gemeente Tubbergen

GEMEENTEBLAD

Officiële uitgave van de gemeente Tubbergen

Nr. 257815

23 oktober 2019

Beleidsregel van de functionaris gegevensbescherming van de gemeente Dinkelland, Tubbergen en de Bedrijfsvoeringsorganisatie Noaberkracht Dinkelland Tubbergen houdende regels omtrent het privacybeleid

Versie: oktober 2018
Status: vastgesteld
Van: de Functionaris Gegevensbescherming
Aan: het Bestuur van Noaberkracht, het College van B&W van de gemeente Dinkelland en het College van B&W van de gemeente Tubbergen
Cc: de Privacybeheerders, de Concerncontroller en overige leden van de Governance Informatieveiligheid en Privacy

Voorwoord

Dit is het privacybeleid dat door de gemeente Dinkelland, gemeente Tubbergen en Bedrijfsvoeringsorganisatie Noaberkracht Dinkelland en Tubbergen (hierna 'de gemeenten en Noaberkracht', of, 'de organisaties' genoemd) is vastgesteld en wordt gehanteerd. Dit privacybeleid stelt kaders en uitgangspunten vast hoe deze de gemeenten en Noaberkracht omgaan met persoonsgegevens. Het beleid is zo opgesteld dat het algemeen is waar mogelijk, en specifiek is waar nodig. Daarnaast is het van belang dat privacy wordt gewaarborgd in de praktijk.

De organisaties spannen zich continu in voor een (verdere) professionalisering van privacy en informatieveiligheid. Onderhoud van het privacybeleid en periodieke toetsen zijn noodzakelijk om het bereikte niveau te handhaven en te verhogen. Bij het opstellen van het beleid is zoveel mogelijk vermeden dat privacywetgeving wordt herhaald of niet concreet wordt.

Naast een intrinsieke motivatie om gegevensbescherming goed te regelen zijn er ook externe aanleidingen om meer werk van gegevensbescherming te maken:

- Inwoners worden er door zowel de private sector als door de overheid steeds bewuster van gemaakt dat gevoelige gegevens beschermd moet worden.
- De Rijksoverheid en koepelorganisaties sporen gemeenten aan om meer werk te maken van gegevensbescherming.
- Gemeenten werken op steeds meer beleidsterreinen samen waardoor de omvang en complexiteit van gegevensstromen, en daarmee het belang van informatieveiligheid en privacy, toeneemt.

Dit beleid is bedoeld om op organisatieniveau te sturen op gegevensbescherming. Na vaststelling van dit beleid is het, op 29 november 2016 door het bestuur van Noaberkracht vastgestelde, 'Privacybeleid 2016' ingetrokken.

1. Inleiding

Binnen de kaders van de Algemene Verordening Gegevensbescherming (AVG) worden door de gemeenten en Noaberkracht persoonsgegevens verwerkt. Deze wet verplicht de gemeenten en Noaberkracht om persoonsgegevens 'in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze' te verwerken. Dit privacybeleid is een invulling van artikel 24 lid 2 van de AVG. In dit privacybeleid werken de gemeenten en Noaberkracht uit hoe persoonsgegevens worden verwerkt en op welke wijze wordt gewaarborgd dat de gegevens behoorlijk en zorgvuldig verwerkt worden.

Dit doen we niet alleen voor de wet, maar vooral omdat inwoners er vanuit mogen gaan dat de organisaties zorgvuldig en vertrouwelijk met persoonsgegevens omgaan. Deze persoonsgegevens hebben de gemeenten en Noaberkracht nodig om betrokkenen van diensten en/of producten te kunnen voorzien.

Reikwijdte en doelstelling van het beleid

De doelstelling van dit privacybeleid laat zich vatten als:

- Compliant zijn met de Nederlandse en Europese wetgeving.
- Houvast bieden om nieuwe wetgeving zoals de meldplicht datalekken en de AVG te implementeren.
- Een kader bieden om (toekomstige) verwerkingen van persoonsgegevens te toetsen aan een vastgesteld kader.
- Taken, bevoegdheden en verantwoordelijkheden die betrekking hebben op de verwerking van persoonsgegevens voor iedereen duidelijk te beleggen.

- Richtlijnen geven hoe om te gaan met persoonsgegevens en verwerkingen daarvan.
- Normen stellen met betrekking tot de bescherming van persoonsgegevens en privacywetgeving.
- De verwerking van gegevens van medewerkers vanwege de werkgever-werknemer relatie vallen ook onder dit privacybeleid.
- Dit beleid geldt voor alle medewerkers, tijdelijke inhuur en externe partijen.

