Omgevingsdienst TWENTE

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 373
30 maart
2023

Officiële uitgave van de gemeenschappelijke regeling Omgevingsdienst Twente

Privacy beleid

Auteur.
1 december 2021
Versie 0.4

1 Inleiding

Overheidsorganisaties, waaronder de Omgevingsdienst Twente (OD Twente), verwerken persoonsgegevens om een dienst te verlenen, een product te leveren of om andere doelen te bereiken. Het belang van de organisatie om persoonsgegevens te verwerken kan op gespannen voet staan met het privacybelang van de betrokkene op wie de verzamelde gegevens betrekking hebben.
Het beschermen van privacybelangen wordt vaak gezien als obstakel bij het uitvoeren van de werkzaamheden, omdat moet worden getoetst of aan de privacywetgeving wordt voldaan. Maar privacy is een belangrijk grondrecht. In de Grondwet is verankerd dat de overheid niet zomaar persoonlijke gegevens mag gebruiken. Het is een wettelijke verplichting dat overheidsorganisaties behoorlijk en zorgvuldig omgaan met persoonsgegevens in verband met de privacy van betrokkenen.
OD Twente heeft daarom hoog op de agenda staan om zo goed mogelijk de Europese Algemene Verordening Gegevensbescherming (AVG) na te leven en is zich ervan bewust dat iedereen recht heeft op bescherming persoonsgegevens. De verwerking van persoonsgegevens moet zorgvuldig, rechtmatig en veilig plaatsvinden. Om hier invulling aan te geven is het privacy beleid geformuleerd, waarin beschreven staat hoe om te gaan met de verwerking van persoonsgegevens.
In het privacy beleid staan de kaders beschreven voor het verwerken van privacygevoelige informatie oftewel persoonsgegevens, de bescherming van deze gegevens en omgang met deze gegevens. Dit beleid dient als kapstok, waarbij er kan worden gekozen voor een specifiek vakgebied een beheerplan of privacy protocol op te stellen
De Autoriteit Persoonsgegevens (AP) is de externe toezichthouder op een behoorlijke en zorgvuldige verwerking van persoonsgegevens binnen Nederlandse organisaties, waaronder overheden.
Het dagelijks bestuur van de OD Twente (DB) is verantwoordelijk voor een juiste verwerking van persoonsgegevens.

2 Uitgangspunten

2.1 Doelstellingen van het beleid

Doelstelling van het beleid is dat op een verantwoorde wijze en binnen wettelijke kaders met privacygevoelige gegevens wordt omgegaan. Het wettelijk kader voor bescherming van persoonsgegevens wordt - naast vele specifieke wetten - gegeven door de AVG (Art. 24.2 AVG een organisatorische maatregel is het hebben van een ‘passend gegevensbeschermingsbeleid’, http://www.privacy-regulation.eu/nl/artikel-24-verantwoordelijkheid-van-de-verwerkingsverantwoordelijke-EU-AVG.htm). De eisen die de AVG stelt aan het verwerken van persoonsgegevens zijn dan ook zorgvuldig geïmplementeerd binnen OD Twente.
OD Twente wil hiermee bereiken dat:

- de basis voor een goed geïmplementeerd beleid op het gebied van privacy en informatiebeveiliging wordt gegarandeerd en dat alle medewerkers zich ten volle bewust zijn van de noodzakelijkheid van een zorgvuldige omgang met persoonsgegevens. Dit vormt de basis voor een toepassing van de wettelijke eisen en voor een respectvolle omgang met de persoonsgegevens van betrokkenen;
- de rechten van betrokkenen worden gerespecteerd en in procedures zijn verankerd;
- het vertrouwen van betrokkenen in de overheid niet wordt beschaamd;
- uitvoering van het privacy beleid binnen OD Twente gezamenlijk en integraal, gericht wordt opgepakt, zodat de wettelijke eisen goed geïmplementeerd zijn;
- het onderwerp zowel bestuurlijk als ambtelijk breed wordt gedragen, als onderdeel van zowel uitvoering van de wettelijke opgave, goed werkgeverschap, opdrachtnemerschap en opdrachtgeverschap;
- de kans op financiële schade door het oplopen van boetes en reputatieschade wordt geminimaliseerd.

