

## Privacybeleid Gemeente Dalfsen

### Privacybeleid gemeente Dalfsen

Dit privacybeleid stelt kaders en uitgangspunten vast hoe de gemeente Dalfsen omgaat met persoonsgegevens. Het beleid is zo opgesteld dat het algemeen is waar mogelijk, en specifiek waar nodig. Het beschrijft hoe de gemeente Dalfsen omgaat met persoonsgegevens, hoe ze beleid ontwerpt, controleert en aanpast. Daarnaast is het van belang dat privacy wordt gewaarborgd in de praktijk.

Het beleid is vastgesteld door het college van B&W als verantwoordelijke voor de gegevensverwerking. Onderhoud van het privacybeleid en periodieke toetsen zijn noodzakelijk om het bereikte niveau te handhaven, te verhogen én voorbereid te zijn op de komende algemene verordening gegevensbescherming (AVG). De AVG zal per mei 2018 de Wet bescherming persoonsgegevens (Wbp) vervangen. Om privacy zo concreet mogelijk te maken beperkt het beleid zich tot onderwerpen die binnen de gemeente Dalfsen noodzakelijk zijn voor het waarborgen van een zorgvuldige omgang met persoonsgegevens. Het helpt tevens bij overwegingen, keuzes en de concrete maatregelen. De concrete maatregelen worden indien nodig in de bijlagen toegevoegd. Bij het opstellen van het beleid is zoveel mogelijk vermeden dat privacywetgeving wordt herhaald of niet concreet wordt. Voor de volledige tekst van de wet verwijzen we naar [wetten.overheid.nl](http://wetten.overheid.nl).

Het beleid omvat het geheel van maatregelen dat kaders en waarborgen schept voor de verwerking van persoonsgegevens. Dit algemene uitgangspunt wordt geconcretiseerd in zaken als duidelijk beschreven processen, meldingen bij de AP, klanten/cliënten informeren dat en hoe hun gegevens worden verwerkt en kwalitatief goede informatiebeveiliging. Het biedt een kader dat de organisatie helpt bij vragen en veranderingen: wat is ons beleid, doen we wat we in ons beleid hebben gezegd te doen en hoe kunnen we verbeteringen doorvoeren?

### Reikwijdte en doelstelling van het beleid

Doelstelling van dit privacybeleid is:

- 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.

### Voor wie is dit beleid bedoeld?

Het beleid heeft drie doelen. Het is in eerste instantie bedoeld voor allen die verantwoordelijkheid dragen over persoonsgegevens binnen de organisatie. 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 opspoorde en dicht. Wel mag van deze medewerker worden verwacht dat hij signalen doorgeeft aan een leidinggevende, CISO of Functionaris Gegevensbescherming (F.G.). De volgende categorieën medewerkers worden onderscheiden:

- Directie
- Leidinggevenden en coördinatoren
- Medewerkers

In tweede instantie is het beleid bedoeld als uitgangspunt voor beleidsmakers en beslissers. Niet alleen gaat het om organisatorische keuzes, ook inkopers en ICT-medewerkers moeten in dit beleid kaders en handvatten vinden. Wanneer de gemeente geconfronteerd wordt met nieuwe taken of als er nieuwe diensten worden ontwikkeld, biedt dit beleid handvatten om privacy by design toe te passen en vanaf het begin te werken volgens de wet. 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.

### Aantoonbaar compliant met het privacybeleid als basis

Dit privacybeleid omvat het voorliggende privacybeleid en verder alle documenten, processen, besluiten enz. die onderdeel maken van het geheel van passende en organisatorische maatregelen die waarborgen en waarmee aangetoond kan worden dat de verwerkingen in overeenstemming met de AVG worden uitgevoerd.

De AVG stelt in art. 5 lid 2 dat de verwerkingsverantwoordelijke verantwoordelijk is voor de kwaliteit en vereisten voor de verwerking van persoonsgegevens. Bovendien moet de verantwoordelijke de naleving van de in art. 5 lid 1 AVG genoemde eisen kunnen aantonen. Het privacybeleid zoals verwoord in art. 24 AVG stelt dat maatregelen geëvalueerd en geactualiseerd moeten worden.

