omgevingsdienst nhn

BESTUURLIJK PRIVACY BELEID

OPSTELLER

Organisatie	:	Omgevingsdienst Noord-Holland Noord
Afdeling	:	Bedrijfsvoering
Projectcoördinator	:	Wendeline Sjouwerman, plaatsvervanger van Berdinald Juddu
Telefoon	:	06 519 999 73
E-mail	:	wsjouwerman@odnhn.nl
Kenmerk	:	AVG, Privacy, Informatiebeveiliging
Adres	:	Postbus 2095
		1620 EB HOORN
Bezoekadres	:	Dampten 2
	:	1624 NR HOORN

OPDRACHTGEVER

Organisatie	:	Omgevingsdienst Noord-Holland Noord
Contactpersoon	:	Rob van Doorn
Telefoon	:	06 826 980 98
E-mail	:	rvandoorn@odnhn.nl

DATUM

2 april 2019

INHOUDSOPGAVE

1 INLEIDING 4
1.1 De scope van het bestuurlijk privacybeleid 4
2 DEFINITIES EN BEGRIPPEN 5
3 HET BELEID 6
3.1 Visie, missie en strategie 6
3.1.1 Visie 6
3.1.2 Missie 6
3.1.3 Doelstelling en strategie 6
4 VERWERKINGSBEGINSELEN 6
5 PRINCIPES 7
5.1.1 Bestuurlijke en beleidsmatige principes 7
5.1.2 Inhoudelijke en uitvoerende principes 8
6 PERSOONSGEGEVENS 8
6.1 Persoonsgegevens 8
7 BIJZONDERE PERSOONSGEGEVENS 9
8 GEVOELIGE PERSOONSGEGEVENS 9
9 VERPLICHTINGEN EN RISICO'S 9
9.1 Voorbeelden van risico's voor de organisatie 10
9.2 Voorbeelden van risico's voor de betrokkene 10
10 RECHTEN BETROKKENEN 10
11 DATALEKKEN 10
12 INBREUKENREGISTER 11
13 TECHNISCHE EN ORGANISATORISCHE MAATREGELEN 11
14 DATA PROTECTION IMPACT ASSESSMENT (DPIA) 11
15 PRIVACY BY DESIGN 12
16 ANONIMISERING EN PSEUDONIMISERING 12
17 OVEREENKOMST 12
17.1 Criteria voor verwerker 13
17.2 Gedeelde verantwoordelijkheid 13
17.3 De OD NHN en verwerkingsverantwoordelijken binnen de keten 13
18 FUNCTIONARIS GEGEVENSBESCHERMING 14
19 BRONNEN 14

1 INLEIDING

Dit document beschrijft het bestuurlijk privacy beleid van de Omgevingsdienst Noord-Holland Noord (OD NHN) gebaseerd op de Algemene Verordening Gegevensbescherming (AVG).

Het bestuurlijk privacy beleid dient wettelijk te worden vastgesteld door het hoogst leidinggevende orgaan en wordt om die reden ter goedkeuring aangeboden aan het bestuur van de OD NHN.

De AVG vervangt de oude Nederlandse Wet bescherming persoonsgegevens (Wbp) en wordt vanaf 25 mei 2018 gehandhaafd door de Nederlandse toezichthouder: de Autoriteit Persoonsgegevens (AP).

De nieuwe wetgeving zet in op uitbreiding van de rechten van burgers, meer transparantie over én controleerbaarheid van de verwerking van persoonsgegevens.

De AVG biedt ruimte aan lidstaten om een (strenger) beleid ten aanzien van privacy te voeren. Binnen Nederland is dit gebeurd door de nationale wet Uitvoeringswet AVG (UAVG). Het boetebeleid is in Nederland iets anders vormgegeven. Eerst wordt een waarschuwing gegeven in de vorm van een last onder dwangsom, in plaats van direct een opeisbare boete.

Organisaties die niet voldoen aan de wet riskeren boetes en lopen kans op imagoschade. Gedurende de komende jaren zullen rechters gaan bepalen hoe bepaalde zaken het beste geïnterpreteerd en geïmplementeerd kunnen worden. Het beschikbaar komen van jurisprudentie kan wijzigingen in dit beleidsdocument tot gevolg hebben.

Een goede invoering vraagt van iedere organisatie een visie op hun privacy beleid. Een dergelijk beleid geeft richting en vorm aan de wijze waarop de organisatie omgaat met privacy én op welke wijze ze voldoen aan de wettelijke eisen.

Het privacy beleid van de OD NHN is afgeleid van universele principes. Deze principes zijn voor de OD NHN leidend en hierna beschreven.

Het voorliggende beleid is een definiëring van het kader, de visie, een missie, strategie en deze principes. Ze wordt afgesloten door een nadere motivering en een beschrijving van de implicaties van de principes.

Met de vaststelling en inrichting van het privacy beleid én met de implementatie van de Privacy Management Organisatie[1] geeft het bestuur van de OD NHN naar behoren invulling aan haar verplichtingen zoals opgenomen in de AVG, en is zij in staat om op elk gewenst moment verantwoording af te leggen.

