gemeente Dalfsen

GEMEENTEBLAD

Officiële uitgave van de gemeente Dalfsen

Nr. 45723

3 februari 2022

Privacyreglement Gemeente Dalfsen 2021-2024

Privacyreglement Gemeente Dalfsen 2021-2024

1. Inleiding

In dit reglement staat hoe de gemeente Dalfsen dagelijks omgaat met persoonsgegevens en privacy, en wat er wettelijk wel en niet toegestaan is.

Privacy speelt een belangrijke rol in de relatie tussen de burger en de overheid en staat daarmee hoog op de bestuurlijke agenda. Gemeenten hebben de verantwoordelijkheid over persoonsgegevens en gegevensuitwisseling op alle terreinen waar ze actief zijn. Gemeenten zijn verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens van burgers. Goed en zorgvuldig omgaan met persoonsgegevens is een dagelijkse bezigheid van gemeenten.

Het beschermen van de privacy is complex en wordt steeds complexer door technologische ontwikkelingen, de decentralisaties, grote uitdagingen op het terrein van veiligheid en nieuwe Europese wetgeving. De gemeente Dalfsen vindt het dan ook belangrijk om transparant te zijn over de manier waarop zij met persoonsgegevens omgaat en hoe zij de privacy waarborgt.

De gemeenteraad, het college van burgemeester en wethouders en de burgemeester van de gemeente Dalfsen stellen, ieder voor zover het zijn bevoegdheid betreft, het privacyreglement vast.

2. Wetgeving en definities

De Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) vormen het juridisch kader voor de omgang met persoonsgegevens. In dit beleid worden de begrippen overeenkomstig de AVG gehanteerd. Enkele veelgebruikte begrippen uit de AVG worden onderstaand benoemd, gedefinieerd vanuit de AVG en vertaald naar hedendaagse taal (artikel 4 van de AVG):

Begrip	Definitie vanuit AVG	Vertaalde definitie
Betrokkene	Een geïdentificeerde of identificeerbare natuurlijke persoon.	De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.
Verwerker	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.	De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator 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.	Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld; naam, adres, geboortedatum). Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren of het Burgerservicenummer (BSN).
Data Protection Impact Assessment (DPIA)	Een beoordeling van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.	Met een DPIA worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy.
Verwerkings-verantwoordelijke	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.	Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.
Verwerking	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van	Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen.

	persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, 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.	
Baseline Informatiebeveiliging Overheid (BIO)		De BIO is een normenkader met beveiligingsmaatregelen dat een goed basis-beveiligingsniveau voor de overheid neerlegt.

3. Reikwijdte
De kaders die in dit reglement staan beschreven gelden voor iedereen (zowel intern als voor externe verwerkers) die gegevens verwerken voor of in opdracht van de gemeente Dalfsen.

4. Verantwoordelijke
De gemeenteraad
De gemeenteraad is eindverantwoordelijk om te waarborgen dat persoonsgegevens – die worden verwerkt door de griffie – worden beschermd in overeenstemming met wet- en regelgeving en op een behoorlijke en zorgvuldige manier.

Het college van B&W en de burgemeester
Het college van B&W en de burgemeester zijn eindverantwoordelijk om te waarborgen dat persoonsgegevens – die worden verwerkt door de ambtelijke organisatie – worden beschermd in overeenstemming met wet- en regelgeving en op een behoorlijke en zorgvuldige manier. Er is een directe relatie met de beginselen van behoorlijk bestuur.

Griffie
De griffier is verantwoordelijk voor kaderstelling en sturing en;
- ziet toe op de juiste uitvoering van privacybeleid en –reglement en stuurt op (concern) risico's;
- borgt dat de functionaris voor gegevensbescherming (FG) zijn bevoegdheden ongehinderd kan uitvoeren;
- beoordeelt periodiek het privacybeleid en –reglement.