De gemeente Dalfsen voorziet in deze verplichting door

- het opzetten, inrichten en uitvoeren van het privacybeleid
- het inrichten van privacybeheer en
- het inrichten van een privacyorganisatie

Met deze maatregelen wordt invulling gegeven aan de verplichtingen die voortkomen uit de AVG.

### Rollen en verantwoordelijkheden t.a.v. het privacybeleid

Dit hoofdstuk beschrijft de verantwoordelijkheden en rollen zoals deze voortkomen uit de Wbp en AVG, toegepast op de gemeente Dalfsen. Een goede verdeling van verantwoordelijkheden is een belangrijke pijler onder een goede toepassing van de Wbp en AVG.

Bij de verdeling van verantwoordelijken ten aanzien van de verwerking van persoonsgegevens zijn de definities uit de Wbp en AVG bepalend. Met de invoering van de AVG veranderen enkele termen.

| Term Wbp          | Term AVG                     | Inhoud begrip AVG  |
|-------------------|------------------------------|--|
| verantwoordelijke | verwerkingsverantwoordelijke | de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.                                  |
| bewerker          | verwerker                    | degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.   |
| subbewerkers      | andere verwerker             | Van een subverwerker is sprake wanneer de bewerker andere bewerkers inschakelt. Deze laatste term geeft aan dat een ketenverantwoordelijkheid met verschillende partijen kan ontstaan. De AVG spreekt over een 'andere verwerker'. |

### Gedeelde verantwoordelijkheid binnen de organisatie

Onder de verantwoordelijkheid van de gemeente Dalfsen kunnen ondersteunende of aanvullende service providers of gemeenschappelijke regelingen 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.

Het zorgvuldig en goed omgaan met persoonsgegevens is uiteindelijk een verantwoordelijkheid van de z.g. verwerkingsverantwoordelijke. Wie dit is is afhankelijk van welke taak er wordt uitgevoerd. In de meeste gevallen zal dit het College van B&W zijn maar dit kan ook de Burgemeester of de Raad zijn. Incidenteel kan ook de Rekenkamer verwerkingsverantwoordelijke zijn.

De uitvoering is een verantwoordelijkheid van een leidinggevende ('intern beheerder'). Hieronder vallen ook het instrueren van medewerkers, het goed uitvoeren van getroffen maatregelen en het aanpassen van procedures. Vanuit hun gedeelde verantwoordelijkheid spreken de organisatieonderdelen elkaar aan wanneer door nalatigheid of onzorgvuldig handelen de kwaliteit van maatregelen lager wordt dan afgesproken.

### Gezamenlijke verwerkingsverantwoordelijken

Door de opzet en structuur van de gemeente Dalfsen kan sprake zijn van verschillende verwerkingsverantwoordelijken. Ook kan sprake zijn van gezamenlijke verantwoordelijkheden in het geval van een samenwerking of project met een of meerdere andere organisaties. In die gevallen stellen de gezamenlijke verwerkingsverantwoordelijken 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

Bij gemeenschappelijke regelingen is het van belang of er sprake is van mandaat of delegatie. Is er sprake van mandaat dan blijft de gemeente verwerkingsverantwoordelijke en treedt de gemandateerde instantie op als verwerker. Is er sprake van delegatie dan gaat de verwerkingsverantwoordelijkheid over naar de gedelegeerde organisatie.

## Uitgangspunten van een rechtmatige verwerking

### Integriteit en vertrouwelijkheid

De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt de gemeente voor passende beveiliging van persoonsgegevens.

### Transparantie

De gemeente Dalfsen is transparant over hoe ze persoonsgegevens verwerkt. Hierdoor weten burgers en personen die benaderd worden wie de gemeente Dalfsen is, dát ze persoonsgegevens verwerkt, waarom dit gebeurt en welke maatregelen de gemeente Dalfsen treft om zorgvuldig met gegevens om te gaan.

De belangrijkste manieren om betrokkenen te informeren over de verwerking van persoonsgegevens zijn:

- algemene voorwaarden bij inschrijven
- additionele informatie bij het aanvragen van specifieke diensten
- alle websites geven, indien vereist, een cookie melding en hebben een privacyverklaring inclusief cookiebepaling
- de gemeente Dalfsen biedt laagdrempelige mogelijkheden om inzage te krijgen in de verwerking van persoonsgegevens. Zie hiervoor ook het kopje 'rechten betrokkene'.

