Nederlandse Organisatie voor Wetenschappelijk Onderzoek

Privacybeleid NWO 2018 - 2019

Tekst van het privacybeleid van de Nederlandse Organisatie voor Wetenschappelijk Onderzoek, zoals vastgesteld bij besluit van de raad van bestuur op 23 mei 2018.

INHOUDSOPGAVE

Privacyverklaring NWO

NWO respecteert de persoonlijke levenssfeer van subsidieaanvragers, onderzoekers, medewerkers en alle andere relaties van NWO. Informatie wordt niet langer bewaard dan nodig voor het doel waarvoor deze is verzameld en niet gebruikt voor doelen die hier niet mee verenigbaar zijn. NWO verwerkt persoonsgegevens overeenkomstig de Algemene verordening gegevensbescherming (AVG).

Bij de verwerking van persoonsgegevens gaat NWO uit van de begrippen subsidiariteit en proportionaliteit. Bij subsidiariteit stelt NWO zich de vraag of de doelen waarvoor zij gegevens verwerkt ook op een andere wijze kunnen worden behaald, met minder persoonsgegevens, of met persoonsgegevens die minder inbreuk maken op de privacy van de betrokkene(n). Een verwerking van persoonsgegevens moet daarnaast proportioneel zijn aan het beoogde doel. NWO verzamelt niet meer gegevens dan zij nodig heeft voor het beoogde doel.

Persoonsgegevens worden adequaat beveiligd en zo zorgvuldig als mogelijk behandeld. Er is aandacht voor privacy binnen alle processen en activiteiten van NWO.

Het onderhavige privacybeleid biedt medewerkers en betrokkenen inzicht in hoe privacy geregeld is bij NWO.

1 Inleiding

Privacy krijgt steeds meer aandacht. Op 25 mei 2018 treedt de Algemene verordening gegevensbescherming (AVG) in werking, als opvolger van de huidige richtlijn waarop de Wet bescherming persoonsgegevens (Wbp) is gebaseerd. Door middel van een periodiek te actualiseren privacybeleid op te stellen, wil NWO aan alle verplichtingen op basis van de AVG voldoen.

Het gebruik van persoonsgegevens is noodzakelijk voor de bedrijfsprocessen van NWO. Opslag en verwerking van deze persoonsgegevens dient met de grootste zorgvuldigheid te gebeuren omdat misbruik van persoonsgegevens grote schade kan berokkenen aan medewerkers en andere betrokkenen. De Raad van Bestuur van NWO is wettelijk verantwoordelijk voor het op een juiste manier verwerken van persoonsgegevens (verwerkingsverantwoordelijke).

Met de maatregelen beschreven in dit beleidsdocument neemt NWO haar verantwoordelijkheid om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren en daarmee te voldoen aan de relevante privacywet- en regelgeving.

Definities en afkortingen staan in Bijlage A.

1.1 Reikwijdte en doelstelling van het privacybeleid

Het privacybeleid is van belang voor alle medewerkers, onderzoekers, subsidieaanvragers en alle andere relaties van NWO. Het heeft consequenties voor het werk van alle medewerkers die met persoonsgegevens werken. Het privacybeleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen NWO, waaronder in ieder geval alle medewerkers, gasten, bezoekers en externe relaties (inhuur/outsourcing).

Het privacybeleid betreft niet het verwerken van persoonsgegevens voor persoonlijk of huishoudelijk gebruik, zoals persoonlijke werkaantekeningen of een verzameling visitekaartjes. Het privacybeleid betreft de geheel of gedeeltelijk geautomatiseerde en/of systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van NWO alsmede de daaraan ten grondslag liggende (al dan niet elektronische) documenten. Eveneens is het privacybeleid van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Bij NWO wordt het beschermen van persoonsgegevens breed geïnterpreteerd. Er is een belangrijke relatie en gedeeltelijke overlap met het beleidsterrein informatiebeveiliging, waarbij het gaat om de beschikbaarheid, integriteit en de vertrouwelijkheid van data, waaronder persoonsgegevens. Er wordt aandacht geschonken aan deze raakvlakken en er wordt zowel planmatig als inhoudelijk afstemming gezocht.

Het privacybeleid heeft als doel om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet worden gevonden tussen privacy, functionaliteit en veiligheid.

Beoogd wordt de persoonlijke levenssfeer van de betrokkene zoveel mogelijk te respecteren. De gegevens, die betrekking hebben op een betrokkene dienen beschermd te worden tegen onwettelijk en ongeautoriseerd gebruik en tegen verlies dan wel misbruik op basis van het fundamenteel recht op bescherming van zijn/haar persoonsgegevens. Dit brengt met zich mee dat het verwerken van persoonsgegevens dient te voldoen aan relevante wet- en regelgeving en dat persoonsgegevens veilig zijn bij NWO.

Het privacybeleid geeft medewerkers en andere betrokkenen inzicht in hoe privacy geregeld is bij NWO. Daarnaast helpt het bij het creëren van bewustwording over het belang en de noodzaak van het beschermen van persoonsgegevens.

Het privacybeleid beoogt:

- Het bieden van een kader om (toekomstige) verwerkingen van persoonsgegevens te toetsen aan een vastgestelde norm en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie eenduidig te beleggen.
- Het nemen van verantwoordelijkheid door de Raad van Bestuur door de uitgangspunten en de organisatie van het verwerken van persoonsgegevens vast te leggen voor NWO.
- Daadkrachtige implementatie van het privacybeleid door duidelijke keuzes in maatregelen te maken en actieve controle toe te passen op de uitvoering van de beleidsmaatregelen.
- Compliant zijn met de Nederlandse en Europese wetgeving.

Naast bovenstaande concrete doelstellingen is een meer algemeen doel het creëren van bewustwording van het belang en de noodzaak van het beschermen van persoonsgegevens, mede ter vermijding van risico's als gevolg van het niet compliant zijn met de relevante wet- en regelgeving.

2 Beleidsprincipes verwerking persoonsgegevens

Algemeen beleidsuitgangspunt is dat persoonsgegevens in overeenstemming met de relevante wet- en regelgeving op behoorlijke en zorgvuldige wijze worden verwerkt. Hierbij dient een goede balans te worden gevonden tussen het belang van NWO om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens.

Om aan bovenstaand beleidsuitgangspunt te voldoen gelden de volgende aan de AVG ontleende principes:

- Persoonsgegevens worden alleen verwerkt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking geformuleerd (5 AVG).
- Een verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen zoals genoemd in de Algemene Verordening Gegevensbescherming (6 AVG).
- Bij een verwerking van persoonsgegevens, blijft de hoeveelheid en het soort gegevens beperkt tot de persoonsgegevens die noodzakelijk zijn voor het specifieke doeleinde. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn (dataminimalisatie).
- Verwerking van persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde (doelbinding).
- Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.
- Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen.
- Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
- Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de verwerking, hierbij worden de van toepassing zijnde bewaar- en vernietigtermijnen in acht genomen.
- Iedere betrokkene heeft een wettelijk recht op inzage respectievelijk verbetering, aanvulling, verwijdering of afscherming van de in de afzonderlijke verwerkingen hem betreffende persoonsgegevens, en heeft in bepaalde gevallen het recht van verzet.
- Bij alle registraties die niet strikt noodzakelijk zijn voor een bedrijfsproces zal aan de betrokkene voor zover technisch mogelijk een eenduidige zogenaamde opt-out procedure worden aangeboden.

3 Wet- en regelgeving

Voor NWO zijn in het kader van de gegevensbescherming de volgende wetten en regelingen relevant:

3.1 BIR

De basisregels uit het door de rijksoverheid opgestelde “Baseline Informatiebeveiliging Rijksdienst (BIR)” worden gebruikt als leidraad.

