GRSociaal
Sociale Dienst Drechtsteden X Drechtwerk

Privacybeleid

Gemeenschappelijke Regeling Sociaal Drechtsteden

Vastgesteld op XXXXX

Inhoudsopgave

Visie, Ambitie, Kernwaarden en Missie Gemeenschappelijke Regeling Sociaal

"Iedereen een zelfstandig en volwaardig bestaan" is de regionale visie Sociaal Domein Drechtsteden. De ambitie van de Gemeenschappelijke Regeling (GRS) vloeit hier uit voort "Alle inwoners van de Drechtsteden kunnen zelfstandig en volwaardig leven, wonen en meedoen. Waar dat niet lukt, helpen we die mogelijkheden te vergroten."

Deze ondersteuning is opgebouwd uit met 3 kernwaarden:
Mensgericht
De GRS organiseert zijn dienstverlening om de mens heen en op een klantgerichte manier. Dit wordt onder andere bereikt door zoveel mogelijk aan te sluiten op de behoefte, leefwereld en situatie van de inwoners. Transparantie is daarin belangrijk zodat de inwoners precies weten wat ze kunnen verwachten maar ook welke persoonsgegevens er verwerkt worden en voor welke doeleinden.

Samenwerken
Op basis van eigen verantwoordelijkheid wordt er gezamenlijk gewerkt om doelen te bereiken. De GRS streeft ernaar dat de inwoner niet elke keer zijn verhaal opnieuw moet vertellen en dezelfde gegevens meermaals moet aanleveren. Wanneer hulp nodig is dan biedt de GRS deze aan of kijkt buiten de eigen organisatie waar deze hulp aangeboden kan worden. In kader van transparantie geeft de GRS ook aan met welke partijen gegevens uitgewisseld worden.

Vernieuwend
Gedreven door eigen verantwoordelijkheid en nieuwsgierigheid wordt gezocht naar de beste oplossingen. De GRS stimuleert de eigen verantwoordelijkheid en vakmanschap hij de medewerkers. Er wordt uitgegaan van de professionaliteit van de medewerkers. Privacy is een verantwoordelijkheid van elke medewerker van de GRS. Hierin wordt gezocht naar de juiste balans tussen de wettelijke taken, optimale dienstverlening en privacybescherming. De GRS gelooft dat privacybescherming, dienstverlening en werkbaarheid samen kunnen gaan.

Dit allen resulteert in de missie: samen werken aan zelfstandigheid. Dit op gebied van:

- Bieden van zorg en ondersteuning om mensen met een beperking of gezondheidsproblemen zelfstandig te kunnen laten wonen.
- Het geven van advies en ondersteuning bij het vinden van werk.
- Wanneer mensen niet in eigen inkomen voorzien, het verstrekken van bijstand
- Het verzorgen van budgetadvies en schuldhulpverlening voor mensen met financiële problemen.

Het verwerken van persoonsgegevens alsmede het uitwisselen van gegevens is een randvoorwaarde om te werken volgens de visie. De Algemene Verordening Gegevensbescherming (AVG) brengt verplichtingen met zich mee op gebied van het beschermen van persoonsgegevens. De inwoners van de Drechtsteden moeten ervanuit kunnen gaat dat hun persoonsgegevens veilig zijn en er zorgvuldig mee wordt omgegaan.

1. Aanleiding

1.1 Waarom een privacybeleid

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Deze verordening is vastgesteld door het Europees Parlement en de Raad van Ministers van de Europese Unie op 27 april en is van toepassing op de gehele Europese Unie. Voor individuele lidstaten zijn de mogelijkheden tot het vaststellen van aanvullende of afwijkende regelgeving op het gebied van het verwerken van persoonsgegevens hierdoor beperkt. In Nederland kennen wij wel de Uitvoeringwet AVG (UAVG). De AVG is de opvolger van de Wet Bescherming Persoonsgegevens (Wbp).
In Nederland is de Autoriteit Persoonsgegevens (AP) de nationale toezichthouder. Zij zien toe op een behoorlijke en zorgvuldige verweking van persoonsgegevens binnen Nederlandse organisaties. Zij kunnen ook handhavend optreden bij overtredingen en daarbij boetes opleggen.

De GRS verwerkt veel persoonsgegevens met name van burgers, voornamelijk voor het uitvoeren van de wettelijke taken die door middel van delegaat of mandaat[1] door de 7 Drechtsteden gemeenten[2] bij ons zijn belegd. De AVG brengt een aantal verplichtingen met zich mee die de Gemeenschappelijke Regeling Sociaal (GRS) uitdaagt ten aanzien van het beschermen van de persoonsgegevens die zij verwerkt, zowel voor de burgers als voor de medewerkers en andere (keten)partners. Alle betrokkenen moeten er immers vanuit kunnen gaan en op kunnen vertrouwen dat diens persoonsgegevens veilig zijn en er zorgvuldig mee wordt omgegaan. Daarnaast wordt ook de samenleving kritischer en veeleisender en krijgen privacy en informatiebeveiliging steeds meer aandacht ook in de landelijke media. Nieuwe technologieën, kunstmatige intelligente (Artificial Intelligence of AI), de digitale overheid en een integrale aanpak binnen het Sociaal domein stellen nieuwe eisen omtrent de bescherming van persoonsgegevens.

De principes op het gebied van bescherming van persoonsgegevens alsmede de achtergrond, principes en bevoegdheden zijn uitgewerkt in dit privacybeleid. Privacy en hiervoor de verantwoordelijkheid voelen en nemen is belangrijk voor elke individuele medewerker van onze organisatie. Het 'privacyproof' zijn en werken vraagt dan ook inzet van alle medewerkers en een rol voor bestuur en management om dit te waarborgen. Het Dagelijks Bestuur en het Algemeen Bestuur dragen uiteindelijk de (bestuurlijke) eindverantwoordelijkheid voor de juiste verwerking van persoonsgegevens op basis van de Verordening Gemeenschappelijke Regeling Sociaal.

1.2 Doelstelling

Met dit beleid wil de GRS transparant laten zien hoe zij omgaan met de gegevensverwerkingen van klanten en medewerkers, hoe zij invulling geven aan de vereisten vanuit de verschillende wetgevingen[3] en geven zij een kader voor het verantwoord omgaan met persoonsgegevens. Daarnaast worden in dit beleid taken en verantwoordelijkheden beschreven op het gebied van naleving van de privacywetgeving.

Dit beleid is van toepassing op de gehele organisatie (zowel Sociale Dienst Drechtsteden als Drechtwerk) en dient als koepel waaronder de uitvoering in de praktijk plaatsvindt. Nadere uitwerking van dit beleid ligt, waar nodig, vast in specifieke werkafspraken of werkinstructies. Het privacybeleid is een verdere uitwerking van de regionale visie sociaal domein Drechtsteden en het vervolg op deze visie specifiek op gegevensverwerkingen.

---

[1] Artikel 5 en 6 Verordening Gemeenschappelijke Regeling Sociaal: https://zoek.officielebekendmakingen.nl/bgr-2021-1131.html

[2] Alblasserdam, Dordrecht, Hardinxveld-Giessendam (niet voor Drechtwerk), Hendrik-Ido-Ambacht, Papendrecht, Sliedrecht en Zwijndrecht

[3] De AVG , de uitvoeringswet AVG maar ook specifieke wetten zoals de Participatiewet, Wet Gemeentelijke Schuldhulpverlening en de WMO 2015.

De ontwikkeling in het sociaal domein alsmede de organisatieontwikkeling van de GRS staan niet stil. Daarin heeft samenwerking met de regio en ketenpartners een belangrijke rol. Om dit te bewerkstelligen is het verhogen van de privacy bewustwording en de professionalisering van de privacy functie binnen de GRS belangrijk. Een goed privacy beheersing vereist een integrale aanpak, eigenaarschap en een hoog risicobewustzijn. Iedere medewerker is verantwoordelijk voor het naleven van de privacywetgeving alsmede het uitdragen en naleven van dit privacybeleid.

De bewustwording, alsmede de eigenaarschap voelen en nemen, op gebied van de privacy wetgeving is een continu proces en de basis voor een goed geïmplementeerd privacybeleid. Een hoog bewustzijn zorgt voor zorgvuldigheid in de omgang met persoonsgegevens waardoor de inwoners uit de Drechtsteden ook kunnen vertrouwen op de GRS.