Mensen worden in ieder geval geïnformeerd over:

- de identiteit van de verantwoordelijke
- de doeleinden van de gegevensverwerking
- nadere informatie, waarmee de betrokkene zich een beeld kan vormen van maatregelen die de organisatie treft om gegevens te beschermen.

### 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.
- De gemeente Dalfsen verwerkt alleen gegevens voor de doelen waarvoor ze van burgers gekregen zijn. Onder het kopje Transparantie is aangegeven hoe en wanneer personen op de hoogte worden gesteld van de verwerking van persoonsgegevens. De organisatie zorgt ervoor dat de persoonsgegevens alleen voor deze doelen worden verwerkt. Wanneer de wens ontstaat om persoonsgegevens voor andere doelen te verwerken wordt een Privacy Impact Analyse (PIA) uitgevoerd, om de vraag te beantwoorden of de verwerking 'niet onverenigbaar is' met het oorspronkelijke doel. Dit vereiste volgt uit art. 9 Wbp en art. 5 lid 1 sub b AVG.
- Bij multidisciplinaire teams, zowel binnen als buiten de gemeentelijke organisatie, moet de doelbinding bij convenant worden vastgelegd.

### Rechtmatige grondslag

Een organisatie mag alleen persoonsgegevens verwerken wanneer hier een grondslag voor bestaat. Deze grondslag is terug te vinden in artikel 6, lid 1 onder a t/m f AVG. De gemeente Dalfsen verwerkt vanuit haar wettelijke taken per definitie ook bijzondere persoonsgegevens. Ook hiervoor geldt de genoemde wettelijke grondslag. Opgemerkt moet worden dat verwerking van gegevens met toestemming van betrokkene voor de gemeente veelal geen grondslag kan zijn aangezien cliënten/burgers in een afhankelijke positie zijn.

### Kwaliteit van gegevens

De gemeente Dalfsen treft maatregelen om de kwaliteit van gegevens te borgen. Onder kwaliteit wordt verstaan dat gegevens juist, nauwkeurig en actueel zijn. Voordat gegevens worden verwerkt vinden (geautomatiseerde) controles plaats om onjuiste benadering van personen te voorkomen doordat gegevens niet juist zijn.

In ieder geval zijn de volgende maatregelen getroffen:

- Bij de invoer van gegevens vindt een kwaliteitscontrole plaats door het verifiëren van gegevens
- ICT-systemen valideren gegevens door middel van invoer controles en validaties.
- ICT-systemen zijn daar waar persoonsgegevens worden gebruikt direct of indirect gekoppeld aan de Basis Registratie Personen zodat altijd wordt beschikt over de actuele gegevens.
- Klanten/cliënten hebben de mogelijkheid gegevens in te zien en te corrigeren indien nodig.

### **Dataminimalisatie**

De gemeente verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

### **Bewaartermijn**

Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven. Bewaartermijnen zijn opgenomen in het register van verwerkingen dat als bijlage is bijgevoegd.

### **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. 5 en 35-42 Wbp en 15-20 AVG. Betrokkenen worden gewezen op hun rechten in het privacystatement dat op de website is geplaatst (zie bijlage) en in de informatie die nieuwe klanten/cliënten krijgen. Zij kunnen hun rechten uitoefenen waarbij de gemeente Dalfsen waarborgt dat verzoeken correct worden afgehandeld.

### **Recht op inzage**

De gemeente Dalfsen kan ook gegevens verwerken van personen die geen directe relatie hebben met de gemeente. Denk hier bijvoorbeeld aan nabestaanden ivm de huur van een graf. Deze persoonsgegevens worden opgevraagd in de landelijke GBA-V database en de personen worden geïnformeerd over de verwerking.

Op de volgende manieren kan een betrokkene inzage krijgen in de gegevens die door de gemeente Dalfsen worden verwerkt:

- door schriftelijk of via het internet inzage te vragen bij de gemeente Dalfsen.
- via de klachtencommissie, als sprake is van een klacht.

