Gemeenschappelijke
Regeling Sociaal

# *Privacybeleid*
# *Gemeenschappelijke Regeling Sociaal*

**Versie september 2022**

# 1. Inleiding

Gemeentelijke organisaties verwerken persoonsgegevens om een dienst te verlenen, een product te leveren of om andere doelen te bereiken. Zij moeten hierbij voldoen aan de privacywetgeving en ervoor zorgen dat zij behoorlijk en zorgvuldig omgaan met de persoonsgegevens. Dit in verband met de bescherming van de privacy van degenen wiens persoonsgegevens worden gebruikt. Privacy is immers een belangrijk grondrecht. In de Grondwet is verankerd dat de overheid niet zomaar persoonlijke gegevens mag gebruiken.

De Europese Algemene Verordening Gegevensbescherming (hierna: AVG) bevat de belangrijkste privacyregels waaraan overheids- en andere organisaties moeten voldoen. In dit privacybeleid staat hoe de Gemeenschappelijke regeling Sociaal van de Drechtsteden (hierna: GR Sociaal) daaraan invulling geeft. Dit beleid is gebaseerd op een modelbeleid van de VNG en is opgesteld.

De Gemeenschappelijke Regeling Drechtwerk heeft een eigen privacybeleid opgesteld maar handelt in de geest van het privacybeleid van de Gemeenschappelijke regeling Sociaal.

De GR Sociaal vindt het belangrijk dat de verwerkingen van persoonsgegevens zorgvuldig, rechtmatig en veilig plaatsvinden. Dat staat in dit privacybeleid. Het bevat de kaders voor het verwerken van persoonsgegevens en de bescherming van en omgang met deze gegevens. Dit beleid dient als een koepel, waaronder de uitvoering in de praktijk plaatsvindt.

Het privacybeleid sluit aan bij het Informatiebeveiligingsbeleid Drechtsteden. Immers, informatiebeveiliging en het veilig en verantwoord werken met persoonsgegevens volgens de AVG overlappen elkaar voor een groot deel. Een goede uitvoering van het Informatiebeveiligingsbeleid zorgt mede voor het borgen van de bescherming van persoonsgegevens.

De Autoriteit Persoonsgegevens (hierna: AP) ziet toe op de behoorlijke en zorgvuldige verwerking van persoonsgegevens binnen Nederlandse organisaties, waaronder overheden. Zij kan handhavend optreden indien zij een overtreding constateert (bijvoorbeeld een boete van maximaal 20 miljoen euro opleggen). Het dagelijks bestuur en algemeen bestuur is verantwoordelijk voor een juiste verwerking van de persoonsgegevens waar hij verantwoordelijk voor is.

# 2. Uitgangspunten

## 2.1 Doelstellingen van het beleid

Dit beleid beschrijft hoe de GR Sociaal verantwoordelijk en binnen wettelijke kaders met persoonsgegevens omgaat.

Het wettelijk kader voor bescherming van persoonsgegevens wordt, naast vele specifieke wetten, gegeven door de AVG en de Uitvoeringswet AVG. De GR Sociaal heeft de eisen uit de AVG en de Uitvoeringswet zorgvuldig geïmplementeerd. Als startpunt is in 2018 een bewustwordingsprogramma voor alle werknemers opgezet. De privacybescherming is zo stapsgewijs verhoogd en vormt de basis voor de vergroting van het privacy-bewustzijn en de verdere professionalisering binnen alle organisaties. Bewustwording over het zorgvuldig omgaan met persoonsgegevens is binnen de GR Sociaal een continue proces.

De GR Sociaal wil hiermee onder andere bereiken dat zij:

- De basis voor een goed geïmplementeerd privacybeleid garanderen en dat alle werknemers zich ten volle bewust zijn van de noodzaak om zorgvuldig om te gaan 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 respecteren en in procedures verankeren.
- Het vertrouwen van betrokkenen in de overheid niet beschamen.
- Draagvlak verkrijgen voor de bescherming van persoonsgegevens binnen alle bestuurlijke en ambtelijke lagen van de GR Sociaal, als onderdeel van de uitvoering van de wettelijke taken, goed werkgeverschap, opdrachtnemerschap en opdrachtgeverschap.
- De kans op financiële schade door het oplopen van boetes en reputatieschade minimaliseren.