2.2 Begrippenkader
Begrippen die voor een goede uitvoering van het privacy beleid van groot belang zijn en worden gehanteerd binnen de AVG zijn hierna beschreven.

- Accountability: het kunnen aantonen op welke manier de persoonsgegevens worden verwerkt conform de AVG. Hiertoe dienen passende en effectieve maatregelen te worden genomen, zoals:
  - Documentatieplicht: het bijhouden van een register van verwerkingen;
  - Het beschermen van gegevens door ontwerpprincipes als Privacy by Design en Privacy by Default;
  - Indien van toepassing: het uitvoeren van een Data Protection Impact Assessment (DPIA);
  - Het treffen van passende technische en organisatorische maatregelen, waaronder juridische en beveiligingsmaatregelen;
  - Het opstellen van een procedure om beveiligingsincidenten en datalekken te documenteren, alsmede een procedure voor het melden van een datalek aan AP;
  - Het aanstellen van een Functionaris Gegevensbescherming (FG).

- Betrokkene: de natuurlijke persoon van wie de gegevens worden verwerkt.
- DB: het dagelijks bestuur van ODT.
- Data Protection Impact Assessment (DPIA): methode om de effecten en risico's van nieuwe of bestaande verwerkingen op de bescherming van privacy te beoordelen.
- Functionaris Gegevensbescherming (FG): de FG is de interne toezichthouder op de verwerking van persoonsgegevens. De FG dient in alle onafhankelijkheid zijn werkzaamheden te kunnen uitvoeren en ontvangt daarbij geen instructies van opdrachtgevers of verwerkers. Hij is aangemeld bij de AP als contactpersoon en aanspreekpunt voor de meldingen van datalekken. Hij functioneert als tussenpersoon tussen verschillende belanghebbenden en is daarmee ook verlengstuk van de Autoriteit Persoonsgegevens (AP).
- Governance: de wijze waarop de daadwerkelijke implementatie van richtlijnen en strategie is gegarandeerd, zodat vereiste processen op de juiste manier worden gevolgd om te kunnen voldoen aan wet- en regelgeving. Governance bevat het definiëren van rollen en verantwoordelijkheden, meten en rapporteren, nemen van acties om geïdentificeerde kwesties op te lossen.
- Inbreuk op persoonsgegevens (datalek): een inbreuk op de beveiliging die al dan niet per ongeluk op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.
- Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene) als bedoeld in de AVG of daarvoor in de plaats tredende wetgeving. Naast gewone persoonsgegevens, zoals naam en adresgegevens, zijn er ook bijzondere persoonsgegevens, zoals etnische achtergrond, politieke voorkeur, gezondheid en strafrechtelijke gegevens. In de Uitvoeringswet AVG is bovendien opgenomen dat speciale regels gelden voor verwerking van een nationaal identificatienummer (BSN).
- Privacybescherming: het omgaan met persoonsgegevens conform de eisen in de AVG.
- Proceseigenaren: Degenen die binnen de organisatie zijn aangewezen als verantwoordelijke voor een proces. Zij zijn verantwoordelijk voor de privacybescherming binnen de processen waarvoor zij/hun organisatieonderdeel verantwoordelijk zijn/is.
- Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedures, 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. Ook het publiceren van informatie op het internet kan zo'n verwerking zijn.
- Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die of dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. ODT heeft in de praktijk te maken met meerdere verwerkers waarmee verwerkersovereenkomsten zijn afgesloten.
- Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst die of een ander orgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In de relatie met de deelnemers in de gemeenschappelijke regeling van ODT dient ODT te worden beschouwd als verwerkingsverantwoordelijke. Dat betekent dat ODT zelf verantwoordelijk is voor de naleving van de AVG en daarop aanspreekbaar is.

