Privacybeleid

Dienst Gezondheid & Jeugd Zuid-Holland Zuid

Inhoudsopgave

1. Inleiding

Gemeenten en gemeentelijke organisaties, zoals de Dienst Gezondheid & Jeugd ZHZ (DG&J), verwerken persoonsgegevens om een dienst te verlenen, een product te leveren of om andere doelen te bereiken. Het belang van deze organisaties om persoonsgegevens te verwerken kan op gespannen voet staan met het privacybelang van de betrokkene op wie de verzamelde gegevens betrekking hebben.

Het beschermen van privacybelangen wordt vaak gezien als obstakel bij het uitvoeren van de werkzaamheden, omdat moet worden getoetst of aan de privacywetgeving wordt voldaan. Maar privacy is een belangrijk grondrecht. In de Grondwet is verankerd dat de overheid niet zomaar persoonlijke gegevens mag gebruiken. Het is een wettelijke verplichting dat overheidsorganisaties behoorlijk en zorgvuldig omgaan met persoonsgegevens in verband met de privacy van betrokkenen.

De DG&J heeft, in samenwerking met de gemeenten in Drechtstedenverband, de naleving van de Europese Algemene Verordening Gegevensbescherming (AVG) hoog in het vaandel staan. Deze organisaties zijn zich bewust dat iedereen recht heeft op bescherming van persoonsgegevens. De verwerking van persoonsgegevens moet zorgvuldig, rechtmatig en veilig plaatsvinden. Om hier invulling aan te geven heeft de DG&J in met organisaties in Drechtstedenverband een gezamenlijk privacybeleid geformuleerd, waarin is beschreven hoe om te gaan met de verwerking van persoonsgegevens.

In het privacybeleid staan kaders beschreven voor het verwerken van privacygevoelige informatie, of te wel persoonsgegevens, de bescherming van deze gegevens en omgang met deze gegevens. Dit privacybeleid dient als kapstok, waarbij voor een specifiek vakgebied een beheerplan of privacyprotocol dient te worden opgesteld.
Het privacybeleid sluit aan bij het Informatiebeveiligingsbeleid Drechtsteden. Immers, informatiebeveiliging en het veilig en verantwoord werken met persoonsgegevens overlappen elkaar voor een groot deel. Voor het borgen van de bescherming van persoonsgegevens is het naleven van wat is geregeld in het Informatiebeveiligingsbeleid Drechtsteden dan ook van cruciaal belang.

De Autoriteit Persoonsgegevens (AP) is de externe toezichthouder op een behoorlijke en zorgvuldige verwerking van persoonsgegevens binnen Nederlandse organisaties, waaronder overheden. Er kan vanaf 25 mei 2018 een boete worden opgelegd door de AP die een substantieel en afschrikwekkend karakter zal hebben, indien zij een overtreding constateert (maximaal 20 miljoen euro). Het dagelijks bestuur (DB) van de DG&J is verantwoordelijk voor een juiste verwerking van persoonsgegevens binnen de organisatie. De DG&J werkt daarbij nauw samen met andere overheidsorganisaties in Drechtstedenverband, vandaar dat in dit privacybeleid met regelmaat naar de Drechtsteden wordt verwezen. Daarmee wordt dan in eerste instantie de DG&J bedoeld als de formeel verantwoordelijke organisatie.

2 Uitgangspunten

2.1 Doelstellingen van het beleid

Doelstelling van het beleid is dat op een verantwoordelijke wijze en binnen wettelijke kaders met privacy gevoelige gegevens wordt omgegaan. Binnen de wettelijke kaders wordt in Drechtstedenverband geprobeerd creatieve oplossingen te vinden om de regulieren werkprocessen en innovaties goed uit te kunnen voeren. Het wettelijk kader voor bescherming van persoonsgegevens wordt -naast vele specifieke wetten- aangegeven door de AVG. De eisen die de AVG stelt aan het verwerken van persoonsgegevens worden dan ook zorgvuldig in Drechtstedenverband geïmplementeerd door de DG&J. Als startpunt is een verplicht bewustwordingsprogramma voor alle medewerkers opgezet. De privacybescherming kan zo stapsgewijs worden verhoogd en vormt de basis voor de vergroting van het privacybewustzijn en de professionalisering binnen de DG&J.