De medewerkers van de griffie (inclusief inhuur/externen) zijn verantwoordelijk voor de bescherming van de privacy van betrokkenen. Dat betekent dat iedereen zorgt, binnen de kaders van zijn rol/functie, voor:
- een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens;
- het actief kennisnemen van – en deelnemen aan – bewustwordingscampagnes;
- het direct melden van mogelijke datalekken en beveiligingsincidenten;
- het navolgen van instructies en maatregelen om een goede en veilige verwerking mogelijk te maken.

Het directieteam
Het directieteam is verantwoordelijk voor kaderstelling en sturing;
- ziet toe op de juiste uitvoering van privacybeleid en -reglement en stuurt op (concern) risico's;
- borgt dat de functionaris voor gegevensbescherming (FG) zijn bevoegdheden ongehinderd kan uitvoeren;
- beoordeelt periodiek het privacybeleid en –reglement.

Het managementteam, projectleiders en proceseigenaren
Hieronder vallen alle eenheidsmanagers, teamleiders, projectleiders, programmamanagers en proceseigenaren. Zij zijn verantwoordelijk voor:
- het (laten) opstellen, indien nodig, van het voor dat betreffende organisatieonderdeel specifieke protocol en vragen hierover advies aan de privacy officer en FG en leggen het waar nodig aan het college voor ter vaststelling;
- het borgen van wet- en regelgeving, het privacybeleid en privacyreglement;
- het erop toezien dat, waar nodig, een DPIA wordt uitgevoerd;
- zijn verantwoordelijk voor de te nemen maatregelen, die n.a.v. een DPIA, moeten worden getroffen om de privacy van betrokkenen te beschermen.
- indien daar aanleiding toe is, het rapporteren aan het directieteam over naleving van wet- en regelgeving en het privacybeleid, met vertrekking van en afschrift aan de FG;

- het tijdig betrekken van de FG bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens;
- het maken van afspraken met andere organisatieonderdelen over het borgen van de privacy in geval van informatie die stroomt tussen verschillende organisatieonderdelen.

De medewerkers (inclusief inhuur/extern)
Alle medewerkers (inclusief inhuur/externen) en functioneel beheerders zijn verantwoordelijk voor de bescherming van de privacy van betrokkenen. Dat betekent dat iedereen zorgt, binnen de kaders van zijn rol/functie, voor:
- een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens;
- het actief kennisnemen van – en deelnemen aan – bewustwordingscampagnes;
- het direct melden van mogelijke datalekken en beveiligingsincidenten;
- het navolgen van instructies en maatregelen om een goede en veilige verwerking mogelijk te maken.

De functionaris voor gegevensbescherming (FG)
De FG:
- informeert en adviseert over de verplichtingen die de organisatie heeft met betrekking tot de bescherming van persoonsgegevens;
- ziet toe op de naleving van wet- en regelgeving en het door het college vastgestelde beleid met betrekking tot de bescherming van persoonsgegevens;
- ziet toe op het toewijzen van verantwoordelijkheden, bewustmaking en opleiding van de organisatie op het gebied van de bescherming van persoonsgegevens;
- geeft advies over DPIA;
- werkt samen met en treedt op als contactpersoon voor de Autoriteit Persoonsgegevens;
- in samenspraak met de privacy officer evalueren van het privacybeleid, opstellen van voorstellen tot implementatie en aanpassingen van het privacybeleid;
- bewaakt samen met de privacy officer het verwerkingenregister;
- rechtstreeks rapporteren aan het college en/of de gemeenteraad.

De privacy officer
De privacy officer:
- ondersteunt de organisatie bij het ontwikkelen en toepassen van het privacybeleid;
- is het eerste aanspreekpunt in geval van privacyvraagstukken en datalekken;
- bevordert en adviseert de organisatie gevraagd en ongevraagd over de bescherming van persoonsgegevens en het toepassen van het privacybeleid;
- controleert en evalueert de naleving van wet- en regelgeving en het door het college vastgestelde beleid met betrekking tot de bescherming van persoonsgegevens;
- verzorgt rapportages over de status;
- evalueert, in samenspraak met de FG, het privacybeleid, doet voorstellen tot implementatie en aanpassingen van het privacybeleid;
- rapporteert rechtstreeks aan de FG en het directieteam.