2.3 Juridisch kader – basiseisen uit de AVG
Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkenen voorop. Er moet worden voorkomen dat er onnodige of te verregaande inbreuken worden gemaakt. De AVG regelt het algemene kader voor de omgang met persoonsgegevens binnen de landen van de Europese unie.

De AVG is de hoogste wetgeving voor privacybescherming en fungeert als een parapluwet die van toepassing is voor alle verwerkingen van persoonsgegevens door organisaties, zowel bedrijven als overheden. De uitgangspunten van de AVG zijn:
Rechtmatigheid, behoorlijkheid, transparantie
Verwerking op rechtmatige, behoorlijke en transparante wijze (artikel 5 lid 1 sub a AVG).

Grondslag en doeleinden
- Verzamelen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (artikel 5 lid 1 sub b AVG);
- Alleen verwerking op één van de in de AVG opgenomen grondslagen (artikel 6 AVG).

Dataminimalisatie
OD Twente verwerkt alleen de persoonsgegevens die noodzakelijk zijn voor een voorafgaand bepaald doel. OD Twente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

Bewaartermijn
De AVG schrijft voor dat gegevens niet langer bewaard mogen worden dan noodzakelijk voor het doel waar ze voor nodig zijn. Dit doel wordt beschreven in verschillende wetten, waardoor de bewaartermijnen van persoonsgegevens uiteen lopen.

Integriteit, vertrouwelijkheid en communicatie
OD Twente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. OD Twente zorgt voor passende beveiliging van persoonsgegevens. Betrokkenen moeten erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. OD Twente maakt daarom inzichtelijk op welke wijze persoonsgegevens worden verwerkt en beheerd. Dit is vastgelegd in het verwerkingsregister en de privacyverklaring.

Delen met derden
Een rechtstreeks gevolg van het uitvoeren van wettelijke taken en regelingen is het verwerken van persoonsgegevens. OD Twente deelt alleen persoonsgegevens als zij hiervoor een wettelijke grondslag heeft. In andere gevallen vragen wij hiervoor toestemming. Een betrokkene moet weten dat zijn of haar gegevens worden verwerkt worden wanneer een melding of aanvraag wordt gedaan. Het is hierom van belang dat OD Twente de betrokkene informeert hoe zijn of haar gegevens worden verwerkt.
Als wij informatie laten verwerken door derden dan maken wij hierover afspraken.
Subsidiariteit
Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt.

Proportionaliteit
De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot en met het te dienen doel van verwerken.

Rechten van betrokkenen
Verzoeken van betrokkenen op het gebied van rechten zoals ‘het recht om vergeten te worden’, ‘het recht op inzage’ en ‘ het recht op rectificatie’ kunnen zonder belemmeringen worden gedaan bij OD Twente. In hoofdstuk 3 worden de rechten van betrokkenen verder behandeld.

3 Rechten van betrokkenen

Binnen de AVG hebben betrokkenen nieuwe privacy rechten gekregen en hun bestaande rechten zijn sterker geworden. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden (accountability).
De rechten van de betrokkene moeten binnen de organisaties op transparante wijze zijn ingericht. Betrokkenen hebben namelijk recht op:
- inzage van gegevens (artikel 15 AVG);
- rectificatie van gegevens (artikel 16 AVG);
- gegevenswissing, oftewel "vergetelheid" (artikel 17 AVG);
- beperking van de verwerking (artikel 18 AVG);
- kennisgevingplicht inzake rectificatie, wissing of beperking (artikel 19 AVG);

- overdraagbaarheid van gegevens, dataportabiliteit (artikel 20 AVG);
- het niet onderworpen worden aan geautomatiseerde besluitvorming (artikel 22 AVG);
- Recht op verzet;
- Recht op informatie.

OD Twente geeft hieraan onder andere uitvoering door betrokkenen op de website helder te informeren hoe van deze rechten kan worden gebruik gemaakt.