NWO heeft een stelsel van maatregelen ingericht voor het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens en informatiesystemen. Dit stelsel wordt onderhouden en periodiek geëvalueerd, zoals beschreven in het Informatiebeveiligingsbeleid 2018-2019 van NWO. Dit beleid geeft richting aan de uitvoering van de dagelijkse werkzaamheden en de verantwoorde omgang met informatie. De basisregels uit het door de rijksoverheid opgestelde besluit BIR worden bij het Informatiebeveiligingsbeleid gebruikt als leidraad.

3.2 Algemene Verordening Gegevensbescherming (AVG)

NWO heeft de wettelijke vereisten (waaronder het rechtmatig en zorgvuldig verwerken van persoonsgegevens en nemen van passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking van data c.q. persoonsgegevens) geïmplementeerd door middel van dit privacybeleid alsmede het Informatiebeveiligingsbeleid 2015 - 2018.

3.3 Archiefwet

NWO houdt zich aan de voorschriften ten aanzien van bewaartermijnen, zoals die bijvoorbeeld in de Archiefwet zijn vastgelegd, en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d.

3.4 Telecommunicatiewet

De Telecommunicatiewet beschrijft onder meer aan welke regels cookies op websites dienen te voldoen.

3.5 Auteurswet

De Auteurswet beschrijft onder meer dat het publiceren van afbeeldingen, foto’s en video’s niet toegestaan is wanneer een redelijk belang van de betrokkene zich daartegen verzet. Dit wordt ook wel het portretrecht genoemd.

4 Rollen en verantwoordelijkheden met betrekking tot Verwerking Persoonsgegevens

Om de verwerkingen van persoonsgegevens gestructureerd en gecoördineerd op te pakken is een aantal rollen en verantwoordelijkheden aan functionarissen in de bestaande organisatie toegewezen.

4.1 Raad van Bestuur

De Raad van Bestuur (RvB) is eindverantwoordelijk voor de rechtmatige en zorgvuldige verwerking van persoonsgegevens binnen NWO en stelt het beleid, de maatregelen en de procedures op het gebied van verwerking met dit privacybeleid vast. Op basis van de Bevoegdhedenregeling NWO 2017 zijn de domeinbesturen krachtens mandaat verantwoordelijk voor de verwerkingen binnen het eigen domein.

4.2 Portefeuillehouder Bedrijfsvoering en financiën

De portefeuillehouder bedrijfsvoering en financiën is het bestuurslid dat privacy in portefeuille heeft. De portefeuillehouder is eindverantwoordelijk voor de bescherming en beveiliging van persoonsgegevens binnen NWO.

4.3 Directeur Bedrijfsvoering en financiën

De directeur Bedrijfsvoering en financiën is verantwoordelijk voor de implementatie van het privacybeleid binnen NWO. De directeur is ook verantwoordelijk voor persoonsgegevens die vanuit NWO in een applicatie worden ingevoerd.

4.4 Leidinggevende(n)

Het creëren van bewustwording en de naleving van het privacybeleid is onderdeel van de integrale bedrijfsvoering (ook binnen de domeinen). Iedere leidinggevende heeft de taak om:

- er voor te zorgen dat zijn/haar medewerkers op de hoogte zijn van (de voor hun relevante aspecten van) het privacybeleid;
- het privacybewustzijn van zijn/haar medewerkers toereikend te laten zijn;
- toe te zien op de naleving van het privacybeleid door zijn medewerkers;
- periodiek het onderwerp privacy onder de aandacht te brengen in werkoverleggen.

4.5 Overlap met informatiebeveiliging

De Chief Information Security Officer (CISO) is nauw betrokken bij de implementatie van het privacybeleid. Het zorgvuldig omgaan met persoonsgegevens valt namelijk deels onder de algemene regels rondom Informatiebeveiliging (Informatiebeveiligingsbeleid NWO 2018-2019).

4.6 Functionaris gegevensbescherming

De AVG verplicht NWO zelf een interne ‘toezichthouder’ op de verwerking van persoonsgegevens aan te stellen. Deze toezichthouder wordt de Functionaris voor de Gegevensbescherming (FG) genoemd. De FG houdt binnen NWO toezicht op de toepassing en naleving van de Privacywetgeving. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie.

De FG adviseert en informeert de gehele organisatie en de individuele organisatieonderdelen omtrent het toepassen van de privacywetgeving. De FG draagt zorg voor de voorlichting over verwerking van persoonsgegevens aan medewerkers en leidinggevenden. De FG bevordert het privacybewustzijn van medewerkers, bijvoorbeeld door het plaatsen van informatie en blogs op JOOST.

De FG is aanspreekpunt en vraagbaak voor degenen die vragen hebben over de bescherming van persoonsgegevens en beheert (samen met de CISO) het register van meldingen van verwerkingen van persoonsgegevens.

De FG heeft als taak:

- er voor zorgen dat de gegevensverwerkingen worden bijgehouden;
- zorgdragen voor bewustwording en training;
- als privacyvraagbaak te functioneren;
- het afstemmen met de directeur bedrijfsvoering en de CISO over privacy-aangelegenheden;
- het deelnemen aan het Privacyteam
- het betrokken zijn bij de afhandeling van datalekken en andere incidenten;
- Het opstellen van een privacyjaarverslag;
- Het frequent herzien van het privacybeleid om aan te sluiten bij nieuwe ontwikkelingen.

4.7 De applicatie eigenaar

De applicatie eigenaar is er verantwoordelijk voor dat de applicatie en bijbehorende ICT-faciliteiten een goede ondersteuning bieden aan het bedrijfsproces waar deze verantwoordelijk voor is en voldoet aan het privacybeleid. Dit betekent dat de applicatie eigenaar er voor zorgt dat zowel nu als in de toekomst de applicatie blijft beantwoorden aan de eisen en wensen van de gebruikers en aan wet- en regelgeving. De directeur wordt hierin ondersteund door het privacyteam, dat naast de directeur bestaat uit de CISO en de FG.

4.8 Gelieerde instellingen

Aan NWO gelieerde instellingen en stichtingen zijn zelf verantwoordelijk voor het voldoen aan de privacywetgeving. Het is aan de gelieerde instelling zelf om compliancy te realiseren. NWO zal het belang hiervan benadrukken en inzicht vragen in hoe de compliancy gerealiseerd is.

Voor advies kunnen gelieerde instellingen een beroep doen op de FG en CISO van NWO.

5 Implementatie privacybeleid

De Raad van Bestuur is verantwoordelijk voor verwerkingen van de persoonsgegevens waarvan hij het doel en de middelen voor de verwerking vaststelt. De RvB wordt aangemerkt als de verwerkingsverantwoordelijke in de zin van de AVG. De feitelijke verwerking van persoonsgegevens wordt echter op allerlei plekken binnen NWO uitgevoerd.

Het goed, efficiënt en verantwoord leiden van een organisatie wordt vaak aangeduid met de term governance. Het omvat vooral ook de relatie met de belangrijkste belanghebbenden van de instelling, zoals de medewerkers en de samenleving. Een goede governance zorgt er voor dat alle belanghebbenden hun rechten en plichten kennen en er naar handelen.

5.1 Verdeling van verantwoordelijkheden

De Raad van Bestuur is eindverantwoordelijk voor alle gegevensverwerkingen van NWO. De verantwoordelijkheden worden binnen de domeinen en de staven in de lijn belegd, waarbij iedere medewerker overeenkomstig zijn rol een eigen verantwoordelijkheid heeft.
Zie hoofdstuk 4, Rollen en verantwoordelijkheden met betrekking tot verwerking van persoonsgegevens.

Privacy is een lijnverantwoordelijkheid**.** Dit betekent dat leidinggevenden de primaire verantwoordelijkheid dragen voor een zorgvuldige verwerking van persoonsgegevens binnen hun team. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan. Onder de lijnverantwoordelijkheid valt ook de taak om het beleid met betrekking tot de verwerking van persoonsgegevens te communiceren met alle relevante partijen, binnen de grenzen van het redelijke.