## 2.2 Begrippenkader

De volgende begrippen worden in dit privacybeleid gebruikt:

| **Begrip** | **Omschrijving** |
|---|---|
| Accountability | Het kunnen aantonen op welke manier de persoonsgegevens worden verwerkt. Hiertoe dienen passende en effectieve maatregelen te worden genomen, zoals:<br><br>- Documentatieplicht: het bijhouden van een Register van verwerkingen.<br>- Het beschermen van persoonsgegevens door ontwerp principes als Privacy by Design en Privacy by Default.<br>- Het uitvoeren van een Data Protection Impact Assessment (DPIA) indien nodig.<br>- Het treffen en registeren van passende technische en organisatorische maatregelen, waaronder juridische en beveiligingsmaatregelen.<br>- Het opstellen van een procedure om beveiligingsincidenten en datalekken te documenteren en te melden. |

| | |
|---|---|
| | - Het aanstellen van een Functionaris Gegevensbescherming. |
| Betrokkene | De natuurlijke persoon van wie de persoonsgegevens worden verwerkt. |
| Functionaris Gegevens-bescherming (FG) | De FG is de interne toezichthouder op de verwerking van persoonsgegevens. De FG dient onafhankelijk zijn werkzaamheden te kunnen uitvoeren en ontvangt daarbij geen instructies van opdrachtgevers of verwerkers. De FG is formeel aangemeld bij de AP. |
| Gegevensbeschermings-effectbeoordeling (Data Protection Impact Assessment (DPIA) | Een methode om de effecten en risico's van nieuwe of bestaande verwerkingen op de bescherming van de privacy te beoordelen. |
| Governance | De wijze waarop de daadwerkelijke implementatie van het privacybeleid is gegarandeerd, zodat vereiste procedures 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 in verband met persoonsgegevens, ofwel 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 geïdentificeerd of identificeerbaar natuurlijk 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 of gezondheid. |
| Privacybescherming | Het omgaan met persoonsgegevens conform de eisen in de AVG. |
| Privacy-coördinatoren | Werknemers binnen de GR Sociaal die het interne aanspreekpunt zijn over privacybescherming. |
| 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. |

| | |
|---|---|
| Verwerker | Een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die of dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Met een verwerker wordt een verwerkersovereenkomst afgesloten. |
| Verwerkings-verantwoordelijke | Een natuurlijk 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. |
| Werknemer(s) | Met de term werknemer wordt in dit beleid gedoeld op elke persoon die voor de GR Sociaal werkzaam is, op welke titel dan ook. Ook bijvoorbeeld ingehuurde krachten en stagiaires vallen hieronder. |

## 2.3 Juridisch kader – basiseisen uit de AVG

Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkenen voorop. Onnodige of te verregaande inbreuken moeten worden voorkomen. 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:

- Verwerking van persoonsgegevens vindt plaats op rechtmatige, behoorlijke en transparante wijze (artikel 5a AVG).
- Verwerking van persoonsgegevens mag alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (artikel 5b AVG).
- Verwerking van persoonsgegevens mag alleen op een van de in de AVG opgenomen grondslagen (artikel 6 AVG).
- Alleen de persoonsgegevens die voor het beoogde doel noodzakelijk zijn mogen worden verwerkt.
- De persoonsgegevens moeten juist zijn en blijven.
- De persoonsgegevens mogen niet langer bewaard worden dan nodig voor het beoogde doel.
- De persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging.
- De verantwoordelijke moet kunnen aantonen aan deze regels te voldoen.

Persoonsgegevens mogen alleen worden verwerkt voor een duidelijk omschreven doel, de doelbinding. Hieruit kan de grondslag voor verwerking vastgesteld worden. De grondslagen zijn limitatief opgesomd in artikel 6 AVG:

- De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden.
- De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.
- De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.

- De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een ander natuurlijk persoon te beschermen.
- Verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.
- De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen.

