GEMEENTE NOORDENVELD

GEMEENTEBLAD

Officiële uitgave van de gemeente Noordenveld

Nr. 337907

25 juli

2022

Privacybeleid 2022

1. Inleiding

De bescherming van privacy en verantwoorde omgang met persoonsgegevens staan bij Gemeente Noordenveld hoog in het vaandel. Persoonlijke gegevens behandelen we zorgvuldig en voorzien wij van passende beveiliging. In dit beleid leggen we vast hoe we met persoonsgegevens omgaan en wat we verwachten van onze medewerkers.

1.1 Reikwijdte

Dit beleid is van toepassing op de omgang met persoonsgegevens van betrokkenen, waaronder bewoners van Gemeente Noordenveld, medewerkers, ketenpartners en stakeholders en de daaraan ten grondslag liggende documenten, zowel digitaal, als niet-digitaal.
Dit privacybeleid is gebaseerd op de privacyregels die voortkomen uit de Algemene verordening gegevensbescherming (hierna: AVG).

1.2 Functionaris gegevensbescherming

Een Functionaris Gegevensbescherming (hierna: FG) is de onafhankelijke AVG toezichthouder binnen een organisatie. Hij of zij wordt opgenomen in het register voor functionarissen gegevensbescherming van de Autoriteit Persoonsgegevens (hierna: AP). De FG monitort de interne verwerkingen van persoonsgegevens binnen een organisatie. De AVG en de Autoriteit Persoonsgegevens vereisen dat de FG de volgende taken uitvoert :

- Contactpersoon zijn voor de Autoriteit Persoonsgegevens;
- aanspreekpunt zijn voor inwoners voor vragen of klachten over privacy;
- toezichthouden op de naleving van de AVG;
- rapporteren aan College van Burgemeester en Wethouders (hierna: het college);
- gevraagd en ongevraagd adviseren en informeren van organisatie en het college;
- aanspreekpunt zijn binnen de organisatie voor vragen of klachten over privacy;
- signaleren van interne en externe ontwikkelingen;adviseren m.b.t. (de uitvoering van) Data Protection Impact Assessments (DPIA's);
- training en bewustwording van medewerkers.

Voor vragen of opmerkingen rondom privacy kun je contact opnemen met de Functionaris Gegevensbescherming via fg@noordenveld.nl.

1.3 Privacy Officer

Wij streven ernaar om privacy continu te blijven waarborgen in deze gemeente. Daarom is de regie voor de implementatie van privacyborging belegd bij een privacy officer. Taken die vallen binnen het takenpakket van privacy officer zijn:

- Begeleiden proces voor de rechten van betrokkenen;
- deelname in projectgroepen, borgen privacy by design;
- regie houden register gegevensverwerkingen;
- input leveren bij opstellen protocollen, reglementen en procedures;
- bijhouden datalekken- en incidentenregister;
- het ordenen en updaten van privacydocumentatie;
- het ontwikkelen van interne privacyregelingen;
- data protection impact assessment (DPIA) op (nieuwe) processen en projecten;
- training en bewustwording van medewerkers;
- contractmanagement verwerkersovereenkomsten;
- coördinatie procedure datalekken;
- het volgen van interne en externe ontwikkelingen.

Met de privacy officer kun je contact opnemen via Veldnet.

1.4 Chief Information Security Officer

De Chief Information Security Officer (hierna: CISO) draagt zorg voor de bescherming van alle soorten gegevens die verwerkt worden binnen de Gemeente Noordenveld. Vanuit dit privacybeleid is de CISO specifiek belast met de beveiliging van persoonsgegevens. Dit vraagt om een informatiebeveiligings-programma en een 'passende beveiliging' waarbij de drie uitganspunten van informatiebeveiliging: beschikbaarheid, integriteit en vertrouwelijkheid worden geborgd. De Baseline Informatiebeveiliging Overheid (BIO) is het normenkader waar de beveiliging door de gemeente aan dient te voldoen.

Taken die vallen binnen het takenpakket van de CISO zijn:

- Implementeert informatiebeveiliging in de organisatie
- Zorgt voor adequate registratie, analyse en rapportage van informatiebeveiligings-incidenten
- Initieert en managet informatiebeveiligingsprojecten
- Stemt informatiebeveiligingsactiviteiten en -projecten af met andere beveiligings-domeinen, waaronder persoonsgegevensbescherming met de FG en privacy officer en fysieke beveiliging met de verantwoordelijke voor het gebouw
- Zorgt voor training en opleiding m.bt. informatiebeveiligingsbewustzijn
- Voert risicoanalyses van informatiesystemen uit
- Monitort informatiebeveiligingsrisico's en rapporteert daarover
- Vertaalt de informatiebeveiligingsbehoefte van de organisatie naar beveiligingsmaatregelen
- Zorgt voor informatiebeveiligingsontwerpen en -oplossingen en de implementatie van security -by-design en privacy-by-design in informatiesystemen
- Presenteert informatiebeveiligingsoplossingen aan collega's en leidinggevenden
- Realiseert en monitort informatiebeveiligingsassessments, -tests, -reviews en -audits
- Presenteert verbetervoorstellen aan het MT met betrekking tot informatiebeveiliging en -risico's

De CISO heeft regelmatig overleg met de privacy officer en FG.

2. Wet- en regelgeving

Sinds 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van kracht. Deze verordening geldt in de hele Europese Unie. Naast de AVG geldt in Nederland de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG).

2.1 Wat zijn persoonsgegevens?

Persoonsgegevens zijn gegevens die te herleiden zijn tot een persoon: de natuurlijke persoon kan direct of indirect worden geïdentificeerd. Dit kan onder andere aan de hand van een naam, een identificatienummer, locatiegegevens of van één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Er zijn verschillende soorten persoonsgegevens te onderscheiden:

1. Algemene persoonsgegevens
Dit zijn gegevens die bij het alledaagse gebruik horen. Voorbeelden van algemene persoonsgegevens zijn namen, telefoonnummers, e-mailadressen en geboortedata.
2. Gevoelige gegevens
Dit zijn gegevens die een grote impact hebben op de privacy van het individu, maar die geen bijzondere persoonsgegevens zijn. Het belangrijkste voorbeeld is informatie over de financiële situatie van een persoon.
3. Bijzondere persoonsgegevens
Dit zijn gegevens die grote invloed hebben op iemand zijn privacy. In de AVG staan deze bijzondere gegevens apart genoemd. Bijzondere persoonsgegevens mogen in de regel niet worden verwerkt, tenzij aan in de wet vastgelegde uitzonderingsgronden wordt voldaan. Bijzondere persoonsgegevens zijn: religieuze/levensbeschouwelijke overtuigingen, ras/etnische afkomst, politieke opvattingen, gezondheidsgegevens, seksueel gedrag of gerichtheid, lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens en strafrechtelijke gegevens. Het Burgerservicenummer (BSN) wordt in Nederland op dezelfde wijze als bijzondere persoonsgegeven beschermd.

2.2 De Algemene Verordening Gegevensbescherming (AVG)

Gemeente Noordenveld leeft de volgende vuistregels van de AVG na:

1. Doelbinding
Persoonsgegevens mogen slechts voor bepaalde en gerechtvaardigde doeleinden worden verzameld en niet worden verwerkt voor doeleinden die daarmee onverenigbaar zijn.

2. Rechtmatige grondslag
Elk gebruik van persoonsgegevens moet gebaseerd zijn op een rechtmatige grondslag uit de AVG. Deze grondslagen zijn: de uitvoering van een overeenkomst, nakoming van een wettelijke plicht, de bescherming van een vitaal belang, een taak van algemeen belang of een taak voor het openbaar gezag, een gerechtvaardigd belang en ondubbelzinnige toestemming van de betrokkene. Op de laatste twee grondslagen (gerechtvaardigd belang en toestemming) mag de gemeente zich echter niet beroepen in uitoefening van haar publieke taken.

3. Kwaliteit en dataminimalisatie
De persoonsgegevens moeten zoveel mogelijk juist, nauwkeurig, toereikend en ter zake dienend zijn. Er mogen niet meer gegevens worden verwerkt dan noodzakelijk is voor het doel van de verwerking.

4. Bewaren en vernietigen
De verwerkte gegevens mogen niet langer bewaard worden dan noodzakelijk is voor het bereiken van het doel.

5. Transparantie of openheid
De persoon van wie persoonsgegevens worden verwerkt moet kunnen overzien door wie en voor welke doeleinden zijn/haar gegevens worden verwerkt. Gemeente Noordenveld moet de betrokkene actief informeren over de gegevensverwerking.

6. Passende beveiliging
Gemeente Noordenveld heeft een beveiligingsplicht. De organisatie moet ter beveiliging van de persoonsgegevens, passende technische en organisatorische maatregelen treffen.

7. Rechten van betrokkenen
De rechten van betrokkenen dienen nageleefd te worden, deze rechten worden toegelicht in hoofdstuk zes.

8. Meldplicht datalekken
Wanneer Gemeente Noordenveld een inbreuk in verband met persoonsgegevens (datalek) constateert, dienen we deze in veel gevallen binnen 72 uur te melden bij de Autoriteit Persoonsgegevens (AP). Afhankelijk van de aard en omvang van het lek dienen ook de betrokkenen te worden geïnformeerd.

9. Verwerkersovereenkomsten
Met leveranciers, die namens Gemeente Noordenveld persoonsgegevens verwerken, sluiten we een verwerkersovereenkomst waarin we de plichten van partijen en rechten van betrokkenen regelen op grond van de AVG.

2.3 Autoriteit persoonsgegevens (AP)

De Autoriteit Persoonsgegevens (AP) is de nationale toezichthouder op de AVG en deze heeft, naast een controlerende bevoegdheid, ook een boetebevoegdheid. Daarnaast doet de AP onderzoek naar onderwerpen die betrekking hebben op privacy, geeft ze advies aan zowel organisaties als betrokkenen en zijn ze een meldpunt voor datalekken.
De Functionaris Gegevensbescherming van Gemeente Noordenveld houdt de nieuwsberichten, richtsnoeren en beleidsregels van de AP goed in de gaten en geeft naar aanleiding hiervan advies. Hij/zij deelt de relevante ontwikkelingen met de betreffende medewerkers en brengt deze actief onder de aandacht.