Privacy is ieders verantwoordelijkheid. Van medewerkers en derden wordt verwacht dat ze zich integer gedragen en zorgvuldig omgaan met persoonsgegevens.

5.2 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om bij medewerkers het bewustzijn m.b.t. privacy (en security) voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en goed gedrag wordt aangemoedigd. Good practices kunnen gedeeld worden met anderen in de organisatie, bijvoorbeeld via de NWO-Academy.

Onderdeel van de uitvoering van het Privacybeleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers en derden.

Verhoging van het security- en privacy bewustzijn van medewerkers is de verantwoordelijkheid van de leidinggevenden, daarin ondersteund door de FG en CISO.

5.3 Controle en naleving

De FG houdt toezicht op de naleving van de privacywetgeving en het privacybeleid, inclusief de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van personeel.

Aanvullend hierop maken audits op de naleving van de privacywetgeving en het privacybeleid het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit.

Het verwerken van persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten NWO maken het noodzakelijk om periodiek te bezien of men nog voldoende op koers zit met het privacybeleid.

6 Rechtmatige en zorgvuldige verwerking van persoonsgegevens

6.1 Grondslag, doelbinding en belangenafweging

Het verwerken van persoonsgegevens moet gebaseerd zijn op een van de wettelijke gronden zoals beschreven in artikel 6 AVG. De verwerkingsverantwoordelijke omschrijft vooraf de doeleinden voor de verwerking. Deze doeleinden zijn concreet en specifiek geformuleerd. Bij elke verwerking wordt getoetst in hoeverre het verwerken van persoonsgegevens noodzakelijk is. Hierbij worden de verschillende belangen afgewogen en wordt gekeken naar de doelmatigheid, proportionaliteit en subsidiariteit.

Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Past een verwerking niet binnen de wettelijke taakuitoefening van NWO danwel ontbreekt een gerechtvaardigd belang, is de uitdrukkelijke toestemming van de betrokkene vereist.
NWO treft de nodige maatregelen om te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, juist en nauwkeurig zijn.

Bij infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt vanaf de start rekening gehouden met de inrichting van privacy door een Privacy Impact Assessment (PIA) uit te voeren. NWO hanteert bij de implementatie de principes “Privacy by Design” en “Privacy by Default”.

6.2 Melden en documenteren van verwerkingen

Een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens dient gemeld te worden bij de FG van NWO. De FG beoordeelt de rechtsgeldigheid van de registratie en draagt zorg voor adequate documentatie.

6.3 De organisatie van de beveiliging

NWO draagt zorg voor een adequaat beveiligingsniveau en legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige Verwerking. Deze maatregelen zijn er mede op gericht onnodige c.q. onrechtmatige verzameling en verwerking van p ersoonsgegevens te voorkomen.

Een risicoanalyse op privacybescherming en informatiebeveiliging maakt deel uit van het intern risicobeheersings- en controlesysteem van NWO. Dit gebeurt via de classificatie van een applicatie.

6.4 Geheimhouding

Bij NWO worden alle persoonsgegevens als vertrouwelijk geclassificeerd. Een ieder behoort de vertrouwelijkheid van persoonsgegevens te kennen en daarnaar te handelen.

Ook personen voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

6.5 Bewaartermijnen / vernietigingstermijnen per soort gegeven

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of worden gebruikt. Persoonsgegevens dienen na het verlopen van de bewaartermijn buiten het bereik van de actieve administratie gebracht te worden. NWO zal de persoonsgegevens na het verlopen van de bewaartermijn vernietigen of, indien de persoonsgegevens bestemd zijn voor historische, statistische of wetenschappelijke doeleinden, in een archief bewaren.

6.6 Bijzondere persoonsgegevens

Het verwerken van bijzondere persoonsgegevens is in beginsel verboden, tenzij er sprake is van een wettelijke grondslag, uitdrukkelijke toestemming van de betrokkene of een zwaarwegend algemeen belang. Tevens gelden zwaardere eisen voor de beveiliging van deze persoonsgegevens. Daar waar de basisbescherming niet voldoende is moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen.

Onder bijzondere persoonsgegevens vallen gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijke gegevens.

6.7 Doorgifte persoonsgegevens aan derden

6.7.1 Uitbesteden van Verwerking aan een Verwerker

Indien NWO persoonsgegevens laat verwerken door een v*erwerker*, wordt de uitvoering van verwerkingen geregeld in een schriftelijke overeenkomst tussen NWO, de verwerkingsverantwoordelijke, en de verwerker. Een standaard format is beschikbaar bij de afdeling Juridische Zaken.

6.7.2 Doorgifte Persoonsgegevens binnen de Europese Unie

NWO verstrekt persoonsgegevens alleen aan derden, als deze doorgifte is gebaseerd op een wettelijke grondslag (6 AVG).

Met betrekking tot bijzondere persoonsgegevens worden deze niet aan derden verstrekt zonder expliciete toestemming van de betrokkene.

6.7.3 Doorgifte Persoonsgegevens buiten de Europese Unie

NWO verstrekt persoonsgegevens alleen aan derden die zich bevinden in een land buiten de Europese Unie indien dat land in zijn geheel of dat bedrijf/die instelling specifiek een passend beschermingsniveau waarborgt. Voor landen met een passend beschermingsniveau hanteert NWO de lijst van landen ten aanzien waarvan de Europese Commissie een adequaatheidsbesluit heeft genomen. Hieronder is ook het EU/VS Privacy Shield Programma begrepen.

NWO verstrekt persoonsgegevens alleen aan landen zonder passend beschermingsniveau op basis van een wettelijke uitzondering. Eén van die uitzonderingen is “ondubbelzinnige toestemming”: degene van wie persoonsgegevens doorgegeven wordt, heeft ondubbelzinnige toestemming gegeven. Een andere wettelijke uitzondering is doorgifte op basis van een modelcontract (zoals opgesteld door de Europese Commissie). Bij wijzigingen van of aanvullingen op het modelcontract is een vergunning van de minister van Veiligheid en Justitie vereist.

7 Incidenten met betrekking tot Persoonsgegevens

Iedere klacht of melding met betrekking tot de verwerking van persoonsgegevens binnen NWO is een privacy incident. De bekendste vorm van zo'n incident is een datalek.

Dit hoofdstuk beschrijft het beleid met betrekking tot de melding, registratie en afhandeling van incidenten of het vermoeden van incidenten in de reguliere bedrijfsvoering en in bijzondere omstandigheden.

7.1 Melding en registratie

Medewerkers van NWO zijn verplicht om een (vermoedelijk) 'datalek' en andere privacy incidenten direct te melden. Dit kan via het meldpunt-datalek@nwo.nl.

Van elk incident en de afhandeling daarvan wordt een registratie bijgehouden. Meldingen worden vertrouwelijk behandeld. De melder kan er op vertrouwen dat het doen van een melding geen persoonlijke consequenties heeft voor de melder. Een melder dient zolang het incident nog niet is afgehandeld vertrouwelijk met de melding om te gaan en hierover niet te communiceren met betrokkenen of anderen.

7.2 Afhandeling

De afhandeling van incidenten heeft als doel het probleem op te lossen, de schade te beperken en de wetgeving na te leven. NWO heeft een apart team voor datalekken (bestaande uit de FG, CISO en medewerkers van I&A) die beoordeelt of er waarschijnlijk sprake is van een datalek. Dit datalekteam is een onderdeel van het privacyteam.

Als het incident een datalek betreft dan wordt conform de regels van de AP gemeld. Een melding aan de AP dient onverwijld binnen 72 uur na constatering plaats te vinden, tenzij het niet waarschijnlijk is dat het datalek (de inbreuk op de privacy) redelijkerwijs een risico voor de betrokkene met zich brengt.