De DG&J wil hiermee onder meer bereiken dat:

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

2.2 Begrippenkader

Begrippen die voor een goede uitvoering van het privacybeleid van groot belang zijn en worden gehanteerd binnen de AVG zijn:

Begrip	**Omschrijving**
Accountability	Het kunnen aantonen op welke manier de persoonsgegevens worden verwerkt conform de AVG. Hiertoe dienen passende en effectieve maatregelen te worden genomen, zoals: • documentatie plicht: het bijhouden van een Register van verwerkingen; • het beschermen van gegevens door ontwerp principes als Privacy by Design en Privacy by Default; • indien van toepassing het uitvoeren van een Privacy Impact Assessment, PIA; • het treffen van passende technische - en organisatorische maatregelen, waaronder juridische - en beveiligingsmaatregelen; • het opstellen van een procedure om beveiligingsincidenten en datalekken te documenteren. Vervolgens een procedure voor het melden van een datalek aan AP; • het aanstellen van een Functionaris Gegevensbescherming.

Dagelijks bestuur (DB)	Het dagelijks bestuur van de gemeenschappelijke regeling Dienst Gezondheid & Jeugd Zuid-Holland Zuid.
Betrokkene	De natuurlijke persoon van wie de gegevens worden verwerkt.
Functionaris Gegevens-bescherming (FG)	De FG is de interne toezichthouder op de verwerking van persoonsgegevens. De FG dient in alle onafhankelijkheid zijn werkzaamheden te kunnen uitvoeren en ontvangt daarbij geen instructies van opdrachtgevers of verwerkers. Hij is aangemeld bij de AP als contactpersoon en aanspreekpunt voor de meldingen van datalekken. Hij functioneert als tussenpersoon tussen verschillende belanghebbenden en is daarmee ook verlengstuk van de Autoriteit Persoonsgegevens (AP).
Gegevensbeschermings-effectbeoordeling, ofwel Privacy Impact Assessment (PIA)	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 richtlijnen en strategie is gegarandeerd, zodat vereiste processen op de juiste manier worden gevolgd om te kunnen voldoen aan wet- en regelgeving. Governance bevat het definiëren van rollen en verantwoordelijkheden, meten en rapporteren, nemen van acties om geïdentificeerde kwesties op te lossen.
Inbreuk 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.
In privacywetgeving gespecialiseerde juridische adviseur	De in privacywetgeving gespecialiseerde juridisch adviseurs van het Juridisch Kenniscentrum Drechtsteden (JKC) die onder meer als taak hebben om concrete vragen uit de regio te beantwoorden, medewerkers in de regio te adviseren en op te leiden. Deze gespecialiseerde juridische adviseurs worden ondersteund en geadviseerd door de FG. Anderzijds vullen zij de FG aan, die zich vanuit zijn functie als Toezichthouder niet met advisering in concrete gevallen bezig kan houden.
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene) als bedoeld in de AVG of daarvoor in de plaats tredende wetgeving. Naast gewone persoonsgegevens, zoals naam en adresgegevens, kent de wet ook bijzondere persoonsgegevens, zoals etnische achtergrond, politieke voorkeur of gezondheid.
Privacybescherming	Het omgaan met persoonsgegevens conform de eisen in de AVG.
Privacycoördinatoren	Medewerkers binnen de Drechtsteden die worden getraind door de in privacywetgeving gespecialiseerde adviseurs. Zij zijn het interne aanspreekpunt voor de organisaties en communiceren en rapporteren aan/met de FG.
Proceseigenaren	Degenen die binnen de organisatie zijn aangewezen als verantwoordelijke voor een proces.
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.
Verwerkings-verantwoordelijke	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst die of een ander orgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

2.3 Juridisch kader – basiseisen uit de AVG

Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkenen voorop. Er moet worden voorkomen dat er onnodige of te verregaande inbreuken worden gemaakt. De AVG regelt het algemene kader voor de omgang met persoonsgegevens binnen de landen van de Europese Unie. De AVG is de hoogste wetgeving voor privacybescherming en fungeert als een parapluwet die van toepassing is voor alle verwerkingen van persoonsgegevens door organisaties, zowel bedrijven als overheden. De uitgangspunten van de AVG zijn:

- Verwerking op rechtmatige, behoorlijke en transparante wijze (artikel 5a AVG);
- Verzamelen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (artikel 5b AVG);
- Alleen verwerking op één van de in de AVG opgenomen grondslagen (artikel 6 AVG).

Van belang is dat persoonsgegevens 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 een 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 het sluiten 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 andere natuurlijke persoon te beschermen;
- De 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 fundamentele vrijheden van betrokkene, die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen.