Vervolgens moet worden vastgesteld dat de verwerkte persoonsgegevens proportioneel zijn: er worden niet meer gegevens verwerkt dan noodzakelijk voor het uitoefenen van de taak. Ook moet aan het subsidiariteitsbeginsel worden voldaan: de taak kan niet op een voor de betrokkene minder belastende manier worden uitgevoerd.

Er zijn ook enkele bijzondere categorieën van persoonsgegevens. Dit zijn persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken. Ook kan het gaan om genetische en biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid of gegevens over iemands seksueel gedrag of seksuele gerichtheid (artikel 9 AVG). Financiële gegevens en het burgerservicenummer (BSN) zijn gevoelige persoonsgegevens. Het verwerken van bijzondere en gevoelige persoonsgegevens (artikel 9 AVG) en het verder verwerken van reeds verzamelde gegevens (artikel 6.4 AVG), is aan zeer strikte voorwaarden gebonden.

Een betrokkene kan altijd inzage of wijziging van de verwerkte persoonsgegevens vragen.

De GR Sociaal heeft de wettelijke verplichting om gegevensbescherming te borgen. Dit moeten zij doen door passende technische en organisatorische maatregelen te treffen. Informatieveiligheid is hier een groot onderdeel van. Samen met onder andere informatiebeheer, het juridisch kader en privacy-bewustzijn zorgt informatieveiligheid voor de borging van bescherming en beveiliging van persoonsgegevens. De GR Sociaal werkt binnen de kaders van het Informatiebeveiligingsbeleid op basis van de Baseline Informatiebeveiliging Overheid (BIO).

Dit privacybeleid gaat uit van het voldoen aan de eisen van de AVG en de Uitvoeringswet AVG. Daarnaast zijn er diverse specifieke wetten, zoals de Basis Registratie Personen, Wet maatschappelijke ondersteuning, Participatiewet, Wet gemeentelijke schuldhulpverlening en de Politiewet, die aanvullende eisen stellen aan privacybescherming. Deze wetten worden in dit beleidsstuk niet ingevuld. Zij worden bij de uitvoering van die concrete wettelijke taken meegenomen.

## 2.4 Wijze van inrichten gegevensverwerking

Door het cyclische karakter van de aangegeven maatregelen en door privacy vast op de agenda's van de verschillende verantwoordelijken te plaatsen, ontstaat een continue proces van veranderen en verbeteren. De kwaliteit van het omgaan met privacyvraagstukken wordt verhoogd door op verschillende niveaus en vanuit verschillende rollen telkens weer een cyclus van plan-do-check-act te doorlopen. Hierdoor ontstaat een evenwichtig privacybeheersingssysteem. Organisaties werken zo actief aan privacy-bewustzijn, het opbouwen van kennis bij werknemers en aan verantwoorde procesuitvoering.

Leidinggevenden en werknemers moeten zich er voortdurend van bewust zijn dat privacy een normaal en standaard onderdeel van hun werkproces is, waar zorgvuldig mee moet

worden omgegaan. De GR Sociaal kan daarbij advies vragen aan het Juridisch Kenniscentrum (JKC) van de Servicegemeente Dordrecht (SGD) en aan de Adviseurs Gegevensbescherming.

Het borgen van de privacy is onlosmakelijk verbonden met informatiebeveiliging. De beveiliging van persoonsgegevens valt uiteen in twee aspecten: de **bescherming** van persoonsgegevens en het **beveiligen** van informatie. **Bescherming** gaat over het recht van bescherming van de persoonlijke levenssfeer, **beveiliging** is het geheel van maatregelen om een te beveiligen doel te beschermen tegen schadelijke invloeden

De GR Sociaal gaat zorgvuldig om met persoonsgegevens en behandelen deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgen de GR Sociaal voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid.

## 2.5 Doelgroep

Het privacybeleid voor de GR Sociaal is van toepassing op alle taken en processen waar de GR Sociaal voor verantwoordelijk is. Dit privacybeleid en een juiste uitvoering ervan richt zich tot *alle* werknemers binnen de GR Sociaal. Het is vooral gericht op diegenen die werken met persoonsgegevens en op diegenen die namens de GR Sociaal persoonsgegevens verwerken. De bestuurders en het management spelen een belangrijke rol bij de besluitvorming over dit onderwerp en de sturing ervan in de planning- & control cyclus.