3. Algemene uitgangspunten privacybeleid

Bij onze dagelijkse werkzaamheden ontkomen we er niet aan om persoonsgegevens te verwerken. Onder verwerken wordt verstaan: alle handelingen die medewerkers kunnen uitvoeren met persoonsgegevens, van verzamelen tot en met vernietigen. Hierbij kun je denken aan: het verzamelen, creëren, inzien, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.
Wij zijn verantwoordelijk voor de verwerking van persoonsgegevens. Daarom is het belangrijk om betrokkenen, ketenpartners, stakeholders en medewerkers te informeren over de omgang met en het gebruik van persoonsgegevens. Wij informeren hen ook over hun rechten met betrekking tot de persoonsgegevens. Dit wordt vermeld in het privacy statement op onze website.
Gemeente Noordenveld neemt de privacy van betrokkenen serieus en hanteert een privacybeleid. We hanteren de volgende uitgangspunten met betrekking tot privacy:

- We verwerken persoonsgegevens alleen ten behoeve van het doel waarvoor zij zijn verkregen en verwerken daarbij niet meer gegevens dan noodzakelijk;
- we gaan zorgvuldig om met persoonlijke informatie en nemen passende organisatorische en technische maatregelen om de persoonsgegevens te beschermen;
- we beschouwen alle persoonsgegevens als vertrouwelijke informatie, waar een geheimhoudingsplicht voor geldt. Intern wordt gewerkt op basis van het need-to-know principe, dat houdt in dat medewerkers en leveranciers alleen toegang krijgen tot gegevens voor zover deze gegevens noodzakelijk zijn voor hun taakuitoefening;
- we houden ons aan de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) en andere toepasselijke wet- en regelgevingen omtrent de verwerking van persoonsgegevens.

4. Doeleinden en voorwaarden voor gegevensbescherming

4.1 Doeleinden

Gemeente Noordenveld verwerkt persoonsgegevens voor in ieder geval de volgende doeleinden:

- Gemeentelijke taken: Gemeenten hebben op basis van de wet verschillende taken die zij moeten uitvoeren en waarbij persoonsgegevens moeten worden verwerkt. Denk hierbij aan taken als het heffen en innen van belastingen, het uitvoeren van de jeugdwet, WMO en participatiewet of de behandeling van een vergunningsaanvraag.
- Personeelsadministratie: verwerkingen van persoonsgegevens van personeelsleden in dienst van of werkzaam voor Gemeente Noordenveld.
- Salarisadministratie: verwerkingen van gegevens van personeelsleden in dienst van of werkzaam voor Gemeente Noordenveld.
- Sollicitanten: verwerkingen van gegevens van sollicitanten die bij Gemeente Noordenveld hebben gesolliciteerd om werkzaam te zijn in dienst van of voor Gemeente Noordenveld.
- Debiteuren en crediteuren: verwerkingen van persoonsgegevens van debiteuren en crediteuren van Gemeente Noordenveld (het gaat hierbij om financiële administraties als boekhoudingen en soortgelijke administraties).
- Archiefbestemming: verwerkingen van persoonsgegevens voor het archiefbeheer.
- Documentenbeheer: verwerkingen van inkomende en uitgaande documenten. Je kunt hierbij denken aan bijvoorbeeld postregistratie en e-mailarchivering.
- Communicatieapparatuur: verwerkingen van persoonsgegevens in verband met het gebruik van communicatieapparatuur die ter beschikking wordt gesteld aan personeelsleden in dienst van of werkzaam voor Gemeente Noordenveld.
- Computersystemen: verwerkingen van persoonsgegevens die uitsluitend zijn gericht op het onderhoud, het beheer, de beveiliging, het gebruik en de goede werking van computersystemen of computerprogramma's binnen Gemeente Noordenveld.
- Toegangscontrole: verwerkingen van persoonsgegevens voor het geven van toegang tot (onderdelen van) gebouwen of informatiesystemen aan personeelsleden in dienst van of werkzaam voor Gemeente Noordenveld.
- Overig intern beheer: verwerkingen van persoonsgegevens van personen in dienst van of werkzaam voor Gemeente Noordenveld, die niet onder een andere categorie vallen.

4.2 Voorwaarden

Gmeente Noordenveld verwerkt niet meer persoonsgegevens dan nodig is voor de in dit hoofdstuk, dan wel de in het verwerkingenregister genoemde doeleinden. Het verwerkingsregister is in beheer bij de privacy officer.
Verwerking van persoonsgegevens vindt alleen plaats als één of meer van de volgende punten van toepassing is:

a. De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene (persoon op wie de gegevens betrekking hebben) partij is of wenst te worden.
b. Er sprake is van een vitaal belang (kwestie van leven of dood).
c. De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de Gemeente Noordenveld is opgedragen.
d. De gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen.
e. De gegevensverwerking valt niet onder de uitoefening van de gemeente haar publieke taken en is nodig voor het behartigen van een gerechtvaardigd belang van Gemeente Noordenveld en de met haar verbonden ondernemingen of instellingen, voor zover dat belang in dat geval zwaarder weegt dan de privacyrechten van betrokkenen.

Als geen van bovenstaande punten van toepassing is, dan moet door de betrokkene schriftelijk, expliciet, geïnformeerd en vrijelijk toestemming gegeven worden. Dat wil zeggen dat voor betrokkene duidelijk moet zijn waar toestemming voor gegeven wordt, waar de gegevens voor nodig zijn, hoe er met de gegevens omgegaan wordt en dat betrokkene vrij is toestemming te weigeren. Deze toestemming kan betrokkene op elk gewenst moment weer intrekken. Binnen het Sociaal Domein kan deze grondslag echter vrijwel nooit worden gebruikt, vanwege de afhankelijkheidsrelatie tussen de betrokkene en de Gemeente Noordenveld. Daarbinnen moet één van de andere grondslagen gebruikt worden.

5. Gegevensverstrekking aan verwerkers en derde partijen

Het uitwisselen van persoonsgegevens met andere partijen brengt risico's voor de privacy met zich mee. Dit doen wij dus nooit zomaar. Gemeente Noordenveld is immers verantwoordelijk voor wat er met de persoonsgegevens van betrokkenen gebeurt.
Bij het verzenden/aanleveren van (grote delen van) onze inwonersgegevens of medewerkersgegevens moet altijd eerst worden vastgesteld of de regels die uit dit beleid gevolgd worden. Bij twijfel dient men de privacy officer vooraf te raadplegen. Het verzenden van gevoelige, bijzondere of grote hoeveelheden normale persoonsgegevens per onbeveiligde e-mail is niet toegestaan.

5.1 Verwerkers

Vele verwerkingen van persoonsgegevens zijn door ons uitbesteed aan leveranciers. Deze leveranciers worden 'verwerkers' genoemd, omdat de dienst hoofdzakelijk ziet op het verwerken van persoonsgegevens namens Gemeente Noordenveld. Voorbeelden van verwerkers zijn de ICT- en softwareleveranciers of administratiekantoren. Deze leveranciers hebben toegang tot de persoonsgegevens in bijvoorbeeld onze systemen of maken voor ons de back-ups en slaan voor ons de gegevens op. In een standaard verwerkersovereenkomst heeft Gemeente Noordenveld met deze partijen afspraken gemaakt over hoe zij om dienen te gaan met onze persoonsgegevens. Gemeente Noordenveld blijft verantwoordelijk voor de gegevensverwerkingen die deze partijen namens ons uitvoeren, dat betekent dat boetes en aansprakelijkheid in eerste instantie bij ons komen te liggen.
Het afsluiten van een verwerkersovereenkomst is een wettelijke verplichting, de Gemeente Noordenveld hanteert de VNG standaard verwerkersovereenkomst.

5.2 Derden

We verstrekken soms persoonsgegevens aan derde partijen die noodzakelijk betrokken zijn bij werkzaamheden. We verstrekken enkel de noodzakelijke persoonsgegevens aan derden. Gemeente Noordenveld moet zorgen voor de vereiste contractuele en organisatorische maatregelen om te verzekeren dat de persoonsgegevens uitsluitend voor vastgelegde doeleinden door de derde partij worden gebruikt.

5.2.1 Wettelijke verplichting

Gemeente Noordenveld is in sommige gevallen wettelijk verplicht persoonsgegevens aan derden te verstrekken. Denk bijvoorbeeld aan de verstrekking van gegevens aan de Belastingdienst op grond van wet- en regelgeving. Een ander voorbeeld is het verstrekken van gegevens aan de politie in het kader van een strafrechtelijk onderzoek. In het laatste geval worden slechts persoonsgegevens verstrekt indien de politie hier uitdrukkelijk en gericht om vraagt en daarnaast aangeeft op grond van welke wettelijke regeling de gegevens verstrekt moeten worden (bijvoorbeeld op bevel van de rechter-commissaris).

5.3 Stakeholders en relaties

Gemeente Noordenveld kan op grond van samenwerkingsconvenanten gegevens uitwisselen met bijvoorbeeld woningcorporaties, politie en zorginstellingen. De gegevensuitwisseling dient binnen de wettelijke kaders plaats te vinden en zal niet meer persoonsgegevens omvatten dan strikt noodzakelijk is.
In convenanten maken we afspraken over welke gegevens we uitwisselen, met welk doel, op basis van welke rechtsgrond, welke beveiliging we toepassen, hoe de aansprakelijkheid geregeld is en hoe we omgaan met de rechten van betrokkenen. Daarmee scheppen we de kaders die nodig zijn om persoonsgegevens met onze samenwerkingspartners te kunnen uitwisselen.
Meer informatie over de geldende convenanten en de bijbehorende kaders voor gegevensuitwisseling zullen worden opgenomen in de verwerkingenregister van Gemeente Noordenveld.