Doelgroepen
Het beleid is bedoeld voor drie doelgroepen. Het is in eerste instantie bedoeld voor allen die verantwoordelijkheid dragen over persoonsgegevens binnen de organisaties. In feite wordt van alle personen die persoonsgegevens verwerken of beleid maken verwacht dat zij behoorlijk en zorgvuldig handelen. Ieder draagt een verantwoordelijkheid die past bij zijn niveau en rol. Zo wordt bijvoorbeeld van een 'gewone' medewerker niet verwacht dat deze beveiligingslekken opspoort en dicht. Wel mag van deze medewerker worden verwacht dat hij signalen doorgeeft aan een leidinggevende, CISO of FG.

In tweede instantie is het beleid bedoeld als uitgangspunt voor beleidsmakers en beslissers. Niet alleen gaat het om organisatorische keuzes, ook medewerkers (bijvoorbeeld op het gebied van HRM, IT, Juridische Zaken en Inkoop) moeten in dit beleid kaders en handvatten vinden. Wanneer een team of een afdeling een nieuw product of dienst wil aanschaffen of implementeren, biedt dit beleid handvatten om Privacy by Design toe te passen en vanaf het begin te werken volgens de wet. Privacy by Design houdt in dat de gemeenten Noaberkracht al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) ten eerste aandacht besteedt aan privacy verhogende maatregelen. Ten tweede worden zo min mogelijk persoonsgegevens, dat wil zeggen alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking, verwerkt. Het beleid kan helpen bij het uitvoeren van Privacy Impact Assessments (PIA's).

Als derde, tot slot, vormt het beleid een vertrekpunt voor audits, periodieke onderzoeken en om aantoonbaar compliant te zijn voor de toezichthouder.

2. Rollen en verantwoordelijkheden
Dit hoofdstuk beschrijft de verantwoordelijkheden en rollen zoals deze voortkomen uit de AVG, toegepast op de deelnemende gemeenten en Noaberkracht.

Verwerkersverantwoordelijke en verwerker
Door de opzet en structuur van de gemeenten en Noaberkracht is er sprake van verschillende verantwoordelijken. Alle organisaties kunnen 'verwerkingsverantwoordelijke' in de zin van de AVG zijn wanneer de organisatie diegene is die 'doel en middelen vaststelt'. De verwerkingsverantwoordelijke heeft ten aanzien van de verwerking van persoonsgegevens dus een bepalende rol en stelt het privacybeleid vast.

Een verwerker is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Soms kan er ook sprake zijn van sub-verwerkers wanneer de verwerker andere verwerkers inschakelt. Zo zie je dat veel gemeenten taken omtrent de Participatiewet aan een derde partij hebben uitbesteed. Deze derde partij kan vervolgens onderdelen uit het contract aan een andere partij hebben uitbesteed, bijvoorbeeld een SaaS (Software as a Service) -oplossing in het gebruik van een applicatie. De term sub-verwerker geeft aan dat een ketenverantwoordelijkheid met verschillende partijen kan ontstaan. De AVG spreekt over een 'andere verwerker' en stelt hier eisen aan.

Gedeelde en gezamenlijke verantwoordelijkheid
Onder de verantwoordelijkheid van de gemeenten en Noaberkracht kunnen bijvoorbeeld ook of Gemeenschappelijke Regelingen of andere vormen van samenwerking vallen. De algemene bepalingen van dit privacybeleid zijn ook op hen van toepassing. Zij vallen direct onder de verantwoordelijkheid, alleen of in gezamenlijkheid, van de deelnemende partijen.

Ook kan sprake zijn van gezamenlijke verantwoordelijkheden in het geval van een samenwerking of project met een of meerdere organisaties. In die gevallen stellen de gezamenlijke verwerkingsverantwoordelijkheden een overeenkomst op waarin zij:

- Gezamenlijke doel(en) en middelen benoemen.
- Omgang met verzoeken van betrokkene om hun rechten uit te oefenen beschrijven.
- De inrichting, kaders en voorwaarden van de onderlinge relatie regelen.
- Afspraken over informatiebeveiliging maken.

Personeel

Personeel wordt aangesteld en valt daarmee onder het ambtenarenreglement. In dit reglement wordt een medewerker gewezen op de geheimhouding van persoonsgegevens, het belang van een vertrouwelijke omgang met deze gegevens en andere verantwoordelijkheden die samenhangen met de verwerking van persoonsgegevens.

Personeel wordt actief herinnerd aan de zorgvuldige verwerking van persoonsgegevens en het gewenste gedrag. Specifieke aandacht aan het onderwerp wordt gegeven na incidenten, bij vragen die breed leven of zodra (intern) onderzoek laat zien dat bijscholing nodig is.

Samenwerkingsverbanden
De gemeenten en Noaberkracht werken samen in regionaal verband. Zo kennen de gemeenten en Noaberkracht onder andere samenwerkingen op het gebied van zorg en veiligheid. De gemeenten en Noaberkracht dienen zorg te dragen dat ook deze samenwerkingspartners vallen onder het privacybeleid of dat er separate afspraken worden gemaakt om de privacy te waarborgen.