De Concerncontroller – Controller informatiebeveiliging
De concerncontroller / controller informatiebeveiliging rapporteert aan het directieteam en aan de griffier over naleving van wet- en regelgeving en het privacybeleid, richtlijnen en processen.

Naast de bovengenoemde taken en verantwoordelijkheden, zijn per specifiek onderdeel van het privacybeleid taken uitgewerkt in bijlage 1 van dit privacyreglement.

5. Verwerkingen
De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. In de AVG valt onder een verwerking:
- verzamelen, vastleggen en ordenen;
- bewaren, bijwerken en wijzigen;
- opvragen, raadplegen, gebruiken;
- verstrekken door middel van doorzending;
- verspreiding of enige andere vorm van ter beschikkingstellen;
- samenbrengen, met elkaar in verband brengen;
- afschermen, uitwissen of vernietigen van gegevens.

Uit deze opsomming blijkt dat alles wat je met een persoonsgegeven doet een verwerking is.

Doeleinden (artikel 5 van de AVG)
Volgens de wet mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. De gegevens mogen niet voor andere doelen verwerkt worden. Voor de uitvoering van sommige wetten, zoals bijvoorbeeld de Jeugdwet, zijn de doelen voor het verwerken in de wet al vastgelegd, net als de persoonsgegevens die gevraagd en verwerkt mogen worden.

Rechtmatige grondslag (artikel 6 van de AVG)
De wet zegt dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag uit de wet van toepassing moet zijn. Dat betekent dat de verwerking alleen mag plaatsvinden:
- om een verplichting na te komen die in de wet staat;
- voor de uitvoering van een overeenkomst waar de betrokkene onderdeel was;
- om een ernstige bedreiging voor de gezondheid van de betrokkene te bestrijden;
- voor de goede vervulling van de gemeentelijke taak;
- wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking;
- wanneer het belang van de gemeente bij een verwerking zwaarder weegt dan het belang en het recht op privacy van een betrokkene. Dit is niet van toepassing bij de uitvoering van publieke taken.

Wijze van verwerking
De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de wet, en op een zorgvuldige wijze. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De wet gaat uit van subsidiariteit. Dit betekent dat verwerking alleen is toegestaan wanneer het doel niet op een andere manier kan worden bereikt.

In de wet wordt ook gesproken over proportionaliteit. Dit betekent dat persoonsgegevens alleen mogen worden verwerkt als dit in verhouding staat tot het doel. Wanneer met geen, of minder (belastende), persoonsgegevens hetzelfde doel bereikt kan worden moet daar altijd voor gekozen worden.

De gemeente zorgt ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden. Deze gegevens worden alleen verwerkt door personen met een geheimhoudingsplicht. Daarnaast beveiligt de gemeente alle persoonsgegevens. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft.

De kaders hiervoor zijn vastgelegd in het informatieveiligheidsbeleid van de gemeente. Uitwerkingen hiervan liggen vast in procedures en protocollen, gebaseerd op de BIO, die jaarlijks worden geëvalueerd. Een overzicht van de relevante verwante procedures en protocollen is opgenomen in bijlage 2 van dit document. Op de intranetpagina van de gemeente Dalfsen is een actueel overzicht van de toepasselijke procedures en protocollen opgenomen onder het kopje “Privacy en Informatiebeveiliging”.

Doorgifte (artikel 44 t/m 50 van de AVG)
De gemeente geeft alleen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie op grond van goedgekeurde afspraken door de Europese Commissie.

Privacy by design/default (artikel 23 van de AVG)
Privacy by design houdt in dat al tijdens de ontwikkeling van producten en diensten aandacht wordt besteed aan privacy verhogende maatregelen. De gemeente voert dit uit in een vroegtijdig stadium om mogelijke kostbare en tijdrovende aanpassingen te voorkomen. Privacy by default houdt in dat de gemeente technische en organisatorische maatregelen neemt om alleen persoonsgegevens te verwerken die noodzakelijk zijn voor het specifieke doel.