6. Rechten van betrokkenen

Gemeente Noordenveld is verplicht betrokkenen te informeren over de verwerkingen en zijn of haar rechten in deze. Inwoners of medewerkers die vragen, opmerkingen of klachten hebben over de verwerking van persoonsgegevens, kunnen contact opnemen met de Functionaris Gegevensbescherming. Betrokkenen hebben het recht op inzage, correctie en wissing van de eigen persoonsgegevens, alsmede het recht zich tegen een bepaalde verwerking te verzetten en/of de verwerking te beperken (uitzonderingen daargelaten). Daarnaast hebben betrokkenen het recht zich te onttrekken aan profiling. Verzoeken dienen schriftelijk, waaronder ook begrepen per e-mail, te worden gedaan. De privacy officer heeft te regie over dit verzoek, de benodigde medewerkers dienen zich in te zetten om het verzoek tijdig en zorgvuldig te kunnen afhandelen.

6.1 Recht op informatie

De betrokkene heeft het recht om in heldere taal informatie te ontvangen over de wijze waarop en waarom van de gegevensverwerking plaatsvindt. Dit geldt zowel voor het geval dat de persoonsgegevens bij de betrokkene zelf worden verzameld, als wanneer dit via anderen gebeurt.

6.2 Recht op inzage en afschrift

Betrokkenen hebben het recht de eigen persoonsgegevens die bij ons bekend zijn op te vragen, te vragen voor welke doeleinden die gegevens worden gebruikt en met wie deze gegevens worden gedeeld. Zij hebben ook het recht hiervan een afschrift te ontvangen. Indien gegevens van een derde zijn opgenomen in het dossier waarin betrokkene inzage wenst, dan worden deze gegevens afgeschermd, tenzij expliciete toestemming voor inzage door deze derde wordt verleend.

6.3 Recht op correctie en aanvulling

Betrokkenen hebben het recht gegevens te laten verbeteren of aanvullen. Het corrigeren of aanvullen van informatie kan alleen als de gegevens onjuist - denk bijvoorbeeld aan een telefoonnummer of bankgegevens - of onvolledig zijn. De betrokkene zal altijd moeten specificeren welke gegevens aangepast dienen te worden en met welke reden.

6.4 Recht op gegevenswissing

De betrokkene heeft het recht om zonder onredelijke vertraging gegevenswissing (verwijdering) van zijn/haar betreffende persoonsgegevens te verkrijgen. Gemeente Noordenveld is verplicht dit te doen, onder andere in een van de volgende gevallen:

- de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld;
- de persoonsgegevens zijn onrechtmatig verwerkt;
- de betrokkene zijn of haar toestemming intrekt (indien de verwerking hierop is gebaseerd).

6.5 Recht op beperking

De betrokkene heeft het recht te vragen de verwerking van uw persoonsgegevens (tijdelijk) te beperken (het gebruik van de gegevens te stoppen), indien een van de volgende punten van toepassing is:

- De betrokkene betwist de juistheid van de persoonsgegevens; de verwerking wordt beperkt gedurende de periode die wij nodig hebben de juistheid van de persoonsgegevens te controleren;
- de verwerking is onrechtmatig en de betrokkene verzet zich tegen het wissen van de persoonsgegevens en verzoekt in de plaats daarvan om beperking van het gebruik ervan;
- Wij hebben de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden, maar de betrokkene heeft deze nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- De betrokkene heeft bezwaar gemaakt tegen de verwerking en is in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van Gemeente Noordenveld zwaarder wegen dan die van de betrokkene.

6.6 Recht op dataportabiliteit

De betrokkene heeft het recht op dataportabiliteit, ook wel overdraagbaarheid van gegevens genoemd. Dat wil zeggen dat betrokkene het recht heeft de hem betreffende persoonsgegevens, die hij aan Gemeente Noordenveld heeft verstrekt, in een gestructureerd en gangbaar digitaal bestand te verkrijgen. Tevens heeft hij het recht die gegevens aan een andere organisatie over te dragen, zonder daarbij te worden gehinderd door Gemeente Noordenveld.

Dit recht is alleen van toepassing op gegevens die:
- digitaal verwerkt worden
- die in het kader van een overeenkomst of op basis van toestemming (zie rechtsgronden in het verwerkingenregister) worden verwerkt.

Let op dat ook hier de privacy van anderen niet geschaad mag worden (zie recht op inzage, paragraaf 2).

6.7 Recht op verzet
Het recht op bezwaar staat ook bekend als het recht op verzet. Als de verwerking van persoonsgegevens plaats vindt op basis van de rechtsgrond 'publiek belang' of 'gerechtvaardigd belang', dan heeft de betrokkene het recht om bezwaar te maken tegen de verwerking van uw persoonsgegevens.

7. Bewaartermijn

Gemeente Noordenveld bewaart persoonsgegevens niet langer dan wettelijk is toegestaan en noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor de persoonsgegevens worden verwerkt. Hoe lang bepaalde gegevens worden bewaard is afhankelijk van de aard van de gegevens en de doeleinden waarvoor zij worden verwerkt. De bewaartermijn kan dus per doel verschillen.
Een overzicht van alle gehanteerde bewaartermijnen is terug te vinden in de meest recente versie van de Selectielijst van de VNG.
Wanneer de bewaartermijnen zijn verstreken zorgt Gemeente Noordenveld ervoor dat vernietiging van de betreffende persoonsgegevens op een beveiligde manier plaatsvindt. Gemeente Noordenveld vindt het belangrijk dat ook het vernietigen van de persoonsgegevens met zorg plaatsvindt.

8. De beveiliging van persoonsgegevens

Aan de beveiliging van persoonlijke gegevens geeft Gemeente Noordenveld prioriteit. De persoonsgegevens moeten worden geclassificeerd op basis van de soort gegevens (algemeen, bijzonder of gevoelig). Hoe gevoeliger de gegevens zijn, hoe hoger de beveiliging dient te zijn. De gegevens die zijn opgeslagen, worden daarom met technische en organisatorische maatregelen beschermd om verlies of misbruik door derden effectief te voorkomen. Vooruitlopend op de uitkomst van deze classificatie hebben wij reeds een hoog beveiligingsniveau vastgesteld, omdat veel persoonsgegevens als gevoelig of bijzonder aangemerkt zullen kunnen worden.

9. Klachtenregeling

Klachten en geschillen over de toepassing, uitvoering en/of interpretatie van dit beleid, de toepassing van privacywet– en regelgeving kunnen schriftelijk en gemotiveerd worden voorgelegd aan de Functionaris Gegevensbescherming. Betrokkene krijgt, indien nodig, binnen twee weken na ontvangst een uitnodiging om de klacht toe te lichten. Betrokkene ontvangt binnen vier weken na ontvangst van de klacht of binnen twee weken na de toelichting, een beslissing op de klacht.

10. Wijzigingen van het privacybeleid

Dit privacybeleid treedt in werking op 1 juli 2022. Gemeente Noordenveld kan dit privacybeleid wijzigen. Om goed op de hoogte te blijven van de manier waarop wij met persoonsgegevens omgaan, raden we alle medewerkers aan om dit privacybeleid regelmatig te raadplegen. Indien het privacybeleid wijzigt zal dit gecommuniceerd worden via intranet.

11. Contact

Indien je vragen of opmerkingen hebt naar aanleiding van dit privacybeleid, dan kun je contact opnemen met de Functionaris Gegevensbescherming via fg@noordenveld.nl.

Bijlagen

Bijlage 1: Datalekkenprotocol

1.1 Inleiding

Sinds 25 mei 2018 is elke organisatie die persoonsgegevens verwerkt op grond van de Algemene verordening gegevensbescherming (hierna: AVG) verplicht om datalekken te melden aan de Autoriteit Persoonsgegevens (hierna: AP) en in aantal gevallen ook aan betrokkene(n).
Dit document omschrijft hoe je een datalek kunt herkennen en hoe je hiermee dient om te gaan. De procedure biedt een handvat om het gehele proces gestructureerd en efficiënt te doorlopen. Het proces bestaat uit vijf stappen waarbij het proces begint bij het constateren dat het mogelijke datalek en het vaststellen van de meldplichten en eindigt bij de registratie van het lek in de eigen administratie. Gelijktijdig met het doorlopen van de stappen neemt Gemeente Noordenveld maatregelen om het lek te dichten. Hieronder vind je een overzicht van de stappen:

1. Constatering en interne melding incident door medewerker
2. Vaststellen van het datalek en meldplicht aan toezichthouder en betrokkene(n)
3. Melden datalek bij AP via webformulier
4. Melden datalek aan betrokkene(n)
5. Bijwerken intern incidentenregister

Voordat je de stappen van het proces gaat doorlopen is het belangrijk om eerst vast te stellen of de meldplicht van de AVG van toepassing is. Er dient sprake te zijn van verwerking van persoonsgegevens en Gemeente Noordenveld dient de verwerkingsverantwoordelijke te zijn.

Persoonsgegevens zijn gegevens die direct of indirect te herleiden zijn naar een natuurlijk persoon. Daarbij moet gedacht worden aan identificatoren zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
Onder verwerken valt alles wat iemand met persoonsgegevens kan doen, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
De verwerkingsverantwoordelijke is de organisatie die doel en middelen van de verwerking bepaalt, je bent dus bent geen verwerker die persoonsgegevens verwerkt in opdracht van bedrijf X op basis van een verwerkersovereenkomst.
Indien Gemeente Noordenveld gebruik maakt van verwerkers die in opdracht van de organisatie persoonsgegevens verwerken op basis van een verwerkersovereenkomst, dan kan de meldplicht procedure anders verlopen. Hierover kun je meer lezen in paragraaf 3.