Wanneer het informeren van betrokkenen verplicht is conform de regels van de AP of anderszins gewenst is, wordt de communicatie vanuit het betreffende domein of afdeling in samenspraak met V&C verzorgd. De melder wordt geïnformeerd over de afhandeling van het incident.

Het complete proces van melding van datalekken staat uiteengezet in Bijlage B .

7.3 Evaluatie

Het is van belang om te leren van incidenten. Registratie van incidenten en een periodieke rapportage daarover horen thuis bij een professionele manier van verwerken van persoonsgegevens. De rapportage(s) over incidenten met betrekking tot persoonsgegevens maken daarom een vast onderdeel uit van het privacyjaarverslag van de FG.

Bijlage A Definities en afkortingen

AP: Autoriteit Persoonsgegevens.

AVG: Algemene Verordening Gegevensbescherming. Verordening (EU) 2016/679. De Europese opvolger van de Wbp die vanaf 25 mei 2018 van toepassing is.

Betrokkene: een individueel en natuurlijk persoon op wie een persoonsgegeven betrekking heeft.

Datalek: Persoonsgegevens die in handen vallen van derden die geen toegang tot die gegevens (mogen) hebben.

Derde: Ieder ander, niet zijnde de betrokkene, de verwerkersverantwoordelijke of de verwerker, of enig persoon die onder rechtstreeks gezag valt van de verwerkersverantwoordelijke of de verwerker en gemachtigd is om persoonsgegevens te verwerken.

FG: Functionaris Gegevensbescherming.

Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijk persoon.

Opt-in: Bij opt-in heeft een betrokkene expliciet en aantoonbaar toestemming gegeven voor het ontvangen van e-mail van een bepaalde mailinglist.

Opt-out: Bij een opt-outsysteem zijn betrokkenen automatisch op een mailinglijst geplaatst van een nieuwsbrief en hebben zij de mogelijkheid zich hiervoor uit te schrijven.

PIA: Privacy Impact Assessment.

Privacy by default: Wanneer gebruikers de keuze wordt geboden tussen verschillende opties, dan geeft de standaard instelling de beste privacy garanties.

Privacy by design: Het beheer van de gehele levenscyclus van persoonsgegevens, vanaf het verzamelen tot het verwerken en verwijderen, waarbij stelselmatig aandacht wordt besteed aan allesomvattende waarborgen m.b.t. nauwkeurigheid, vertrouwelijkheid, integriteit, fysieke veiligheid en verwijdering van de persoonsgegevens.

Privacy Impact Assessment / Gegevensbeschermingseffectbeoordeling: Een hulpmiddel dat helpt bij het identificeren van privacy risico's en de handvaten levert om deze risico's te verkleinen tot een acceptabel niveau.

Verwerkingsverantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Bij NWO is de RvB d e verwerkingsverantwoordelijke.

Verwerker: degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

Verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Bijlage B Procesbeschrijving Meldplicht Datalekken

Inleiding

Op 1 januari 2016 is de meldplicht datalekken in werking getreden. Deze meldplicht vormde destijds een nieuw onderdeel van de Wet bescherming persoonsgegevens (Wbp). De meldplicht datalekken houdt in dat organisaties direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra er sprake is van een ernstige datalek waar persoonsinformatie bij is gelekt of verloren gegaan.

Vanaf 25 mei 2018 is de nieuwe privacy verordening AVG van kracht. Deze verordening schrijft voor dat ook niet-ernstige datalekken moeten worden gemeld bij de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat het datalek (de inbreuk op de privacy) redelijkerwijs een risico voor de betrokkene met zich brengt (33 AVG).

In de Wbp/AVG wordt een datalek gedefinieerd als ‘een inbreuk op de beveiliging’. Voorbeelden waarbij sprake kan zijn van een datalek zijn: een gestolen laptop, een inbraak door een hacker, een malware-besmetting of een calamiteit (bijv. brand) in een datacentrum. Echter, deze voorbeelden vallen alleen onder de definitie van een datalek, wanneer persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt. Om dit te kunnen beoordelen, dient een aantal stappen te worden doorlopen, die beschreven staan in deze procesbeschrijving. Dit document heeft als doel het (benoemen en) beschrijven wanneer welke partijen welke rol spelen in dit proces.

Toepassingsbereik: verwerkingsverantwoordelijke en verwerker

NWO is een organisatie die persoonsgegevens verwerkt waarbij de AVG van toepassing is. Dat betekent dat de meldplicht datalekken ook voor NWO, als verwerkingsverantwoordelijke, geldt. Daarnaast werkt NWO met verwerkers voor de verwerking van persoonsgegevens. Bij verwerkers gaat het in principe ook om leveranciers van IT-diensten die persoonsgegevens verwerken. Ook in deze gevallen, dient de verwerkingsverantwoordelijke (NWO) ervoor te zorgen dat de verwerker voldoende waarborgen biedt ten aanzien van de naleving van de meldplicht voor datalekken. Hiervoor dienen, op basis van een verwerkersovereenkomst, schriftelijke afspraken te worden gemaakt tussen de verwerkingsverantwoordelijke en de verwerker.

NWO is gehouden de vereisten uit de meldplicht in de (bestaande en toekomstige) contracten met de verwerkers/leveranciers van NWO te borgen. De afspraken met verwerkers dienen zich in ieder geval te richten op hoe een geconstateerd datalek via de verwerker terecht komt in het reguliere meldproces zoals dat in dit document is beschreven. Daarnaast dient in de afspraken met verwerkers te worden opgenomen dat eventuele kosten bij nalatigheid van de verwerker m.b.t. de meldplicht datalekken op deze partij kunnen worden verhaald. Dit is met het format-verwerkersovereenkomsten (beschikbaar bij JZ) in januari 2018 gerealiseerd.

Het proces van een melding

Het proces van het melden van een datalek tot aan de melding aan de Autoriteit Persoonsgegevens en betrokkene(n), wordt hieronder geschetst. Dit proces bestaat uit een aantal stappen die ook worden beschreven in de richtsnoeren van de Autoriteit Persoonsgegevens:

Signaleren van een datalek:

- Bepaling of daadwerkelijk sprake is van een datalek, analyse en advies over vervolg
- Melding aan de Autoriteit Persoonsgegevens
- Melding aan betrokkene(n)

In deze bijlage wordt bij elke stap kort stilgestaan, bij de acties die hierbij verwacht worden en door wie deze uitgevoerd dienen te worden. Aan de voorkant van het proces, bij het signaleren van een datalek, hebben medewerkers, verwerkers/leveranciers en applicatie-eigenaren de verantwoordelijkheid om signalen van een datalek zo spoedig mogelijk door te geven.