6. Transparantie en communicatie
Via de Wet openbaarheid van bestuur (Wob) is het mogelijk om een verzoek om informatie in te dienen bij de gemeente. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

Wet hergebruik van overheidsinformatie
De Wet hergebruik van overheidsinformatie regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

Informatieplicht (artikel 13 en 14 van de AVG)

De gemeente Dalfsen informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de gemeente geven, worden zij op de hoogte gesteld van de manier waarop de gemeente met persoonsgegevens om zal gaan.

De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de gemeente persoonsgegevens van hem/haar verzamelt en verwerkt en weet voor welk doel dat gebeurt. Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze voor de eerste keer worden verwerkt.

Verwijdering
De gemeente bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van gemeentelijke taken, of zoals vastgelegd in de Archiefwet. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel worden deze zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden, of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren.

Rechten van betrokkenen (artikel 13 t/m 20 van de AVG)
De wet bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten worden ook wel de rechten van betrokkenen genoemd, en bestaan uit de volgende rechten:

Recht op informatie
Betrokkenen hebben het recht om aan de gemeente te vragen of zijn/haar persoonsgegevens worden verwerkt.

Inzagerecht
Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt.

Correctierecht
Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren.

Recht van verzet
Betrokkenen hebben het recht aan de gemeente te vragen om hun persoonsgegevens niet meer te gebruiken.

Recht om vergeten te worden
In gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen.

Recht op bezwaar
Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens. De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

Indienen van verzoek
Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als digitaal worden ingediend. De gemeente heeft één maand de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is (indien dit niet binnen één maand lukt, kan deze termijn met twee maanden worden verlengd). Binnen die termijn zal de gemeente laten weten wat er met het verzoek gaat gebeuren. Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij de gemeente, of een klacht in te dienen bij de Autoriteit Persoonsgegevens. Aan de hand van een verzoek kan de gemeente aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

Geautomatiseerde verwerkingen, profilering (artikel 22 van de AVG)
Profilering vindt plaats wanneer er een geautomatiseerde verwerking van persoonsgegevens wordt verricht waarbij aan de hand van de persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon wordt gekeken om deze persoon te categoriseren en te analyseren, of om zaken te kunnen voorspellen. Voorbeelden van persoonlijke aspecten kunnen zijn: financiële situatie, interesses, gedrag of locatie.

Om profilering wat duidelijker te maken, wordt het volgende voorbeeld gebruikt:
Wanneer een bezoeker op de gemeentelijke website naar een bepaalde dienst kijkt, mag de gemeente geen actie ondernemen om de dienst aan te bieden. Gemeenten mogen wel bekijken hoe vaak een

bepaalde dienst is bekeken, maar zij mogen niet specifiek gericht adverteren. Daarnaast geeft de wet aan dat er geen besluit mag worden genomen op basis van profilering.

Op grond van de AVG is het niet toegestaan om profilering te gebruiken. In het tweede lid van artikel 22 van de AVG worden de uitzonderingen opgesomd:
- noodzakelijk voor de uitvoering van een overeenkomst tussen de betrokkene en verwerkingsverantwoordelijke;
- toegestaan door Nederlands/EU recht;
- na toestemming van de betrokkene.

Inzet van camera's
Binnen de gemeente Dalfsen wordt er onderscheid gemaakt tussen twee vormen van cameratoezicht. Cameratoezicht van gemeentelijke gebouwen (beveiliging) en cameratoezicht ten behoeve van toezicht in de openbare ruimte (openbare orde of veiligheid).
Dit laatste vindt plaats namens de gemeente, na een daartoe strekkend besluit van de burgemeester en wordt gebruikt voor het vergroten van de veiligheid op straat.