## 2.6 Ingangsdatum

Dit beleid is per 1 januari 2022 in werking getreden en vervangt de Drechtsteden brede versies uit 2018 en 2020.

# 3. Rechten van betrokkenen

Met de AVG hebben betrokkenen nieuwe privacy rechten gekregen en zijn hun bestaande rechten sterker geworden. Organisaties die persoonsgegevens verwerken hebben meer verplichtingen gekregen. De nadruk ligt, meer dan onder de voormalige Wbp, 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 recht op:

- Inzage van gegevens (artikel 15 AVG).
- Rectificatie van gegevens (artikel 16 AVG).
- Gegevenswissing, recht op "vergetelheid" (artikel 17 AVG).
- Beperking van de verwerking (artikel 18 AVG).
- Kennisgeving 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.

De GR Sociaal geeft hieraan onder andere uitvoering door betrokkenen op hun website helder te informeren hoe van deze rechten gebruik kan worden gemaakt.

## 3.1 Recht op inzage van gegevens (artikel 15 AVG)

De betrokkene heeft het recht om van de verwerkingsverantwoordelijke inzicht 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 (zie nader artikel 20 AVG). De verwerkingsverantwoordelijke kan verlangen dat de betrokkene zich op adequate wijze identificeert. Het recht van inzage is mede bedoeld om uitoefening van de rechten van een rectificatie (artikel 16 AVG) gegevenswissing (artikel 17 AVG) of beperking (artikel 18 AVG) mogelijk te maken.

## 3.2 Recht op rectificatie van gegevens (artikel 16 AVG)

Wanneer verwerkte persoonsgegevens aantoonbaar onjuist of onvolledig zijn, heeft de betrokkene het recht deze te laten corrigeren of aanvullen. Dit artikel is een uitwerking van artikel 5, lid 1, sub d, het beginsel van juistheid van persoonsgegevens. De verwerkingsverantwoordelijke en de verwerker moeten alle redelijke maatregelen nemen om er voor te zorgen dat onjuiste persoonsgegevens worden gerectificeerd. Het is daarbij irrelevant of de onjuistheden berusten op een fout van de verwerkingsverantwoordelijke of van de verwerker.

## 3.3 Recht op gegevenswissing, recht op "vergetelheid" (artikel 17 AVG)

De betrokkene heeft het recht van de verwerkingsverantwoordelijke zonder onredelijke vertraging, wissing van hem betreffende persoonsgegevens te verkrijgen. De

verwerkingsverantwoordelijke is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer dit van toepassing is.

Op grond van de beginselen van juistheid (artikel 5 lid 1, sub d AVG) en opslagbeperking (artikel 5 lid 1, sub 2 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 de corresponderende plicht voor de verwerkingsverantwoordelijke (en uiteraard zijn verwerkers) om die gegevens te wissen.

## 3.4 Recht op beperking van de verwerking (artikel 18 AVG)

De betrokkene heeft het recht van de verwerkingsverantwoordelijke de beperking van de verwerking te verkrijgen.

Beperking is in artikel 4 AVG gedefinieerd als het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken. Kort gezegd komt het erop neer dat men een tijdelijk slot op de verwerking van persoonsgegevens wil totdat een bezwaar of een probleem is opgelost.

## 3.5 Kennisgevingsplicht inzake rectificatie, wissing of beperking (artikel 19 AVG)

De verwerkingsverantwoordelijke stelt iedere ontvanger (niet zijnde betrokkene) aan wie persoonsgegevens zijn verstrekt, in kennis van elke rectificatie of wissing van betreffende persoonsgegevens of beperking van de verwerking overeenkomstig artikel 16 AVG, artikel 17 AVG en artikel 18 AVG, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. De verwerkingsverantwoordelijke verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.