Op de volgende manieren kan een betrokkene inzage krijgen in de gegevens die door de gemeente Dalfsen worden verwerkt:

- door inzage te vragen via een van de kanalen die de gemeente Dalfsen aanbiedt
- via de klachtencommissie, als sprake is van een klacht.

### **Afhandeling verzoeken**

Wanneer iemand om inzage vraagt krijgt deze zo snel mogelijk zijn gegevens. De wettelijke termijn is vier weken. Artikel 12, lid 3 van de AVG biedt de mogelijkheid deze termijn met twee maanden te verlengen als er sprake is van complexe verzoeken. Eventueel wordt contact opgenomen met de betrokkene om na te gaan welke informatie gewenst is.

### **Identiteit vrager vaststellen**

De identiteit van de vrager wordt vastgesteld via de Procedure identiteit vaststellen en machtigen. De gemeente verstrekt telefonisch slechts in uitzonderlijke gevallen informatie over personen nadat de identiteit van de gesprekspartner afdoende is vastgesteld.

### **Hoeveelheid informatie en overleg**

Bij een inzageverzoek wordt volgens art. 35 Wbp (15 AVG) ook meegedeeld waarvoor de persoonsgegevens worden gebruikt. Wanneer een inzageverzoek het doel heeft te controleren of iemand goed in het systeem staat, is het overbodig om het volledige dossier inclusief achtergrond toe te sturen.

Een inzageverzoek kan een achterliggend motief hebben, anders dan checken of de gegevens kloppen. De behandelende medewerker moet er alert op zijn dat achter het inzageverzoek geen klacht verscholen ligt.

### **Minderjarigheid**

Wanneer een inzageverzoek wordt gedaan door een minderjarige dan ontvangen ook zijn wettelijke vertegenwoordigers de informatie. Dit wordt vooraf ook aan de minderjarige verteld. Inzageverzoeken voor een minderjarige jonger dan 16 jaar kunnen alleen door, of met toestemming van, een persoon met ouderlijk gezag worden gedaan.

### **Gegevens verbeteren, aanvullen, verwijderen of afschermen**

Een verzoek om inzage kan worden gevolgd door een verzoek de persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. Dit kan als de gegevens feitelijk onjuist of niet volledig zijn

of niet ter zake doen. Een verzoek kan worden ingediend op dezelfde manieren als bij het verzoek om inzage. Aan een verzoek wordt binnen vier weken gehoor gegeven, tenzij er redenen zijn hieraan geen gehoor te geven. In dat geval wordt de betrokkene hiervan op de hoogte gesteld.

### **Bijdrage**

De gemeente Dalfsen vraagt geen bijdrage voor de uitvoer van de rechten van de betrokkene.

### **Geautomatiseerde besluitvorming**

Een besluit waaraan rechtsgevolgen verbonden zijn mag niet worden genomen alleen op basis van geautomatiseerde verwerking. De gemeente Dalfsen past dergelijke verwerkingen niet toe.

### **Relatie met het personeel**

Onder de term personeel worden diegenen bedoeld die door de gemeente Dalfsen conform artikel 1 van de Ambtenarenwet zijn aangesteld als ambtenaar in Algemene dienst.

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.

### **Relatie's met anderen**

De gemeente Dalfsen werkt samen in regionaal verband. Zo kent de gemeente Dalfsen onder andere samenwerkingen op het gebied van zorg en veiligheid. De gemeente Dalfsen dient zorg te dragen dat ook deze samenwerkingspartners vallen onder het privacybeleid of dat er separate afspraken worden gemaakt om de privacy te waarborgen.

### **Algemeen beleid t.a.v. externe leveranciers**

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

### **Overeenkomsten voor levering van ICT diensten - en apparatuur**

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 waarborgt de gemeente Dalfsen 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 gemeente Dalfsen. Alleen verwerkers die afdoende garanties bieden ten aanzien van de bescherming van persoonsgegevens worden ingehuurd. Met alle verwerkers wordt een verwerkersovereenkomst gesloten.