1.2 De Procedure in vijf stappen

Stap 1: Constatering en interne melding incident door medewerker

Een datalek, officieel 'een inbreuk in verband met persoonsgegevens', is een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot persoonsgegevens.
Indien een medewerker een mogelijk datalek constateert, dient hij of zij zo snel mogelijk melding te maken bij de privacy officer. Hierna pakt de privacy officer het incident verder op. Incidenten waarbij sprake kan zijn van een datalek zijn bijvoorbeeld:

- een kwijtgeraakte USB-stick
- een gestolen telefoon of laptop
- een papieren dossier aanbieden als oud papier
- een mailtje waarbij verkeerde mensen in de CC staan
- een inbraak in een databestand door een hacker
- een malware-besmetting
- een calamiteit, zoals een brand in een datacentrum

Omdat een datalek binnen 72 uur na ontdekking gemeld moet worden en de privacy officer daarvoor het lek dient te analyseren is het noodzakelijk dat hij of zij van de melder zo veel mogelijk informatie betreffende het incident ontvangt. De vragen die de medewerker zoveel mogelijk dient te beantwoorden omtrent het incident zijn te vinden in bijlage 1.

Stap 2: Vaststellen van het datalek en meldplicht autoriteit en betrokkene(n)

VASTSTELLEN DATALEK EN MELDPLICHT AUTORITEIT

De privacy officer kwalificeert het incident in samenspraak met de Functionaris Gegevensbescherming; is er sprake van een datalek dat gemeld moet worden bij de AP en bij betrokkene(n)? Alle medewerkers dienen, waar nodig, de privacy officer van alle nodige informatie te voorzien.
Het is belangrijk om een onderscheid te maken tussen zwakke beveiliging en een informatiebeveiligingsincident, aangezien een zwakke plek in de beveiliging niet per definitie tot een incident hoeft te leiden. Ook is niet ieder beveiligingsincident een datalek.

- Beveiligingsincident: er is sprake van een inbreuk op de beveiliging van gegevens. Dit kan zowel persoonsgegevens als andere gegevens betreffen.
- Datalek: een beveiligingsincident dat persoonsgegevens betreft en waarbij sprake is van één van de volgende inbreuken:
  - "Vertrouwelijkheidsinbreuk" in geval er ongeautoriseerde of onbedoelde toegang tot of publicatie van persoonsgegevens is.
  - "Beschikbaarheidsinbreuk" – in geval er sprake is van ongeautoriseerd(e) of onbedoeld(e) verlies, vernietiging of anderszins ontoegankelijke persoonsgegevens.
  - "Integriteitsinbreuk" – in geval sprake is van ongeautoriseerde of onbedoelde wijziging van persoonsgegevens.

In principe moeten alle datalekken gemeld worden bij de AP, tenzij het onwaarschijnlijk is dat het datalek een risico voor de privacybescherming van betrokkene(n) inhoudt. Dit kan bijvoorbeeld het geval zijn als het apparaat dat gestolen is, voldoende encrypted is.

VASTSTELLEN MELDPLICHT BETROKKENE(N)
Naast de autoriteit moeten betrokkene(n) in bepaalde gevallen ook geïnformeerd worden over het datalek. Het datalek moet bij betrokkene(n) gemeld worden als het datalek waarschijnlijk een hoog risico voor de privacybescherming van betrokkene(n) inhoudt. Van een hoog risico is in ieder geval sprake als de inbreuk gevoelige of bijzondere persoonsgegevens betreft of als betrokkenen door de inbreuk een hoger risico lopen om het slachtoffer te worden van phishingmail of andere cybercrime.
Alleen indien er zwaarwegende gronden aanwezig zijn om de melding achterwege te laten en dit noodzakelijk is in het belang van de bescherming van de betrokkene(n) mag de melding aan betrokkenen alsnog achterwege gelaten worden. Een voorbeeld is de situatie dat er gegevens zijn gelekt over medische en psychosociale hulpvragen die kinderen buiten medeweten van hun ouders hebben gedaan. In dat geval wordt de melding niet gedaan aan (de vertegenwoordigers) van betrokkenen(n).

Stap 3: Melden datalek bij AP via webformulier
Het datalek dient binnen 72 uur na constatering gemeld te worden aan de autoriteit. Mocht het niet mogelijk zijn om de melding binnen 72 uur volledig te doen, dan dient een melding te worden ingestuurd met de informatie die op dat moment bekend is bij Gemeente Noordenveld. Het is mogelijk om wijzigingen over de melding na te sturen, of om de melding in te trekken mocht hier reden voor zijn.
Melden kan via het webformulier dat de autoriteit op hun website beschikbaar stelt (datalekken.autoriteitpersoonsgegevens.nl). Na de melding ontvang je een ontvangstbevestiging.
Als de melding de autoriteit aanleiding geeft tot nadere actie, dan zal deze daarover contact met Gemeente Noordenveld opnemen. In eerste instantie zal het daarbij gaan om verificatie dat de gedane melding daadwerkelijk van Gemeente Noordenveld afkomstig is, en om eventuele inhoudelijke vragen over de melding.
Binnen Gemeente Noordenveld is de privacy officer bevoegd om de melding bij de AP namens Gemeente Noordenveld te doen. Hij/zij brengt daarover verslag uit aan het College van Burgemeester en Wethouders.

Stap 4: Melden datalek aan betrokkene(n)
Na het ontdekken van het datalek mag je enige tijd mag nemen voor nader onderzoek zodat je de betrokkene op een behoorlijke en zorgvuldige manier kunt informeren. Wel moet je er rekening mee houden dat de betrokkene naar aanleiding van de melding mogelijk maatregelen moet nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder de betrokkene daarover geïnformeerd wordt, hoe eerder de persoon in actie kan komen.
Indien uit stap 2 blijkt dat je de betrokkene(n) moet informeren, dan dient de melding (minimaal) de onderstaande informatie te bevatten:

- Een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens.
- De instanties waar de betrokkenen meer informatie over de inbreuk kan krijgen. Meld de contactgegevens waar mensen terecht kunnen met eventuele vragen (in de meeste gevallen zal dat de privacy officer zijn).
- De waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- De maatregelen die Gemeente Noordenveld de betrokkene(n) aanbeveelt om te nemen om de negatieve gevolgen van de inbreuk te beperken. Denk hierbij bijvoorbeeld aan het veranderen

van gebruikersnamen en wachtwoorden. Daarnaast informeer je ook welke maatregelen je organisatie heeft genomen om de inbreuk aan te pakken.

Het uitgangspunt is dat betrokkenen worden bereikt met informatie die hen helpt om de gevolgen van het datalek voor hun persoonlijke levenssfeer zo veel mogelijk te beperken. Met enkel een bericht in de media wordt dat doel normaal gesproken niet bereikt.
De melding aan betrokkene(n) wordt gedaan door of namens de privacy officer.

Stap 5: Interne overzicht datalekken bijwerken
Organisaties zijn verplicht om een register bij te houden met de gemelde datalekken. In dit register staan minimaal:

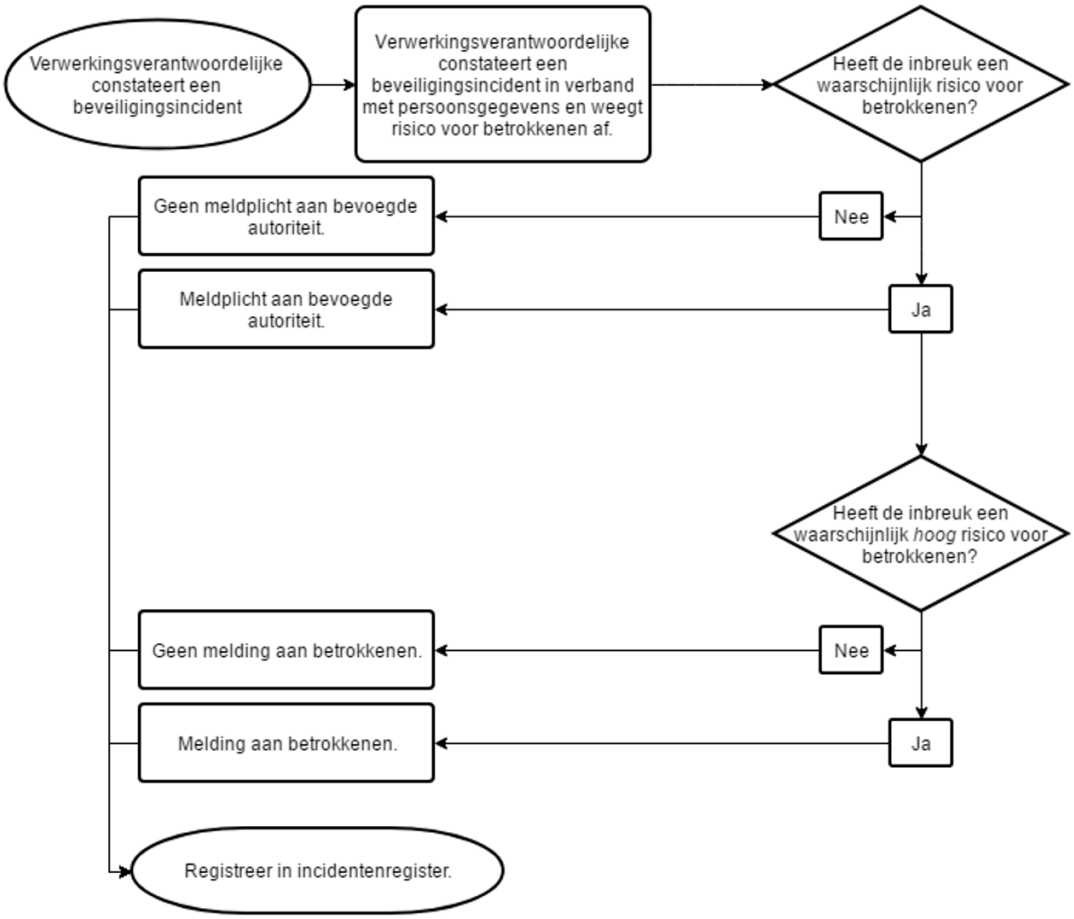
- Feiten en gegevens omtrent aard en inbreuk:
  - Oorzaak van het lek
  - Wat er gebeurd is
  - De persoonlijke data die het betreft
- Het effect en de consequenties van het lek
- Maatregelen die genomen zijn om de negatieve gevolgen van de inbreuk te beperken

BEWAARTERMIJNEN DATALEKKENREGISTER
Gemeente Noordenveld is verplicht een register bij te houden van alle datalekken en incidenten, inclusief de datalekken die niet gemeld zijn. Het is aan te raden om de gegevens minimaal 3 jaar te bewaren. Evalueer in het laatste geval jaarlijks of betrokkenen niet alsnog geïnformeerd dienen te worden.
De privacy officer is verantwoordelijk voor het bijhouden van het register.