1.3 Reikwijdte en verantwoording

De GRS verwerkt persoonsgegevens van medewerkers (inclusief inhuur of andere externen), klanten, derden met een relatie naar de klant, ondernemers en anderen (keten) partners. Gezamenlijk zijn zij de betrokkenen. Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens binnen de processen van de GRS, ongeacht of deze digitaal of handmatig plaatsvinden. Ook verwerkingen die zijn uitbesteed, aan bijvoorbeeld de Servicegemeente Dordrecht, vallen onder dit beleid omdat de eindverantwoordelijkheid nog steeds bij de GRS ligt. Gegevensuitwisselingen met derde partijen zoals bij samenwerkingsverbanden vallen zover het de verwerkingsverantwoordelijkheid van de GRS betreft ook onder dit privacybeleid. Dit privacybeleid en een juiste uitvoering ervan richt zich tot alle werknemers binnen de GRS. Dit privacybeleid is daarmee ook rand voorwaardelijk bij de inrichting van nieuwe processen.

Dit beleid is uitsluitend van toepassing op de AVG binnen de GRS. De Wet Politiegegevens heeft een eigen wetgeving op gebied van verwerkingen van persoonsgegevens. De AVG is hierop niet van toepassing[4]. Hiervoor is separaat een privacybeleid opgesteld gezien de specifieke verwerkingen en aparte wet en regelgeving omtrent gegevensverwerking. .
Materiewetten die aanvullende eisen kunnen stellen aan gegevensverwerking of privacy, zoals de Participatiewet, WMO 2015 of Wet Gemeentelijke Schuldhulpverlening, worden in dit beleidsstuk niet separaat ingevuld. Dit wordt meegenomen in de uitvoering van deze processen en bijvoorbeeld bij het opstellen van het register van verwerkingen of bij het uitvoeren van risicoanalyses (DPIA's).

Dit beleid is vastgesteld door het Managementteam (MT) op 24 oktober 2023 als operationeel verantwoordelijke alsmede het Dagelijks Bestuur (DB) op XXX en het Algemeen Bestuur (AB) op XXX als bestuurlijke eindverantwoordelijke. Dit beleid vervangt eerdere versies.
Het beleid wordt minimaal eens per 3 jaar opnieuw beoordeeld en indien nodig herzien. Indien er aanleiding toe is (zoals bij een organisatieverandering of wetswijziging) kan het beleid eerder herzien worden.

[4] Artikel 2 lid 2d van de AVG.

2. Theoretisch en juridisch kader

2.1 Verwerkingsverantwoordelijke en verwerker

De verwerkingsverantwoordelijke (dit kan zijn een natuurlijk persoon, rechtspersoon, (bestuurs)orgaan of instantie) is degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. De verwerkingsverantwoordelijke is verantwoordelijk voor het naleven van de beginselen vanuit de AVG (hoofdstuk 2.2) alsmede voor het nemen van maatregelen om te waarborgen dat gegevens worden verwerkt binnen de kaders van de AVG en dit aan te kunnen tonen (accountability).

Een verwerker (dit kan zijn een natuurlijk persoon, rechtspersoon, (bestuurs)orgaan of instantie) voert een verwerking uit binnen de doel en middelen die een verwerkersverantwoordelijke heeft vastgesteld. Een verwerker neemt geen beslissingen over de wijze van verwerking, het gebruik van de gegevens, de bewaartermijnen of de verstrekking aan derden.

De GRS voert wettelijke taken uit die door de Drechtsteden gemeenten zijn gedelegeerd of gemandateerd welke staan vastgelegd in de Verordening Gemeenschappelijke Regeling Sociaal[5]. Doorgaans wanneer het delegeerde taken betreft gaan de verwerkingsverantwoordelijkheid over naar de GRS. In het geval van een mandaat zal de GRS in de meeste gevallen een verwerker worden van de gemeente. Daarnaast heeft de GRS een aantal taken uitbesteed aan andere partijen, zoals de Servicegemeente Dordrecht, die dan de verwerker is van de GRS. Hiervoor worden verwerkingsovereenkomsten afgesloten (zie hoofdstuk 2.5)

2.2 Basisbeginselen vanuit de AVG

De AVG regelt een algemeen kader voor de omgang met persoonsgegevens binnen de landen van de Europese Unie. De AVG is de hoogste wetgeving op gebied van privacybescherming en fungeert als een parapluwet. In dit artikel zijn de zes basisbeginselen van de AVG opgenomen. Het is aan de GRS om als verwerkingsverantwoordelijke/verwerker deze beginselen na te leven en dit ook te kunnen aantonen.

<u>Rechtmatigheid, behoorlijkheid en transparantie</u>
Persoonsgegevens mogen door de GRS alleen worden verwerkt indien er een rechtmatige verwerkingsgrondslag bestaat (zie hoofdstuk 2.3). Voor alle betrokkenen moet duidelijk zijn op welke manier gegevens worden verwerkt en welke rechten zij hebben.

<u>Doelbinding</u>
De GRS verwerkt alleen gegevens voor de taken die zij uitvoeren. De persoonsgegevens mogen niet verder verwerkt (bijvoorbeeld delen met derden) worden tenzij er sprake is van een verenigbaar doel. Bij een verenigbaar doel moeten de twee doelen aan elkaar verwant zijn mogen er geen nadelige gevolgen zijn voor de betrokkenen, dan wel extra maatregelen hiervoor getroffen.
Er kan nooit een gerechtvaardigd doel zijn als de wettelijke grondslag ontbreekt.
Er wordt steeds gekeken of het doel niet op een minder ingrijpende manier kan worden bereikt (subsidiariteit).

<u>Minimale gegevensverwerking</u>
De GRS verwerkt enkel gegevens die in verhouding staan tot het doel (proportionaliteit). Wanneer dit doel zonder of met minder persoonsgegevens kan worden bereikt dan zal de GRS dit doen, ook als de betrokkene zelf de gegevens aangeleverd heeft.

[5] Artikel 5 en 6 Verordening Gemeenschappelijke Regeling Sociaal: https://zoek.officielebekendmakingen.nl/bgr-2021-1131.html

Juistheid
De GRS zal altijd alle redelijke maatregelen treffen zodat de persoonsgegevens die verwerkt worden zoveel mogelijk juist en actueel zijn. Indien dit niet zo is moet de GRS deze direct aanpassen of verwijderen (rechten van betrokkenen).

Opslagbeperking
De AVG kent zelf geen concrete bewaartermijnen maar geeft aan dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk is voor de verwerking. De GRS conformeert zich aan de bewaartermijnen zoals opgenomen in de VNG selectielijst[6]. In de VNG selectielijst staan, indien van toepassing, alle bewaartermijnen afkomstig uit de materiewetten opgenomen. Wanneer er geen termijn op basis van de selectielijst is, dan stelt de GRS zelf een termijn vast op basis van noodzakelijkheid. De bewaartermijnen staan allemaal ook opgenomen in het register van verwerkingen van de GRS, (al dan niet vanuit de archiefwet overgenomen).

Integriteit en vertrouwelijkheid
De GRS is verantwoordelijk voor een goede beveiliging van de persoonsgegevens die zij verwerkt. De GRS zorgt onder meer voor een actueel autorisatiebeleid zodat persoonsgegevens beschermd zijn tegen ongeoorloofde of onrechtmatige verwerkingen.

2.3 Grondslagen vanuit de AVG

Om rechtmatig gegevens te verwerken moet er sprake zijn van een grondslag. De AVG kent zes grondslagen; toestemming, uitvoering overeenkomst, wettelijke verplichting, vitaal belang, publiekrechtelijke taak en gerechtvaardigd belang. Hieronder staan de meest voorkomende binnen de GRS nader toegelicht.

Toestemming
Aan toestemming zitten specifieke eisen. Zo moet toestemming in vrijheid worden gegeven en moet er duidelijk en specifiek worden vastgelegd welke persoonsgegevens, voor welk doel en voor welke periode worden verwerkt. De toestemming moet aantoonbaar zijn en een actieve handeling is nodig (een vooraf aangevinkt hokje mag niet). Toestemming mag ook altijd worden ingetrokken.
Voor de GRS kan toestemming alleen in zeer uitzonderlijke gevallen worden gebruikt. Tussen de GRS en zijn medewerkers en tussen de GRS en zijn (portentiele) klanten zit een afhankelijkheidsrelatie. Dat houdt in dat toestemming veelal niet vrijelijk kan worden gegeven.