Bij het afsluiten van alle overeenkomsten verwerkers gelden de Algemene Inkoopvoorwaarden van de gemeente Dalfsen, en de aanvullende voorwaarden ICT (bij levering van ICT-diensten en -apparatuur of de verwerking van persoonsgegevens). Wanneer sprake is van de verwerking van persoonsgegevens door een verwerker wordt naast de overeenkomst een verwerkersovereenkomst gesloten en tekent de verwerker voor geheimhouding van de persoonsgegevens.

In deze verwerkersovereenkomst maakt de gemeente Dalfsen 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
- De melding van datalekken. Deze moeten binnen 24 uur gemeld worden
- Doorgifte van persoonsgegevens naar het buitenland
- Verdeling van verantwoordelijkheden met de gemeente Dalfsen 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 is een standaard verwerkersovereenkomst beschikbaar die de gewenste bepalingen bevat.

### **Gebruik verwerkersovereenkomst van verwerker**

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 op minimaal de volgende elementen. Afwijken van deze criteria kan alleen in overleg met de FG. De FG wordt betrokken vanuit zijn taken rondom naleving (art 39 lid 1 onder b AVG) en zijn adviserende rol bij PIA's (art 39 lid 1 onder c AVG). Opgenomen zijn in ieder geval bepalingen:

- De gemeente Dalfsen verwerkt bijzondere gegevens: de verwerker is zich hiervan bewust en treft maatregelen die passend zijn bij deze categorie persoonsgegevens
- Het is verwerkers niet toegestaan gegevens te verwerken voor andere doelen dan is bepaald in de overeenkomst
- De verwerker handelt alleen in opdracht van de verantwoordelijke
- De verwerker is aansprakelijk voor eventuele schade aan de gemeente Dalfsen of aan personen van wie persoonsgegevens zijn verwerkt, voor zover ontstaan door zijn werkzaamheden of (nalaten van) handelen
- De verwerker treft passende maatregelen en is bij voorkeur ISO 27001 gecertificeerd en kan een informatiebeveiligingsplan overleggen
- De gemeente Dalfsen heeft het recht ter plekke onderzoek uit te (laten) voeren door (externe) deskundigen
- Bij datalekken meldt een verwerker deze datalekken binnen 24 uur, neemt actie om lekken te dichten en werkt samen met de gemeente Dalfsen om gevolgen te beperken
- Bij datalekken bij een verwerker worden betrokkenen door de gemeente Dalfsen geïnformeerd
- Vastgesteld wordt of een verwerker sub-verwerkers (AVG: andere verwerkers) mag inschakelen. Sub-verwerkers mogen na schriftelijke toestemming worden ingeschakeld, zolang ze gevestigd zijn binnen de EU, de gegevens alleen binnen de EU verwerkt worden en deze derde partijen minimaal eenzelfde niveau van beveiliging hebben als de verwerker zelf heeft getroffen
  - Persoonsgegevens worden niet buiten de EU opgeslagen en niet in de VS verwerkt. Dit geldt ook voor cloudopslag. De gemeente Dalfsen kan na advies van de FG een uitzondering toestaan
  - Wanneer een verwerker gevestigd is buiten de EU dan heeft de verwerker een vertegenwoordiger in de EU aangewezen
  - De verwerker werkt desgevraagd mee met de toezichthouder
  - De verwerker houdt een overzicht bij van alle categorieën persoonsgegevens die in opdracht van verwerkingsverantwoordelijke worden verwerkt
  - Indien nodig stelt de verwerker een functionaris voor gegevensbescherming aan en stelt hier de gemeente Dalfsen van op de hoogte

### **Beleid t.a.v. derden**

De gemeente Dalfsen gaat zorgvuldig om met persoonsgegevens van klanten/cliënten en derden, zoals bezoekers van de websites, deelnemers aan diensten waarbij persoonsgegevens bij de gemeente Dalfsen terecht komen. Dit is onder andere beschreven in het privacystatement. Het privacystatement van de gemeente Dalfsen is als bijlage toegevoegd

De gemeente Dalfsen maakt voor wat betreft de beschermende maatregelen geen onderscheid tussen klanten en niet-klanten en derden. Het (hoge) niveau van beschermende maatregelen wordt overal toegepast.