Inkoop en aanbesteding
Wanneer een contractuele overeenkomst wordt aangegaan met externe leveranciers dan gelden de Algemene Inkoopvoorwaarden van de organisaties. Deze zijn vastgesteld door de verantwoordelijke. Wanneer uitvoerende partijen aanpassingen op de inkoopvoorwaarden aanbrengen dan mogen deze niet met de Algemene Inkoopvoorwaarden conflicteren.

Wanneer sprake is van ICT-diensten en -apparatuur dan gelden aanvullende voorwaarden. Wanneer voor de uitvoer van een overeenkomst persoonsgegevens worden verwerkt dan geldt de externe leverancier als verwerker. In deze gevallen worden aanvullende bepalingen opgenomen in een verwerkersovereenkomst. Leveranciers en verwerkers zijn gehouden aan geheimhouding. Door middel van de overeenkomsten wordt gewaarborgd dat een leverancier of verwerker alleen verwerkingen van persoonsgegevens uitvoert binnen de noodzakelijkheid van de daarin overeengekomen doelstellingen.

Overeenkomsten met verwerkers
Verwerkers verwerken persoonsgegevens in opdracht van de gemeenten en Noaberkracht. Alleen verwerkers die afdoende garanties bieden ten aanzien van de bescherming van persoonsgegevens worden ingehuurd. Met alle verwerkers wordt een verwerkersovereenkomst gesloten.

In deze verwerkersovereenkomst maken de gemeenten en Noaberkracht in ieder geval afspraken over:

- De uit te voeren werkzaamheden en de rol van persoonsgegevens daarin.
- Afspraken over het door de verwerker inhuren van andere verwerkers (sub-verwerkers).
- Technische en organisatorische maatregelen om gegevens te beveiligen.
- Afspraken over geheimhouding en vertrouwelijkheid.
- Doorgifte van persoonsgegevens naar het buitenland.
- Verdeling van verantwoordelijkheden met de gemeenten en Noaberkracht als verwerkingsverantwoordelijke en de opdrachtnemer als verwerker.
- Wanneer en hoe persoonsgegevens vernietigd worden.
- Afspraken over het afhandelen van verzoeken aangaande de rechten van een betrokkene.
- Afspraken over heronderhandeling en beëindiging.

Er wordt door de gemeenten en Noaberkracht is een standaard verwerkersovereenkomst gebruikt die de gewenste bepalingen bevat. Wanneer een verwerker een eigen voorstel voor een verwerkersovereenkomst heeft, kan besloten worden deze overeenkomst aan te houden. In deze gevallen wordt de overeenkomst getoetst. Afwijken kan alleen in overleg met de Functionaris Gegevensbescherming en eventueel na toestemming van de colleges van beide gemeenten en het bestuur van Noaberkracht.

Persoonsgegevens van derden
De gemeenten en Noaberkracht gaan zorgvuldig om met persoonsgegevens van inwoners en derden, zoals bezoekers van de websites, deelnemers aan diensten waarbij persoonsgegevens bij de gemeenten en Noaberkracht terecht komen. Dit is onder andere beschreven in de privacyverklaring op de websites.

Functionaris voor Gegevensbescherming (FG)
Beide gemeenten en Noaberkracht hebben aan de wettelijke verplichting voldaan om een FG aan te stellen. Samenvattend heeft de FG als taak:

- Het informeren en adviseren van de organisatie over verplichtingen uit de AVG.
- Het toezien op de naleving van: privacywet- en regelgeving, het privacybeleid, speciaal de toewijzing van verantwoordelijkheden en audits.

- De FG is verplicht desgevraagd een advies over een privacy impact assessment (PIA) te geven en ziet toe op de uitvoering van zijn advies.
- Het controleren van documentatie en registers zoals: het register van de verwerkingsactiviteiten en een overzicht van datalekken.
- Het rapporteren aan het hoogste orgaan van de organisatie, onder andere met een eigen jaarverslag.
- Het beheersen van risico's .
- Communiceren met betrokkenen en de Autoriteit Persoonsgegevens. De FG is het belangrijkste contactpunt voor de Autoriteit Persoonsgegevens.
- De FG is gebonden aan beroepsgeheim.

De organisaties maken het mogelijk voor de FG om de taken zo goed mogelijk uit te kunnen voeren door:

- De FG te betrekken in alle zaken omtrent gegevensbescherming.
- Middelen beschikbaar te stellen.
- De FG te ondersteunen in het verwerven en onderhouden van de noodzakelijke kennis.
- De FG onafhankelijk zijn of haar taken uit te laten voeren.
- De FG niet te bestraffen voor het uitvoeren van deze taken.
- De FG niet in een situatie te brengen waar tegengestelde belangen gelden.