1.3 Wordt gebruik gemaakt van verwerkers?
Veel organisaties maken gebruik van leveranciers die voor hen informatie inclusief persoonsgegevens verwerken. Deze leveranciers worden ook wel verwerkers genoemd. De organisatie blijft zelf verantwoordelijk voor de persoonsgegevens. Het is aan te raden om een artikel in de verwerkersovereenkomst op te nemen over het melden van datalekken. In het geval van verwerkers zijn er twee mogelijkheden voor de melding wanneer de verwerker een datalek constateert.

1. De verwerker stelt eerst de verantwoordelijke op de hoogte van het datalek en voorziet hem van alle benodigde informatie om een melding te kunnen maken. De verantwoordelijke meldt het datalek zelf bij de autoriteit. De verantwoordelijke informeert zelf de betrokkenen.
2. De verwerker onderzoekt het datalek en verzorgt zelf de initiële melding aan de autoriteit. Hij stelt zo snel mogelijk de verantwoordelijke op de hoogte van het datalek en stuurt ook de inhoud van de melding toe. De verantwoordelijke kijkt de melding na en doet eventueel (in samenspraak met de verwerker) nog aanpassingen aan de melding en stuurt deze na naar de autoriteit. De verantwoordelijke informeert zelf de betrokkenen.

Let op: In beide gevallen moet rekening worden gehouden met de meldplicht bij de autoriteit binnen 72 uur na constatering van het datalek.



1.4 Schematische weergave

Processtap	Specificaties	Uitvoerende
Vermoeden datalek/beveiligingsincident	Stap 1: Start proces. Incidenten worden gemeld bij de privacy officer.	Iedere medewerker van de organisatie kan incidenten melden.
Vaststellen datalek	Stap 2: Beveiligingsincident of datalek?	Privacy officer
Vaststellen meldplicht AP en betrokkene(n)	Stap 2: Meldplicht AP en aan betrokkene(n)?	Privacy officer + Functionaris Gegevensbescherming
	Regulier incidentbeheer	Indien beveiligingslek of geen meldplicht autoriteit.
Bepalen mitigerende maatregelen	Er worden mitigerende maatregelen bepaald en uitgezet.	IT-afdeling
Melden datalek bij AP	Stap 3: Melding van het datalek dient binnen 72 uur te worden gedaan bij de autoriteit	Functionaris Gegevensbescherming
Datalek melden aan betrokkene(n)	Stap 4: Betrokkene(n) worden geïnformeerd over de inbreuk en benodigde maatregelen	Privacy officer
Bijwerken register	Stap 5: Het interne register datalekken wordt bijgewerkt met de aard van het datalek, de maatregelen en de communicatie	Privacy officer

Bijlage 2: Procedure rechten van betrokkenen

Betrokkenen zijn de personen op wie persoonsgegevens betrekking hebben. Bij Gemeente Noordenveld zijn dit in ieder geval de inwoners en de medewerkers van de gemeente. Betrokkenen hebben bepaalde rechten op grond van de Algemene verordening gegevensbescherming (AVG).
Alle personen waarvan Gemeente Noordenveld persoonsgegevens in bezit heeft hebben het recht op informatie over de verwerking (art. 13 en 14 AVG) , het recht om deze gegevens in te zien (art. 15 AVG), ze te verbeteren of aan te vullen (art. 16 AVG), te laten wissen (art. 17 AVG), het recht om de verwerking van hun gegevens te beperken (art. 18 AVG), het recht op dataportabiliteit (art. 20 AVG) en het recht op verzet tegen de verwerking (art. 21 AVG). Indien Gemeente Noordenveld gebruik maakt van profiling

(geautomatiseerde besluitvorming), dan heeft de betrokkene het recht daar niet aan onderworpen te worden (art. 22 AVG).

1.1 Algemene procedure

Deze procedure gaat uit van een verzoek door een bewoner van Gemeente Noordenveld, maar kan tevens worden toegepast op andere categorieën van betrokkenen, zoals leveranciers en medewerkers.
Bewoners kunnen op verschillende manieren een verzoek indienen:

- direct bij de FG of privacy officer
- telefonisch (denk aan controlevragen)
- via een andere medewerker per e-mail, die verifieert de afzender (is er sprake van een bekend e-mailadres?) en stuurt het verzoek door naar de privacy officer

In alle gevallen geldt dat het verzoek van de betrokkene pas kan worden ingewilligd nadat (redelijkerwijs) is vastgesteld dat het verzoek daadwerkelijk van de betrokkene zelf afkomstig is. De identiteit van de verzoeker kan bijvoorbeeld worden gecontroleerd door het tonen van een legitimatiebewijs.

Reageren op een verzoek

Voor alle verzoeken geldt dat Gemeente Noordenveld binnen een maand dient te antwoorden, ook wanneer uw organisatie het verzoek weigert. Bij een weigering moet een motivatie en een verwijzing naar het klachtrecht bij de Autoriteit Persoonsgegevens (AP) toegevoegd worden. In het geval van een complex verzoek, of veel verzoeken, mag de reactietijd met twee maanden worden verlengd, mits de verzoeker daarvan wel binnen die eerste maand van op de hoogte wordt gesteld.
Het antwoorden op een verzoek en het verstrekken van informatie moet altijd schriftelijk, in heldere taal en in toegankelijke vorm gedaan worden.
De privacy officer is voor het afhandelen van alle verzoeken verantwoordelijk, maar kan de taak delegeren.

Beperken op de rechten van betrokkenen

Gemeente Noordenveld mag onder bepaalde omstandigheden geen gehoor geven aan de rechten van betrokkenen. Dat is het geval wanneer die beperking noodzakelijk is voor de waarborging van:

- de nationale veiligheid, landsverdediging of openbare veiligheid
- de voorkoming, onderzoek, opsporing en vervolging van strafbare feiten, of tenuitvoerlegging van straffen
- de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepenschendingen van de beroepscodes van gereglementeerde beroepen
- andere belangrijke doelstellingen van algemeen belang van Nederland of de Europese Unie
- de bescherming van de onafhankelijkheid van rechters en rechterlijke procedures
- taken op het gebied van toezicht, inspectie of regelgeving op de hierboven genoemde gebieden.

Verder is het mogelijk de rechten van de betrokkenen te beperken wanneer dit noodzakelijk is voor de waarborging van:

- de bescherming van de betrokkene zelf of van de privacy van anderen
- de inning van civielrechtelijke vorderingen.

Hierbij dient altijd een afweging met de privacyrechten van betrokkene gemaakt te worden.
Tot slot mag u het verzoek weigeren als het verzoek duidelijk heel ongegrond of buitensporig is (bijvoorbeeld als betrokkene telkens dezelfde vraag stelt).

Jongeren onder de 16

De verzoeker dient 16 jaar of ouder te zijn en is niet onder curatele gesteld. Indien dit wel het geval is, moet de wettelijk vertegenwoordiger het verzoek doen. Gemeente Noordenveld dient het antwoord dan ook aan die persoon sturen.
Wanneer er meerdere wettelijk vertegenwoordigers zijn dient rekening te worden gehouden met alle partijen. Wanneer één van meerdere wettelijk vertegenwoordigers het verzoek doet, dient de privacy van de andere wettelijk vertegenwoordiger(s) gewaarborgd te worden. Wanneer verzocht wordt om wissing of correctie van gegevens dienen alle wettelijke vertegenwoordigers hiermee akkoord te gaan.

1.2 Recht op informatie

Betrokkenen hebben het recht om in heldere taal informatie te ontvangen over het hoe en waarom van de gegevensverwerking. Dit geldt zowel voor het geval dat de gegevens bij betrokkene zelf worden verzameld, als wanneer dit via anderen gebeurt.
Gemeente Noordenveld mag zelf bepalen hoe zij dit recht op informatie inkleden, zolang het maar passend is bij de doelgroep en (het risico van) de verwerking. De meest gangbare vorm van informatieverstrekking is een privacy statement (ook wel privacyverklaring of privacyreglement genoemd) op

de website. Deze moet in ieder geval duidelijk vindbaar en leesbaar zijn voor alle betrokkenen. Ook de werknemers van Gemeente Noordenveld moeten worden ingelicht over hoe er met hun gegevens omgegaan wordt.
Informatieverstrekking naar betrokkene bevat in ieder geval de onderstaande elementen.
Wanneer de gegevens bij de betrokkene zelf verzameld worden:

- de contactgegevens van Gemeente Noordenveld
- indien een functionaris voor gegevensbescherming aangesteld is, de contactgegevens van deze functionaris
- doel en rechtsgrond van de persoonsgegevensverwerking
- de eventuele ontvangers of categorieën ontvangers van de gegevens
- in geval van verstrekking aan derde landen (buiten de EU/EER):
    - of er een adequaatheidsbesluit van de Commissie bestaat
    - of passende waarborgen zijn getroffen, welke dit zijn en of hier een kopie van kan worden verkregen, dan wel waar die waarborgen kunnen worden geraadpleegd
- de bewaartermijn, of als dat niet mogelijk is de criteria voor het bepalen ervan
- de rechten van de betrokkene (zoals beschreven in dit document)
- dat de betrokkene het recht heeft een klacht in te dienen over onze verwerking bij de AP
- in het geval van toestemming, dat de betrokkene die toestemming altijd weer kan intrekken
- of het verwerken van persoonsgegevens een wettelijke verplichting is of noodzakelijk is voor de uitvoering of het aangaan van een overeenkomst, of de betrokkene verplicht is die gegevens te verstrekken en wat de gevolgen zijn van het niet verstrekken van die gegevens voor de betrokkene (denk aan het gebruik van verplichte velden in een formulier)
- ingeval van profiling, nuttige informatie over de onderliggende logica, het belang van de verwerking en de verwachte gevolgen van die verwerking voor de betrokkene.