3.1 Recht op inzage van gegevens
De betrokkene heeft het recht om van OD Twente uitsluitsel te krijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens.
De betrokkene heeft het recht om te informeren of zijn persoonsgegevens worden verwerkt. Als dat het geval blijkt, heeft hij recht op uitleg over het wat en het hoe, als ook op inzage en een kopie van zijn persoonsgegevens. OD Twente kan verlangen dat de betrokkene zich op adequate wijze identificeert. Het is immers belangrijk dat de gevraagde persoonsgegevens bij de juiste persoon terecht komen. Het recht van inzage is mede bedoeld om uitoefening van de rechten van een rectificatie, gegevenswissing of beperking mogelijk te maken.

3.2 Recht op rectificatie van gegevens
De betrokkene heeft het recht om van OD Twente een rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen, met in achtneming van de doeleinden van de verwerking.
Wanneer verwerkte persoonsgegevens onjuist of onvolledig zijn, heeft de betrokkene het recht deze te laten corrigeren of aanvullen. Dit artikel is een uitwerking van artikel 5, eerste lid onder d, AVG, het beginsel van juistheid van persoonsgegevens. OD Twente en een eventuele verwerker van de persoonsgegevens moeten alle redelijke maatregelen nemen om ervoor te zorgen dat onjuiste persoonsgegevens worden gerectificeerd. Het is daarbij irrelevant of de onjuistheden berusten op een fout van OD Twente of een verwerker.

3.3 Recht op gegevenswissing, recht op "vergetelheid"
De betrokkene heeft het recht van OD Twente wissing van hem betreffende persoonsgegevens te verkrijgen. OD Twente is verplicht persoonsgegevens te wissen wanneer dit van toepassing is.
Op grond van de beginselen van juistheid en opslagbeperking (beide geregeld in artikel 5 AVG) mogen persoonsgegevens niet langer worden bewaard dan nodig is voor het doel van hun verwerking. Het recht van gegevenswissing werkt dit nader uit tot een recht voor de betrokkene om overtollige persoonsgegevens gewist te krijgen met corresponderende plicht voor OD Twente en een eventuele verwerker.

3.4 Recht op beperking van de verwerking
De betrokkene heeft het recht van OD Twente de beperking van de verwerking te verkrijgen. Indien een betrokkene vraagt om beperking van de verwerking, en artikel 18 AVG is van toepassing, dan zal de verwerking tijdelijk worden stopgezet totdat het bezwaar is behandeld of de bezwaren zijn weggenomen.

3.5 Kennisgevingsplicht inzage rectificatie, wissing of beperking
De verwerkingsverantwoordelijke dient iedere ontvanger (niet zijnde betrokkene) aan wie persoonsgegevens zijn verstrekt, in kennis te stellen van elke rectificatie of wissing van betreffende persoonsgegevens of beperking van de verwerking, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. De verwerkingsverantwoordelijke verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.
Wanneer OD Twente een rectificatie, gegevenswissing of beperking van persoonsgegevens van betrokkene uitvoert, worden alle ontvangers van die persoonsgegevens hierover ingelicht. Doel van deze kennisgeving is dat deze ontvangers de betreffende rectificatie, wissing of beperking ook doorvoeren.

3.6 Recht op overdraagbaarheid van gegevens, dataportabiliteit
Naast het al langer bekende recht van inzage in persoonsgegevens bestaat er in de AVG ook het recht van dataportabiliteit, oftewel overdraagbaarheid van persoonsgegevens.
De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en machinaal leesbare vorm te verkrijgen en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt.

3.7 Recht om niet onderworpen te worden aan geautomatiseerde besluitvorming
Bij geautomatiseerde individuele besluitvorming is geen sprake van (noemenswaardige) menselijke tussenkomst zodat eventuele uitkomst kan worden gecorrigeerd. Het is uitsluitend gebaseerd op geau-

tomatiseerde verwerking van persoonsgegevens. OD Twente zal geen persoonsgegevens verwerken op een manier die onder dit artikel valt.