Wanneer de verwerkingsverantwoordelijke een rectificatie (artikel 16 AVG), gegevenswissing (artikel 17 AVG) of beperking (artikel 18 AVG) van persoonsgegevens van betrokkene uitvoert, is hij verplicht alle ontvangers van die persoonsgegevens hierover in te lichten. Doel van deze kennisgeving is dat deze ontvangers de betreffende rectificatie, wissing of betrekking ook doorvoeren.

## 3.6 Recht op overdraagbaarheid gegevens, dataportabiliteit (artikel 20 AVG)

Naast het al langer bekende recht van inzage in persoonsgegevens (artikel 15 AVG) introduceert de AVG een nieuw recht op 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 (artikel 22 AVG)

Bij geautomatiseerde individuele besluitvorming is geen sprake van (noemenswaardige) menselijke tussenkomst zodat eventuele uitkomsten kunnen worden gecorrigeerd. Het is uitsluitend gebaseerd op geautomatiseerde verwerking van persoonsgegevens.

## 3.8 Recht op bezwaar

Een betrokkene kan onder omstandigheden bezwaar maken tegen de (verdere) verwerking van zijn gegevens en zijn recht op bezwaar inroepen. De verwerkingsverantwoordelijke moet dan de verwerkingen staken.

De betrokkene kan zijn recht op bezwaar in drie situaties inroepen:

1. De betrokkene kan vanwege persoonlijke omstandigheden bezwaar maken tegen verwerkingen die gebaseerd zijn op de grondslagen:
   - noodzakelijk voor de uitoefening van een taak van algemeen belang of openbaar gezag; of
   - het gerechtvaardigd belang van de verwerkingsverantwoordelijke.

   De verwerking moet in dat geval worden gestaakt tenzij er dwingende, gerechtvaardigde gronden zijn waardoor het verwerkingsbelang groter is dan het belang van de betrokkene om de verwerking te laten staken.
2. De betrokkene kan bezwaar maken tegen de verwerking van zijn persoonsgegevens met het oog op direct marketing. Dit recht op bezwaar is absoluut, er moet dus altijd gehoor aan worden geven.
3. De betrokkene kan bezwaar maken tegen de verwerking van zijn gegevens voor wetenschappelijk of historisch onderzoek of voor statistische doeleinden op grond van specifiek met zijn situatie verband houdende redenen. Er moet aan dit bezwaar gehoor worden geven, tenzij de verwerking noodzakelijk is voor de uitvoering van een taak van algemeen belang.

## 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 GR Sociaal heeft dit opgenomen in de privacyverklaring op hun 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

Persoonsgegevens worden alleen verwerkt op grond van een of meer grondslagen uit artikel 6 AVG. Meestal 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. Dit is in overeenstemming met het principe van 'eenmalige uitvraag en meervoudig gebruik' dat door de overheid en de gemeente wordt gepropageerd.

## 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.

Er wordt geïnvesteerd in opleiding, training en communicatie om de bedrijfscultuur in zijn geheel op een "bewust bekwaam" niveau van omgaan met persoonsgegevens te brengen. 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 werknemers die werken met persoonsgegevens weten wat hun verantwoordelijkheid is en hoe zij zorgvuldig om dienen te gaan met persoonsgegevens. Zij moeten in staat 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 ziet toe op de bewustwording en het bewustwordingsniveau. De verantwoordelijkheid om de bewustwording te organiseren ligt bij de organisaties. Werknemers worden getraind in privacy-bewust functioneren door middel van presentaties, workshops en trainingen, door de leermodules in de e-learning omgeving en het altijd voor handen hebben van een interne of externe vraagbaak.

## 4.3 Verplichte maatregelen en procedures

Om te voldoen aan de eisen van de AVG zijn de verplichte registers ingericht. Verder zijn onderstaande maatregelen getroffen:

- In het Informatiebeveiligingsbeleid zijn richtlijnen, primair op basis van de BIO en risico-gedreven, beschreven waaraan processen en informatiesystemen moeten voldoen om de beveiliging van persoonsgegevens te borgen. Deze richtlijnen gelden voor proceseigenaren die nieuwe en bestaande processen en informatiesystemen beheren.
- Er is een procedure voor standaard incidentbeheer ingericht. Dit vormt de basis voor het Register van inbreuk op persoonsgegevens/datalekken.
- Er is een procedure opgesteld waarin is vastgelegd hoe betrokkene(n) worden geïnformeerd bij een datalek.
- Alle gegevensverwerkingen waarin persoonsgegevens worden verwerkt zijn in beeld gebracht en vastgelegd in het Register van verwerkingen, met aantekeningen van DPIA's indien van toepassing.
- Met verwerkers worden verwerkersovereenkomsten gesloten.