Privacybeheerder
Binnen Noaberkracht is rol van Privacybeheerder in het leven geroepen. Deze rol is belegd bij medewerkers verantwoordelijk voor juridisch concern control. In tegenstelling tot de FG is deze rol gericht op coördinerende en uitvoerende taken die uit dit privacybeleid volgen. De beheerder voorziet alle lagen van de organisatie gevraagd en ongevraagd van advies met betrekking tot de AVG en de bescherming van de persoonlijke levenssfeer van degenen van wie persoonsgegevens worden verwerkt.

De Privacybeheerder neemt als adviserend lid deel aan programma's (zoals bijvoorbeeld verbetering dienstverlening) en projecten waarvan het resultaat gevolgen kan hebben voor de wijze van verwerking van persoonsgegevens.

Samenvattend heeft de Privacybeheerder als taak:

- Het adviseren van de organisaties bij privacyvraagstukken.
- Het ondersteunen bij het opstellen van een PIA.
- Het ondersteunen en/of opstellen van verwerkersovereenkomsten.
- Het ondersteunen en/of opstellen van het register van verwerkingsactiviteiten.
- Het ondersteunen bij de coördinatie en beheer van datalekken.
- Een actieve voorlichting richting de organisatie.
- Het opstellen en aanpassen van interne regelingen.
- Vragen en klachten van mensen binnen en buiten de organisatie afhandelen.
- Het opstellen van jaarplannen, uitvoeringsprogramma's en rapportages.

Derden
De organisaties gaan zorgvuldig om met persoonsgegevens van klanten/cliënten en derden, zoals bezoekers van de websites, deelnemers aan diensten waarbij persoonsgegevens bij de gemeenten Dinkelland en Tubbergen terecht komen. Dit is onder andere beschreven in de privacyverklaring en de cookiebepaling.

Er wordt betreft de beschermende maatregelen geen onderscheid gemaakt tussen klanten en niet-klanten en derden. Het (hoge) niveau van beschermende maatregelen wordt overal toegepast.

3. Beleid voor rechtmatige verwerking en zorgvuldige verwerking persoonsgegevens

De Algemene verordening gegevensbescherming (AVG) biedt het normatieve kader van waaruit de specifieke technische en organisatorische maatregelen voor een organisatie moeten worden afgeleid. Dit normenkader is opgenomen in de thema's van dit hoofdstuk. Het uitgangspunt is dat de verwerkingen door gemeenten en Noaberkracht voldoen aan de volgende beginselen:

a) Verwerkingen zijn rechtmatig, behoorlijk en transparant ("rechtmatigheid, behoorlijkheid en transparantie"). Ze hebben een wettelijke grondslag, gegevens worden netjes en verantwoord. verwerkt en gemeenten Dinkelland en Tubbergen is open naar betrokkene toe over verwerkingen.
b) Verwerkingen zijn gebonden aan specifieke verzameldoelen ("doelbinding") (welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden) en wanneer ze voor een ander doel worden verwerkt, is dat doel niet onverenigbaar met het oorspronkelijke doel.

c) Gegevens moeten toereikend en ter zake dienend zijn, maar ook beperkt tot het noodzakelijke ("minimale gegevensverwerking").
d) De gegevens moeten correct en actueel zijn ("juistheid") Gegevens die dat niet (meer) zijn, dienen te worden gewist of gecorrigeerd.
e) De gegevens mogen niet langer worden verwerkt en bewaard dan nodig voor het doel waarvoor ze verzameld zijn en, tenzij een wettelijke bepaling een minimumtermijn stelt aan het bewaren, dan moeten zij worden vernietigd of gewist ("opslagbeperking").
f) De gegevens worden goed beveiligd zijn en blijven vertrouwelijk ("integriteit en vertrouwelijkheid"). Persoonsgegevens worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Overzicht verwerking persoonsgegevens
De verwerkingen van de organisaties zijn opgenomen in het register van de verwerkingsactiviteiten. Het register wordt geüpdatet wanneer de verwerkingen of veranderingen in de organisatie daar aanleiding toe geven.

Op grond van de AVG is de organisatie verplicht een PIA uit te voeren als een verwerking mogelijk een hoog risico inhoudt voor rechten en vrijheden van de betrokkenen. Lukt het niet om (voldoende) maatregelen te vinden om dit risico te beperken? Dan wordt met de Autoriteit Persoonsgegevens (AP) overlegd voordat de verwerking start.

Transparantie
De organisaties zijn transparant over hoe ze persoonsgegevens verwerkt. Hierdoor weten burgers en personen die benaderd worden wie de organisaties zijn, dat persoonsgegevens worden verwerkt, waarom dit gebeurt en welke maatregelen worden getroffen om zorgvuldig met gegevens om te gaan. Belangrijke manieren om betrokkenen te informeren over de verwerking van persoonsgegevens zijn:

- Bij aanvang van vormen van dienstverlening.
- Additionele informatie bij het aanvragen van specifieke diensten.
- Websites hebben een privacyverklaring inclusief cookiebepaling.
- De organisaties bieden mogelijkheden om inzage te krijgen in de verwerking van persoonsgegevens.