3.8 Recht op verzet
De OD Twente voert publiekrechtelijke taken uit, dit is de grondslag voor gegevensverwerking. Ondanks dat heeft iedere betrokkene het recht om, vanwege bijzondere persoonlijke omstandigheden, te vragen zijn of haar persoonsgegevens niet meer te gebruiken (recht van verzet). De OD Twente zal bij dit verzoek beoordelen of de gegevensverwerking gerechtvaardigd is of dat de bijzondere omstandigheden van de betrokkene dusdanig zijn, dat het verzoek moet worden ingewilligd.

3.9 Recht op informatie
De verwerkingsverantwoordelijke heeft de plicht om het publiek te informeren over de gegevensverwerkingen. Meer specifiek hebben betrokkenen het recht om te weten wat er met hun persoonsgegevens gebeurt en waarom. Ook moeten zij bewust worden gemaakt van de risico's van de gegevensverwerking, de regels die ervoor gelden, de wijze waarop hun rechten worden gewaarborgd en de manier waarop zij hun rechten met betrekking tot de verwerking van gegevens kunnen uitoefenen. De OD Twente heeft dit opgenomen in de privacyverklaring op haar website. Voor de situaties waarin betrokkenen wel moeten en niet hoeven te worden geïnformeerd wordt verwezen naar de AVG en de toelichting daarop.

4 Werkprocessen

4.1 Omgaan met persoonsgegevens
OD Twente verwerkt persoonsgegevens alleen indien het doel van de verwerking kan worden gebaseerd op een van de zes rechtsgrondslagen van artikel 6 AVG. In het merendeel van de gevallen worden persoonsgegevens door de betrokkene zelf verstrekt. Veel gebruikte gegevens of al bekende gegevens die zijn opgenomen in basisregistraties of andere authentieke bronnen, worden daaruit opgevraagd indien OD Twente daartoe toegang heeft. Dit is in overeenstemming met het principe van 'eenmalige uitvraag en meervoudig gebruik' dat door de overheid wordt voorgestaan.

4.2 Bewustwording
Zorgvuldig omgaan met persoonsgegevens is enerzijds een kwestie van het organiseren van een goede informatieveiligheid en het zorgvuldig inrichten van werkprocessen, anderzijds is het een zaak van bewustwording en communicatie. Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het bewustzijn wordt voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. De bedrijfscultuur in zijn geheel moet op een "bewust bekwaam" niveau van omgaan met persoonsgegevens worden gebracht. Er moet een constante afweging worden gemaakt tussen "need to know" en "nice to know", waarbij in de laatste categorie geen persoonsgegevens worden verwerkt.
Het is van groot belang dat medewerkers die daadwerkelijk werken met persoonsgegevens weten wat hun verantwoordelijkheid is en hoe zij zorgvuldig om dienen te gaan met persoonsgegevens. Zij dienen in staat te zijn om te beoordelen welke gegevens nodig zijn voor het uitvoeren van de werkprocessen. Er dienen niet te weinig, maar ook niet te veel gegevens te worden verwerkt (artikel 5.1c AVG). De FG zorgt er samen met de CISO voor dat informatie over gegevensbescherming en informatieveiligheid herhaaldelijk onder de aandacht wordt gebracht van leidinggevenden en medewerkers. Medewerkers worden getraind in privacy-bewust functioneren door middel van richtlijnen, presentaties en workshops. Voor vragen of extra toelichting kunnen de medewerkers terecht bij hun eigen leidinggevenden, die dit kunnen afstemmen met de CISO en/of FG.