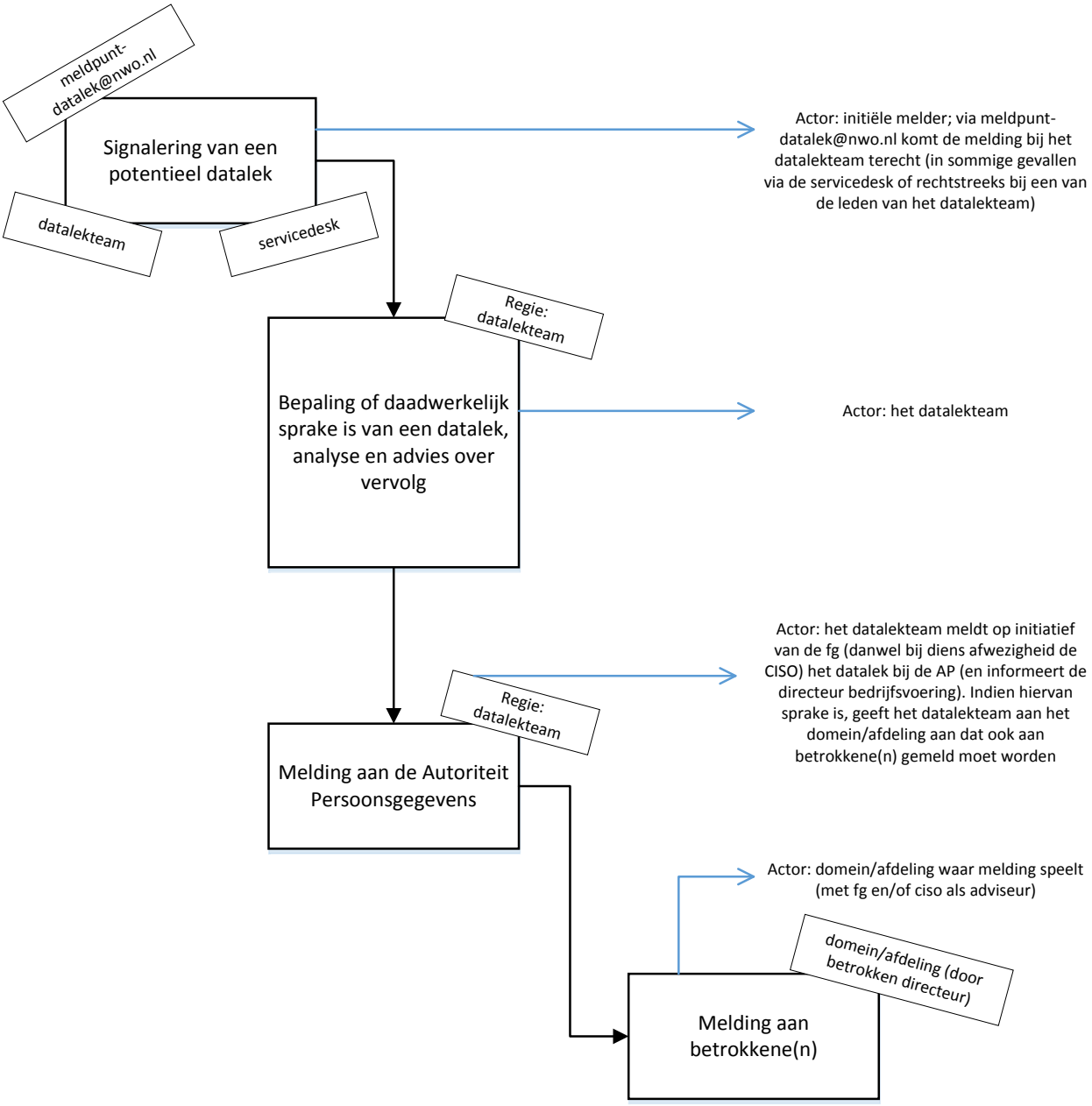
Bij de eerste signalering van een datalek wordt dit zo snel mogelijk doorgegeven aan een centraal meldpunt. Dit wordt gevormd door **meldpunt-datalek@nwo.nl**, waarmee het datalekteam (een onderdeel van het Privacyteam NWO-D) bereikt kan worden. Zo snel mogelijk, omdat de termijn van drie werkdagen waarbinnen datalekken gemeld moeten worden, ingaand vanaf het moment van signalering van het datalek. Het uitgangspunt is dus dat het datalekteam de signalen analyseert op relevantie in het kader van de meldplicht en niet het gebied/afdeling waarbinnen het datalek is opgetreden.

Bij grootschalige beveiligingsincidenten wordt een crisisorganisatie ingericht teneinde adequaat te kunnen ingrijpen en het incident snel op te lossen.

Het primaire uitgangspunt is dat via **meldpunt-datalek@nwo.nl** gemeld wordt. Dit om de melding zo snel mogelijk bij het datalekteam te krijgen. Een deel van de signalen zal echter ook binnen kunnen komen via de Servicedesk of via een van de leden van het datalekteam. Voor de directe meldingen aan het datalekteam kan het bijvoorbeeld gaan om: a) signalen van misbruik of mogelijk misbruik van vertrouwelijke informatie; of b) diefstal van datadragers (denk aan diefstal van telefoons, laptops, tablets, maar ook papieren dossiers e.d.). Signalen van externen zullen veelal binnenkomen via de servicedesk. De servicedesk zal deze signalen doorgeleiden naar het meldpunt-datalek@nwo.nl.

Het datalekteam neemt in het meldproces de registratie, de analyse van het gesignaleerde lek en de advisering over de beoordeling op zich. Het datalekteam gaat daarbij na of de melding van dien aard is, dat deze gemeld moet worden aan de Autoriteit Persoonsgegevens alsmede aan de betrokkenen. Bij het binnenkomen van een signaal informeert het datalekteam ook de directeur bedrijfsvoering. De functionaris gegevensbescherming, danwel bij diens afwezigheid de CISO, verricht de melding bij de AP, tenzij het niet waarschijnlijk is dat het datalek (de inbreuk op de privacy) redelijkerwijs een risico voor de betrokkene met zich brengt. Hierover wordt de directeur bedrijfsvoering achteraf geïnformeerd.

Een betrokkene of betrokkenen wordt / worden door een van de directeuren geïnformeerd na hiertoe informatie vanuit het datalekteam te hebben ontvangen.



Wanneer is sprake van 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 van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens'. Hierbij dient NWO ook rekening te houden met hoe e.e.a. is ingericht en wordt gebruikt in ISAAC, Sharepoint, SURFdrive, etc.

Er is sprake van een datalek als inbreuk wordt gemaakt op de beveiliging van persoonsgegevens. Dit is het geval wanneer persoonsgegevens:

- Blootgesteld zijn aan verlies of onrechtmatige verwerking, en
- Er niet redelijkerwijs kan worden uitgesloten dat persoonsgegevens daadwerkelijk verloren zijn gegaan of onrechtmatig zijn verwerkt.

Soms kan direct de inschatting worden gemaakt of sprake is van verlies of onrechtmatige verwerking. Dan zal het datalekteam al snel tot een oordeel kunnen komen. Het datalekteam kan ook, waar nodig, andere relevante expertise inschakelen, zoals I&A en FB. Het is denkbaar dat in enkele complexe gevallen ook externe expertise nodig is. Denk bij dit laatste aan gevallen waarin systemen zijn besmet met malware. Specialistische kennis voor de beoordeling hiervan kan nodig zijn. Van geval tot geval zal door het datalekteam beoordeeld worden of en welke aanvullende expertise moet worden ingeschakeld. Bij deze beoordeling wordt de directeur bedrijfsvoering betrokken.

Analyse datalek en adviseren over vervolgacties

Als vastgesteld is dat er sprake is van een datalek, dat gemeld moeten worden aan de Autoriteit Persoonsgegevens, moet vervolgens nog worden beoordeeld of dit datalek ernstig genoeg is of van zodanige aard is dat het nodig is om deze ook aan betrokkene(n) te melden. In deze fase ligt de regie bij het datalekteam. Dit team verzorgt de analyse en verzorgt de melding richting de Autoriteit Persoonsgegevens.

Analyse datalek

Brengt het datalek ernstige nadelige gevolgen voor de bescherming van persoonsgegevens met zich? Het datalekteam zal hierover een gefundeerd oordeel vellen. De Autoriteit Persoonsgegevens geeft twee afwegingen die hierbij gemaakt kunnen worden:

- Zijn er persoonsgegevens van gevoelige aard gelekt?
- Leiden de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?

Een aantal categorieën van persoonsgegevens wordt gerekend tot gevoelige gegevens, waaronder BSN-nummers. In de richtsnoer van de AP wordt hier uitgebreid bij stilgestaan, evenals bij de relevante afweging om te bepalen wat de aard en omvang van de inbreuk is.

Het datalekteam legt een aantal gegevens vast over het datalek ten behoeve van de rapportage. De Autoriteit Persoonsgegevens noemt voor deze vastlegging een bewaartermijn van minimaal 1 jaar.