Wettelijke verplichting
De GRS verwerkt de meeste persoonsgegevens vanuit wettelijke verplichting. Zonder de persoonsgegevens kan de GRS geen uitvoering geven aan de taken die zij gedelegeerd of gemandateerd heeft gekregen. Ook doorgifte van gegevens aan derden kunnen voortvloeien vanuit de wettelijke verplichting (zoals bij de Participatiewet).

Publiekrechtelijke taak/ Algemeen belang
Ter uitvoering van de publiekrechtelijke taak van de GRS kunnen ook persoonsgegevens verwerkt worden. Hierbij kun je denken aan de cameratoezicht op het werkplein van de Sociale Dienst Drechtsteden. Deze dienen om de openbare veiligheid te kunnen waarborgen.

2.4 Bijzondere en gevoelige persoonsgegevens

De AVG beschrijft een aantal categorieën persoonsgegevens die extra privacygevoelig zijn, de bijzondere persoonsgegevens. Het verwerken van bijzondere persoonsgegevens (zoals gegevens over

[6] https://vng.nl/artikelen/selectielijst

gezondheid) verbiedt de AVG tenzij hiervoor een uitzonderingsgrond van toepassing is[7]. Voor de GRS zit die uitzondering in het uitvoeren van een wettelijke taak. Zo kan de GRS de taken vanuit de WMO 2015 niet uitvoeren zonder het verwerken van gegevens over iemands gezondheid.
Strafrechtelijke gegevens worden ook als gevoelig bestempeld en ook hier gelden specifieke uitzonderingen voor[8]. De GRS verwerkt binnen de wettelijke taken onder de AVG bij strafrechtelijke gegevens alleen de 'dat' gegevens en niet de 'wat' gegevens. Bij voorbeeld als een klant in detentie zit en dit gevolgen heeft voor de bijstandsuitkering is de reden van detentie niet noodzakelijk.

Hoewel niet formeel in de AVG opgenomen worden een aantal categorieën persoonsgegevens gezien als gevoelige gegevens, zoals bijvoorbeeld financiële gegevens. De GRS verwerkt voor de uitvoering van zijn taken financiële gegevens zoals informatie over schulden, inkomen en salarisstroken. Ook het Burgerservicenummer (BSN) wordt als een gevoelig persoonsgegeven gezien. In Nederland is er een specifieke bepaling opgenomen in de UAVG met betrekking tot het gebruik van het BSN. Deze mag enkel gebruikt worden als dit wettelijk verplicht is en ook alleen voor het doeleinde zoals beschreven in de betreffende wet. Bij de GRS wordt het BSN gebruikt voor de uitvoering van de wettelijke taken maar bijvoorbeeld niet wanneer iemand bij de informatiebalie algemene informatie opvraagt.

In de privacyverklaring staat specifiek omschreven welke bijzondere en gevoelige persoonsgegevens de GRS verwerkt. De GRS gaat uiterst zorgvuldig om met deze persoonsgegevens en zal ze ook enkel verwerken wanneer dit noodzakelijk is voor de uitvoering van de wetgeving.

2.5 Verantwoordingsplicht

Belangrijk binnen de AVG is de verantwoordingsplicht zoals opgenomen in artikel 5 van de AVG. Voor de processen waar de GRS verwerkingsverantwoordelijk voor is zijn zij verantwoordelijk voor de naleving van de AVG. Bij vragen van bijvoorbeeld de Autoriteit Persoonsgegevens moet de GRS kunnen aantonen dat zij de zes basisbeginselen (hoofdstuk 2.2) naleven. Het is dus niet zo dat de Autoriteit Persoonsgegevens of een betrokkene moet aantonen dat de GRS niet voldoet.
Onderstaande punten tonen de verantwoordingsplicht onder andere aan:

<u>Register van verwerkingen</u>
De GRS houdt een register bij van alle verwerkingen die zij doet. Dit zijn de verwerkingen zowel als verwerkingsverantwoordelijke als van verwerker. Het is daarbij niet van belang of het om basisprocessen gaat of om bijvoorbeeld tijdelijke projecten. Dit register is conform de vereisten uit de AVG[9]. Onder meer de verwerkingsdoeleinden, de categorieën persoonsgegevens, met wie de gegevens gedeeld worden (indien van toepassing) en de bewaartermijnen staan in het verwerkingsregister opgenomen. De GRS heeft extra ook de grondslag van de verwerking opgenomen. De proceseigenaar is verantwoordelijk voor de juistheid van de verwerking van de gegevens waar hij eigenaar van is. Jaarlijks worden de verwerkingen gecontroleerd en geaccordeerd door de proceseigenaar. De proceseigenaar staat ook genoemd bij functienaam in het verwerkingsregister.
Nieuwe verwerkingen worden altijd in samenwerking met de Privacy Coördinator aan het register toegevoegd. Op deze wijze weet de GRS zeker dat alle AVG eisen vooraf getoetst zijn.

<u>DPIA (Data Protection Impact Assesment)</u>
Door middel van een DPIA worden vooraf de privacy risico's in kaart gebracht voor nieuwe verwerkingen van persoonsgegevens. Op deze manier kunnen er voordat de verwerking start direct

[7] Artikel 9 AVG
[8] Artikel 10 AVG
[9] Artikel 30 AVG.

maatregelen getroffen worden. De GRS volgt de richtlijnen vanuit de AVG en de Autoriteit Persoonsgegevens om te bepalen of een verwerking DPIA plichtig is[10].
De FG adviseert op de DPIA's en kijkt mee of de maatregelen afdoende zijn en welk restrisico er mogelijk overblijft. Het is aan het MT als operationeel eindverantwoordelijke en het DB als bestuurlijk eindverantwoordelijke om deze mogelijke restrisico's wel of niet te accepteren. Het advies van de FG is een zwaarwegend advies. Indien daarvan wordt afgeweken zal de GRS dit apart onderbouwd documenteren.
Bij de GRS coördineert de Privacy Coördinator de uitvoering van DPIA's. Het is echter de proceseigenaar die verantwoordelijk is voor de uitvoering van de DPIA en dat het DPIA-proces is doorlopen voordat een nieuwe verwerking start. Reeds uitgevoerde DPIA's zullen elke 3 jaar worden herzien en zo nodig geactualiseerd, tenzij dit eerder nodig is.

Autorisatiebeleid
De GRS verwerkt voor de uitvoering van zijn taken op grote schaal persoonsgegevens, doorgaans van een kwetsbare doelgroep. De AVG vereist dat er voldoende technische en organisatorische maatregelen worden getroffen om de informatieveiligheid zo goed mogelijk te garanderen. De GRS heeft daarom een apart autorisatiebeleid opgesteld die is vastgesteld door het MT. In dit beleid wordt omschreven hoe de GRS omgaat met de autorisaties en eventuele logging op autorisaties.

Datalekkenregister en register rechten van betrokkenen
De GRS houdt een register bij van alle datalekken die plaatvinden bij de GRS, ongeacht of er sprake is van opzet. In dit register staan onder andere de oorzaak, het aantal betrokkene, welke persoonsgegevens het betreft en welke acties (zoals het informeren van de betrokkene of melding aan de Autoriteit Persoonsgegevens) zijn genomen.
De GRS heeft tevens een register waar alle aanvragen met betrekking tot de rechten van betrokkenen (zie hoofdstuk 4.1) staan genoteerd. In dit register staat onder andere de datum van aanvraag, de afdeling en de genomen acties.
Beide registers dragen bij aan het in control blijven van de juiste afhandeling en de handhaving van de (wettelijke) termijnen. Elk kwartaal maakt de Privacy Coördinator een rapportage waarbij ook de datalekken en rechten van betrokkenen worden meegenomen. Deze rapportage wordt gedeeld met de FG, opgavemanagers en het MT.

Privacy by design/ Privacy by default
Om de basisprincipes vanuit de AVG goed toe te passen is het belangrijk om bij het ontwerpen en inrichten van processen of applicaties dit al mee te nemen. Aan de voorkant kan dan al worden gecontroleerd of het proces/ de applicatie voldoet aan de vereisten vanuit de AVG.
De GRS dient als verwerkingsverantwoordelijke aan beide begrippen invulling te geven. Dit gebeurt doordat de GRS bij nieuwe processen en applicaties altijd advies inwint bij de Privacy Coördinator, indien er persoonsgegevens bij betrokken zijn. Privacy by Design met terugwerkende kracht zorgt vaak voor vertragingen en kan zelfs extra kosten met zich meebrengen op moment dat bijvoorbeeld applicaties aangepast moeten worden. De Privacy Coördinator kan adviseren over bijvoorbeeld de rechtmatigheid en dataminimalisatie. Wanneer het een nieuwe applicatie betreft zijn ook de informatiemanager en de informatiebeveiligingsadviseur betrokken. Zeker op het gebied van de Privacy by Default (onderdeel van de Privacy by Design) zal de informatiebeveiligingsadviseur kunnen adviseren om de standaardinstellingen zo privacy-vriendelijk mogelijk te maken en er niet meer gegevens verwerkt worden dan voor het doel noodzakelijk.