1.1 De scope van het bestuurlijk privacy beleid

Het bestuurlijk privacy beleid is de kapstok voor de uitvoering van de privacywetgeving binnen de OD NHN. Het is onder meer, maar niet uitsluitend, van toepassing op:

- (Bedrijfsvoerings)processen van de OD NHN waarbij gewerkt wordt met persoonsgegevens.
- Onderliggende voorzieningen voor informatieverwerking en gegevensopslag. Er wordt hierbij geen onderscheid gemaakt tussen analoge of digitale informatieverwerking;
- (Gegevensverwerkings)processen die de OD NHN uitbesteedt, inkoopt of op een andere manier organiseert;
- Gegevensuitwisseling met ketenpartners en derden zoals de veiligheidsregio, de Belastingdienst, politie en justitie etc.;
- De gehele 'gegevensketen': van het genereren of verzamelen van gegevens, het dagelijkse gebruik ervan en de gegevensopslag (zowel digitaal als analoog) tot en met de (eventueel) archivering en vernietiging ervan;
- De verwerking van statistische en/of geanonimiseerde gegevens;
- De toepassing van informatiebeveiliging.

1 Privacy Management Organisatie beschrijft de operationele taken, verantwoordelijkheden en werkwijze en is in een separaat document opgesteld.

2 DEFINITIES EN BEGRIPPEN

Onderstaand worden de meest gebruikte termen en begrippen toegelicht.

AVG – de Europese privacywet ' Algemene Verordening Gegevensbescherming ' (AVG). Deze wet wordt in het Engels ook wel General Data Protection Regulation (GDPR) genoemd.

Uitvoeringswet AVG – dit is de Nederlandse Uitvoeringswet waarin Nederland invulling geeft aan lid statelijke vrijheden.

Verwerkingsverantwoordelijke – een natuurlijke persoon of rechtspersoon, een overheidsinstantie die/dat alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

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

Verwerkersovereenkomst – Wanneer verwerking van persoonsgegevens wordt uitbesteed of wanneer er persoonsgegevens van een andere partij worden verwerkt, moeten er afspraken worden gemaakt tussen de verwerkingsverantwoordelijke en de verwerker. Deze afspraken dienen te worden vastgelegd in een zogenaamde verwerkersovereenkomst.

Verwerkingsregister – Dit is een vanuit de AVG verplicht register wat door organisaties wordt bijgehouden en waarin is vastgelegd wat voor persoonsgegevens zij opslaan of verwerken, van wie deze persoonsgegevens zijn, waar dit wordt opgeslagen en hoe dit is beveiligd.

Betrokkene – dit betreft de persoon of personen wiens persoonsgegevens worden verwerkt. Bijvoorbeeld klanten, partners of medewerkers.

Persoonsgegevens – dit betreft alle informatie waarmee een natuurlijk persoon direct of indirect kan worden geïdentificeerd. Gegevens waarmee direct kan worden geïdentificeerd zijn identificatoren zoals een naam, identificatienummer en locatiegegevens. Gegevens die mede bepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, en ook gegevens die in combinatie met andere gegevens leiden tot identificeerbaarheid, dienen ook te worden beschouwd als persoonsgegevens. Voorbeelden zijn gegevens over: inkomen, vermogen, beroep, woonplaats, kenteken en leeftijd.

Bijzondere persoonsgegevens – zijn naar hun aard vertrouwelijker dan 'gewone' persoonsgegevens en verwerking ervan geschiedt op andere gronden dan 'gewone' persoonsgegevens. Het vertrekpunt is dat verwerking van deze categorieën van gegevens verboden is, tenzij aan een aantal voorwaarden is voldaan zoals genoemd in de AVG of de uitvoeringswet. Met 'bijzondere persoonsgegevens' worden gegevens bedoeld over gezondheid, ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, strafrechtelijke persoonsgegevens en/of persoonsgegevens over onrechtmatig of hinderlijk gedrag.

DPIA – Data Protection Impact Assessment, Gegevensbeschermingseffectbeoordeling
Voorafgaand aan een nieuwe verwerking is het verplicht een risicobeoordeling te maken.

3 HET BELEID

3.1 Visie, missie en strategie

3.1.1 Visie

De visie van de OD NHN in het kader van AVG is als volgt:

Wij verwerken voor opdrachtgevende gemeenten en de provincie NH veel gegevens van ondernemingen en daaraan gerelateerde natuurlijke personen. Tevens verwerken wij veel persoonsgegevens van inwoners en van onze medewerkers. Wij zijn ons bewust van de verantwoordelijkheid die hiermee gepaard gaat. Daarom voeren wij doelbewust een privacy beleid. Wij houden voortdurend rekening met het belang van de inwoners en onze medewerkers bij rechtmatige, behoorlijke en transparante gegevensverwerking. De inwoners, onze medewerkers en opdrachtgevers mogen erop vertrouwen dat zij hun gegevens veilig met ons kunnen delen. Voor het verbeteren van onze taakuitoefening analyseren wij de beschikbare gegevens en leggen verbanden, binnen de ruimte van de wettelijke kaders. Onze medewerkers zijn zich bewust van de positie van inwoners en belangen van ondernemers en gaan professioneel om met de gegevens conform het privacy beleid.