Cameratoezicht voor gemeentelijke gebouwen is een ondersteunend middel bij de bescherming van medewerkers en bezoekers alsmede bij de beveiliging van de eigendommen van de medewerkers en bezoekers. Bij cameratoezicht ten behoeve van toezicht in de openbare ruimte werkt de gemeente samen met de politieorganisatie.

Om de privacy zo goed mogelijk te waarborgen worden afspraken over cameratoezicht vastgelegd in een protocol en (indien en voor zover er sprake is van samenwerking met andere partijen) een overeenkomst of convenant.

Bij inzet van camera's voor gemeentelijke doeleinden dient voorafgaand aan deze inzet advies te worden gevraagd aan de FG.

Personeelsvolgsystemen
De gemeente Dalfsen maakt gebruik van tal van digitale apparatuur en programmatuur. Deze apparatuur en programmatuur zijn in staat om het gebruik (doorgaans door medewerkers van de gemeente Dalfsen) te registeren. Het is belangrijk dat de gemeente haar medewerkers informeert over de omvang en het gebruik van deze registraties. Hiervoor zal een separaat document worden opgesteld dat als "addendum personeelsvolgsystemen" wordt toegevoegd aan dit reglement.

7. Plichten van de gemeente Dalfsen
Register van verwerkingen (artikel 30 van de AVG)
De gemeente is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan de gemeente de verwerkingsverantwoordelijke is. Elk register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt en welke gegevens daarvoor worden gebruikt, namelijk:
- de verwerkingsverantwoordelijke en/of de gezamenlijk verwerkingsverantwoordelijke;
- de doelen van de verwerking;
- een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- een beschrijving van de ontvangers van de persoonsgegevens;
- een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisaties;
- de termijnen waarin de verschillende persoonsgegevens moeten worden gewist
- de specifieke taken en verantwoordelijkheden rond het opstellen en bijhouden van het register van verwerkingen zijn uitgewerkt in bijlage 1 van dit privacyreglement.

Data Protection Impact Assessment (DPIA) (artikel 35 van de AVG)
Met een DPIA worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. De gemeente voert deze uit wanneer er een geautomatiseerde verwerking, een grootschalige verwerking, of een grootschalige monitoring van openbare ruimten plaatsvindt of wanneer een verwerking een hoog risico inhouden voor betrokkenen. Dit geldt in het bijzonder voor verwerkingen waarbij nieuwe technologieën worden gebruikt of wanneer verschillende persoonsgegevens met elkaar worden gecombineerd.

De specifieke taken en verantwoordelijkheden rond het opstellen en bijhouden van een DPIA zijn uitgewerkt in bijlage 1 van dit privacyreglement.

Datalekken (artikel 33 en 34 van de AVG)

Er is sprake van een datalek wanneer er een inbreuk ontstaat op de integriteit, vertrouwelijkheid en beschikbaarheid van persoonsgegevens. Hiermee wordt bedoeld: als persoonsgegevens onbedoeld in handen vallen van personen die geen toegang tot die gegevens mogen hebben, vernietigd worden of onbetrouwbaar raken. Wanneer er een datalek heeft plaatsgevonden, maakt de privacy officer een registratie van het incident. Indien het datalek mogelijk gevolgen heeft voor de betrokkene, meldt de gemeente dit zo snel mogelijk, maar uiterlijk binnen 72 uur nadat er kennis van de inbreuk is vernomen, aan de Autoriteit Persoonsgegevens. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval meldt de gemeente dit aan de betrokkenen in duidelijke taal. Om toekomstige datalekken te voorkomen, worden bestaande datalekken geëvalueerd.

Voor het juist en tijdig beoordelen en afwikkelen van datalekken heeft de gemeente Dalfsen een protocol datalekken vastgesteld. Een nadere taakverdeling is te vinden in bijlage 1 van dit privacyreglement en in het datalekkenprotocol.

Aanstellen van Functionaris voor gegevensbescherming (FG) (artikel 37 t/m 39 van de AVG)
Op grond van de AVG is de gemeente verplicht om een FG aan te stellen. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de FG zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van de Autoriteit Persoonsgegevens. Het is niet de bedoeling dat de FG de taken op het gebied van bescherming van de privacy van de eenheden overneemt. De eenheden hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en de gemeentelijke richtlijnen op het gebied van privacy.