[10] https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia

2.6 Privacy overeenkomsten

In hoofdstuk 2.1 staat omschreven dat de GRS in de uitvoering van zijn taken zowel acteert als verwerkingsverantwoordelijke en verwerker voor de Drechtsteden gemeenten. Daarnaast heeft de GRS zelf ook afspraken met derden die zowel zelfstandig verwerkersverantwoordelijke, gezamenlijk verwerkersverantwoordelijk of verwerker kunnen zijn. Om privacy gerelateerde afspraken goed te borgen wordt er als toevoeging aan de hoofdovereenkomst altijd een privacy overeenkomst gesloten, wanneer er sprake is van persoonsgegevens. Deze privacy overeenkomsten zijn dus geen zelfstandige overeenkomsten. Het afsluiten van de overeenkomsten, alsmede het opslaan en beheren van de contracten wordt door de afdeling Contractmanagement gedaan bij de SDD of wanneer het regionale contracten betreft door de Servicegemeente Dordrecht. De Privacy Coördinator kan hierbij adviseren.

Privacy protocol

Wanneer er vanuit de GRS een overeenkomst is met een partij die zelfstandig verwerkingsverantwoordelijk is dan sluit de GRS een Privacy protocol af. Dit protocol is opgesteld met behulp van het juridisch kenniscentrum en wordt jaarlijks indien nodig geactualiseerd.

Overeenkomst gezamenlijke verantwoordelijkheid

In het geval dat de GRS samen met een derde partij verwerkersverantwoordelijke is over een bepaalde set aan persoonsgegevens en ook gezamenlijk doen en middelen bepaald wordt er een overeenkomst gezamenlijke verantwoordelijkheid afgesloten. Het format overeenkomst wordt indien nodig jaarlijks geactualiseerd.

Verwerkersovereenkomst

Indien er sprake is van een verwerkingsverantwoordelijke-verwerker relatie is de verwerkingsverantwoordelijke degene die verantwoordelijk is voor het afsluiten van een verwerkersovereenkomst[11]. Vanuit de Vereniging Nederlandse Gemeenten (VNG) is er een standaard en bindend model die geldig is voor alle overheidsinstanties en derden partij die werken met overheidsinstanties. In dit model zijn alle vereisten vanuit de VNG opgenomen, zoals doeleinden, geheimhouding en beveiligingsmaatregelen. De GRS gebruikt standaard de laatste versie van dit model.

2.7 Informatiebeveiliging en algoritmes

Informatiebeveiliging is een cruciaal onderdeel in de privacybescherming. De GRS werkt daarnaast binnen de kaders van het Informatieveiligheidsbeleid, dat op basis is van de Baseline Informatiebeveiliging Overheid (BIO). Specifieke beveiligingsmaatregelen liggen vastgelegd in het Informatiebeveiligsbeleid.
Informatieveiligheid heeft betrekking tot:

- Beschikbaarheid (het beschikbaar zijn van de informatie en de middelen op het juiste moment)
- Vertrouwelijkheid (het beschermen van informatie tegen onbevoegden)
- Integriteit (is de informatie correct, volledig en controleerbaar)

Algoritmes zijn een set regels en instructies die een computer uitvoert om bijvoorbeeld problemen te analyseren of beslissingen te nemen. Wanneer er gebruik gemaakt wordt van algoritmes dan wordt deze verwerking extra opgenomen in het algoritmeregister. Daarnaast zal er ook een Impact Assessment voor Mensenrechten bij de inzet van Algoritmes (IAMA) worden uitgevoerd.

[11] Artikel 34 AVG

3. Toepassingen door de GRS

3.1 Veilig werken

De GRS werkt zoveel mogelijk digitaal, dus een goede beveiliging is van essentieel belang. Inwoners uit de Drechtsteden moeten kunnen vertrouwen dat hun gegevens veilig zijn. Bij de uitwerking van de beveiligingsmaatregelen (die kunnen zowel technisch, organisatorisch, procesmatig of communicatief van aard zijn) wordt rekening gehouden met de context en de mate van risico.

Thuiswerken/ Mobiele apparaten

Bij de GRS kan er in de meeste gevallen hybride gewerkt worden. Hiervoor zijn er vanuit de GRS laptops, telefoons en tablets beschikbaar. Deze mobiele apparaten worden beheerd vanuit de Servicegemeente Dordrecht. Alleen afdelingshoofden, opgavemanagers en MT-leden kunnen mobiele apparaten aanvragen. De GRS streeft dat alle mobiele apparaten voorzien van zijn MDM (mobile device management) zodat bij verlies of diefstal direct op afstand het apparaat kan worden gewist. Alle apparaten hebben een wachtwoord welke frequent verandert moet worden. Om in te loggen binnen het GRID is een tweestapsverificatie noodzakelijk.
Zowel op kantoor als thuis is elke medewerker zicht bewust van de mogelijke gevoeligheid van de persoonsgegevens die verwerkt kunnen worden. Persoonlijke gesprekken worden niet buiten gevoerd of naast een open raam. In het zeldzame geval van een papieren dossier worden deze niet buiten de locaties van de GRS meegenomen. Ook bij werken op een openbare plek zoals de trein of een café wordt er bij voorkeur gebruikt gemaakt van een versleutelde wifi op de hotspot van de telefoon. Openbare wifi wordt vermeden.

Rapportages

Binnen de GRS zijn er verschillende soorten rapportages die persoonsgegevens bevatten. Dit kan managementinformatie zijn richting bestuurders en gemeenten maar ook rapportages binnen de afdelingen. Daarnaast zijn het rapportages over klanten maar ook over medewerkers, bijvoorbeeld voor kwaliteitsdoeleinden.
Rapportages binnen de GRS kunnen alleen worden aangevraagd door afdelingshoofden en opgavemanagers en uitsluitend voor hun eigen opgave. Indien er sprake is van opgave-overstijgende rapportages dan worden aanvragen gezamenlijk gedaan. Indien mogelijk worden rapportages zoveel mogelijk gepseudonimiseerd (met een sleutel nog herleidbaar tot natuurlijke personen) of geanonimiseerd (niet meer herleidbaar tot natuurlijke personen). Daarnaast wordt er altijd zorgvuldig gekeken naar welke gegevens binnen een rapportage noodzakelijk zijn.
Op het moment dat een derde partij, zoals het Onderzoekscentrum Drechtsteden, gegevens verwerkt voor de GRS wordt er altijd controleert of alle maatregelen (zoals overeenkomsten) zijn getroffen. Hierbij zijn de privacy coördinator en de informatiebeveiligingsadviseur adviserend.

Klantdossiers

Binnen de GRS zijn er vrijwel alleen maar digitale dossiers. Of het nu een klantendossier betreft of een dossier van een medewerker, het is belangrijk dat de persoonsgegevens voldoende beschermd zijn. Naast de technische maatregelen zijn ook organisatorische maatregelen nodig. De GRS heeft voor de toegang tot klantdossiers een Autorisatiematrix vastgesteld. Medewerkers van de GRS mogen alleen persoonsgegevens verwerken wanneer dit voor de uitvoering van de taak noodzakelijk is. Wanneer een klant extra informatie aanlevert die niet noodzakelijk is voor de uitvoering van de taken dat wordt deze informatie ook niet opgeslagen in het dossier. De GRS neemt daarin ook de verantwoordelijkheid om de klant (of derde partij) te informeren dat bepaalde gegevens niet noodzakelijk zijn en hen te wijzen op hun eigen privacy.

Cameratoezicht

De GRS maakt gebruik van cameratoezicht op openbare plaatsen zoals het werkplein, de in- en uitgangen en de spreekkamers. Deze camera's zijn uitsluitend bedoeld ter beveiliging van de burgers

en medewerkers die aanwezig zijn. Er wordt geen gebruik gemaakt van cameratoezicht op de werkplekken die zich bevinden buiten de openbare ruimten.
In de spreekkamers worden enkel in de zogenoemde 'hoog-risico' kamers beeld- en geluidopnames bewaard. Hierop is een DPIA uitgevoerd. De overige spreekkamers hebben enkel een 'live' beeld. Betrokkenen worden geïnformeerd door middel van stickers alsmede dat de medewerkers dit extra aangeven bij aanvang van de gesprekken.