3.1.2 Missie

Deze visie vertaalt zich naar de volgende missie:

OD NHN ziet het in het kader van de AVG als haar missie om haar bedrijfsvoering en de bijbehorende gegevensverwerking in overeenstemming te brengen met de nieuwe privacy wetgeving en haar ondernemers, inwoners, medewerkers en opdrachtgevers het vertrouwen te geven dat hun gegevens in veilige en professionele handen zijn. Bedrijfsprocessen en de bijbehorende gegevensverwerking zijn evenwichtig en aantoonbaar voorzien van passende waarborgen voor de bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens. Privacy is een vanzelfsprekend kwaliteitsaspect voor de uitvoering van werkzaamheden door eenieder die voor en/of met OD NHN werkt.

3.1.3 Doelstelling en strategie

Om deze verscherpte wetgeving te kunnen implementeren wordt veel aandacht besteed aan bewustwording, kennisontwikkeling, gedragsregels én duidelijke kaders. Medewerkers, en met name proceseigenaren, dienen bekend te zijn met hun eigen verantwoordelijkheid op het gebied van privacy. Het document Privacy Management Organisatie is de operationele beschrijving hoe het privacy beleid wordt uitgevoerd en is daarom in een apart document beschreven. Het beschrijft, onder andere, de taken, rollen en verantwoordelijkheden van alle actiehouders.

Samenvattend zijn er drie belangrijke strategieën om de doelstelling te bereiken:

1. Het vaststellen en toepassen van een privacy beleid met richtinggevende principes;
2. Het zorgen voor bewustwording en kennisdeling in de organisatie rond privacy-aspecten;
3. Het implementeren en onderhouden van de Privacy Management Organisatie met daarvan afgeleide werkinstructies, zodat medewerkers ondersteuning krijgen bij hun dagelijkse werkzaamheden op privacywetgevingsaspecten.

4 VERWERKINGSBEGINSELEN

De AVG introduceert kernbeginselen waaraan alle verwerkingen van persoonsgegevens moeten voldoen. De verwerkingsverantwoordelijke, in dit geval de OD NHN, moet kunnen bewijzen dat wordt voldaan aan deze verwerkingsbeginselen (Accountability). De verantwoordelijke moet hierover afspraken maken met de verwerkers.

Doelbinding– persoonsgegevens mogen alleen voor een bepaald, uitdrukkelijk omschreven doel worden verwerkt. Dit dient te worden vastgelegd in een overeenkomst tussen verwerkingsverantwoordelijke en verwerker. De persoonsgegevens mogen dus niet voor andere doeleinden worden gebruikt, en het doel kan nooit eenzijdig worden aangepast.

Rechtmatigheid– persoonsgegevens mogen alleen worden verwerkt wanneer aan de tenminste één van de volgende grondslagen is voldaan (wanneer er een grondslag is voor de verwerking):

- er is toestemming van de betrokkene;
- de verwerking is noodzakelijk voor de uitvoering van een overeenkomst;
- de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting;
- de verwerking is noodzakelijk om de vitale belangen van betrokkene of andere natuurlijke personen te beschermen;
- de verwerking is noodzakelijk ter vervulling van een taak van algemeen belang of openbaar gezag opgedragen aan de verantwoordelijke;
- de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde.

Dataminimalisatie– uitsluitend voor het doel noodzakelijke gegevens mogen worden verwerkt, en niet meer dan dat.

Datakwaliteit – de verwerkingsverantwoordelijke heeft een vergaande verplichting om te borgen dat gegevens compleet, juist (dus ook actueel) en bruikbaar zijn. Dit hangt deels samen met de verplichting om persoonsgegevens te beveiligingen door het nemen van voldoende technische én organisatorische maatregelen.

Verwerkingsduur – gegevens mogen worden verwerkt gedurende een specifieke vastgestelde periode, en ze mogen voor slechts bepaalde tijd worden bewaard. De organisatie stuurt hier actief op.

Transparantie – de verwerkingsverantwoordelijke zorgt dat verwerking van persoonsgegevens transparant plaatsvindt, en kan zodoende rekenschap afleggen over de exacte verwerking van de persoonsgegevens.

Verantwoordingsplicht – de verwerkingsverantwoordelijke moet verantwoording kunnen afleggen aan de toezichthouder en de betrokkenen. Verwerkingsverantwoordelijke moet hiertoe rekenschap kunnen afleggen over de aard en het doel van de verwerking.

De verwerkingsverantwoordelijke moet kunnen bewijzen dat wordt voldaan aan deze verwerkingsbeginselen (accountability). De verantwoordelijke kan hier natuurlijk afspraken over maken met de verwerker.