Hoe en op welk moment dient een datalek gemeld te worden aan de Autoriteit Persoonsgegevens?

De Autoriteit Persoonsgegevens stelt een webformulier beschikbaar waarmee datalekken kunnen worden gemeld. Hierop staan vragen, waaruit duidelijk wordt welke informatie bij een melding gewenst is.

Het datalek dient onverwijld gemeld te worden. Dit betekent dat na ontdekking van een datalek enige tijd mag worden genomen voor onderzoek. Uiterlijk 72 uur na ontdekking van het incident moet de melding gedaan worden aan de Autoriteit Persoonsgegevens. Deze termijn gaat in op het moment dat de verwerkingsverantwoordelijke of de verwerker op de hoogte raakt van het betreffende incident. Aan het einde van de termijn is het mogelijk dat er nog geen volledig inzicht is op wat er is gebeurd. De melding dient dan gedaan te worden op basis van de op dat moment beschikbare informatie. De melding kan naderhand worden aangevuld of ingetrokken.

Naast een melding aan de Autoriteit Persoonsgegevens, kan het datalek ook van dien aard zijn dat betrokkene(n) moet(en) worden geïnformeerd. Hiervoor is een aantal extra afwegingen van belang, waarop hieronder dieper wordt ingegaan.

Melding doen aan betrokkene(n)

In deze fase is al vastgesteld dat het datalek gemeld moet worden aan de Autoriteit Persoonsgegevens. Voor het bepalen of gemeld moet worden aan de betrokkene(n), gelden de volgende afwegingen:

- Bieden de technische beschermingsmaatregelen die zijn genomen voldoende bescherming om de melding aan betrokkene achterwege te kunnen laten? (zo ja, dan kan de melding achterwege worden gelaten)
- Zal het datalek waarschijnlijk ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene? (zo nee, dan kan de melding achterwege worden gelaten)
- Zijn er zwaarwegende redenen om de melding aan de betrokkene achterwege te laten? (zo ja, dan kan de melding achterwege worden gelaten)

Voor de eerstgenoemde afweging over passende technische beschermingsmaatregelen is specialistische expertise nodig. De Autoriteit Persoonsgegevens noemt een aantal aspecten waar naar gekeken dient te worden:

- Blootstelling aan vernietiging of aantasting: indien persoonsgegevens zijn vernietigd of zijn aangetast (hier biedt versleuteling bijv. geen bescherming tegen), dan dient betrokkene geïnformeerd te worden.

Onrechtmatige verwerking valt ook onder deze categorie en is ook een reden om betrokkene te informeren, indien er ongunstige gevolgen zijn voor de persoonlijke levenssfeer van de betrokkene.

- *Versleuteld op het moment dat de inbreuk plaatsvond*: indien hier geen sprake van is, dient betrokkene geïnformeerd te worden.
- Is de versleuteling adequaat: het gaat hier om een strenge norm waarbij rekening moet worden gehouden met de laatste stand van de techniek.
- Is het restrisico acceptabel? Dan kan de melding achterwege worden gelaten. Aan de hand van het doorlopen van de vorige aandachtspunten dient NWO zich hier zelf een oordeel over te vormen. Hierbij dient meegenomen te worden welke gevolgen het voor de persoonlijke levenssfeer van betrokkene heeft wanneer een kwaadwillende er nu of in de toekomst alsnog in slaagt om kennis te nemen van de getroffen persoonsgegevens.

Voor de inschatting of het datalek ongunstige gevolgen kan hebben voor de persoonlijke levenssfeer, dient in ieder geval meegewogen te worden wat de aard is van de getroffen persoonsgegevens. Indien deze van gevoelige aard zijn, dan kan er van uit worden gegaan dat betrokkenen geïnformeerd moeten worden.

Indien betrokkenen moeten worden geïnformeerd, meldt de directeur bedrijfsvoering dit aan de betrokken domeinen/afdelingen. De melding van de inbreuk op persoonsgegevens aan betrokkene(n) zal plaatsvinden door het domein/afdeling die applicatie-eigenaar is of waar het datalek is geconstateerd. Andere expertise (Communicatie) kunnen hierbij waar nodig/gewenst aangeschakeld worden.

Wat en op welk moment dient gemeld te worden aan betrokkene(n)?

In de melding aan betrokkene dient in ieder geval vermeld te worden:

- De aard van de inbreuk
- De instantie(s) waar betrokkene meer informatie over de inbreuk kan krijgen
- Maatregelen die aan betrokkene worden aanbevolen om de negatieve gevolgen van de inbreuk te beperken

Denk bij dit laatste aan de aanbeveling aan betrokkene om gebruikersnamen en wachtwoorden te wijzigen (ook voor andere accounts dan bij het getroffen systeem als betrokkene dezelfde wachtwoorden en gebruikersnamen gebruikt voor verschillende diensten). In veruit de meeste gevallen zal de verwerkingsverantwoordelijke (NWO) beschikken over de benodigde contactgegevens van betrokkenen en kan er individueel contact worden opgenomen om betrokkene te informeren.

Bij omvangrijke incidenten kan worden gekozen voor een combinatie van algemene voorlichting en informeren op individuele basis (bijv. informatie op de website in combinatie met een email aan alle betrokkenen, of eventueel via andere kanalen). Enkel een bericht in de media volstaat hierbij vaak

niet; essentieel is dat betrokkenen gewezen worden op maatregelen en informatie die helpen om gevolgen van de inbreuk te beperken.

Het datalek dient onverwijld gemeld te worden aan betrokkene(n). Dit betekent dat na ontdekking van het datalek enige tijd genomen mag worden voor nader onderzoek, zodat betrokkene(n) op een behoorlijke en zorgvuldige manier geïnformeerd kan worden. In verband met de vereiste aanbevelingen aan betrokkene over hoe de inbreuk beperkt kan worden, dient de melding echter wel zo snel mogelijk te gebeuren. Er kan ook gekozen worden om, net als bij de melding aan de Autoriteit Persoonsgegevens, betrokkene in eerste instantie te informeren op basis van de tot dan toe beschikbare informatie, om deze vervolgens in een later stadium uitgebreider te informeren. Dit oordeel wordt belegd bij de directeur bedrijfsvoering, die waakt over dit deel van het proces. De melding zelf zal, zoals gezegd, plaats vinden vanuit het betrokken gebied/afdeling.

Wat indien betrokkene zelf heeft gemeld aan het datalekteam?

Bepaalde incidenten worden gemeld bij het datalekteam (zie eerdere beschrijving). Indien een medewerker misbruik van vertrouwelijke informatie rechtsreeks heeft gemeld bij het datalekteam zal dit team betrokkene informeren of de melding onderzoekwaardig is bevonden. Als dat het geval is, dan zal het datalekteam betrokkene informeren over de afronding van het onderzoek en de uitkomst.

Voorbeelden van datalekken zijn:

- een kwijtgeraakte onversleutelde USB-stick met persoonsgegevens;
- een verloren of gestolen onversleutelde telefoon/laptop/tablet (privé of zakelijk) met persoonsgegevens of toegang tot een NWO-account met persoonsgegevens;
- uitgeprinte documenten met persoonsgegevens die onbeheerd bij een kopieerapparaat liggen;
- anonieme enquêteresultaten die toch herleidbaar blijken te zijn tot respondenten;
- toegang tot persoonsgegevens die herleidbaar zijn tot natuurlijke personen waar je geen toegang toe zou moeten hebben;
- inbraak in een computer met persoonsgegevens of toegang tot een NWO-account met persoonsgegevens door een hacker;
- rondsturen van een overzicht met namen, telefoonnummers en woonadressen van medewerkers;
- onbevoegden die camerabeelden kunnen inzien.

Voorbeelden van andere privacy incidenten zijn:

- gegevensverzameling die niet is gemeld bij de FG;
- onveilige werkwijze die makkelijk kan leiden tot datalekken;
- gegevensverzameling op grond van toestemming van betrokkene zonder dat die toestemming daadwerkelijk gevraagd of geregistreerd wordt.