3.2 Integraal werken

De GRS streeft naar een integrale benadering van de inwoner die zich meld en kijkt naar de persoonlijke situatie. Maatwerk is belangrijk voor de GRS. In een aantal gevallen blijkt dat een inwoner zich niet meld met een specifiek probleem op een leefgebied (enkelvoudige problematiek) maar dat er meerdere samenhangende problemen in verschillende leefgebieden spelen binnen 1 gezin (meervoudige problematiek). In dat geval kan een integrale aanpak bijdragen aan een betere dienstverlening richting de inwoner. Zeker in het geval als de betrokkene of de gezinsleden een gevaar voor zichzelf en/of voor zijn/hun omgeving vromen en geen inzicht hebben in de problematiek, waardoor de situatie verergert (meervoudige ernstige problematiek).
Onder integraal werken ziet de GRS het samenwerken met verschillende partijen (o.a. wijkteams en de Drechtsteden gemeenten) waarbij rekening wordt gehouden met alle achterliggende aspecten. Hierbij worden dan verschillende onderdelen binnen het sociaal domein samengebracht om het onderlinge verband in kaart te brengen en indien nodig gezamenlijk aan te pakken. Op deze wijze wordt voorkomen dat de inwoner meerdere malen wordt doorgestuurd, meermaals zijn verhaal moet doen en informatie moet delen en de juiste ondersteuning wordt geboden.

3.3 Gegevensdeling met derden

Vanuit de GRS kunnen er gegevens worden uitgewisseld met derden. Dit kunnen onder meer lokale wijkteams, de gemeenten of zorginstellingen zijn. Indien er sprake is van uitwisseling is hier altijd een grondslag voor en worden de AVG beginselen toegepast. Dat houdt in dat alleen noodzakelijke informatie wordt uitgewisseld en dat de GRS ook transparant is over deze uitwisseling.
De GRS sluit tevens overeenkomsten af met betrekking tot gegevensuitwisseling waarin afspraken gemaakt worden. Dit kunnen bijvoorbeeld samenwerkingsovereenkomsten (convenanten), gegevensleveringsovereenkomsten (GLO's) of soms verwerkersovereenkomsten zijn. De Privacy coördinator kan adviseren bij deze overeenkomsten, echter de verantwoordelijkheid voor de inhoud en het op (laten) stellen ligt bij de proceseigenaar.

De GRS hanteert het uitgangspunt dat persoonsgegevens niet worden doorgegeven aan bedrijven of organisaties buiten de Europese Economische Ruimte (EER). Indien hiervan wordt afgekeken dat worden de geldende richtlijnen van de Autoriteit Persoonsgegevens gevolgd. Daarnaast moet er advies worden ingewonnen bij de FG.

3.4 Taken bij integrale samenwerking

Op het moment dat er sprake is van een meervoudige problematiek kan een integrale aanpak bijdragen aan een betere afstemming van de ondersteuning. De inwoner staat hierbij centraal. Je kunt bij een integrale aanpak 3 verschillende taken van elkaar onderscheiden.

<u>Toeleiding</u>
De klantreis start op het moment dat een inwoner uit de Drechtsteden zich meld bij de GRS (of via een derde zoals een wijkteam wordt aangemeld). Op dat moment vindt de uitvraag plaats bij de klant. Gebaseerd op de uitvraag blijkt of er sprake is van meervoudige problematiek of niet. De inwoner staat hierbij centraal en wordt op transparante wijze meegenomen in de stappen. In gezamenlijkheid kan een integraal plan worden opgesteld. Toeleiding is een gemeentelijke taak, en in geval van delegatie een taak voor de GRS namens de 7 Drechtsteden gemeenten.

Hulpverlening
Nadat er een beschikking of ander besluit is gemaakt vindt er hulpverlening plaats binnen de leefgebieden die van toepassing zijn. In deze fase werken medewerkers van de GRS binnen hun eigen expertise. Hierbij worden ook alleen de gegevens verwerkt die wettelijk gezien noodzakelijk zijn. Op het moment dat er zaken niet lopen zoals afgesproken in de toeleiding is het belangrijk direct te schakelen. Indien nodig dient het plan van aanpak opnieuw te worden bekeken. Binnen het eigen leefgebied van er overlegd worden met collega's en bijvoorbeeld ketenpartners indien dit nodig is voor de uitvoering van deze taken.

Regie of coördinatie
Wanneer er sprake is van een meervoudige vraag en een inwoner weet zijn weg zelf niet te vinden biedt de GRS een integrale regie aan. Binnen de regierol worden lopende hulpverleningstrajecten indien nodig afgestemd en gecoördineerd. Indien nodig kan er tijdig worden bijgesteld. Voor de integrale regierol is samenwerking met de gespecialiseerde partijen nodig. Het draait hier echter voornamelijk om de 'dat-informatie' en niet de 'wat-informatie'. Dat houdt in dat de regievoerder niet inhoudelijk alle persoonsgegevens hoeft te verwerken maar dat hier wordt uitgegaan van de gegevens die noodzakelijk zijn voor het uitvoeren van de regie.

3.5 PDCA-Cyclus

Het Sociaal Domein blijft in verandering en dit vereist ook een continue proces van veranderen en verbeteren bij de GRS. Het doorlopen van de Plan-Do-Check-Act (PDCA) cyclus helpt met het verhogen van de kwaliteit, ook op gebied van omgaan met privacyvraagstukken. Door het volgen van een PDCA-cyclus houdt de GRS dit vast op de agenda van de verschillende verantwoordelijke. Tevens ontstaat een zogenaamd privacybeheersingssysteem waarbij gebouwd wordt aan een steeds grotere en bredere kennis en bewustzijn op gebied van privacybescherming.

De GRS vindt het belangrijk dat continue gewerkt wordt aan de optimalisatie van de dienstverlening voor de klanten. Het is hierbij belangrijk ook nieuwe manieren van werken te ontwikkelen, uit te voeren en de evalueren. Hierbij worden de basisbeginselen van de AVG meegenomen en ook geëvalueerd.

Plan: In deze fase wordt een nieuw proces of bestaand proces geanalyseerd. Hierin worden de wensen meegenomen alsmede de risico's. De Privacy Coördinator kan hierin adviseren. Indien deze aanpassingen gevolgen hebben voor bestaande DPIA's, of er blijkt een nieuwe DPIA nodig te zijn, dan wordt dat in deze fase gedaan.
Do: Op moment dat nieuwe proces duidelijk is en het eventuele DPIA proces is doorlopen dan start de uitvoering.
Check: Afhankelijk van het type proces wordt er op een afgesproken moment geëvalueerd. Bij nieuwe processen of geactualiseerde processen is dit doorgaans tussen de 3 en 12 maanden. Het evalueren gebeurd in een veilig klimaat, waarbij fouten gemaakt mogen worden als deze maar goed worden opgelost. Bij nieuwe of geactualiseerde processen wordt er tevens een check gedaan op de grondbeginselen van de AVG. De verantwoordelijkheid ligt voor deze check bij de proceseigenaren. De privacy coördinator en in aantal gevallen de FG kunnen hierbij adviseren.
Act: Aan de hand van de evaluatie en reflectie, alsmede eventuele interne controles wordt er uitvoering gegeven aan de verbeteracties.

3.6 Bewustwording

De GRS hecht veel waarde aan het conform privacywetgeving inrichten van processen en applicaties, alsmede een goede informatieveiligheid. Maar belangrijker is de kant van gedrag en cultuur.

Bewustwording start met een begrijpelijke en duidelijke communicatie. Het alleen hebben van beleid en maatregelen is niet voldoende.
Voor alle nieuwe medewerkers, inclusief inhuurmedewerkers, is een korte workshop over privacy en informatiebeveiliging onderdeel van het introductieprogramma. Daar bovenop is een halve dag AVG training voorzien in het opleidingsprogramma van de GRS 'Samen Wijzer' en is er voor elke medewerker een (verplichte) e-learning op het gebied van informatieveiligheid.
Elk jaar, doorgaans in oktober, vindt de WIPI (Weet van Informatieveiligheid, Privacy en Integriteit) plaats. Gedurende deze periode (dat kan een week of de hele maand oktober zijn) wordt er op, soms ludieke, wijze aandacht geschonken aan informatieveiligheid, privacy en integriteit.
De GRS wil regelmatig de aandacht vestigen op de eigenaarschap voelen en nemen op gebied van privacywetgeving en de toepassing hiervan. Enerzijds om het bij elke medewerker scherp op het netvlies te houden en het in te bedden in de organisatiecultuur, anderzijds om ook de maatschappelijke ontwikkelingen bij te houden en dit over te brengen binnen de organisatie.
Iedere medewerker is verantwoordelijk voor de naleving van de privacywetgeving. De GRS wil dat elke medewerker ook in staat is zelf een afweging te kunnen maken of een verwerking bijvoorbeeld 'need to know' of 'nice to know' is. De FG ziet toe op de bewustwording en het bewustwordingsniveau.