5 PRINCIPES

In deze paragraaf worden de principes van het privacy beleid schematisch opgesomd. De principes zijn geformuleerd op twee niveaus: bestuurlijk/beleidsmatig en inhoudelijk/uitvoerend.

5.1.1 Bestuurlijke en beleidsmatige principes

1. Het bestuur van de OD NHN voert regie op het privacy beleid
2. Het privacy beleid van de OD NHN is risico gedreven
3. De OD NHN heeft een besturingsmodel ingericht voor het privacy beleid
4. De OD NHN is transparant over de verwerking van persoonsgegevens
5. De OD NHN legt verantwoording af over haar privacy beleid
6. Privacy gerelateerde verzoeken en klachten worden klantgericht afgehandeld
7. De OD NHN zorgt voor ketenregie in de samenwerking met de aangesloten gemeenten de provincie en ketenpartners

5.1.2 Inhoudelijke en uitvoerende principes

1. De gegevensverwerking is legitiem: uitsluitend uit hoofde van de primaire bedrijfsvoering en is wettelijk gerechtvaardigd
2. De gegevensverwerking is gebaseerd op doelbinding
3. De informatievoorziening is gebaseerd op proportionaliteit "need to know"
4. Persoonsgegevens voldoen aan de eisen van informatiekwaliteit
5. Persoonsgegevens worden opgeslagen voor de periode waarin zij nodig zijn
6. Het privacy beleid wordt integraal meegenomen in projecten en bij de inrichting en besluitvorming van alle nieuwe informatievoorzieningen
7. Gegevensverwerking in het kader van analyse en onderzoek wordt waar mogelijk gebaseerd op gepseudonimiseerde of geanonimiseerde persoonsgegevens
8. De OD NHN hanteert een eigen informatieveiligheidsbeleid ondanks afname van diensten van aangesloten gemeenten en provincie
9. PIA's liggen ten grondslag aan risicovolle verwerkingen van persoonsgegevens
10. Inwoners kunnen bij de Privacy Officer van de OD NHN terecht met vragen over privacy. Voor klachten kunnen ze zich wenden tot de FG

6 PERSOONSGEGEVENS

6.1 Persoonsgegevens

Persoonsgegevens betreft alle informatie waarmee een natuurlijk persoon direct of indirect kan worden geïdentificeerd. Gegevens waarmee direct kan worden geïdentificeerd zijn identificatoren zoals een naam, identificatienummer, natte handtekening en locatiegegevens.

Gegevens die mede bepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, en ook gegevens die in combinatie met andere gegevens leiden tot identificeerbaarheid, dienen ook te worden beschouwd als persoonsgegevens. Voorbeelden zijn gegevens over: inkomen, vermogen, beroep, woonplaats en leeftijd.

De AVG verruimt de definitie van het begrip persoonsgegevens. Voor de beeldvorming hieronder een aantal voorbeelden van informatie die worden gezien als persoonsgegevens:

- Voornaam en achternaam
- Adres
- BSN
- Identificatienummers
  - Personeelsnummer
  - Klantnummer
  - Patiëntnummer
  - Bankrekeningnummer
- Geboortedatum / leeftijd
- Locatiegegevens
- Online identificatoren
  - IP-adres
  - MAC-adres
  - Cookies (ook als de naam van de persoon achter het cookie niet bekend is)
  - RFID tag

  - IMEI nummer
- E-mailadres
- Vingerafdruk
- Pasfoto
- Iemands IQ
- Gebruikersnaam
- Persoonskenmerken zoals gewicht, lengte, haarkleur en geslacht, geluidsopname van iemands stem

7 BIJZONDERE PERSOONSGEGEVENS

Het verwerken van bijzondere persoonsgegevens is verboden, tenzij er aan de voorwaarden van de AVG óf aan de uitzonderingen zoals genoemd in de Uitvoeringswet AVG wordt voldaan.
De volgende gegevens worden gezien als bijzondere persoonsgegevens (artikel 9 lid 1):

- Ras of etnische afkomst;
- Politieke opvattingen;
- Religieuze of levensbeschouwelijke overtuigingen;
- Lidmaatschap van een vakbond;
- Genetische gegevens;
- Biometrische gegevens met het oog op de unieke identificatie van een persoon;
- Gegevens over gezondheid;
- Seksueel gedrag of seksuele gerichtheid;
- Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (artikel 10 AVG, artikel 32 en 33 UAVG).

De AVG noemt in artikel 9 lid 2 voorwaarden voor verwerking van bijzondere persoonsgegevens waardoor deze wel rechtmatig verwerkt kunnen worden.

