de gegevens doorgeven aan een andere organisatie.

Op grond van artikel 20 lid 3 van de AVG geldt dit recht niet voor de verwerking die noodzakelijk is 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 verantwoordelijke is verleend. Dit houdt in dat dit recht niet geldt voor zover de ODWH de persoonsgegevens nodig heeft voor de vervulling van zijn taak. Nu de ODWH de persoonsgegevens met name verwerkt voor de vervulling van zijn publieke taak zal dit recht over het algemeen niet gelden voor de door de ODWH verwerkte persoonsgegevens.

5.7. Recht van bezwaar (art. 21 AVG)
Iedere betrokkene dient bezwaar te kunnen maken tegen de verwerking van zijn persoonsgegevens. De ODWH staakt de verwerking van de persoonsgegevens tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen of grondrechten en de fundamentele vrijheden van betrokkene. Op een bezwaar zijn de bepalingen van de Algemene wet bestuursrecht van toepassing.

5.8. Recht om klacht in te dienen
Zie klachtenregeling ODWH