4.3 Verplichte maatregelen en procedures
Om te voldoen aan de eisen van de AVG is een aantal maatregelen getroffen en zijn procedures ingericht:
- Alle bij OD Twente gangbare processen waarin persoonsgegevens worden verwerkt zijn in beeld gebracht en vastgelegd in het 'Register van de verwerkingsactiviteiten'. Voor de primaire processen geldt de Product- en Dienstencatalogus (PDC) van OD Twente als basis. Daarnaast is ook van alle overige processen in beeld gebracht welke persoonsgegevens worden verwerkt. Naast de vanuit de AVG verplichte onderdelen van de registratie is in het register tevens vastgelegd of er extra maatregelen nodig zijn ten opzichte van de standaard van de BIO.
- Met verwerkers worden verwerkersovereenkomsten gesloten.
- OD Twente werkt met meerdere geautomatiseerde systemen, zowel voor de primaire als voor de overige processen. Van alle informatiesystemen is vastgelegd welke niveaus van beschikbaarheid, integriteit en vertrouwelijkheid gelden en welke (inrichtings)maatregelen daarbij passen.

- Er is een procedure vastgesteld voor de afhandeling van incidenten en datalekken, het informeren van betrokkenen in geval van een datalek, voor het afhandelen van verzoeken van burgers op grond van de AVG (de rechten van betrokkenen) en voor de organisatie van de informatiebeveiliging.
- In het Register voor aanvragen van betrokkenen wordt bijgehouden welke aanvragen er zijn gedaan door betrokkenen en het afhandelingstraject van de aanvraag. Het zaaksysteem van OD Twente fungeert als zodanig.
- Voor de rechten van betrokkenen zijn werkprocessen opgesteld.

4.4 Bewaren van gegevens
De AVG schrijft voor dat gegevens niet langer bewaard mogen worden dan noodzakelijk voor het doel waar ze voor nodig zijn. Dit doel wordt beschreven in verschillende wetten, daarom lopen de bewaartermijnen van persoonsgegevens uiteen. Daarnaast geldt de Archiefwet voor het bewaren van papieren en elektronische documenten en past OD Twente de selectielijsten voor de archiefbescheiden van gemeentelijke en intergemeentelijke organen en voor provinciale organen toe. Daar waar er geen wettelijke bepaling is die voorziet in een verplichte bewaartermijn, neemt OD Twente een eigen besluit over de bewaartermijn.

4.5 Delen van gegevens
Een rechtstreeks gevolg van het uitvoeren van wettelijke taken en regelingen is het verwerken van persoonsgegevens. Een betrokkene moet daarom inzien dat wanneer er bijvoorbeeld een melding of aanvraag gedaan wordt, dit gepaard gaat met verwerking van zijn of haar gegevens. Het is hierom van belang dat OD Twente de betrokkene informeert hoe zijn of haar gegevens worden verwerkt. OD Twente doet dit in eerste instantie door betrokkenen hierover op de website te informeren en daar ook het Register van de verwerkingsactiviteiten beschikbaar te stellen, derhalve ook in de gevallen waarin de gegevens niet van een betrokkene zijn verkregen. Betrokkenen ontvangen in individuele gevallen ook een ontvangstbevestiging van hun melding of aanvraag.
In sommige situaties kan het nodig zijn dat gegevens worden gedeeld. Het delen van deze gegevens wordt niet uitgevoerd zonder de expliciete toestemming van betrokkenen of wettelijke grondslag. In welke gevallen gegevens worden gedeeld is vermeld in het Register van de verwerkingsactiviteiten.

4.6 Open communicatie
Betrokkenen moeten erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. OD Twente maakt daarom inzichtelijk, door middel van verschillende communicatiekanalen, op welke wijze persoonsgegevens worden verwerkt en beheerd. Onder meer door informatie over de rechten van betrokkenen en contactgegevens van de FG te publiceren op de website. Betrokkenen worden zo gefaciliteerd in het doen van een beroep op een of meerdere van hun rechten. Processen en informatiesystemen die door OD Twente worden gebruikt, zijn zodanig ingericht dat aan de vraag van betrokkenen kan worden voldaan (artikel 12 AVG).