Wanneer de gegevens buiten de betrokkene om verzameld worden
Wanneer de gegevens buiten de betrokkene om verzameld worden, dan moet in beginsel dezelfde informatie verstrekt worden als wanneer de gegevens van de betrokkene zelf verkregen worden. Het enige dat moet worden toegevoegd is de bron waaruit persoonsgegevens zijn verkregen en welke soort gegevens het betreft. Als de bron van de informatie niet kan worden vastgesteld, bijvoorbeeld omdat de informatie uit verschillende bronnen is samengesteld, dient algemene informatie over de herkomst verstrekt te worden.
Verder moet alle andere informatie worden verstrekt die noodzakelijk is om tegenover de betrokkene een behoorlijke en transparante verwerking te waarborgen.
Als de persoonsgegevens voor andere doelen verder verwerkt gaan worden moet de betrokkene opnieuw geïnformeerd worden, behalve voor zover de betrokkene al van die informatie op de hoogte is.

Uitzonderingen
De informatieplicht geldt niet in de volgende gevallen:

- de betrokkene is al op de hoogte van de informatie
- de informatieverstrekking is onmogelijk (bijvoorbeeld omdat dit het doel van de verwerking onmogelijk maakt) of vergt onevenredig veel inspanning
- de verkrijging of verstrekking van gegevens is wettelijk verplicht en de betreffende wet bevat voldoende waarborgen voor de belangen van betrokkene
- de persoonsgegevens moeten vertrouwelijk blijven in verband met een beroepsgeheim.

1.3 Recht op inzage
Wanneer een betrokkene vraagt om inzage betekent dit dat hij recht heeft op een volledig overzicht van de gegevens die wij over deze betrokkenen hebben, ook heeft betrokkene het recht daar een afschrift van te ontvangen.

Welke gegevens moeten wij verstrekken?
In de eerste plaats krijgt de betrokkene inzage in (en een afschrift van) alle gegevens die wij over deze betrokkene vastgelegd hebben.
Naast alle gegevens over de betrokkene die wij in ons bezit hebben, heeft de betrokkene recht op de volgende informatie:

- de doeleinden waarvoor de gegevens vastgelegd/gebruikt zijn (te vinden in het verwerkingenregister)
- de betrokken categorieën van persoonsgegevens (betreft het algemene gegevens, bijzondere gegevens of gevoelige gegevens)
- de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt

- indien mogelijk, de bewaartermijn voor de gegevens, of indien dat niet mogelijk is, de criteria om die termijn te bepalen
- een verwijzing naar de andere rechten van betrokkene, zoals het recht op verzet of gegevenswissing
- dat de betrokkene het recht heeft klacht in te dienen bij de AP
- wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens
- In geval van profiling: nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Welke gegevens mogen wij niet ter inzage geven?
Betrokkenen hebben het recht op inzage in alle gegevens die de organisatie van hen heeft vastgelegd. Houdt daar dus rekening mee bij het maken van notities in een dossier. Denk aan een zakelijke weergave van feiten en vermijd waar mogelijk gezondheidsgegevens en strafrechtelijke gegevens.
Het is belangrijk om gegevens van eventuele derden te anonimiseren. Soms is het zwartmaken van een naam niet voldoende om de gegevens van een derde te anonimiseren; zo zal bij een klachten- of overlastbrief toch vaak nog duidelijk zijn van wie deze afkomt. In dat geval wordt de betrokkene die om inzage verzoekt wel geïnformeerd over het bestaan van een brief, maar blijft de inhoud en afzender achterwege.

Kosten
Een afschrift verstrekken wij in eerste instantie digitaal (beveiligd bestand, per e-mail). Indien gewenst kan betrokkene ook een papieren afschrift ontvangen, door deze af te halen op het kantoor van Gemeente Noordenveld, na het tonen van een legitimatiebewijs. Voor de eerste papieren kopie mag niets in rekening worden gebracht.
Indien blijkt dat de gegevens moeten worden gecorrigeerd, aangevuld, verwijderd of afgeschermd op basis van het verzoek van betrokkene, dan krijgt de betrokkene de betaalde vergoeding terug.

1.4 Recht op correctie en aanvulling
Betrokkenen hebben naast het recht op inzage ook recht om hun persoonsgegevens te laten corrigeren of aan te vullen. De betrokkene moet hiervoor wel een goede reden hebben. Het corrigeren of aanvullen van informatie kan alleen als de gegevens onjuist zijn - denk bijvoorbeeld aan telefoonnummer of bankgegevens - of als deze onvolledig zijn met inachtneming van het verwerkingsdoeleinde.
De betrokkene zal altijd moeten specificeren welke gegevens hij aangepast wil zien. Let op dat bij verwijdering van gegevens misschien ook verwerkers of andere ketenpartners zoveel mogelijk op de hoogte gesteld dienen te worden, die zullen de verkregen gegevens, voor zover mogelijk, ook moeten aanpassen.

1.5 Recht op gegevenswissing
Het recht op gegevenswissing (ook wel het recht op verwijdering genoemd) moet onder bepaalde omstandigheden ingewilligd worden.

Een verzoek om verwijdering van de eigen gegevens moet worden ingewilligd in de volgende gevallen:
- de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt (zie verwerkingenregister)
- de betrokkene trekt de toestemming waarop de verwerking berust in, en er is geen andere rechtsgrond voor de verwerking (zie verwerkingenregister)
- het bezwaar van betrokkene tegen de verwerking is ingewilligd (zie hieronder, paragraaf 8)
- de persoonsgegevens zijn onrechtmatig verwerkt (bijvoorbeeld omdat zij niet noodzakelijk zijn voor het geformuleerde doel of omdat de rechtsgrond ontbreekt)
- de persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting die op Gemeente Noordenveld rust
- de persoonsgegevens zijn verzameld in verband met een rechtstreeks aanbod van internetdiensten aan een kind.

Het verzoek dient niet te worden ingewilligd indien de gegevens nodig zijn:
- voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;
- voor het nakomen van een wettelijke verplichting die op Gemeente Noordenveld rust, of voor het vervullen van een taak van algemeen belang of het uitoefenen van het openbaar gezag dat aan Gemeente Noordenveld (bij wet) is verleend;
- om redenen van algemeen belang op het gebied van volksgezondheid;
- met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek en het verwijderen de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen;

- voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

De betrokkene zal altijd moeten specificeren welke gegevens hij verwijderd wil zien. Let op dat bij verwijdering van gegevens misschien ook verwerkers of andere ketenpartners zoveel mogelijk op de hoogte gesteld dienen te worden. Deze partijen zullen de verkregen gegevens, voor zover mogelijk, ook moeten wissen.
Let op dat bij het terugzetten van een back-up (recent) verwijderde gegevens niet opnieuw in het systeem terechtkomen.

Het recht om vergeten te worden
Het recht om vergeten te worden hangt nauw samen met het recht op gegevenswissing, maar heeft specifiek betrekking op gegevens die openbaar gemaakt zijn (bijvoorbeeld online) en waarbij de betrokkene gevraagd heeft de gegevens, of verwijzingen naar de gegevens (denk aan zoekmachines), te wissen.

1.6 Recht op beperking
De betrokkene heeft het recht Gemeente Noordenveld te vragen de verwerking van zijn persoonsgegevens (tijdelijk) te beperken (het gebruik van de gegevens te stoppen).
Dit moet door Gemeente Noordenveld worden ingewilligd indien een van de volgende punten van toepassing is:
- de juistheid van de persoonsgegevens wordt betwist door de betrokkene; de verwerking wordt beperkt gedurende de periode die Gemeente Noordenveld nodig heeft de juistheid van de persoonsgegevens te controleren;
- de verwerking is onrechtmatig en de betrokkene verzet zich tegen het wissen van de persoonsgegevens en verzoekt in de plaats daarvan om beperking van het gebruik ervan;
- Gemeente Noordenveld heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden (zie verwerkingenregister), maar de betrokkene heeft deze nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- de betrokkene heeft bezwaar gemaakt tegen de verwerking (zie paragraaf 8), en is in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van Gemeente Noordenveld zwaarder wegen dan die van de betrokkene.

We kunnen een verwerking beperken door de betreffende gegevens tijdelijk over te brengen naar een ander systeem, ze tijdelijk onbeschikbaar te maken of door gepubliceerde gegevens tijdelijk van de website te halen. Indien een betrokkene een beperking van de verwerking heeft verkregen, wordt betrokkene door Gemeente Noordenveld op de hoogte gebracht voordat de beperking van de verwerking wordt opgeheven.

Uitzonderingen
Wanneer de verwerking is beperkt, worden persoonsgegevens, met uitzondering van de opslag ervan, slechts verwerkt:
- met toestemming van de betrokkene, of
- voor de instelling, uitoefening of onderbouwing van een rechtsvordering, of
- ter bescherming van de rechten van een andere natuurlijke persoon of rechtspersoon, of om gewichtige redenen van algemeen belang voor de EU of een lidstaat.