Doelbinding
Met doelbinding wordt bedoeld dat gegevens alleen worden verwerkt voor het doel waarvoor ze verzameld zijn. En als gegevens toch voor andere doelen worden gebruikt, wordt beoordeeld of dit niet te ver afstaat van dat doel. Wanneer de wens ontstaat om persoonsgegevens voor andere doelen te verwerken wordt een PIA uitgevoerd, om de vraag te beantwoorden of de verwerking 'niet onverenigbaar is' met het oorspronkelijke doel. Dit vereiste volgt uit art. 5 lid 1 sub b AVG.

Rechtmatige grondslag
Een organisatie mag alleen persoonsgegevens verwerken wanneer hier een grondslag voor bestaat. De organisaties verwerken gegevens van inwoners, geïnteresseerden, en medewerkers op basis van een grondslag zoals benoemd in de AVG.

Rechten van de betrokkene
Personen over wie persoonsgegevens worden verzameld hebben een aantal rechten, waaronder het recht op inzage, correctie, verwijdering, afscherming en verzet. Dit is geregeld in art. 15-20 AVG. Betrokkenen worden gewezen op hun rechten in het privacyverklaring dat op de website is geplaatst . Zij kunnen hun rechten uitoefenen waarbij wordt gewaarborgd dat verzoeken correct worden afgehandeld.

De betrokkene heeft:
- het recht op informatie over de verwerkingen;
- het recht op inzage in zijn gegevens;
- het recht op correctie van de gegevens als deze niet kloppen;
- het recht op verwijdering van de gegevens en 'het recht om vergeten te worden';
- het recht op beperking van de gegevensverwerking;
- het recht op verzet tegen de gegevensverwerking;
- het recht op overdracht van zijn gegevens (dataportabiliteit);
- het recht om niet onderworpen te worden aan een geautomatiseerde besluitvorming.

Informatiebeveiliging
Om zorgvuldig met persoonsgegevens om te kunnen gaan moeten passende beschermende maatregelen worden getroffen. Deze maatregelen moeten de geheimhouding en beveiliging borgen. De maatregelen gelden voor allen die onder verantwoordelijkheid van de organisaties werken: interne medewerkers,

verwerkers en sub-verwerkers. De maatregelen gelden ook voor diensten en goederen die onderdeel zijn van de beveiliging, zoals beveiliging van het pand, de schoonmaak of leveranciers van hardware. Dit thema is een uitwerking van de artikelen 5 lid 1 sub f en 32 AVG.

De organisaties hebben een gemeente breed informatiebeveiligingsbeleid , waarin op strategisch en tactisch niveau wordt beschreven, welke uitgangspunten ten aanzien van de informatiebeveiliging gelden. Dit document zal samen met de technische beveiligingsmaatregelen en -procedures een adequaat niveau van beveiliging voor de organisatie moeten opleveren waardoor de kwaliteitskenmerken van informatie, te weten: beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van de informatie, binnen de organisatie zijn gewaarborgd.

Bewustwording en training
Periodiek wordt beoordeeld en vastgesteld welke informatiebehoefte de medewerkers hebben ten aanzien van een basisbewustzijn over de zorgvuldige omgang met persoonsgegevens en specifieke thema's. Ook wordt aandacht besteed aan consequenties van het niet-naleven van de vereiste regels, voor zowel de organisatie als de betrokkene.

4. Beleidsuitvoering Noaberkracht

De gemeenten Dinkelland en Tubbergen hebben gekozen voor één ambtelijke organisatie. Daartoe hebben de colleges van burgemeester en wethouders van beide gemeenten Bedrijfsvoeringsorganisatie Noaberkracht Dinkelland Tubbergen opgericht. Het bestuur bestaat uit de voltallige colleges van beide gemeenten. De medewerkers zijn formeel in dienst van Noaberkracht maar zijn materieel nog steeds ondergeschikt aan de beide colleges. Noaberkracht voert namens de beide colleges het beleid uit, zoals dat door de beide colleges is vastgesteld en waarvoor elk van beide colleges zich dient te verantwoorden jegens zijn eigen raad en zijn eigen inwoners.

Hieruit volgt dat elk van beide colleges bevoegd is om het privacybeleid voor zijn eigen gemeente vast te stellen en dat het gehouden is daarvoor verantwoording af te leggen aan zijn gemeenteraad. Noaberkracht dient dit beleid uit te voeren. Noaberkracht heeft formeel rechtspersoonlijkheid en is dus bevoegd om extern op eigen naam op te treden. Maar de organisatie is ook een verlengstuk van elk van beide gemeenten, bestuurd door en ondergeschikt aan de beide colleges. Ook voor de uitvoering door Noaberkracht van het gemeentelijk vastgestelde beleid is het college van elk van beide gemeenten verantwoording verschuldigd aan zijn gemeenteraad.