Bijlage C Privacyregels

Op deelgebieden zijn specifieke privacyregels noodzakelijk. Medewerkers kunnen zich beperken tot de voor hun relevante privacyregels. Door het formeel vaststellen van deze privacyregels wordt de implementatie toetsbaar.

Voor de volgende deelgebieden zijn specifieke privacyregels vastgesteld:

1. *Inventarisatie van gegevensverwerkingen*
2. *Website(s)*
3. *Bedrijfsvoering*
4. *Cameratoezicht*
5. *Aandachtspunten vertrouwelijkheid*

1. Privacyregels – Registratie gegevensverwerkingen

Inleiding

In het privacybeleid wordt aangegeven dat er op deelgebieden specifieke privacyregels noodzakelijk zijn. Een van deze deelgebieden betreft de registratie van gegevensverwerkingen (30 AVG).

Verantwoordelijkheid

1. Gegevensverwerkingen binnen NWO (domeinen en bedrijfsvoering) worden gemeld bij de FG.
2. De FG draagt zorg voor registratie van deze melding in een verwerkingenregister.
3. De FG draagt zorg voor de inventarisatie van de meldingen van de gegevensverwerkingen.

Meldingen

4. Iedere melding bij de FG van een verwerking bevat tenminste de volgende gegevens:
    - Functionele naam van het systeem;
    - Houder van het systeem;
    - Betrokken externe partijen;
    - Doel van de verwerking;
    - Welke categorieën van persoonsgegevens van welke categorieën van betrokkenen worden vastgelegd;
    - Te hanteren bewaartermijnen, dit kan per soort gegeven verschillen;
    - Beschrijving van de genomen beveiligingsmaatregelen;
    - Lijst van organisaties aan wie persoonsgegevens worden verstrekt.
5. Bij het doel van de verwerking wordt ook de wettelijke grondslag vermeld:
    - Toestemming van de betrokkene;
    - Uitvoeren van een overeenkomst;
    - Een wettelijke verplichting;
    - Ter vrijwaring van een vitaal belang van de betrokkene;
    - Uitvoering van een publiekrechtelijke taak;
    - Gerechtvaardigd belang van de verantwoordelijk of derde aan wie gegevens zijn verstrekt.
6. Informatiesystemen die geen persoonsgegevens gebruiken worden niet gemeld.

2. Privacyregels – Website(s)

Inleiding

In het privacybeleid wordt aangegeven dat er op deelgebieden specifieke privacyregels noodzakelijk zijn. Een van deze deelgebieden betreffen de websites van NWO.

Verantwoordelijkheid

1. De afdeling Communicatie is verantwoordelijk voor de implementatie van het privacybeleid op de websites.
2. Websites op subdomeinen vallen onder de verantwoordelijkheid van het betreffende domein en de afdeling Communicatie geeft hen proactief advies.
3. De afdeling communicatie informeert websitebeheerders over de relevante privacyregels wanneer deze met formulieren persoonlijke informatie verzamelen.

Volgen van bezoekers

4. Bezoekers worden alleen gevolgd voor zover daar een goede reden voor is, hierbij wordt het proportionaliteitsprincipe toegepast.
5. Op de websites wordt duidelijk aangegeven hoe en met welk doel bezoekers gevolgd worden.
6. Op de websites wordt duidelijk vermeld welke gegevens worden verzameld.
7. Op de websites wordt duidelijk aangegeven hoe bezoekers de website kunnen bezoeken zonder gevolgd te worden.

Formulieren

8. Formulieren op de websites vragen niet meer persoonlijke informatie dan nodig is voor het doel waarvoor deze verzameld wordt.
9. Ieder formulier maakt duidelijk voor welk doel of welke doelen de gevraagde informatie gebruikt wordt.
10. Ieder formulier maakt deel uit van een informatiesysteem waarop de Privacyregels – Registratie gegevensverwerkingen van toepassing zijn.

IP-adressen

11. IP-adressen worden niet gebruikt om bezoekers te volgen.
12. IP-adressen worden gelogd en kunnen gebruikt worden om security-incidenten en/of technische storingen op te lossen.
13. IP-blokken kunnen gebruikt worden voor statistische analyses.

Hosting

14. Bovenstaande regels zijn van toepassing bij zowel hosting op eigen infrastructuur als hosting bij een leverancier.

15. Indien gebruik wordt gemaakt van hosting bij een leverancier dient deze leverancier te voldoen aan de door NWO gestelde voorwaarden voor SaaS dienstverlening en dient een verwerkersovereenkomst te worden ingevuld en ondertekend.

3. Privacyregels – Bedrijfsvoering

Inleiding

In het Privacybeleid wordt aangegeven dat er op deelgebieden specifieke privacyregels noodzakelijk zijn. Een van deze deelgebieden betreft de bedrijfsvoering. De Securityregels: Informatiesystemen die zijn opgenomen in het Informatiebeveiligingsbeleid 2018 - 2019 zijn van toepassing.

Verantwoordelijkheid

1. De houder of eigenaar van een informatiesysteem is verantwoordelijk voor naleving van de privacyregels.

Verwerving

2. Voor of aan het begin van het project wordt er conform de Classificatierichtlijn Informatie en Informatiesystemen, zoals beschreven in het informatiebeveiligingsbeleid, een classificatie uitgevoerd, zodat de resultaten de vereisten voor het informatiesysteem kunnen meebepalen.
3. Indien gevoelige persoonsgegevens (bijv. BSN-nummers) worden verwerkt dan wordt een Privacy Impact Assessment (PIA) uitgevoerd. De resultaten hiervan worden verwerkt in de business case voor het project. Er wordt getoetst in hoeverre het verwerken van Persoonsgegevens noodzakelijk is. Hierbij worden de verschillende belangen afgewogen.
4. De CISO is bij de uitvoering van de PIA aanwezig/betrokken. Het resultaat van de PIA wordt aan de FG voor advies toegestuurd.
5. Indien een externe verwerker wordt ingeschakeld, wordt eerst een verwerkersovereenkomst afgesloten (raadpleeg afdeling JZ).

Implementatie

6. De principes “Privacy by Design” en “Privacy by Default” worden gehanteerd. Dit betekent o.a. dat vanaf het begin van het ontwerpproces met privacy rekening wordt gehouden en dat dataminimalisatie wordt toegepast.
7. De houder meldt de gegevensverwerking bij de FG voordat het systeem in gebruik wordt genomen.
8. Bewaartermijnen worden vastgelegd, zodat persoonsgegevens niet langer worden bewaard dan noodzakelijk is.
9. Betrokkenen worden door de houder geïnformeerd over de gegevensverwerking.
10. De houder richt een proces in zodat tijdig, binnen vier weken, aan het recht op inzage en het recht op verbetering, aanvulling, verwijdering of afscherming voldaan kan worden
11. Voor testdoeleinden worden in principe geen productiegegevens gebruikt, behalve voor het reproduceren van geconstateerde problemen. Wanneer voor een acceptatietest productiegegevens worden gebruikt, dan dient de autorisatiematrix gelijk te zijn aan die van de productieomgeving.

4. Privacyregels – Cameratoezicht

Inleiding

In het Privacybeleid wordt aangegeven dat er op deelgebieden specifieke privacyregels noodzakelijk zijn. Voor het cameratoezicht bij NWO zijn buiten de Privacyregels – bedrijfsvoering de hieronder opgenomen regels van toepassing.

Verantwoordelijkheid

1. De directeur bedrijfsvoering is als houder van het cameratoezicht verantwoordelijk voor het naleven van de privacyregels bij het cameratoezicht bij NWO.