3.7 Geheimhouding

Iedere medewerker heeft een geheimhoudingsplicht. Bij externe medewerkers of derde die tijdelijk toegang hebben tot persoonsgegevens van de GRS wordt er separaat een geheimhoudingsverklaring opgesteld. De opgavemanagers zijn verantwoordelijk dat de geheimhoudingsverklaringen getekend en bewaard worden. Daarnaast leggen alle medewerkers standaard een ambtseed af.

4. De mens centraal

4.1 Rechten van betrokkenen

Bij de invoering van de AVG hebben betrokkenen nieuwe en sterkere rechten gekregen op het gebied van hun eigen persoonsgegevens. Daarnaast hebben organisaties ook meer verplichtingen gekregen. Hierbij kennen organisaties een grotere verantwoordelijkheid om aan te tonen dat zij zich aan de wet houden. Informatie over de wettelijke rechten van betrokkenen alsmede informatie over de toepassing van deze rechten heeft de GRS helder op hun website gepubliceerd. Betrokkenen voor de GRS zijn naast medewerkers voornamelijk klanten en eventuele derden gelinkt aan de klant (bijvoorbeeld familieleden of huisgenoten).

Recht op informatie (artikel 13 en 14 AVG)

Onder de AVG hebben de betrokkene het recht om te weten wat er met hun persoonsgegevens gebeurd en waarom. De GRS verstrekt aan de betrokkenen welke persoonsgegevens worden verwerkt, het doel hiervan en of de gegevens aan derden worden verstrekt. Een belangrijke kernwaarde van de GRS is mensgericht werken. Belangrijk onderdeel is dat de betrokkene geïnformeerd zijn en worden over de stappen die gezet worden en daarbij ook de persoonsgegevens die de GRS verwerkt.
Informatie over hoe de GRS omgaat met persoonsgegevens is eenvoudig toegankelijk. Op de website staat ten alle tijden een actuele privacyverklaring. Deze wordt jaarlijks, of indien nodig vaker, gecontroleerd. Daarnaast staat ook het privacybeleid gepubliceerd. Indien gewenst kan een papieren versie worden verstrekt.

Recht op inzage van gegevens (artikel 15 AVG)

Alle betrokkene hebben het recht inzicht te krijgen of en zo ja in de persoonsgegevens die een organisatie van hem verwerkt. Daarnaast heeft de betrokkene recht op nadere uitleg (zie recht op informatie) alsmede een kopie van zijn persoonsgegevens. De GRS geeft uitsluitend inzage over eigen persoonsgegevens, tenzij er een wettelijke machtiging is.

Recht op rectificatie van gegevens (artikel 16 AVG)

Wanneer persoonsgegevens aantoonbaar onjuist of onvolledig zijn mag de betrokkene deze laten corrigeren of aanvullen. De GRS heeft de verplichting om zorg te dragen voor de juistheid van de persoonsgegevens. Indien er een rectificatie plaatsvindt zal de GRS alle betrokken partijen informeren (artikel 19 AVG).

Recht op gegevenswissing/ recht op vergetelheid (artikel 17 AVG)

De betrokkene mag een verzoek doen tot gegevenswissing wanneer de betreffende persoonsgegevens niet langer noodzakelijk zijn of wanneer er geen andere bewaarverplichtingen vanuit wetgeving van toepassing is. Indien er een wissing plaatsvindt zal de GRS alle betrokken partijen informeren (artikel 19 AVG).

Recht op beperking van de verwerking (artikel 18 AVG)

De betrokkene mag een beperking (een slot) op de verwerking van persoonsgegevens plaatsen tot bijvoorbeeld een probleem of bezwaar is opgelost. Indien er een beperking op verwerking plaatsvindt zal de GRS alle betrokken partijen informeren (artikel 19 AVG). .

Recht op overdraagbaarheid gegevens (artikel 20 AVG)

Een betrokkene mag zijn gegevens overdragen aan een andere verwerkingsverantwoordelijke wanneer er sprake is van de grondslag toestemming of overeenkomst. De meeste processen binnen de GRS zijn op basis van wettelijke taken. In dat geval kan dit recht niet worden uitgeoefend. Wanneer er sprake is van verhuizing buiten de Drechtsteden kan indien wenselijk of noodzakelijk het dossier worden verstrekt aan de betreffende afdeling(en) van de nieuwe gemeente waar de

betrokkene is ingeschreven. Er is dan echter geen sprake van het overdragen van de gegevens gezien de GRS eigen wettelijke bewaartermijnen kent.

Recht op bezwaar (artikel 21 AVG)
Een betrokkene mag bezwaar maken tegen de (verdere) verwerking van zijn persoonsgegevens. Dat kan bijvoorbeeld vanwege persoonlijke omstandigheden (enkel bij de grondslag algemeen belang of openbaar gezag). De verwerking moet dan gestaakt worden tenzij er dwingende of gerechtvaardigde gronden zijn waardoor het belang van de GRS groter is dan het recht op bezwaar. Dit is een ander recht op bezwaar als wanneer een betrokkene bezwaar aantekent op een besluit van de GRS. De betrokkene mag ook bezwaar maken tegen de verwerking van zijn gegevens voor wetenschappelijk onderzoek of statistische doeleinden. Hieraan geeft de GRS gehoor tenzij er sprake is van een noodzaak voor de uitvoering van een taak van algemeen belang.

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. Hieronder valt ook profilering. De GRS maakt slechts in specifieke gevallen gebruik van geautoriseerde besluitvorming, zoals opgenomen in de privacyverklaring. Een betrokkene heeft het recht om voor die processen een menselijk oordeel aan te vragen, dat kan schriftelijk worden aangevraagd. De GRS doet niet aan geautomatiseerde profilering.

4.2 Uitvoering Rechten van betrokkenen

Een aanvraag om je rechten als betrokkene uit te oefenen[12] moet altijd schriftelijk worden ingediend. Dit kan schriftelijk, via email of door een aanvraag te doen via de website van de Sociale Dienst Drechtsteden[13]. Voor aanvragen via de website is een DigiD noodzakelijk omdat op deze wijze de betrokkene gelegitimeerd kan worden.
Na de aanvraag ontvangt de betrokkene een ontvangstbevestiging binnen 2 werkdagen. Indien nodig neemt een medewerker nog contact op om de uitvraag te specificeren. De GRS informeert de betrokkene binnen 1 maand over het verzoek, dit geldt ook indien het uitvoeren van het verzoek in uitzonderlijke gevallen met 2 maanden verlengd wordt. Verzoeken worden afgehandeld via de vastgestelde procedure van de GRS.
Indien het verzoek wordt toegewezen dan kan een uitdraai van het dossier alleen persoonlijk worden opgehaald en is legitimatie verplicht.

4.3 Datalekken

In het geval van een datalek zijn gegevens onrechtmatig verwerkt, in verkeerde handen gekomen of verloren gegaan. Het maakt hierbij geen verschil of dit doelbewust of per ongeluk is gebeurd. De GRS heeft voor het melden van datalekken een intern proces opgesteld. Alle datalekken worden centraal gecoördineerd door de Privacy Coördinator maar de afhandeling is de verantwoordelijkheid van de opgavemanager en het afdelingshoofd. Datalekken kunnen direct gemeld worden via klantenservice, het contactpersoon of via een formulier op de website.
Wanneer er sprake is van een inbreuk in verband met persoonsgegevens (tenzij het onwaarschijnlijk is dat de inbreuk een risico inhoudt boor de rechten en vrijheden van de betrokkenen) wordt dit direct, binnen 72 uur, gemeld aan de Autoriteit Persoonsgegevens door de Privacy Coördinator of diens vervanger. De GRS houdt een register bij van alle (potentiële) datalekken en zal doorgaans de

[12] Gaat hier om de rechten vanuit artikel 15 t/m 22 AVG
[13] Bij Drechtwerk kan er via de privacy coördinator of via P&O een aanvraag worden gedaan.

betrokkene(n) altijd schriftelijk informeren[14]. Bij elk datalek zal individueel worden gekeken of en welke maatregelen er getroffen kunnen worden.