De organisaties hanteren in de uitvoering van het beleid uitgangspunten op het gebied van dienstverlening en bedrijfsvoering, welke hieronder zijn beschreven.

Dienstverlening
Een inwoner heeft er recht op dat de organisaties zorgvuldig en vertrouwelijk met persoonsgegevens omgaan. Dit moet voor de inwoner echter zo min mogelijk invloed op de dienstverlening hebben, daarom worden de volgende uitgangspunten gehanteerd:

- Inwoners hoeven de over hen bij de overheid bekende en beschikbare gegevens niet steeds opnieuw verstrekken.
- Tenzij de wet anders bepaalt, bepalen inwoners zelf in hoeverre zij hen de betreffende informatie willen vrijgeven. Inwoners beschikken immers over het grondwettelijk recht op privacy, waaronder het recht op informationele privacy, wat inhoudt dat zij bepalen in hoeverre zij hen de betreffende informatie willen vrijgeven.
- De persoonsinformatiehuishouding is op orde.
- De naleving van wet- en regelgeving op het gebied van de privacybescherming is uitgangspunt van handelen bij de uitvoering van primaire processen en bedrijfsvoering. privacybescherming wordt opgevat als een kenmerk van goede dienstverlening / kwaliteit.
- Het privacybeleid moet bestuur, directie, management en medewerkers handvatten bieden om die ruimte zoveel als mogelijk concreet in te vullen.
- Privacy afspraken binnen Noaberkracht dienen zoveel als mogelijk uniform in de organisatie te worden toegepast, waardoor inwoners niet tegen verschillen in de uitvoering kunnen aanlopen.

Bedrijfsvoering
Goede bedrijfsvoering staat aan de basis van goede dienstverlening. Op basis van bovenstaande uitgangspunten zijn er randvoorwaarden voor het inrichten van de interne organisatie te benoemen:

- Elke medewerker die persoonsgegevens nodig heeft voor de uitvoering van diens taak of taken, moet daarover op zo efficiënt mogelijke wijze kunnen beschikken.
- Voor zover een algemeen gegeven (basisgegeven) over een persoon beschikbaar is in één van de basisregistraties, gebruikt de medewerker dat gegeven tenzij dat gegeven onjuist is.

- Het takenpakket van een medewerker is bepalend voor de set aan gegevens waarover een medewerker mag beschikken evenals de wijze waarop deze gegevens ter beschikking worden gesteld.
- Een teamcoach, programmaregisseur of medewerkers met soortgelijke taken blijven echter verantwoordelijk voor privacyvraagstukken binnen het team of organisatieonderdeel. De medewerkers hebben taken, die ze moeten uitvoeren met inachtneming van de privacy regels. Privacy is onderdeel van het werk.
- Bij nieuw uit te voeren processen waarbij de verwerking van persoonsgegevens, waaronder bijzondere persoonsgegevens, qua inhoud en omvang complex is en van substantieel belang is voor de uitvoering van het proces, maakt een PIA deel uit van implementatieproces. Deze assessment heeft als doel bij nieuwe werkzaamheden na te gaan wat dit betekent voor de bescherming van de persoonsgegevens.

5. Privacybeleid in de praktijk

Het opstellen van een privacybeleid en vaststellen van uitgangspunten is meestal een goed begin voor een goede uitvoering. Van groter belang is echter het toezien op die uitvoering en het ervoor zorgdragen dat de organisatie 'in control' is waar het gaat de uitvoering van dit beleid. Om dit te bereiken is het nodig om een goede governance structuur te hebben. Ook moet er (blijvend) aandacht zijn voor goede opleiding, trainingen en privacyvraagstukken voor alle medewerkers.

Bewustwording en training

Medewerkers hebben vanuit hun eigen taakgebied en verantwoordelijkheid natuurlijk ook de taak om goed om te gaan met persoonsgegevens conform dit privacybeleid. Dit betekent nog niet dat zij altijd tot op detail op de hoogte kunnen zijn van informatie rond privacyvraagstukken. Het is dan ook van belang dat zij zich bewust zijn van het voorliggende privacybeleid en dat zij regelmatig met elkaar en de Privacybeheerders spreken over dit thema. De volgende acties worden dan ook ondernomen:

- Voorlichting in werkoverleggen.
- Verspreiden van tips via verschillende media.
- Actuele problematieken bespreken met medewerkers.
- Toepassen van kanaalsturing in casusbespreking.
- Ondersteuning in uitwisseling persoonsgegevens met derden.
- Toets proces datalekken.
- Periodieke beoordelingen bewustwording.