1.7 Recht op dataportabiliteit
De betrokkene heeft het recht op dataportabiliteit, ook wel overdraagbaarheid van gegevens genoemd. Dat wil zeggen dat betrokkene het recht heeft de hem betreffende persoonsgegevens, die hij aan een Gemeente Noordenveld heeft verstrekt, in een gestructureerd en gangbaar digitaal bestand te verkrijgen. Tevens heeft hij het recht die gegevens aan een andere organisatie over te dragen, zonder daarbij te worden gehinderd door Gemeente Noordenveld.

Dit recht is alleen van toepassing op gegevens die:
- digitaal verwerkt worden
- die in het kader van een overeenkomst of op basis van toestemming (zie rechtsgronden in het verwerkingenregister) worden verwerkt.

Let op dat ook hier de privacy van anderen niet geschaad mag worden (zie recht op inzage, paragraaf 3).

1.8 Recht op bezwaar
Het recht op bezwaar staat ook bekend als het recht op verzet. Als de verwerking van persoonsgegevens plaats vindt op basis van de rechtsgrond ‘publiek belang’, dan heeft de betrokkene het recht om van-

wege - met zijn specifieke situatie verband houdende redenen - bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens.
Gemeente Noordenveld staakt de verwerking van de persoonsgegevens tenzij hij dwingende publiekrechtelijke gronden voor de verwerking aanvoert die zwaarder wegen dan de privacyrechten van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering. Verwerkingen voor wetenschappelijk of historisch onderzoek of statistische doeleinden moet worden gestaakt, tenzij er sprake is van noodzakelijkheid voor de uitvoering van een taak van algemeen belang.
Een beroep op het recht op verzet in verband met direct marketing moet altijd ingewilligd worden.

1.9 Recht om niet aan profiling onderworpen te worden
Profiling is het indelen van mensen in profielen op basis van (bepaalde) persoonsgegevens. Als op basis van zo'n profiel automatisch (dus zonder menselijke tussenkomst) besluiten worden genomen over die persoon, of het mensen op een andere wijze wezenlijk treft, dan heeft men het recht daar niet aan onderworpen te worden.
Dit recht komt neer op een verbod op profiling. Het verbod kent drie uitzonderingen:
- profiling is noodzakelijk voor de totstandkoming of uitvoering van een overeenkomst
- de betrokkene heeft uitdrukkelijke toestemming gegeven
- er is een wettelijke uitzonderingsgrond in het nationaal of Europees recht.

In de eerste twee gevallen heeft de betrokkene dan alsnog het recht op menselijke tussenkomst, het recht zijn standpunt kenbaar te maken en het recht om het besluit aan te vechten.

Bijlage 3: Proces uitvoeren data protection impact assessments

1.1 Inleiding
Sinds 25 mei 2018 zijn organisaties die persoonsgegevens verwerkt op grond van de Algemene verordening gegevensbescherming (hierna: AVG) verplicht om in bepaalde gevallen een data protection impact assessment (hierna: DPIA) uit te voeren.
Een DPIA is een hulpmiddel om privacy risico's op structurele wijze in kaart te brengen en moet worden uitgevoerd voordat de geplande verwerking van persoonsgegevens wordt gestart (bij het ontwerp). De DPIA is hiermee in overeenstemming met de vereisten van Privacy by Design en Privacy by Default uit de AVG.

Een DPIA zorgt ervoor dat rekening wordt gehouden met de gegevensbescherming en privacy. Het stimuleert het creëren van oplossingen en compliance.

Dit document omschrijft wanneer en hoe DPIA's uitgevoerd dienen te worden. De procedure biedt een handvat om het gehele proces gestructureerd en efficiënt te doorlopen. Het proces bestaat uit vijf stappen waarbij het begint bij het constateren dat een proces met een mogelijk hoog privacy risico ingericht of gewijzigd gaat worden. Gelijktijdig met het doorlopen van de stappen neemt de Gemeente Noordenveld maatregelen om de privacy risico's te mitigeren.

Hieronder vind je een overzicht van de 5 stappen:
1. Constatering (beoogde of wijziging in een)
1. gegevensverwerking met mogelijk hoog risico
2. Beoordelen of uitvoeren DPIA verplicht is
3. Uitvoeren DPIA
4. Advies Functionaris Gegevensbescherming (hierna: FG)
5. Beslissen over gegevensverwerking en voorafgaande raadpleging

1.2 De procedure in vijf stappen
Wanneer de Gemeente Noordenveld voornemens is een nieuw gegevensverwerking te gaan uitvoeren of wijzigingen worden aangebracht in een bestaande gegevensverwerking dient er altijd aandacht te zijn voor privacy. Privacy by design is onderdeel van het privacybeleid van de Gemeente Noordenveld. In sommige gevallen is de Gemeente Noordenveld in het kader hiervan verplicht om voorafgaand aan de start van de uitvoering van de nieuwe of gewijzigde gegevensverwerking een DPIA uit te voeren. Het is van groot belang dat mogelijke risico's vroeg gesignaleerd worden en er gedurende het project of inrichting van het proces voldoende ruimte is om de DPIA uit te voeren en evt. verbetermaatregelen die daaruit naar voren komen te implementeren. Het uitvoeren van de DPIA zal door de privacy officer en de verantwoordelijke voor het project of proces gezamenlijk worden opgepakt. De privacy officer en FG stellen naast de DPIA een advies inclusief verbetermaatregelen op. Afhankelijk van dit advies kan de gegevensverwerking uitgevoerd gaan worden of is extra besluitvorming hierover nodig.

Stap 1: Constatering beoogde (of wijziging in een) gegevensverwerking met mogelijk hoog risico
Alle medewerkers zijn verantwoordelijke voor het opvolgen van het privacybeleid. Onderdeel daarvan is het herkennen van mogelijke privacyrisico's en hier de nodige aandacht op vestigen. Managers, teamleiders en projectleiders zullen in het bijzonder betrokken zijn en kennis hebben van beoogde nieuwe werkprocessen en wijzigingen in werkprocessen. Stap 2 van deze procedure kan worden gebruikt om te beoordelen of sprake is van een mogelijk hoog privacyrisico, wanneer dit het geval is of hierover twijfel bestaat dient contact te worden opgenomen met de privacy officer.
Het moment van constatering is belangrijk omdat de DPIA, mits verplicht, uitgevoerd moet worden voorafgaand aan de start van de gegevensverwerking. Dit kan betekenen dat wanneer gedurende een project getest wordt of een pilot wordt uitgevoerd de DPIA vóór de start daarvan reeds uitgevoerd moet zijn. Het niet of te laat uitvoeren van de wettelijk verplichte DPIA is een overtreding van de AVG.

Stap 2: Beoordelen of uitvoeren DPIA verplicht is
Wanneer moet een DPIA worden uitgevoerd?
De Gemeente Noordenveld is niet verplicht om voor elke verwerking van persoonsgegevens een DPIA uit te voeren. Een DPIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen.
Dat is in ieder geval zo als de Gemeente Noordenveld:
- Systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profiling;
- Op grote schaal bijzondere persoonsgegevens verwerkt;
- Op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld bij de inzet van cameratoezicht).

Buiten deze drie situaties heeft de Autoriteit Persoonsgegevens (AP) een lijst gepubliceerd van 17 verwerkingen waarvoor een DPIA in ieder geval verplicht is. Deze lijst is opgenomen in bijlage.
Wanneer de beoogde gegevensverwerking niet terug te vinden is in de AVG of de lijst van de AP dient aan de hand van 9 criteria beoordeelt te worden of het risico mogelijk hoog is. Wanneer van de onderstaande lijst twee of meer criteria sprake is is een DPIA verplicht:

DPIA-check

	Ja	Nee
Is de verwerking grootschalig?		
Bent u van plan bijzondere persoonsgegevens, strafrechtelijke gegevens of gevoelige gegevens te verwerken?		
Worden databases gekoppeld voor deze verwerking?		
Worden er gegevens verwerkt met betrekking tot kwetsbare betrokkenen?		
Houdt de verwerking stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten in?		
Bent u van plan om een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen uit te voeren, die is gebaseerd op geautomatiseerde verwerking, zoals profiling?		
Wordt op basis van deze verwerking besluiten gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen?		
Wordt er gebruik gemaakt van innovatieve nieuwe technologische oplossingen?		
Kan als gevolg van de verwerking de betrokkene een recht niet uitoefenen of geen beroep kunnen doen op een dienst of een overeenkomst?		
Conclusie DPIA-check		
Houdt de verwerking een hoog risico in voor de rechten en vrijheden van de betrokkene (twee of meer keer 'ja', zie uitleg)?		

Stap 3: Uitvoeren DPIA
Wanneer er een verplichting of wens is om de DPIA uit te voeren zal dit worden gedaan onder begeleiding van de privacy officer. De privacy officer dient voldoende informatie en medewerking te krijgen van de collega's die kennis hebben van de beoogde (wijziging van de) gegevensverwerking. De proces– of projectverantwoordelijke is eindverantwoordelijk voor het tijdig opleveren van de DPIA. De DPIA wordt uitgevoerd doormiddel van het invullen van de IBD DPIA tool.

Stap 4: Advies Functionaris Gegevensbescherming
Na het invullen van de concept DPIA wordt de FG om advies gevraagd. Deze brengt naar eigen inzicht advies uit op de concept DPIA. De proces– of projectverantwoordelijke en privacy officer nemen dit advies in overweging en passen zo nodig de DPIA aan n.a.v. nieuwe inzichten. Daar waar het advies van de FG niet gevolgd wordt, dient hierover verantwoording te worden vastgelegd. Dit gebeurt in een memo die onderdeel wordt van de DPIA.