4.4 Klachten

Een betrokkene heeft het recht een klacht in te dienen of bezwaar te maken tegen de wijze waarop zijn/haar gegevens verwerkt worden. Een klacht kan worden ingediend via het digitale klachtenformulier op de website[15], middels een brief of direct bij de FG. Bij klachten wordt de vastgestelde klachtenprocedure gevolgd. De Privacy Coördinator en de FG zijn altijd betrokken bij klachten omtrent privacy. Klachten worden geïnventariseerd en in de lijn besproken. Indien dit nodig is worden werkprocessen opnieuw bekeken en/of aangepast.
Mochten klachten direct bij de Autoriteit Persoonsgegevens zijn ingediend, dan fungeert de FG als tussenpersoon voor zowel de GRS als voor de Autoriteit Persoonsgegevens.

[14] Conform artikel 33 en 34 AVG
[15] Alleen bij de Sociale Dienst Drechtsteden

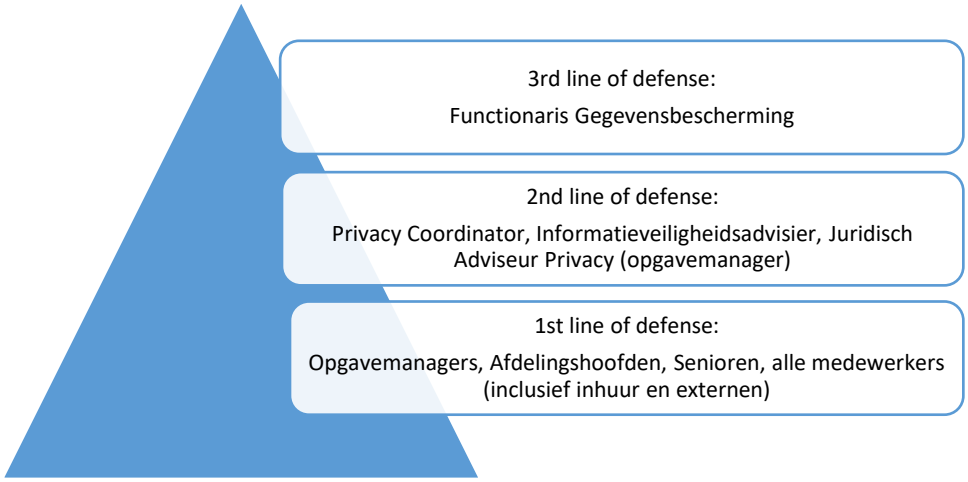
5. Governance

5.1 Informatiebeveiliging en Privacy

Informatiebeveiliging en Privacy worden vaak in 1 adem genoemd. Alhoewel er zeker raakvlakken zijn hebben beide specialismen ook een eigen werkveld.
Informatiebeveiliging heeft een bredere scope dan alleen persoonsgegevens maar gaat om de bescherming van alle data op gebied van integriteit, vertrouwelijkheid en beschikbaarheid. Het informatieveiligheidsbeleid is echter wel een voorwaarde vanuit de AVG op het gebied van persoonsgegevens.

5.2 Risicomanagement en eigenaarschap

Het 'Three Lines of Defense Model' wordt gebruikt om inzichtelijk te krijgen op gebied van risicomanagement maar ook de eigenaarschap op het gebied van privacy. In onderstaand model staat de situatie voor de GRS.



Eerste defensieve lijn

De eerste lijn zit in de operatie en ligt ook de primaire eigenaarschap op het gebied van de privacybescherming. Dit geldt tevens voor kwaliteitsmanagement, risico- en procesmanagement. Dat kan onder andere door het implementeren van beheersmaatregelen zoals kwaliteitsprocessen, checklists en werkinstructies. Ook is de eerste lijn verantwoordelijk voor het beantwoorden van primaire vragen op gebied van privacy en informatieveiligheid.

Tweede defensieve lijn

In de tweede lijn zitten voornamelijk ondersteunende functies op het gebied van risico's en vraagstukken. In geval van vraagstukken of advisering waarbij de eerste lijn er niet zelf uitkomt kan de tweede lijn worden geraadpleegd.
Op gebied van risicomanagement behoort de opgavemanager ook in de tweede lijn. De opgavemanager is verantwoordelijk voor het monitoren en rapporteren op het gebied van risico's, al dan niet met ondersteuning van de privacy coördinator.

Derde defensieve lijn

Binnen de derde lijn zitten de interne toezichthouder, op gebied van privacy de Functionaris Gegevensbescherming. De FG houdt toezicht op de correcte toepassing van de bepalingen uit de AVG. Onderdeel is ook controle op de werking van het risicomanagement in de eerste en tweede lijn. De FG rapporteert aan de management team en/of het bestuur.

In de zogenaamde vierde lijn (niet meegenomen in dit model) zitten externe auditors of toezichthouders zoals de accountants en de Autoriteit Persoonsgegevens.

5.3 Verantwoordelijkheden

In onderstaand RACI-model staat de verantwoordelijkheden op gebied van privacy nader beschreven voor de GRS. Dit is een breder en overkoepelend model.

Verantwoordelijke		
R	Responsible (Feitelijk verantwoordelijk)	- Managementteam, opgavemanagers en afdelingshoofden - Alle medewerkers (inclusief inhuur en externen) die persoonsgegevens verwerken
A	Accountable (Eindverantwoordelijk)	- Dagelijks Bestuur - Algemeen Bestuur
C	Consulted (Adviserend)	- Privacy Coördinator - CISO - Informatieveiligheidsadviseur - Juridisch Adviseur Privacy - Functionaris Gegevensbescherming
I	Informed (Geïnformeerd)	- Managementteam, Algemeen en Dagelijks Bestuur (en via hen de gemeenteraden) - Functionaris Gegevensbescherming - Betrokkenen

5.4 Functies nader uitgewerkt

Hieronder staan de eerder genoemde functies nader uitgewerkt op gebied van verantwoordelijkheid bij privacybescherming.

Algemeen en Dagelijks Bestuur

Op basis van de Verordening Gemeenschappelijke Regeling Sociaal Drechtsteden zijn aan de GRS wettelijke taken gemandateerd of gedelegeerd[16]. In geval van delegaat gaat de verantwoordelijkheid, en daarmee ook de verwerkingsverantwoordelijkheid zoals bedoeld in de AVG, over op de gedelegeerde partij (of in sommige gevallen een gezamenlijke verantwoordelijkheid). Bij mandaat treedt de gemandateerde partij doorgaans op als verwerker.
Het Dagelijks Bestuur informeert binnen de jaarlijkse planning & control cyclus het Algemeen Bestuur over de toepassing van het privacybeleid. 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.
Het Algemeen en Dagelijks Bestuur is bestuurlijk eindverantwoordelijk voor de naleving van de privacywetgeving binnen de GRS. Zowel in de rol als verwerker als van verwerkingsverantwoordelijke dient de privacywetgeving te worden nageleefd.

Managementteam

Het managementteam (MT) is eindverantwoordelijk voor de naleving van de privacywetgeving voor de uitvoering van de taken binnen de GRS. Documenten zoals uitgevoerde DPIA's, adviezen van de FG, de FG rapportages en het privacybeleid gaan doorgaans[17] eerst langs met MT. Het MT stuurt de opgavemanagers aan.

[16] Artikel 5 Verordening Gemeenschappelijke Regeling Sociaal: https://zoek.officielebekendmakingen.nl/bgr-2021-1131.html
[17] De FG mag direct naar het hoogste bestuurlijke orgaan indien hij/zij dit noodzakelijk acht

Opgavemanagers
Opgavemanagers zijn eindverantwoordelijk voor de naleving van de privacywetgeving binnen hun eigen opgave en in het gezamenlijk met andere opgavemanagers uitzetten van de lijnen op gebied van de integrale dienstverlening. Zij zijn tevens verantwoordelijk voor de uitvoering van het privacybeleid binnen hun opgave. De opgavemanagers zijn verantwoordelijk het actueel houden van DPIA's en het register van verwerkingen (in samenwerking met de privacy coördinator).

Afdelingshoofden (en senioren/coördinatoren)
De afdelingshoofden zijn verantwoordelijk voor de naleving van de privacywetgeving binnen hun afdeling. Met de senioren zijn zij tevens verantwoordelijk voor de naleving van het privacybeleid en gelden zij samen met alle medewerkers als de eerste lijn op gebied van privacyvraagstukken.