8. Afsluiting
Als de gemeente een wettelijke verplichting niet nakomt, kan de betrokkene een klacht indienen. Deze zal via de klachtenregeling van de gemeente worden behandeld.

In gevallen waar het reglement niets over zegt, beslist het verantwoordelijke bestuursorgaan van de gemeente.

Bijlage 1: Overzicht taken en verantwoordelijken

In deze bijlage is de privacy governance van de gemeente Dalfsen voor de processen op het gebied van privacy nader toegelicht.

N.B. Onder het managementteam – genoemd in onderstaande tabellen – worden gerekend: eenheidsmanagers, teamleiders, proceseigenaren, projectleiders en programmamanagers die met de betreffende verwerking zijn belast.

1. Beheer van het register van verwerkingen

Vanuit de AVG is het verplicht een register van verwerkingen op te stellen en actueel te houden van alle gegevensverwerkingen binnen de organisatie. In het register moeten minimaal de volgende gegevens opgenomen worden: van wie gegevens worden verwerkt, welke gegevens worden verwerkt en voor welke doeleinden, hoe lang de gegevens bewaard worden, wie de gegevens ontvangen, of er gegevens buiten de EU worden verstrekt, hoe de gegevens worden beveiligd en de naam en contactgegevens van de verantwoordelijke en van de FG.

Handeling	Managementteam & griffie	Privacy officer	CISO	FG
Actieve aanlevering van nieuwe verwerkingen bij de privacy officer	X			
Zorgdragen voor de actualiteit van verwerkingen(register)	X			
Coördinatie van de actualisatie van het register van verwerkingen		X		
Beheer van het register van verwerkingen		X		
Toetsing op kwaliteit, actualiteit, juistheid en volledigheid van (register van) verwerkingen				X

2. Registratie, beheer en actualisatie van verwerkersovereenkomsten

Als de verantwoordelijke een andere organisatie inschakelt om persoonsgegevens voor haar te verwerken, dan moet met deze organisatie een verwerkersovereenkomst afgesloten worden. In deze overeenkomst moeten de volgende elementen opgenomen worden:

- omschrijving van het onderwerp, de duur, de aard en het doel van de verwerking;
- het soort persoonsgegevens, de categorieën van betrokkenen en de rechten en plichten van de verantwoordelijke;
- verwerking vindt alleen plaats op basis van de schriftelijke instructies van de verantwoordelijke;
- geheimhoudingsplicht voor personen in dienst van of werkzaam voor de verwerker;
- het treffen van passende technisch en organisatorische maatregelen om de verwerking te beveiligen;
- er worden geen subverwerkers ingeschakeld zonder voorafgaande schriftelijke toestemming van de verantwoordelijke;
- de verwerker helpt de verantwoordelijke bij het voldoen van de plichten als betrokkenen hun privacyrechten uitoefenen en voor het nakomen van andere verplichtingen, zoals het melden van datalekken en het uitvoeren van een DPIA;
- na afloop van de verwerkingsdiensten verwijdert de verwerker de gegeven of geeft deze terug (inclusief eventuele kopieën);
- de verwerker werkt mee aan audits.

De gemeente Dalfsen heeft een standaard verwerkersovereenkomst die in principe gebruikt wordt (overeenkomstig het meest recente model van de VNG).

Handeling	Managementteam & griffie	Privacy officer	CISO	FG
Afsluiten van verwerkersovereenkomsten	X			
Actualiseren en beheren van de modelverwerkersovereenkomst		X	X	
Advies aan de organisatie ten aanzien van werken met verwerkers en verwerkersovereenkomsten		X		
Coördinatie registratie verwerkers en archivering van verwerkersovereenkomsten	X			
Toezicht op registratie verwerkers en verwerkersovereenkomsten				X

3. Deelname aan overleg over privacy en informatiebeveiliging

Er is een regulier privacy- en informatiebeveiligingsoverleg waaraan de privacy officer, de CISO en de FG deelnemen. Daarnaast nemen deze personen deel aan overleggen van afdelingen, projectgroepen en werkgroepen waarin privacy- en informatiebeveiligingsvraagstukken aan de orde komen.