Governance

Voor de organisatie moet worden vastgelegd welke taken en bevoegdheden bepaalde functionarissen hebben bij de verwerking van persoonsgegevens en aan wie zij verantwoording afleggen. Voor het opstellen van deze governance structuur is aansluiting gezocht bij de inrichting van de Baseline Informatiebeveiliging Gemeenten. Gemiddeld wordt 5 maal per jaar met een groep medewerkers vergaderd om vanuit verschillende vakgebieden naar informatieveiligheid en privacy te kijken. Hier worden verslagen van vastgelegd. Daarnaast wordt jaarlijks over het functioneren en de voortgang van het Governance overleg gerapporteerd. De volgende rollen zijn vertegenwoordigd in dit overleg:

- De CISO
- De Functionaris Gegevensbescherming
- De Concerncontroller
- Beveiligingsbeheerders BRP/WD, BAG en DigiD
- Beveiligingsbeheerders FZ , IT, HRM en INF
- Beveiligingsbeheerders Sociaal Domein
- Een Privacybeheerder

Communicatie met inwoners

Transparantie is een belangrijk uitgangspunt voor de uitvoering van de AVG. De inwoner wordt (onder andere) via de website van de gemeenten geïnformeerd over:

- Het privacybeleid.
- Op welke wijze waarop persoonsgegevens worden verwerkt.
- De wijze waarop de inwoner zijn rechten (inzage, correctie, verzet) kan uitoefenen.

De gemeenten en Noaberkracht streven er verder naar om contact met inwoners, bedrijven en externen altijd via veilige kanalen te laten lopen. Hiervoor wordt gemaakt van beveiligde koppelingen, verbindingen en portalen, en in mindere mate van email.

Verzoek tot inzage, correctie of verwijdering

Een betrokkene heeft het recht om persoonsgegevens in te zien, te corrigeren of te laten verwijderen. Via verschillende kanalen kan verzoek tot inzage, correctie of verwijdering worden gestuurd naar de gemeenten. Hierbij worden de volgende uitgangpunten gehanteerd:

- Verzoeken kunnen via het centrale nummer, schriftelijk of e-mail (privacy@noaberkracht.nl) aan de gemeente worden gesteld. Informatie hierover is in ieder geval gemakkelijk op de website te benaderen.
- Deze verzoeken worden door de Privacybeheerder beoordeeld. Deze functionaris behandeld of belegd het verzoek in de organisatie afhankelijk van het verzoek.
- Voor het behandelen van een verzoek wordt de aanvrager om legitimatiebewijs gevraagd.
- Inzageverzoeken voor een minderjarige jonger dan 16 jaar kunnen alleen door, of met toestemming van, een persoon met ouderlijk gezag worden gedaan.
- De Functionaris Gegevensbescherming ziet toe dat de rechten van de betrokkene worden gewaarborgd.
- De organisaties streven ernaar om binnen een 1 maand te schriftelijk of per e-mail te reageren op verzoeken.
- Bij complexe of meervoudige verzoeken kan nadere specificatie worden gevraagd aan de betrokkene. Het is mogelijk dat vervolgens voor de afhandeling een langere periode wordt gereserveerd (2 maanden).
- Informatie die wordt gedeeld met de inwoner vindt plaats via niet-openbare en veilige kanalen.
- Klachten lopen via de reguliere klachtenprocedures.

Privacy Impact Assessment
Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van op privacy gebied. Dit heet ook wel een PIA. Een PIA wordt uitgevoerd wanneer een (nieuwe) gegevensverwerking mogelijk een hoog risico oplevert voor de rechten van betrokkenen. Hierbij worden de volgende uitgangspunten gehanteerd:

- Een PIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacy risico oplevert voor de mensen van wie de organisatie gegevens verwerkt.
- Een PIA wordt uitgevoerd bij nieuwe risicovolle verwerkingen en bij bestaande risicovolle verwerkingen eens in de drie jaar. Dit is in ieder geval in verwerkingen waarbij:
  - systematisch en uitgebreid persoonlijke aspecten worden geëvalueerd gebaseerd op geautomatiseerde verwerking, waaronder *profiling*, waarop besluiten worden gebaseerd die gevolgen hebben voor mensen;
  - op grote schaal bijzondere persoonsgegevens worden verwerkt of strafrechtelijke gegevens verwerkt ;
  - op grote schaal en systematisch mensen worden gevolgd in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

- Door de CISO en Privacybeheerder wordt een meerjarenplanning opgesteld, hiervoor wordt advies ingewonnen bij de FG. Door alle besturen wordt deze planning vastgesteld.
- Voordat een beslissing wordt genomen over nieuwe of wijzigingen van bestaande bewerkingen, wordt door middel van een PIA aangetoond dat de Privacy voldoende is gewaarborgd en worden de al dan niet te nemen maatregelen gemotiveerd.
- De FG geeft over de PIA een bindend advies.
- De PIA wordt waar mogelijk in een Directie-, College- of Bestuursadvies meegenomen ter onderbouwing van het besluit.
- Er wordt gebruikt gemaakt van een PIA format op basis van een best practice.