### **Informatiebeveiliging**

Voor informatiebeveiliging wordt de Baseline Informatiebeveiliging voor Nederlandse Gemeenten (BIG) gebruikt. Dit is een algemeen geaccepteerde standaard voor beheer van informatiebeveiliging en te treffen maatregelen binnen gemeenten. De informatiebeveiligingsmaatregelen zijn opgenomen in het Gemeentebreed Informatiebeveiligingsbeleid dat in 2015 is vastgesteld en de daarbij behorende bijlagen.

### **Privacy Impact Assessment (PIA)**

Een privacy impact assessment (PIA) is een risicoanalyse om de impact van een nieuwe verwerking, nieuwe technologie, of een andere inrichting van de verwerkingen te bepalen. Een PIA biedt een instru-



ment om te bepalen of de verwerking is toegestaan, of de impact van de verandering opweegt tegen negatieve gevolgen en of ingestelde waarborgen afdoende (kunnen) zijn om risico's en negatieve gevolgen te verminderen.

Daarnaast is in artikel 35, lid 3 van de AVG opgenomen dat bij het grootschalig verwerken van bijzondere categorieën persoonsgegevens een PIA verplicht is. Geadviseerd wordt om registraties waarin gevoelige informatie verwerkt worden periodiek aan een PIA te onderwerpen. In het privacybeheer zullen jaarlijks minimaal drie PIA's worden ingepland en uitgevoerd. De "Procedure uitvoeren PIA" is als bijlage bijgevoegd.

### **Beleid t.a.v. bewustwording en training**

Medewerkers van de gemeente Dalfsen worden periodiek herinnerd aan een goede en zorgvuldige omgang met persoonsgegevens. Periodiek wordt beoordeeld en vastgesteld welke informatiebehoefte de medewerkers hebben ten aanzien van hun basisbewustzijn over de zorgvuldige omgang met persoonsgegevens en specifieke thema's. De informatie hierover kan komen uit de periodieke beoordelingen die op basis van het privacybeheerplan worden opgesteld, signalen of een vraag bij leidinggevenden.

### **Beleid t.a.v. controle en naleving**

Voor het controleren op naleving en de kwaliteit van privacywet- en regelgeving en het privacybeleid is privacybeheer en een privacybeheerorganisatie opgezet. Dit is verder uitgewerkt in het 'privacybeheersysteem gemeente Dalfsen'. Op basis van de opzet van het privacybeheer wordt een privacybeheerplan opgesteld waarin staat beschreven welke activiteiten worden ondernomen om op naleving en verbetering van de kwaliteit te controleren. De controle op de naleving van het privacybeleid wordt als opdracht verstrekt aan de Functionaris gegevensbescherming. Het "privacybeheersysteem gemeente Dalfsen" is als bijlage toegevoegd.

### **Functionaris voor gegevensbescherming**

De gemeente Dalfsen stelt een functionaris voor gegevensbescherming (FG) aan. De FG ziet toe op de volgende organisatieonderdelen en verwerkingsactiviteiten:

- De FG informeert en adviseert de verantwoordelijke over zijn verplichtingen uit hoofde van de wet- en regelgeving.
- De FG ziet toe 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.
- De FG ziet toe op de bewustmaking en de opleiding van het bij de verwerking betrokken personeel.
- De FG kan verantwoordelijk zijn voor het beheren van documentatie en registers zoals:
  - het register van de verwerkingsactiviteiten
  - het register datalekken.

De taken van de FG zijn, naast de wettelijke taken:

- Het ontwikkelen van Interne regelingen.
- Adviseren over technologie en beveiliging (privacy by design).
- Input leveren bij het opstellen of aanpassen van een gedragscode.
- Meldingen van gegevensverwerkingen bijhouden.
- Vragen en klachten van mensen binnen en buiten de organisatie afhandelen.