8 GEVOELIGE PERSOONSGEGEVENS

Gevoelige persoonsgegevens zijn niet als zodanig gedefinieerd in de wet. Voor gevoelige persoonsgegevens moet mede gekeken worden naar de context. Voor deze gegevens kunnen extra beschermingsmaatregelen nodig zijn, zoals financiële gegevens en/of economische gegevens van betrokkene, gegevens die stigmatiserend kunnen werken, gebruikersnamen, wachtwoorden en andere inloggegevens, gegevens die onder beroepsgeheim/ geheimhoudingsplicht vallen, wettelijk identificatienummer (BSN).
Indien sprake is van een datalek en er zijn ook nog gevoelige gegevens gelekt zal vaak ook de betrokkene hiervan op de hoogte moeten worden gebracht.

9 VERPLICHTINGEN EN RISICO'S

Dit hoofdstuk geeft een beknopt overzicht van de taken die ten behoeve van de verantwoordelijkheden van de OD NHN uitgevoerd dienen te worden.
De OD NHN heeft een documentatieplicht (artikel 30). Dit betekent onder andere dat wij moeten kunnen aantonen wat voor informatie wij opslaan of verwerken, van wie deze data is, waar dit wordt opgeslagen en hoe dit is beveiligd. Er wordt een Verwerkingenregister bijgehouden waarin dit wordt vastgelegd.
Compliance risico's
Het niet voldoen aan de bepalingen uit de AVG vormt een risico. Wanneer de OD NHN de beginselen of grondslagen van de AVG overtreedt, of de privacy-rechten van betrokkenen schendt,

dan kan de Autoriteit Persoonsgegevens een boete van maximaal €20 miljoen of, indien dat bedrag hoger uitkomt, 4% van de wereldwijde jaaromzet opleggen. In de UAVG is de bepaling opgenomen dat er eerst een last onder dwangsom kan worden opgelegd.

Een boete door de handhavende instantie is echter niet het enige risico als gevolg van onzorgvuldige omgang met persoonsgegevens. In de volgende paragrafen volgen nog een aantal voorbeelden van mogelijke risico's binnen een AVG context.

9.1 Voorbeelden van risico's voor de organisatie

- Negatieve publiciteit en imagoschade.
- Dwangmaatregelen of boetes opgelegd door de toezichthouder wegens het niet naleven van de wetgeving.
- Persoonlijke schade voor bestuurders i.v.m. bestuurdersaansprakelijkheid.
- Schadeclaims door betrokkenen.
- Hogere kosten bij het achteraf nemen van privacy maatregelen.
- Slechte datakwaliteit leidt tot slechtere performance van de business.

9.2 Voorbeelden van risico's voor de betrokkene

- Persoonsgegevens worden gedeeld en gebruikt op onrechtmatige wijze.
- Persoonsgegevens worden gebruikt voor doeleinden waar de betrokkenen niet van op de hoogte zijn.
- Kwetsbare groepen personen, zoals ouderen en laaggeletterden, worden eerder het slachtoffer van oneigenlijk gebruik van hun persoonsgegevens en kunnen hierdoor gevolgen van ondervinden als uitsluiting, discriminatie of stigmatisering.
- Persoonsgegevens worden niet of onjuist gemanaged waardoor er een wildgroei aan bestanden met persoonsgegevens ontstaat; hierdoor stijgt de kans op datalekken en veiligheidsrisico's.

10 RECHTEN BETROKKENEN

De rechten van betrokkenen ten aanzien van de verwerkingsverantwoordelijke zijn onder de AVG aanzienlijk versterkt. Om de juiste naleving van de AVG zelfstandig en/of makkelijker af te kunnen dwingen (de zogenaamde horizontale handhaving) heeft de betrokkene hiertoe de volgende rechten en middelen:

- Recht op informatie;
- Recht van inzage;
- Recht op rectificatie;
- Recht op gegevenswissing/ vergeten mogen worden;
- Recht op beperking van de verwerking;
- Recht op overdraagbaarheid/ meenemen van data;
- Recht van bezwaar;
- Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming/profilering.

De OD NHN dient ervoor te zorgen dat betrokkenen zich te allen tijde kosteloos kunnen beroepen op deze rechten, en dat er binnen de wettelijk geldende termijn van 4 weken wordt gereageerd op verzoeken van betrokkenen. Een verlenging met maximaal twee maanden is mogelijk, mits die binnen één maand wordt gemeld en de extra benodigde tijd goed is onderbouwd.

11 DATALEKKEN

Een datalek is een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, verlies, wijziging of ongeoorloofde toegang tot de doorgezonden, opgeslagen of anderszins verwerkte gegevens. Niet alle datalekken zijn meldenswaardig. Als gegevens zodanig

beveiligd zijn door bv encryptie hoeft het niet gemeld te worden bij de toezichthouder, maar wel opgenomen in het incidentenregister.

De OD NHN is verplicht de betrokkene onverwijld in kennis te stellen, wanneer het datalek *waarschijnlijk* ongunstige gevolgen kan hebben voor diens persoonlijke levenssfeer.

Het datalek dient binnen 72 uur te worden gemeld aan de Autoriteit Persoonsgegevens, en mogelijk ook aan de betrokkenen.

De AVG gaat uit van het principe "melden tenzij" de verwerkings-verantwoordelijke kan aantonen dat het onwaarschijnlijk is dat een inbreuk risico's voor de rechten en vrijheden van natuurlijke personen met zich meebrengt.