Stap 5: Beslissen over gegevensverwerking en voorafgaande raadpleging

Na het advies van de FG en het maken van laatste aanpassingen kan de DPIA, mits compleet, vastgesteld worden. De DPIA geeft goed inzicht in de beoogde gegevensverwerking en eventuele risico's en maatregelen die getroffen of gepland zijn.
Afhankelijk van het resultaat van de DPIA worden deze op de volgende wijze vastgesteld:

- Uitsluitend lage netto risico's: De proces– of projectverantwoordelijke stelt de DPIA vast en maakt deze onderdeel van de afdelings– en/of projectadministratie. Een kopie wordt aan de privacy officer verschaft en het MT wordt hierover geïnformeerd.
- Eén of meer middel netto risico's: De proces– of projectverantwoordelijke en privacy officer stellen een begeleidende memo op en lichten de risico's toe in het MT. Het MT beslist over de voortgang van de gegevensverwerking.
- Eén of meer hoge netto risico's: De proces– of projectverantwoordelijke en privacy officer stellen een begeleidende memo op en lichten de risico's toe in het MT en, indien nodig, aan het College. Omdat er een hoog netto risico overblijft bestaat er een wettelijke verplichting om de AP te raadplegen voorafgaand aan de start van de gegevensverwerking. De eindverantwoordelijke voor het project/proces beslist of voorafgaande raadpleging wordt gedaan.

Wanneer er geen hoge risico's zijn en de DPIA is vastgesteld kan de beoogde gegevensverwerking starten. Wanneer de gegevensverwerking in de toekomst wijzigt moet de DPIA hierop aangepast worden, stappen 3, 4 en 5 van deze procedure dienen in dat geval herhaald te worden. Wanneer geen wijzigingen in het proces plaatsvinden dient 3 jaar nadat de DPIA is vastgesteld hierop een review plaats te vinden. Hiervoor dienen stap 3, 4 en 5 uit deze procedure herhaald te worden. De verantwoordelijkheid voor het tijdig uitvoeren van deze herzieningen en reviews ligt bij de procesverantwoordelijke.

1.3 Voorafgaande raadpleging
Wanneer een hoog netto risico overblijft dient de AP geraadpleegd te worden. Bij een voorafgaande raadpleging geeft de AP advies over hoe de risico's van de voorgenomen verwerking beperkt kunnen worden. Als deze maatregelen worden uitgevoerd, mag de gegevensverwerking starten. Het kan ook dat de AP adviseert om helemaal van de verwerking af te zien. Soms is een advies van de AP niet nodig, bijvoorbeeld omdat de risico's toch voldoende blijken te zijn afgedekt. In dat geval mag gelijk met de verwerking gestart worden.

Procedure Autoriteit Persoonsgegevens
Om voorafgaande raadpleging aan de vragen vult de privacy officer het aanvraagformulier voorafgaande raadpleging in op de website van de AP. De DPIA en andere relevante stukken worden tevens aangeleverd aan de AP.
De wettelijke behandeltermijn voor de voorafgaande raadpleging op grond van de AVG is maximaal 14 weken. De AP kan deze termijnen verlengen als de voorgenomen verwerking erg complex is.
Heeft de AP tijdens de beoordeling meer informatie nodig, dan vraagt de AP aan om deze informatie binnen een bepaalde termijn te leveren. Wanneer dit niet haalbaar is kan hiervoor uitstel gevraagd worden. De behandeltermijn van de voorafgaande raadpleging wordt in deze gevallen onderbroken.
Tijdens deze procedure mag u nog niet beginnen met verwerken van persoonsgegevens.

Bijlage 3.1 : AP-lijst van verwerkingen waarvoor een DPIA verplicht is

AP-lijst
1. Heimelijk onderzoek
Grootschalige en/of systematische verwerkingen van persoonsgegevens waarbij informatie wordt verzameld door middel van onderzoek zonder dat de betrokkene daarvan vooraf op de hoogte te stellen. Bijvoorbeeld heimelijk onderzoek door particuliere recherchebureaus, onderzoek in het kader van fraudebestrijding en onderzoek op internet in het kader van bijvoorbeeld online handhaving van auteursrechten. Heimelijk cameratoezicht door werkgevers in het kader van diefstal- of fraudebestrijding door werknemers (bij deze laatste verwerking dient ook in incidentele gevallen een DPIA te worden uitgevoerd).
2. Zwarte lijsten
Verwerkingen waarbij persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten, gegevens over onrechtmatig of hinderlijk gedrag (artikel 33, lid 4, aanhef en onder c, UAVG) of gegevens over slecht betalingsgedrag door organisaties of particulieren worden verwerkt en gedeeld met derden. Bijvoorbeeld heimelijk onderzoek door particuliere recherchebureaus, onderzoek in het kader van fraudebestrijding en onderzoek op internet in het kader van bijvoorbeeld online handhaving van auteursrechten. Heimelijk cameratoezicht door werkgevers in het kader van diefstal- of fraudebestrijding door werknemers (bij deze laatste verwerking dient ook in incidentele gevallen een DPIA te worden uitgevoerd).
3. Fraudebestrijding
Grootschalige en/of systematische verwerkingen van (bijzondere) persoonsgegevens in het kader van fraudebestrijding.

Bijvoorbeeld fraudebestrijding door sociale diensten of door fraudeafdelingen van verzekeraars.

4. Creditscores

Grootschalige en/of systematische gegevensverwerkingen die leiden tot of gebruik maken van inschattingen van de kredietwaardigheid van natuurlijke personen, bijvoorbeeld tot uitdrukking gebracht in een creditscore.

5. Financiële situatie

Grootschalige en/of systematische verwerkingen van financiële gegevens waaruit de inkomens- of vermogenspositie of het bestedingspatroon van mensen valt af te leiden.
Bijvoorbeeld overzichten van bankoverschrijvingen, overzichten van de saldi van iemands bankrekeningen of overzichten van mobiele- of pinbetalingen.

6. Genetische persoonsgegevens

Grootschalige en/of systematische verwerkingen van genetische persoonsgegevens. Bijvoorbeeld DNA-analyses ten behoeve van het in kaart brengen van persoonlijke kenmerken, bio-databanken.

7. Gezondheidsgegevens

Grootschalige verwerkingen van gegevens over gezondheid (bijvoorbeeld door instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, arbodiensten, reïntegratiebedrijven, (speciaal)onderwijsinstellingen, verzekeraars, en onderzoeksinstituten) waaronder ook grootschalige elektronische uitwisseling van gegevens over gezondheid.
Let op: individuele artsen en individuele zorgprofessionals zijn op grond van overweging 91 van de AVG uitgezonderd van de verplichting een DPIA uit te voeren.

8. Samenwerkingsverbanden

Het delen van persoonsgegevens in of door samenwerkingsverbanden waarin gemeenten of andere overheden met andere publieke of private partijen bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard (zoals gegevens over gezondheid, verslaving, armoede, problematische schulden, werkloosheid, sociale problematiek, strafrechtelijke gegevens, betrokkenheid van jeugdzorg of maatschappelijk werk) met elkaar uitwisselen.
Bijvoorbeeld in wijkteams, veiligheidshuizen of informatieknooppunten.

9. Cameratoezicht

Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten met behulp van camera's, webcams of drones

10. Flexibel cameratoezicht

Grootschalig en/of systematisch gebruik van flexibel cameratoezicht.
Bijvoorbeeld camera's op kleding of helm van brandweer- of ambulancepersoneel, dashcams gebruikt door hulpdiensten.

11. Controle werknemers

Grootschalige en/of systematische verwerking van persoonsgegevens om activiteiten van werknemers te monitoren.
Bijvoorbeeld controle van e-mail en internetgebruik, GPS-systemen in (vracht)auto's van werknemers of cameratoezicht ten behoeve van diefstal- en fraudebestrijding.

12. Locatiegegevens

Grootschalige en/of systematische verwerking van locatiegegevens van of herleidbaar tot natuurlijke personen.
Bijvoorbeeld door (scan)auto's, navigatiesystemen, telefoons, of verwerking van locatiegegevens van reizigers in het openbaar vervoer.

13. Communicatiegegevens

Grootschalige en /of systematische verwerking van communicatiegegevens inclusief metadata herleidbaar tot natuurlijke personen, tenzij en voor zover dit noodzakelijk is ter bescherming van de integriteit en de veiligheid van het netwerk en de dienst van de betrokken aanbieder, of het randapparaat van de eindgebruiker.

14. Internet of things

Grootschalige en/of systematische verwerkingen door verantwoordelijken van persoonsgegevens die worden gegenereerd door apparaten die verbonden zijn met internet en die via internet of anderszins gegevens kunnen versturen of uitwisselen.
Bijvoorbeeld 'internet of things'- toepassingen, zoals slimme televisies, slimme huishoudelijke apparaten, connected toys, smart cities, slimme energiemeters, medische hulpmiddelen, etc.

15. Profilering

Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profilering).
Bijvoorbeeld beoordeling van beroepsprestaties, prestaties van leerlingen, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag.

16. Observatie en beïnvloeding van gedrag

Grootschalige verwerkingen van persoonsgegevens waarbij op systematische wijze via geautomatiseerde verwerking gedrag van natuurlijke personen geobserveerd, verzameld, vastgelegd of beïnvloed wordt, inclusief gegevens die voor het doel online behavioural advertising worden verzameld.

Begrippen

In de lijst van soorten verwerkingen waarvoor een DPIA verplicht is, komen de begrippen ‘grootschalig’, ‘systematisch’ en ‘stelselmatig’ voor. Het begrip grootschalig is door de Europese privacy toezichthouders verder ingevuld.
Op Europees niveau zijn de begrippen ‘systematisch’ en ‘stelselmatig’ (nog) niet verder ingevuld. Waar in onderstaande lijst wordt gesproken over ‘systematisch’ of ‘stelselmatig’ moet u denken aan verwerkingen die volgens een bepaald systeem plaatvinden. Een verwerking van persoonsgegevens die is opgenomen in de systemen of in het beleid van de organisatie moet worden beschouwd als een systematische of stelselmatige verwerking. Gegevensverwerkingen die ad hoc of incidenteel plaatsvinden moeten niet beschouwd worden als systematische of stelselmatige verwerkingen.
Bron: Website Autoriteit Persoonsgegevens