### **Gegevensverkeer met landen buiten de EU**

- **Inleiding.** Wanneer gegevens verwerkt worden in een land buiten de EU zijn de AVG artikelen 44 en verder van toepassing. Alle landen van de EU werken onder dezelfde verordening waarmee een zorgvuldige verwerking verondersteld wordt. Wanneer gegevens naar een land buiten de EU worden doorgegeven om daar verwerkt te worden, zal verwerkingsverantwoordelijke ook in deze situaties de wet moeten naleven en een zorgvuldige verwerking moeten borgen. Dat kan op een

aantal manieren. Bijvoorbeeld doordat gegevens alleen naar een land worden doorgegeven dat een passend niveau van beveiliging kent. Een overzicht is te vinden op de site van de Europese Commissie. Vervolgens moet duidelijk zijn dat de betreffende organisatie voldoende maatregelen heeft getroffen om de persoonsgegevens te beschermen. Wanneer het betreffende land niet op de lijst voorkomt, bestaan andere mogelijkheden alsnog persoonsgegevens door te geven. Deze mogelijkheden zijn opgenomen in de betreffende AVG-artikelen. Het is de bedoeling alleen met verwerkers samen te werken die voldoende maatregelen hebben getroffen om een zorgvuldige omgang te waarborgen.

- **Beleid.** Het beleid ten aanzien van de overdracht van gegevens naar buiten de EU is opgenomen in Gegevensverkeer met landen buiten de EU
- **Verwerkers en leveranciers.** Van verwerkers en leveranciers is bekend waar zij gegevens opslaan. Gegevens worden alleen buiten de EU opgeslagen wanneer daarover in de verwerkersovereenkomst een afspraak is gemaakt. De algemene inkoopvoorwaarden en de aanvullende bepalingen vormen een verplicht onderdeel in de contractuele afspraken. De opslaglocatie van de gegevens en de locatie van de verwerking van gegevens wordt bijgehouden door de verantwoordelijke afdeling.
- **Cloud.** Wanneer cloudopslag of cloudverwerkingen worden gebruikt wordt in eerste instantie gekozen voor cloudservers binnen de EU.
- **Tracking cookies van derden.** Op websites wordt gebruik gemaakt van tracking cookies zoals van Google Analytics. Via de afname van deze diensten kan informatie over gebruikers van de site verwerkt worden buiten de EU. Ook deze verwerking valt onder het beleid (zie boven). Hoe wordt om gegaan met de cookies wordt opgenomen in de cookiebepaling van het privacystatement dat op iedere website benaderbaar is.

## Datalekken en beveiligingsincidenten

Per 1 januari 2016 is de meldplicht datalekken van kracht en is opgenomen in artikel 34a Wbp. In de AVG is dit opgenomen in de artikelen 33 en 34. Wanneer beveiligingsmaatregelen niet afdoende zijn gebleken en persoonsgegevens (mogelijk) zijn gelekt, kan sprake zijn van een datalek. Binnen de gemeente Dalfsen is het proces meldplicht datalekken opgezet en van kracht. In dit proces is beschreven hoe de organisatie reageert op datalekken. De procedure melding datalekken is inmiddels vastgesteld en maakt deel uit van het Gemeentebreed Informatie Beveiligingsbeleid.

## Jaarverslag

Jaarlijks wordt voor 1 februari een privacyjaarverslag opgesteld over het voorgaande jaar. De FG stelt het jaarverslag op in samenwerking met de privacybeheerder en biedt het jaarverslag aan aan de verwerkingsverantwoordelijke. Hierin staan in ieder geval:

- toevoegingen en aanpassingen van het privacybeleid en aanverwante documenten (zoals het privacystatement en de cookiebepaling), aan de hand van vigerende wet- en regelgeving
- een overzicht van toezicht, incidenten en controles op de naleving van genomen maatregelen
- ondernomen acties en adviezen ten aanzien van PIA's
- ondernomen activiteiten ten aanzien van opleidingen en awareness van medewerkers
- een overzicht van uitgevoerde activiteiten, inclusief die van externe partijen, die naleving en kwaliteit van privacybescherming borgen en verbeteren
- een beschrijving van de kwaliteit van naleving van privacywetgeving volgens de FG
- alle overige relevante zaken die voor de verwerkingsverantwoordelijke nodig zijn om het gevoerde beleid te kunnen beoordelen op effectiviteit en kwaliteit, en hierop aanvullend om corrigerende maatregelen te kunnen treffen.

*Aldus vastgesteld door het college van burgemeester en wethouders van de gemeente Dalfsen in haar vergadering van 22 mei 2018.*

*Het college voornoemd,*

*de burgemeester, de gemeentesecretaris/algemeen directeur,*

*drs. H.C.P. Noten drs. J.H.J. Berends*