4.7 Meldpunt datalekken
Bij een datalek kan gedacht worden aan het kwijtraken van een USB-stick met persoonsgegevens, inbraak door een hacker, maar ook aan onbevoegde autorisaties in een informatiesysteem of aan het toegestuurd krijgen van informatie met bijzondere persoonsgegevens die niet voor de ontvanger is bestemd (brief of e-mail), het in de post zoekraken van een dossier, enzovoort. Ook het intern verwerken van te veel bijzondere persoonsgegevens is een datalek.
Wanneer er sprake blijkt van een inbreuk in verband met persoonsgegevens, oftewel een datalek, moet dit datalek zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking worden gemeld aan de AP. Een melding aan de AP en/of betrokkene is niet noodzakelijk wanneer het niet waarschijnlijk is dat er een risico is. De betrokkene(n) worden alleen geïnformeerd als er sprake is van een hoog risico. Het gaat hier om datalekken waarvoor de OD Twente verantwoordelijk is. Daaronder vallen ook datalekken die ontstaan bij een derde partij die werkzaamheden uitvoert voor OD Twente. Hierover zijn afspraken vastgelegd in de verwerkersovereenkomsten die OD Twente met externe verwerkers heeft afgesloten.
Een melding moet - indien van toepassing - ook onverwijld aan betrokkenen worden gedaan (artikel 34 AVG). Om aan de wet te kunnen voldoen hanteert OD Twente een procedure voor standaard incidentbeheer: de datalekprocedure die hier goed op aansluit. OD Twente documenteert alle inbreuken i.v.m. persoonsgegevens in de vorm van een Datalekregister.

4.8 Verwerkersovereenkomsten
Bij veel processen worden gegevens verwerkt door derden. Hierbij kan onder andere worden gedacht aan de werkzaamheden die medewerkers van OD Twente uitvoeren via een applicatie in de Cloud. Ook de gemeente Almelo, in haar hoedanigheid als leverancier van de ICT-infrastructuur van OD Twente, is in die zin te beschouwen als een verwerker.

Het verlenen van opdrachten aan derden (verwerkers) brengt risico's met zich mee op het gebied van gegevensverwerking en informatieveiligheid. OD Twente blijft echter verantwoordelijk voor de verwerking van de persoonsgegevens. Het afsluiten van verwerkersovereenkomsten geeft de mogelijkheid erop toe te zien dat ook door verwerkers gegevens juist worden beschermd en juist worden verwerkt (artikel 32 AVG). Bij contracten waar persoonsgegevens door verwerkers worden verwerkt sluit OD Twente dan ook verwerkersovereenkomsten af. In de verwerkersovereenkomsten worden minimaal afspraken gemaakt over:

- de doeleinden waarvoor de gegevens mogen worden verwerkt;
- hoe de verwerker met de persoonsgegevens moet omgaan;
- welke beveiligingsmaatregelen moeten worden genomen;
- welke vormen van toezicht de eigenaar mag uitoefenen;
- de geheimhoudingsplicht;
- inschakeling van derden en onderaannemers;
- de locatie van de data;
- aansprakelijkheid van schade door het niet naleven van regelgeving;
- een exit strategie.

Ten einde te borgen dat er verwerkersovereenkomsten worden gesloten, vormt dit een vast onderdeel in het inkoopproces. De verwerkersovereenkomsten worden opgenomen in het Register voor Verwerkersovereenkomsten en worden gearchiveerd, bij voorkeur samen met de hoofdovereenkomst.