De definitie van onrechtmatige verwerking is breed. Het betreft onder andere het aanpassen en/of veranderen van persoonsgegeven en onbevoegde toegang tot, of afgifte daarvan. Er is dus niet alleen sprake van een datalek als een hacker toegang tot persoonsgegevens krijgt. Er is bijvoorbeeld ook sprake van een datalek in de volgende situaties:

- Verlies van een gegevensdrager (USB-stick, harde schijf, laptop, telefoon).
- Het sturen van een mailing met adressen in het AAN of CC veld (in plaats van het BCC veld).
- Het verloren gaan van gegevens terwijl er geen back-up beschikbaar is.
- De onbevoegde ongedaanmaking van pseudonimisering (hoofdstuk 16).
- Tweezijdig geprinte brieven met op iedere zijde de naam van een andere geadresseerde

12 INBREUKENREGISTER

De AVG verplicht de OD NHN tot het documenteren van alle inbreuken c.q. incidenten in verband met persoonsgegevens, inclusief de gevolgen en de genomen maatregelen om dit in de toekomst te voorkomen (artikel 33 lid 5). Ook wanneer deze inbreuken nadrukkelijk niet hebben geleid tot een datalek. De Autoriteit Persoonsgegevens kan toegang verlangen tot deze documentatie (artikel 58 lid 1 punt a), en de documentatie moet adequaat zijn om de toezichthouder te laten controleren of datalekken daadwerkelijk worden gemonitord en opgevolgd.

13 TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

Verwerkingsverantwoordelijke en verwerker moeten passende technische en organisatie maatregelen nemen om zogenaamde onrechtmatige verwerkingen van persoonsgegevens te voorkomen. De term ‘passend’ kan worden bepaald door te kijken naar het risico in verhouding tot de mogelijkheden en kosten om het risico af te dekken.

Met de richtlijn beveiligingsafspraken derden wordt geborgd dat leveranciers voldoende maatregelen nemen om persoonsgegevens te beschermen. Aangezien de OD NHN geen eigen ICT voorzieningen onderhoudt, kan met deze richtlijn grotendeels invulling worden gegeven aan de wettelijke eis van een ‘passend beveiligingsniveau’.

14 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

De AVG verplicht organisaties tot het uitvoeren van een DPIA (in het Nederlands de gegevensbeschermingseffectbeoordeling) wanneer er wijzigingen in de verwerking van persoonsgegevens worden doorgevoerd die mogelijk/waarschijnlijk een hoog risico (een potentiële inbreuk) inhouden voor de rechten en vrijheden van natuurlijke personen (betrokkenen). De achterliggende gedachte is dat de DPIA inzicht geeft in de risico’s waardoor de juiste maatregelen genomen kunnen worden om de risico’s tot een acceptabel niveau te verlagen.

Het toepassen van een DPIA werk in feite als een drietrapsraket:

1. Bij iedere verwerking moet de verwerkingsverantwoordelijke een eerste beoordeling maken van de risico's die daarbij kunnen bestaan (classificatie);
2. Wanneer uit de eerste beoordeling blijkt dat er sprake is van een hoog risico, dan dient een uitgebreide DPIA worden uitgevoerd;
3. Wanneer uit de DPIA blijkt dat het hoge risico niet kan worden beperkt met redelijke middelen, dan moet de toezichthouder eerst worden geraadpleegd.

15 PRIVACY BY DESIGN

De AVG verplicht de OD NHN om invulling te geven aan de begrippen privacy by design en privacy by default. Dit betekent dat de ICT voorzieningen die de OD NHN inzet voor haar bedrijfsvoering zodanig dient te zijn ingericht (door middel van ontwerp- en standaardinstellingen) dat slechts noodzakelijke persoonsgegevens worden verwerkt voor het beoogde doel en niet langer worden bewaard dan noodzakelijk. Het is belangrijk om hier bij grote wijzigingen of projecten expliciet bij stil te staan en dit ook vast te leggen.

16 ANONIMISERING EN PSEUDONIMISERING

Puur anonieme gegevens vallen buiten de scope van de AVG. Deze zijn namelijk niet herleidbaar tot een persoon. Bij pseudonimisering ligt dat anders. Pseudonimisering zorgt er namelijk voor dat gegevens niet kunnen worden herleid tot een individu zolang de gegevens geïsoleerd worden beschouwd. Dit betekent dat de herleidbaarheid is beperkt, maar niet voorgoed onmogelijk is gemaakt. Met behulp van "aanvullende informatie" zijn gepseudonimiseerde gegevens wederom te herleiden naar persoonsgegevens. Om deze reden worden pseudonieme persoonsgegevens door de AVG gezien als persoonsgegevens, waardoor de AVG op dergelijke gegevens onverminderd van toepassing is. Overigens worden beide methoden door de AVG gezien als belangrijke maatregel om persoonsgegevens te beschermen. Dit wordt doorgaans het meest expliciet in het geval van testdata.