Register van verwerkingen en verwerkersovereenkomsten
De Functionaris voor de Gegevensbescherming (FG) controleert namens de verantwoordelijke de verwerkingen van persoonsgegevens het daartoe bestemde register. Hierbij worden de volgende uitgangspunten gehanteerd:

- Er wordt gebruikt gemaakt van een format op basis van een best practice . Binnen elk team van Noaberkracht is een aanspreekpunt dat zorgt voor het up-to-date houden van het register.
- De Privacybeheerder gaat periodiek het gesprek aan met deze teams over de actualiteit van de beschreven verwerkingen.
- Het register van verwerkingen wordt jaarlijks door alle organisaties vastgesteld, of wanneer er zich grote wijzigingen voordoen.
- De FG voert jaarlijks een controle uit op het totale bestand en voert regie over het totale register.

Ook in het gebruik van verwerkersovereenkomsten worden uitgangspunten gehanteerd:

- Er zal wordt gebruik gemaakt van het model op basis van best practice,

- Binnen elke afdeling of elk team is de medewerker aangewezen voor inkoop, budgetbeheer, contractbeheer en subsidies, verantwoordelijk voor het afsluiten en onderhouden van verwerkersovereenkomsten.
- Aandacht voor gegevensverwerking in het kader van Privacy by Design is opgenomen in het inkoopproces.

6. Datalekken en beveiligingsincidenten

Wanneer beveiligingsmaatregelen niet afdoende zijn gebleken en persoonsgegevens (mogelijk) zijn gelekt, kan er sprake zijn van een datalek. Binnen de organisaties is het proces meldplicht datalekken opgezet en van kracht. In dit proces is beschreven hoe de organisatie reageert op datalekken. Hieronder is de procedure kort beschreven.

Procedure

Wanneer er sprake van een beveiligingsincident en zijn (mogelijk) persoonsgegevens gelekt dan meldt een medewerker dit bij de CISO of via het daarvoor bestemde emailadres (meldpuntdatalekken@noaberkracht.nl). Alleen een mailtje naar de ICT-servicedesk is bij een melding van een datalek absoluut onvoldoende. Inwoners en externen kunnen via bovenstaand e-mailadres ook een melding doen. Vervolgens wordt door de CISO in het Zaaksysteem het proces gestart. Medewerkers kunnen zelf een zaak starten in het Zaaksysteem bij het ontdekken van een incident. Incidenten die direct worden gemeld zijn:

- Elk incident met een informatiedrager.
- Elk vermoeden dat met de beveiliging van gegevens iets mis is.

Enkele voorbeelden van datalekken:

- Apparaat, gegevensdrager (bijv. mobiele telefoon, laptop of toegangskaart) en/of papier met
- persoonsgegevens kwijtgeraakt of gestolen.
- Brief of postpakket met persoonsgegevens kwijtgeraakt of geopend retour ontvangen.
- Hacking, malware (bijv. ransomeware) en/of phishing.
- Persoonsgegevens nog aanwezig op afgedankt apparaat of gegevensdrager.
- Persoonsgegevens per ongeluk gepubliceerd.
- Persoonsgegevens van verkeerde klant getoond in klantportaal.
- Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger.
- Persoonsgegevens onbeveiligd verstuurd of ontvangen (bijvoorbeeld via email) .

Nadat een melding is gemaakt overleggen de CISO, de FG en de Privacybeheerders of het een datalek betreft en of de datalekprocedure moet worden gevolgd. Zo ja, dan wordt een datalekteam geactiveerd. In het datalekteam zitten in ieder geval de CISO, adviseur Informatie & Techniek, een Privacybeheerder, adviseur Communicatie, eventueel aangevuld met de manager van de afdeling waar het lek heeft plaatsgevonden. Met dit team wordt het meldingsproces vervolgd en het datalek bestreden. Vervolgens wordt bepaald welke stakeholders worden geïnformeerd. Ook wordt de afweging gemaakt om de betrokkene(n) te benaderen. De FG meldt een meldingswaardig datalek direct aan de Autoriteit Persoonsgegevens.

Als laatste wordt het proces gedocumenteerd voor verantwoording en feedback, en wordt het incident opgenomen in het register met datalekken. Het overzicht wordt gebruikt om gegevensbescherming en Informatieveiligheid verder te professionaliseren.

Wanneer er sprake is van een datalek bij een verwerker van onze gegevens, dan is in de verwerkersovereenkomst opgenomen dat deze de organisaties van wie zij de persoonsgegevens verwerken zo snel mogelijk van het datalek op de hoogte stelt, en op welke manier die dient te gebeuren. Het informeren van getroffen personen wordt door de verantwoordelijke uitgevoerd.