Handeling	Managementteam & griffie	Privacy officer	CISO	FG
Voorzitten privacy- en informatiebeveiligingsoverleg				X
Deelnemen aan privacy- en informatiebeveiligingsoverleg		X	X	X
Uitnodigen behandelend specialist voor bijwonen overleggen met privacy- en informatiebeveiligingsvraagstukken	X			
Deelnemen aan project-, team- en themaoverleggen met betrekking tot privacy- en informatiebeveiligingsvraagstukken		X	X	X

4. Afhandeling en veiligheidsincidenten
Een datalek is een inbreuk op de beveiliging van persoonsgegevens. Dit is heel breed. Het kan bijvoorbeeld gaan over een hacker die toegang heeft gekregen tot persoonsgegevens of een brand waarmee de serverruimte wordt vernietigd, een verloren usb-stick met persoonsgegevens of zelfs het versturen van een brief naar een verkeerd adres, waarbij de bewoner de brief ook geopend heeft.

Elke medewerker binnen Dalfsen moet veiligheidsincidenten melden. Het meldingsformulier is opgenomen in Topdesk (button datalek).

Handeling	Managementteam & griffie	Medewerker	Privacy officer	CISO	FG
Inventariseren van feiten en omstandigheden en opstellen verslag feiten en omstandigheden	X	X	X	X	
Uitvoeren analyse	X		X	X	
Verstrekken advies				X	X
In geval van dilemma's in analyse en/of advies afstemmen met de betrokken medewerker(s), gemeentesecretaris en/of burgemeester				X	X
Opstellen en versturen rapportage veiligheidsincident			X	X	
Afstemmen incident en resultaten met secretaris			X	X	
Controle rapportage veiligheidsincident				X	X
Melden datalek bij Autoriteit Persoonsgegevens			X		X
Melden datalek aan betrokkenen	X	X			
Implementeren adviezen uit rapportages	X				
Toetsing op implementatie adviezen					X

5. Advies en voorlichting aan de organisatie
Het goed omgaan met de privacy staat of valt met het gedrag van de personen die de persoonsgegevens verwerken. Het is daarom belangrijk dat alle (griffie)medewerkers, het managementteam, het directieteam, het college en de gemeenteraad goed op de hoogte zijn van wat kan en mag; zij moeten zich bewust zijn van de risico's die het verwerken van persoonsgegevens met zich meebrengen.

Handeling	Managementteam & griffie	Privacy officer	CISO	FG
Gevraagd en ongevraagd advies geven aan bestuur, managementteam en (griffie)medewerkers met betrekking tot privacy- en informatiebeveiligingsvraagstukken		X	X	X
Voorlichting en communicatie over privacy aan de organisatie (bewustwording), inclusief het opstellen van een awareness-plan		X		
Continue aandacht voor privacy op de afdeling	X	X		

6. Uitvoering data protection impact assessment (DPIA)
De AVG verplicht de verantwoordelijke in bepaalde gevallen voor het beginnen van het verwerken van gegevens voor een bepaald doel een DPIA uit te voeren. Dit is nodig als de gegevensverwerking een hoog privacyrisico oplevert voor de mensen van wie de gegevens verwerkt worden. Een goed uitgevoerde DPIA geeft inzicht in de risico's die de verwerking oplevert voor betrokkenen en in de maatregelen die de verantwoordelijke moet nemen om de risico's af te dekken. Daarnaast is het soms ook nodig om een DPIA uit te voeren voor een bestaande gegevensverwerking, bijvoorbeeld als er nog nooit een onderzoek heeft plaatsgevonden of als er veranderingen zijn ten opzichte van de vorige DPIA, zoals het

gebruiken van een nieuwe technologie of als de gegevens voor een ander doel gebruikt worden. Dit is ook nodig als het risico of de omgeving verandert.