17 OVEREENKOMST

Bij het uitbesteden van een verwerking of bij het verwerken van persoonsgegevens van een andere partij moeten afspraken worden gemaakt tussen de (mede)verwerkingsverantwoordelijke en de verwerker. Deze afspraken kunnen worden vastgelegd in een overeenkomst die vaak 'verwerkersovereenkomst' wordt genoemd. Dit is een gangbare, maar geen officiële term uit de AVG. De afspraken kunnen ook volgen uit een andere rechtshandeling krachtens Unierecht of lid statelijk recht. Van belang is dat onder meer verantwoordelijkheden worden benoemd, bijvoorbeeld bij wie de regie berust en waar betrokkenen een aanspreekpunt kunnen vinden met betrekking tot de verwerking.

Volgens de AVG wordt in een verwerkersovereenkomst minimaal het volgende geregeld:

- Het doel van de verwerking (doelbinding);
- Persoonsgegevens mogen uitsluiten worden verwerkt op basis van schriftelijke instructies van de verantwoordelijke;
- Personen betrokken bij de verwerking borgen vertrouwelijkheid door bijvoorbeeld het ondertekenen van een geheimhoudingsverklaring als onderdeel van de arbeidsovereenkomst of een non-disclosure agreement (NDA);
- De technische en organisatorische maatregelen die door de verwerker worden genomen zijn vastgelegd in een bijlage;
- Of er sprake is van algemene of specifieke toestemming voor het inschakelen van sub-verwerkers door verwerker;
- Dat er met de sub-verwerker door verwerker een sub-verwerkersovereenkomst wordt gesloten die voldoet aan de AVG;
- Of en, zo ja, hoe verwerker de verwerkingsverantwoordelijke bijstaat in het geval betrokkenen hun rechten ingevolge de AVG wensen uit te oefenen;

- Of en, zo ja, hoe verwerker de verwerkingsverantwoordelijke bijstaat bij:
  - Beveiliging van de verwerking;
  - Melding inbreuken aan Autoriteit Persoonsgegevens (datalekken);
  - Mededeling inbreuken aan betrokkenen;
  - Gegevensbeschermingseffectbeoordeling (DPIA);
  - Indien nodig: voorafgaande raadpleging Autoriteit Persoonsgegevens.
- Na afloop van de verwerking worden persoonsgegevens gewist en indien de verwerkingsverantwoordelijke dit wenst, eerst teruggegeven aan de verwerkingsverantwoordelijke;
- Verwerkingsverantwoordelijke stelt alle informatie ter beschikking die nodig is om de nakoming van de verplichtingen onder de AVG aan te tonen;
- De verwerker laat audits door de verwerkingsverantwoordelijke, of door een door verwerkingsverantwoordelijke aangewezen auditor, toe om te controleren of verwerker aan de verplichtingen ingevolgde de AVG en verwerkersovereenkomst voldoet of heeft voldaan;
- De verwerker stelt verwerkingsverantwoordelijke onmiddellijk op de hoogte wanneer verwerker van mening is dat een instructie van de verwerkingsverantwoordelijke in strijd is met de AVG;
- Of verwerker gecertificeerd is, zodat hiermee kan worden aangetoond dat verwerker voldoende garanties biedt.

17.1 Criteria voor verwerker

De bepaling of een partij een verwerker is, moet gebeuren aan de hand van de feitelijke/werkelijke situatie. Primair is hierbij van belang in welke mate een partij invloed kan uitoefenen op de doelen van de verwerking. Secundair is de invloed van een partij op de middelen van de verwerking. Wanneer bijvoorbeeld de klant het doel bepaalt en de leverancier de middelen, is niet meteen duidelijk of een leverancier als verwerker is te zien. In een dergelijk geval geeft de doelbepalende partij (de klant) de doorslag. Er kan worden gesteld dat de doelbepalende partij (de klant) de middelen van de leverancier (de partij die de middelen bepaalt) goedkeurt, en ze daarmee heeft vastgesteld. De klant is dan verwerkingsverantwoordelijke en de leverancier verwerker.

17.2 Gedeelde verantwoordelijkheid

De OD NHN is een gemeenschappelijke regeling (GR) die taken uitvoert die bij wet aan haar klanten (gemeenten en provincie) zijn toegekend. In het geval van mandaat of machtiging worden de bevoegdheden door de OD NHN namens de gemeenten en of provincie uitgeoefend. De gemeenten of provincie zijn in deze situatie verwerkingsverantwoordelijke en de OD NHN ook. Men spreekt dan van een gedeelde verantwoordelijkheid.

17.3 De OD NHN en verwerkingsverantwoordelijken binnen de keten

De doorgifte van persoonsgegevens aan een andere verwerkingsverantwoordelijke in een keten is alleen toegestaan als de onderlinge verantwoordelijkheden duidelijk zijn. Het is van belang dat iedere verwerkingsverantwoordelijke zijn deel van de verantwoordelijkheid invult en vastlegt hoe die invulling plaatsvindt. De OD NHN sluit met de ketenpartners convenanten. Bij de invulling daarvan moeten dus steeds alle partijen betrokken worden, om eenduidig als keten te kunnen functioneren.