5 Governance

5.1 Verantwoordelijken voor uitvoering en naleving AVG

Het DB van de OD Twente is verantwoordelijk voor de juiste uitvoering van de AVG en naleving van het privacy beleid. Het is verantwoordelijk voor het verwerken van persoonsgegevens door de eigen organisatie en voor de taken die met toepassing van de gemeenschappelijke regeling en van de mandaatbesluiten van de bestuursorganen van gemeenten en provincie door OD Twente worden uitgevoerd. De FG zorgt voor onafhankelijk toezicht en controle op de kwaliteit van de uitvoering van het privacy beleid.
Het DB zal binnen de jaarlijkse planning- en control cyclus het algemeen bestuur (AB) informeren over de toepassing van het beleid.
Op grond van de AVG wordt de uitvoering van het privacy beleid elk jaar door de FG geauditeerd. De FG rapporteert aan het DB. Het afleggen van jaarlijkse verantwoording door de FG doet overigens niet af aan de algemene informatieplicht van het DB aan het AB op grond van artikel 19a van de Wgr.
Het DB meldt bijzonderheden ten aanzien van gegevensverwerking, te denken valt aan ernstige inbreuk op of verlies van persoonsgegevens, afzonderlijk en proactief aan het AB.

5.2 Functionaris Gegevensbescherming

Voor onafhankelijk toezicht en controle op de kwaliteit van de uitvoering van het privacy beleid heeft OD Twente op grond van artikel 37 AVG een FG aangesteld. De FG heeft een onafhankelijke positie in de organisatie. De werkzaamheden die een FG uitvoert hebben een wettelijke grondslag in de artikelen 37 t/m 39 AVG.
De interne verantwoording is gewaarborgd door proceseigenaren binnen OD Twente, zijnde de teammanagers. Zij rapporteren onverwijld bij datalekken conform de vastgestelde datalekprocedure. Afwijkingen van de uitvoering van het privacy beleid worden direct door de FG gerapporteerd aan het DB.
OD Twente maakt afspraken met de FG over een privacy-assessmentplan (voor de evaluatie van de compliance van OD Twente aan de AVG). De FG houdt toezicht op het uitvoeren van het assessmentplan en voert daarnaast zelfstandig controles uit. De FG rapporteert jaarlijks over zijn bevindingen. Daarbij worden risico's beschreven en aanbevelingen gedaan. Daarnaast kan de FG tussentijds over risico's rapporteren en aanbevelingen doen.
Het is de verantwoordelijkheid van het management dat het bestuur in control is en dat de registers op orde zijn. Ook in geval van calamiteiten moeten de procedures goed werken en dient de organisatie in control te zijn. De FG ziet toe op de prioritering van de processen en de wijze van implementatie van maatregelen.

De FG toetst de toepassing van het privacy beleid door OD Twente en treedt op als adviseur op beleidsniveau. De FG heeft, na formeel verzoek, het recht op toegang tot alle informatie en systemen en processen waarin privacygegevens een rol (kunnen) spelen. De FG geniet ontslagbescherming en doet zijn werk vrij van last en opdracht.

De AVG verplicht tot het bijhouden van een register van verwerkingsactiviteiten, ook wel verwerkingsregister genoemd, met aantekeningen van DPIA's. Het management is verantwoordelijk voor de volledigheid, actualiteit en juistheid van dit register.

5.3 Overige registers

- Register van inbreuken op persoonsgegevens, datalekregister (CISO);
- Register voor aanvragen van betrokkenen. OD Twente houdt de overige registers bij.

5.4 Sturing en monitoring

De proceseigenaren zijn verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens die binnen zijn of haar team plaatsvindt. Zij zijn daarom ook verantwoordelijk om te monitoren of persoonsgegevens zorgvuldig worden verwerkt en dienen dit zo nodig bij te sturen.
Een belangrijk uitgangspunt in de AVG, waarop de AP zal gaan handhaven, is accountability: de verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van art. 5.1a AVG en dient dit te kunnen aantonen (verantwoordingsplicht op grond van artikel 5.2 AVG). Proceseigenaren zorgen er dus voor dat zij kunnen aantonen op welke wijze uitvoering is gegeven aan de privacywetgeving binnen hun werkprocessen.

Aldus vastgesteld door het dagelijks bestuur van de Omgevingsdienst Twente op 18 februari 2022