## 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. Daar waar er geen wettelijke bepaling is die voorziet in een verplichte bewaartermijn, dienst de GR Sociaal een eigen besluit over de bewaartermijn te nemen. Daarnaast geldt de Archiefwet voor het bewaren van papieren en elektronische documenten. De bewaartermijnen staan vermeld in het register van verwerkingen.

## 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 een melding of aanvraag gedaan wordt, dit gepaard gaat met verwerking van zijn persoonsgegevens. Het is hierom van belang dat de GR Sociaal de betrokkene informeert hoe zijn gegevens worden verwerkt.

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.

## 4.6 Open communicatie

Betrokkenen moeten erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. Dat vertrouwen wordt gecreëerd door inzichtelijk te maken, door middel van verschillende communicatie kanalen, op welke wijze persoonsgegevens worden verwerkt en beheerd. Op de websites van de GR Sociaal is een privacyverklaring te vinden waarin op hoofdlijnen wordt aangegeven welke persoonsgegevens waarom en op welke manier worden verwerkt.

## 4.7 Meldpunt datalekken

Bij een datalek kan gedacht worden aan het kwijtraken van een USB stick met persoons-gegevens, inbraak door een hacker, maar ook aan onbevoegde autorisaties in een informatiesysteem of informatie met (bijzondere) persoonsgegevens toegestuurd krijgen van de GR Sociaal die niet voor de ontvanger is bestemd (brief of e-mail), het in de post zoekraken van een dossier. Ook het intern verwerken van te veel persoonsgegevens is een datalek.

Wanneer er sprake blijkt van een inbreuk in verband met persoonsgegevens moet dit datalek zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking worden gemeld aan de AP. Het gaat hier om datalekken waar de organisaties voor verantwoordelijk zijn. Daaronder vallen ook datalekken die ontstaan bij een derde partij die werkzaamheden uitvoert voor de Drechtsteden. Hierover zijn afspraken vastgelegd in de verwerkersovereenkomsten.

Een melding moet indien van toepassing ook onverwijld aan betrokkenen worden gedaan (artikel 33 AVG). Om aan de wet te kunnen voldoen hanteert de GR sociaal een procedure voor standaard incidentbeheer die hierop aansluit. Het vormt de basis voor het verplichte Register van inbreuken op persoonsgegevens/datalekken. De Functionaris Gegevensbescherming van de GR Sociaal is via het algemeen bestuur gemandateerd voor het melden van datalekken aan de AP.

Het doorgeven van een (vermoedelijk) datalek door betrokkenen is mogelijk via de procedure zoals beschreven op de websites van de Sociale Dienst Drechtsteden.

## 4.8 Verwerkersovereenkomst

Een verwerker is een derde partij die in opdracht van de verwerkersverantwoordelijke persoonsgegevens verwerkt. Bij veel gemeentelijke processen worden gegevens verwerkt door derden. Denk hierbij naast werkzaamheden die uitgevoerd worden door leveranciers (van bijvoorbeeld Cloud-applicaties) ook aan samenwerkingsverbanden.

Het verlenen van opdrachten aan verwerkers brengt risico's met zich mee op het gebied van gegevensverwerking en informatieveiligheid. De GR Sociaal blijft verantwoordelijk voor de verwerking van de gegevens. 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 waarmee persoonsgegevens door verwerkers worden verwerkt sluit de GR Sociaal dan ook verwerkersovereenkomsten af. De modelovereenkomst van de VNG is het uitgangspunt.

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.
- Geheimhoudingsplicht.
- Inschakeling van derden en onderaannemers.
- Locatie van de data.
- Aansprakelijkheid van schade door het niet naleven van regelgeving.
- Exit-strategie.