Voor de onderlinge samenhang van de keten is de aanstelling van een onafhankelijke ‘ketenregisseur’ die als ‘spin in het web’ functioneert voor het maken van en wijzigen van afspraken in de keten noodzakelijk. De rolverdeling in de keten wordt duidelijk gemaakt; niet alleen voor de onderlinge verantwoordelijkheidsverdeling en aansprakelijkheden, maar ook voor de omgang met de betrokkenen. Het is voor betrokkenen eenduidig inzichtelijk wie ze moeten benaderen voor hun vragen over de verwerking van hun gegevens en het uitoefenen van hun rechten. Om deze

benodigde transparantie te bereiken wordt de verantwoordelijkheidsverdeling openbaar gemaakt. Daardoor kunnen de rechten van betrokkenen gewaarborgd worden en is het bovendien duidelijk voor de ketenpartners welke informatieplicht zij hebben.

18 FUNCTIONARIS GEGEVENSBESCHERMING

Een functionaris gegevensbescherming (FG), ook wel Data Protection Officer (DPO) genoemd, houdt toezicht op de toepassing en naleving van de AVG binnen een organisatie. Het aanstellen van een functionaris gegevensbescherming is verplicht voor overheden en publieke organisaties.

19 BRONNEN

Bij het opstellen van dit privacy beleid zijn de onderstaande bronnen geraadpleegd.

- **Algemene Verordening Gegevensbescherming;** Publicatieblad van de Europese Unie; 4.5.2016; L 119/1; VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016
- **Uitvoeringswet Algemene Verordening Gegevensbescherming;** Staatsblad van het Koninkrijk der Nederlanden; Jaargang 2018; 144 Wet van 16 mei 2018, houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming)
- **Memorie van toelichting op het wetsvoorstel van de Algemene Verordening Gegevensbescherming:** https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming
- **Boek:** "Tekstuitgave Privacyverordening & UAVG", door Jan Berkvens en Cathérine Jakimowicz, Boom Juridische uitgevers,
ISBN : 9789462904828, tweede druk, publicatiedatum: 05-2018
- **Boek:** "De Algemene Verordening Gegevensbescherming Editie 2017" door Arnoud Engelfriet, Lisette Meij, Peter Kager. ISBN: 9789082083446. Eerste druk.
- **CIP Privacy Baseline v3.0:** https://www.cip-overheid.nl/wp-content/uploads/2018/05/20180210-BIR2017-definitief.pdf
- **Strategische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten:** https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2016/07/Strategische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-v1.02.pdf
- **Tactische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten:** https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2016/07/Tactische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-v1.02.pdf
- **Ketensamenwerking:** https://www.cip-overheid.nl/wp-content/uploads/2018/03/20180212-Privacyafspraken-in-ketensamenwerking-v1_0.pdf
- **Meldplicht:** https://www.cip-overheid.nl/wp-content/uploads/2018/01/20170126_Meldplicht_v2_2-def.pdf
- Whitepaper AVG – GDRP van Stimmt B.V.
- **Factsheet meldplicht datalekken:** https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2018/02/2018_IBD_Factsheet_Meldplicht_Datalekken_v1.1.pdf.pagespeed.ce.yQMcOjemWR.pdf
- **PIA vragenlijst door Norea:** https://www.norea.nl/download/?id=522
- **Guideline on Data Protection Officers**: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp243_rev01_enpdf_0.pdf
- **Functionaris gegevens bescherming:** https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/functionaris- voor-de-gegevensbescherming-fg
- **Derde landen:** https://www.baaten.com/kennis/wet-en-regelgeving-informatiebeveiliging/persoonsgegevens- buiten-europa/

- http://dirkzwagerieit.nl/2017/12/13/uitvoeringswet-avg-uavg-gepubliceerd-eerste-analyse/
- **Ontslagbescherming FG:** https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming
- **Verwerker:** https://cms.law/nl/NLD/Publication/Privacy-de-begrippen-verantwoordelijke-en-bewerker-nader- uitgelegd
- **Opinion 1/2010 on the concepts of "controller" and "processor**": http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf
- **Test data:** https://www.it-jurist.nl/nieuws/testen-met-productie-data-mag-data
- **Privacy by design en Privacy by default:** https://www.nederlandict.nl/news/avg-uitgelegd-deel-3-privacy-by-design-privacy-by-default/
- **Guidelines DPIA door WP29:** https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp248_rev.01_nl.pdf
- **DPIA:** https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia
- **Gemeenschappelijke regeling:** https://www.vijverbergjuristen.nl/publicaties/gemeenschappelijke-regeling-verwerkingsverantwoordelijke-of-verwerker-in-AVG
- **Verplichte DPIA:** https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-ap-voor-een-verplichte-dpia-6667