Doel en transparantie

2. De gegevens worden uitsluitend gebruikt voor de volgende doeleinden:
   a. Bescherming van de veiligheid en gezondheid van natuurlijke personen;
   b. Beveiliging van de toegang tot gebouwen en terreinen;
   c. Bewaking van zaken die zich in gebouwen of op terreinen bevinden;
   d. Vastleggen van incidenten.
3. Camera's zijn duidelijk zichtbaar opgehangen of er wordt ter plekke, bijvoorbeeld middels stickers, aangegeven dat gebruik wordt gemaakt van camerabewaking.

Toegang

4. De live beelden zijn alleen toegankelijk voor de medewerkers die belast zijn met de beveiliging en bewaking bij NWO.
5. Toegang tot opgenomen beelden is alleen mogelijk in een speciaal daartoe ingerichte ruimte.
6. Toegang tot opgenomen beelden hebben alleen het hoofd van de verantwoordelijke afdeling en diens plaatsvervanger.
7. Betreffende medewerkers hebben een geheimhoudingsplicht met betrekking tot gegevens die tot personen herleidbaar zijn.

Opslag

8. Opgenomen camerabeelden worden zo opgeslagen dat deze niet toegankelijk zijn voor anderen.
9. Opgenomen camerabeelden worden niet langer dan twee weken bewaard. Camerabeelden, opgenomen in opdracht van de facilitaire Dienst van NWO, worden maximaal 4 dagen bewaard.

Incidenten

10. Na een incident kan na het constateren dat relevant beeldmateriaal beschikbaar is, besloten worden deze beelden veilig te stellen en zo lang te bewaren als voor het betreffende onderzoek nodig is.
11. In het geval er sprake is van een redelijk verdenking of vermoeden van een ongeoorloofde handeling kan na schriftelijke opdracht van de Raad van Bestuur gebruik gemaakt worden van verdekt geplaatste camera's zonder dat betrokkenen hierover worden geïnformeerd.
12. Beelden worden alleen aan derden verstrekt indien het belang van NWO dit vordert na een overeenkomstig besluit door de Raad van Bestuur. De politie kan de beelden alleen op vordering verkrijgen, of ná toestemming van de (hulp)officier van justitie.

5. Privacyregels – Aandachtspunten vertrouwelijkheid

1. Autorisatie. Het is van belang zeker te zijn dat alleen die personen toegang hebben tot vertrouwelijke informatie die die gegevens ook nodig hebben. Inrichting van een autorisatiebeleid kan hiervoor zorgdragen. Attent zijn op het gebruik van een account van een ander, ook bij tijdelijke vervanging zoals bv. bij zwangerschapsverlof.
2. Authenticatie. Voorkomen dat iemand zich voor iemand anders kan uitgeven en bij vertrouwelijke informatie kan komen. Voorkom dat medewerkers wachtwoorden delen of opschrijven. Overweeg tweefactorauthenticatie.
3. Toegang van elders dan de vaste werkplek. Thuiswerken of werken op een andere locatie kan tot extra risico's leiden. Dit is te voorkomen door te filteren op IP-adres.
4. Invoer van gegevens. Bedenk dat aantekeningen en tijdelijke documenten ook vertrouwelijke informatie kunnen bevatten. Zorg voor gecontroleerde afvoer of vernietiging van dergelijke papieren en bestanden.
5. Verwerken en raadplegen van gegevens. Wanneer een medewerker informatie opvraagt of toevoegt, kan vertrouwelijke informatie, als deze niet noodzakelijk is voor de handeling, worden verborgen of achter een extra knop gezet worden.
6. Onderbreken van het werk. Denk om het gebruik van screensavers en om het niet zichtbaar laten liggen van vertrouwelijke papieren.
7. Uitwisselen gegevens met andere systemen. Wissel niet meer gegevens uit dan noodzakelijk. Wanneer vertrouwelijke informatie wordt verstrekt, wees er dan zeker van dat die gegevens ook vertrouwelijk blijven. Maak duidelijke afspraken vooraf.
8. Produceren van rapportages. Per rapport zal bepaald moeten worden welke mate van vertrouwelijkheid er moet gelden. Wanneer bekend is dat een rapport vertrouwelijk is, dan kan dat er standaard op vermeld worden.
9. Opslaan van gegevens. Kritiek vertrouwelijke informatie hoort versleuteld opgeslagen te worden. Bij centrale opslag is dat van belang om te voorkomen dat hackers of beheerders toegang hebben. Bij decentrale opslag speelt meer het risico van virussen en diefstal. Papier met kritiek vertrouwelijke informatie, bijvoorbeeld een dossier, dient opgeslagen te worden in een afgesloten kast.
10. Bewaren van email. Het bewaren van vertrouwelijke informatie in het emailsysteem betekent dat deze informatie via ieder device, dus ook de telefoon en tablet, langdurig toegankelijk blijft. Denk bijvoorbeeld aan ziektemeldingen, sollicitatiebrieven en functionerings-gesprekken. Verwijder emails met vertrouwelijke informatie zo snel mogelijk.
11. Archiveren van informatie. Leg de bewaartermijn en de regels omtrent toegang en vernietiging vast.
12. Afdrukken van gegevens. Papier met kritiek vertrouwelijke informatie mag alleen geprint worden als de medewerker er zelf bijstaat, mag niet blijven rondslingeren, mag niet zomaar meegenomen worden en moet na gebruik gecontroleerd afgevoerd of vernietigd worden.
13. Meenemen van digitale gegevens. Informatie kan op USB-stick, harde schijf, laptop, etc. meegenomen worden. Bedenk eerst of alle informatie wel nodig is, kan de vertrouwelijke informatie niet weggelaten worden? Kritiek vertrouwelijke informatie hoort versleuteld opgeslagen te worden.
14. Werken in publieke ruimtes. Andere personen kunnen van scherm of papier meelezen. Voorkom dit bij het raadplegen van vertrouwelijke informatie. Denk hierbij aan gang, kantine, cafés, restaurants, wachtruimtes, trein, vliegtuig, etc.
15. Bespreken van informatie. Bedenk bij het bespreken van informatie, ook bij het gebruik van een telefoon, dat anderen mee kunnen luisteren.
16. Versturen van informatie. Controleer of de betreffende persoon deze informatie wel nodig heeft, probeer de verstrekte informatie te minimaliseren. Controleer of we als NWO deze informatie wel aan betreffende persoon mogen verstrekken. Wanneer vertrouwelijke

informatie per email of anderszins digitaal verstuurd wordt, dan dient dit versleuteld te gebeuren.

17. Audittrail. Middels een logfile moet na te gaan zijn wie toegang tot welke vertrouwelijke informatie heeft gehad.
18. Diefstal van informatie. Wanneer papier met vertrouwelijke informatie of een informatiedrager (USB-stick, tablet, etc.) wordt verloren, welke procedures gelden er dan? Enerzijds minimaliseren verdere schade, door wachtwoord aan te passen etc. Wat verder te doen wordt verder in de procedure Meldplicht Datalekken uitgewerkt.
19. Schrijven van procedures. Neem de rollen van medewerkers op in procedures en niet de namen van individuen.
20. Uitbreiden of nieuw ontwerpen/aanschaffen van applicaties. Bedenk vooraf welke beveiligingsaspecten een rol spelen. De Classificatierichtlijn en een PIA kunnen hierbij helpen. Halverwege een project met extra eisen komen zorgt voor hogere kosten.
21. Testen van applicaties. Voor het testen van een applicatie wordt vaak met de live-data gewerkt, die is immers realistisch. Maar voor de meeste tests kan de kritiek vertrouwelijke informatie prima weggelaten worden. Dit kan door bepaalde velden in een database met andere informatie te overschrijven of te verhaspelen en geen originele vertrouwelijke documenten te gebruiken.
22. Uitbesteden van werk of gebruik van clouddiensten. Maak heldere afspraken en als er persoonsgegevens worden uitgewisseld sluit dan een verwerkersovereenkomst af.