Om te borgen dat er verwerkersovereenkomsten worden gesloten, vormt dit een vast onderdeel van het inkoopproces. De verwerkersovereenkomsten worden gearchiveerd, bij voorkeur samen met de hoofdovereenkomst.

Overigens is niet iedere derde met wie persoonsgegevens worden gedeeld een verwerker. De AP verwoordt dat als volgt: "Als u als verwerkingsverantwoordelijke aan een andere partij persoonsgegevens verstrekt zodat die andere partij een product of een dienst kan leveren aan een betrokkene, dan is die andere partij zelf verwerkingsverantwoordelijke. De leverancier van het product of de dienst stelt zelf namelijk het doel en de middelen vast voor de verwerking van de persoonsgegevens die hij ontvangt van de opdrachtgever voor het leveren van een product of een dienst aan betrokkene. In dat geval bent u beide verwerkingsverantwoordelijke." Kortom, onder andere het RIEC, de accountant, het UWV en het ABP zijn geen verwerker namens de GR Sociaal, maar verwerkingsverantwoordelijke.

## 4.9 Registers

De AVG verplicht tot het bijhouden van registers. De GR Sociaal beheert de volgende verplichte registers:

- Register van verwerkingen, met aantekeningen van DPIA's.
- Register van inbreuken op persoonsgegevens, datalekken.

# 5. Governance

## 5.1 Verantwoordelijken voor uitvoering en naleving AVG

De bestuursorganen van de GR Sociaal zijn verantwoordelijk voor de juiste uitvoering van de AVG en naleving van het privacybeleid. Zij zijn verantwoordelijk voor het verwerken van persoonsgegevens door de GR Sociaal. Zij hebben deze verantwoordelijkheid gekregen voor alle gemeentelijke processen die door middel van een delegaat bij de GR Sociaal zijn belegd.
De door GR Sociaal aangestelde FG zorgt voor onafhankelijk toezicht en controle op de kwaliteit van de uitvoering van het privacybeleid. Daarnaast zijn er bij GR Sociaal diverse functionarissen aangesteld of taken toebedeeld om de uitvoering van de privacywetgeving en het privacybeleid te ondersteunen en begeleiden. Uitgangspunt daarbij is dat de proceseigenaren verantwoordelijk zijn voor de juiste toepassing van de privacywetgeving in het primaire proces dat onder hun leiding wordt uitgevoerd.

## 5.2 Verantwoording het algemeen bestuur van een gemeenschappelijke regeling

Het dagelijks bestuur informeert binnen de jaarlijkse planning & control cyclus het algemeen bestuur over de toepassing van het beleid. Op grond van de AVG wordt de uitvoering van het privacybeleid elk jaar door de FG geauditeerd. De FG rapporteert aan de secretaris van de GR Sociaal. Het afleggen van jaarlijkse verantwoording door de FG doet overigens niet af aan de algemene informatieplicht van het dagelijks bestuur.

## 5.3 Functionaris Gegevensbescherming

Voor onafhankelijk toezicht en controle op de kwaliteit van de uitvoering van het privacybeleid heeft de GR Sociaal een FG aangesteld (artikel 37 AVG). Deze functie is verplicht voor overheidsorganisaties. De FG heeft een onafhankelijke positie in de organisatie. De werkzaamheden die een FG uitvoert hebben een wettelijke grondslag (artikel 39 AVG).

De FG stelt een privacy-auditplan op en voert dat uit. Ook voert de FG incidentele 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.

De FG toetst de toepassing van de privacyregels, inclusief de nakoming van het privacybeleid, door de GR Sociaal. 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.

## 5.4 Sturing en monitoring

Proceseigenaren zijn verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens binnen de processen van de eenheid waaraan zij leiding geven. Zij zijn daarom ook verantwoordelijk om te monitoren of persoonsgegevens zorgvuldig worden verwerkt en dit zo nodig bij te sturen.

Een belangrijk uitgangspunt in de AVG is accountability: de verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van artikel 5.1a AVG en kan deze 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.