Handeling	Managementteam & griffie	Privacy officer	CISO	FG
Initiëren / aanvragen DPIA	X	X		
Uitvoeren DPIA	X	X		
Inhoudelijke en procedurele ondersteuning van de afdeling bij het doorlopen van de DPIA		X	X	
Adviseren over de DPIA				X
Opstellen verslag inclusief aanbevelingen, verwerken en archiveren van de resultaten van de DPIA		X		
Uitvoeren acties / implementeren maatregelen voortkomend uit de DPIA	X			
Toetsen uitgevoerde acties / geïmplementeerde maatregelen		X		X
Toetsen op de procedure, de resultaten, de effectuering en de naleving van de resultaten uit de DPIA				X

7. Afhandeling verzoek rechten van betrokkenen met betrekking tot persoonsgegevens

Onder de AVG heeft de betrokkene een aantal rechten om controle te houden over hun persoonsgegevens. Het gaat hierbij om:

1. recht op inzage;
2. recht op vergetelheid;
3. recht op rectificatie en aanvulling;
4. recht op dataportabiliteit;
5. recht op beperking van verwerking;
6. recht om bezwaar te maken;
7. recht op een menselijke blik bij besluiten;
8. recht op duidelijke informatie over wat met hun persoonsgegevens gebeurt.

Het gaat hier om de rechten 1 tot en met 6. De precieze werkwijze bij het uitvoeren van de rechten van betrokkene is vastgelegd in het "Protocol rechten van betrokkenen".

Handeling	Managementteam & griffie	Privacy officer	CISO	FG
Verantwoordelijk voor het opstellen van procedures voor afhandeling verzoeken		X		X
Ontvangen verzoek, uitzetten vraag binnen de organisatie, verzamelen informatie en terugkoppeling naar aanvrager bij afdelingsoverstijgend verzoek	X	X		
Verzoek uitvoeren	X			
Procedureel en inhoudelijk ondersteunen bij de procedures verzoek rechten van betrokkenen		X		
Optimalisatie van de procedure, verzorgen van communicatie en voorlichting en verkrijgen van draagkracht binnen de organisatie rond de procedures over verzoeken rechten van betrokkenen			X	X
Toezicht op doorlopen procedures verzoek rechten van betrokkenen				X

8. Ontwikkelen en beheer van procedures, formats en beleid

Om ervoor te zorgen dat de medewerkers op een uniforme en goede manier met privacy omgaan moeten procedures, formats en beleid ontwikkeld en beheerd worden.

Handeling	Management team & griffie	Privacy officer	CISO	FG
De ontwikkeling, de optimalisatie en de interne en extern communicatie rond gemeentebrede procedures, formats en beleid met betrekking tot privacy		X	X	X
Vertalen van het gemeentebrede beleid en procedures naar de afdelingsspecifieke situatie (zoals het schrijven van het afdelingsspecifieke privacybeleid en opstellen van afdelingsspecifieke privacyprocedures)	X			
Ten uitvoer brengen van het beleid	X			
Het beheer en de archivering van procedures, formats en beleid met betrekking tot privacy		X		

Toezicht op de kwaliteit, archivering, communicatie en toepassing van de procedures, formats en beleid				X

9. Het ontvangen en behandelen van klachten

Alle personen van wie de gemeente Dalfsen persoonsgegevens verwerkt of gaat verwerken, kunnen zich direct wenden tot de FG. Dit geldt voor vragen, maar ook voor klachten over het handelen van de organisatie met betrekking tot de verwerking van persoonsgegevens.

Handeling	Managementteam & griffie	Privacy officer	CISO	FG
Het ontvangen en afhandelen van vragen en klachten gericht aan de functionaris gegevensbescherming				X

Bijlage 2: Overzicht verwante procedures en protocollen

1. Protocol datalekken, 2021;
2. Protocol rechten van betrokkenen, 2021.