Functionaris Gegevensbescherming
Op basis van de AVG artikel 37 is de GRS verplicht een FG aan te stellen. Binnen de GRS heeft het Algemeen en het Dagelijks bestuur de FG aangewezen en is de FG formeel aangemeld bij de Autoriteit Persoonsgegevens. De FG heeft een onafhankelijke toezichthoudende en adviserende positie op de naleving van de privacywetgeving. De FG rapporteert jaarlijks over zijn bevindingen waarbij risico's en aanbevelingen genoemd worden. De FG kan ook tussentijds gevraagd en ongevraagd (zwaarwegend) advies uitbrengen. De FG heeft, al dan niet na een formeel verzoek het recht op toegang tot alle informatie en systemen en processen waarin privacygegevens een rol (kunnen) spelen. De werkzaamheden van de FG staat ook wettelijk omschreven in artikel 39 van de AVG.

Privacy Coördinator
De Privacy Coördinator zit gepositioneerd onder de opgave dienstverlening.[18] De Privacy Coördinator is het interne aanspreekpunt voor privacy gerelateerde vragen. De Privacy Coördinator werkt daarbij samen met de informatieveiligheidsadviseur. De Privacy Coördinator heeft een ondersteunende en monitorende rol op gebied van uitvoering van het beleid, DPIA's, register van verwerkingen, datalekken, klachten, verwerkersovereenkomsten en rechten van betrokkenen maar is daarvoor niet verantwoordelijk.

Juridisch Adviseur Privacy
Het Juridisch Kenniscentrum (JKC) zit gepositioneerd bij de Servicegemeente Dordrecht. Binnen het JKC zijn er juridisch adviseurs gespecialiseerd in de privacywetgeving. Zij kunnen gevraagd adviseren aan de GRS voor vraagstukken waar aanvullend juridisch advies noodzakelijk of wenselijk is.

Chief Information Security Officer (CISO)
De CISO zit gepositioneerd bij de Servicegemeente Dordrecht en verantwoordelijk voor de regionale toepassing en implementatie van technische en organisatorische maatregelen in het kader van de bescherming van persoonsgegevens. De CISO is betrokken bij grote informatieveiligheidsincidenten en meldt deze indien er sprake is van persoonsgegevens tijdig bij de FG en Privacy Coördinator.

Informatieveiligheidsadviseur (IB adviseur)
De GRS heeft een eigen IB adviseur onder de opgave bedrijfsvoering[19]. De IB adviseur is het interne aanspreekpunt voor informatieveiligheid. Wanneer het persoonsgegevens betreft werkt de IB adviseur daarin samen met de Privacy Coördinator. De IB adviseur neemt namens de GRS deel aan het regionale overleg van IB adviseurs.

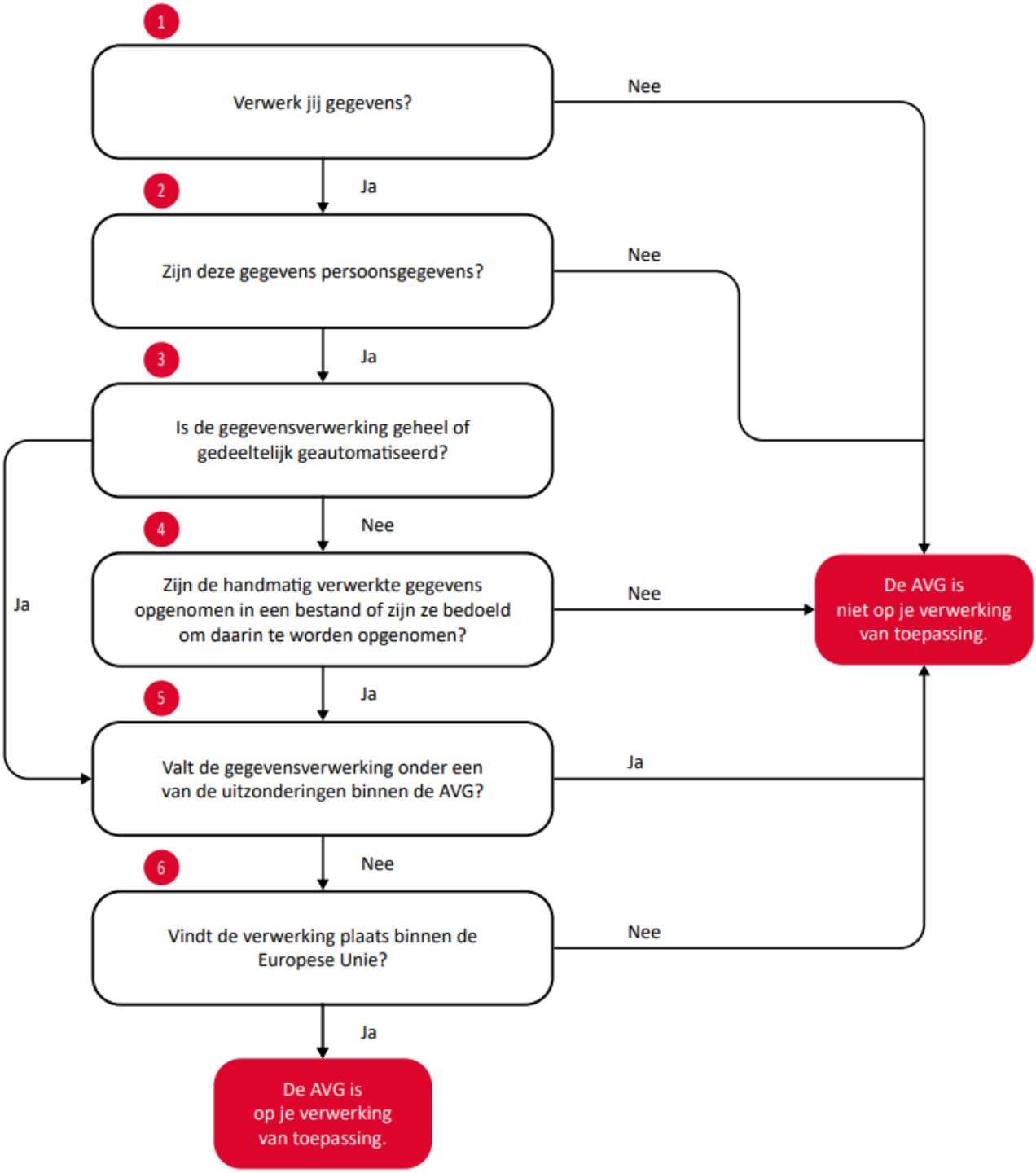
[18] Specifiek voor de Sociale Dienst Drechtsteden. Bij Drechtwerk valt deze functie onder het management
[19] Specifiek voor de Sociale Dienst Drechtsteden. Bij Drechtwerk is deze rol geborgd binnen de afdeling ICT

Bijlage 1: Begrippenkader

Begrip	Omschrijving
Autoriteit Persoonsgegevens	
Bestuur	Algemeen Bestuur: Het algemeen bestuur van de GRS bestaat uit een afvaardiging van collegeleden van alle deelnemende gemeenten. Elke gemeente heeft 1 collegelid aangewezen, m.u.v. Dordrecht, zij hebben er 2. Dagelijks Bestuur: Het dagelijks bestuur bestaat uit 3 leden, inclusief de voorzitter. Zij zijn gekozen uit de leden van het algemeen bestuur.
Betrokkene	De natuurlijke persoon van wie de persoonsgegevens worden verwerkt.
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.
DPIA (Data Protection Impact Assesment ook Gegevenseffectenbeoordeling)	Een methode om de effecten en risico's van nieuwe of bestaande verwerkingen op de bescherming van de privacy te beoordelen.
Functionaris Gegevensbescherming (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.
Gemeenschappelijke Regeling Sociaal	Het openbaar lichaam dat op basis van de Verordening Gemeenschappelijke Regeling Sociaal op basis van delegaat of mandaat is aangewezen tot de uitvoering van de daar gedefinieerde taken.
Informatiebeveiligingsadviseur	Werknemer binnen de GR Sociaal die het interne aanspreekpunt zijn over informatiebeveiliging.
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 Coördinator	Werknemer binnen de GR Sociaal die het interne aanspreekpunt zijn over privacybescherming.
Proceseigenaar	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.
Verwerkingsverantwoordelijke	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.

Bijlage 2: Is de AVG van toepassing?



Bijlage 3: Stroomschema rechtmatige verwerking