Vervolgens moet worden vastgesteld, dat de verwerkte persoonsgegevens proportioneel zijn (worden er niet meer gegevens verwerkt dan noodzakelijk voor het uitoefenen van de taak), en dat aan het subsidiariteitsbeginsel wordt voldaan (is er een voor de betrokkene minder belastende manier om de taak uit te voeren).

'Bijzondere' categorieën van persoonsgegevens zijn persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid blijkt (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.

De betrokkene kan altijd inzage of wijziging van de verwerkte persoonsgegevens opvragen. Om het proces van gegevensverwerking ordelijk te laten verlopen en betrokkenen makkelijk toegang te geven tot de betrokken organisaties stelt het dagelijks bestuur van de Gemeenschappelijke regeling Drechtsteden één of meerdere personen aan voor de functie van Functionaris Gegevensbescherming (FG) (artikel 37 AVG) die als

zodanig kan functioneren voor de eigen gemeenschappelijke regeling en voor de daarin deelnemende gemeenten. Het dagelijks bestuur van de DG&J kan met een afzonderlijk besluit dezelfde FG aanwijzen voor de eigen organisatie.

De DG&J heeft de wettelijk verplichting om gegevensbescherming te borgen, onder meer door technische en organisatorische maatregelen te treffen (artikel 15 AVG). Hiervan is de Informatieveiligheid een groot onderdeel. Samen met onder andere informatiebeheer, het juridisch kader en privacybewustzijn zorgt informatieveiligheid voor de borging van bescherming van privacygevoelige gegevens. Voor de informatieveiligheid werken de Drechtsteden binnen de kaders van het Informatiebeveiligingsplan en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Het Privacybeleid Drechtsteden gaat uit van het voldoen aan de eisen van de AVG en de Uitvoeringswet AVG. Daarnaast zijn er diverse specifieke wetten, zoals de Basisregistratie Personen (BRP), de Wet maatschappelijke ondersteuning (Wmo), de Jeugdwet, en de Politiewet, die aanvullende eisen stellen aan privacybescherming. Die wetten worden in dit beleidsstuk niet ingevuld. Deze wetten worden later meegenomen in de verdere uitwerking van het privacybeleid. Deze wetten zijn vanzelfsprekend van belang voor de medewerkers die op basis van deze wetten taken uitvoeren.

2.4 Wijze van inrichten gegevensverwerking

Door het cyclische karakter van de aangegeven maatregelen en door de bescherming van persoonsgegevens onderdeel te laten zijn van het kwaliteitsmanagementsysteem van de DG&J, en daarmee vast op de verschillende agenda's te plaatsen, ontstaat een continue proces van veranderen en verbeteren. De kwaliteit van het omgaan met vraagstukken over privacy wordt verhoogd door op verschillende niveaus en vanuit verschillende rollen telkens weer de kwaliteitscyclus van 'plan-do-check-act' te doorlopen. Hierdoor ontstaat een evenwichtig privacybeheersingssysteem. Zo wordt gewerkt aan privacybewustzijn, aan het opbouwen van kennis bij medewerkers en aan verantwoorde procesuitvoering. Het borgen van de privacy is onlosmakelijk verbonden met informatiebeveiliging.
In dat kader werkt de DG&J nauw samen met het Servicecentrum Drechtsteden (SCD).

2.5 Doelgroep

Het privacybeleid is van toepassing op alle taken en processen waarvoor de DG&J verantwoordelijk is. Het betreft zowel de taken die de DG&J op grond van de gemeenschappelijke regeling, al dan niet in mandaat, uitvoert voor de gemeenten, alsmede voor de taken die de DG&J uitvoert als rechtspersoon in het kader van de Wet gemeenschappelijke regelingen, en als werkgever. DG&J geldt hier als verwerkingsverantwoordelijke in de zin van de AVG.

Dit privacybeleid en een juiste uitvoering hiervan richt zich tot alle interne en externe medewerkers binnen de organisatie. Het is vooral gericht op diegenen die werken met persoonsgegevens, dan wel persoonsgegevens laten verwerken door externe partners. De bestuurders en het management spelen een belangrijke rol bij de besluitvorming over dit onderwerp en de sturing ervan in de planning- en control cyclus.

2.6 Ingangsdatum

De AVG is per 25 mei 2018 van toepassing. De Wet bescherming persoonsgegevens (Wbp) en de Europese Richtlijn 95/46, waarop de Wbp is gebaseerd, komen per gelijke datum te vervallen. Dit privacybeleid treedt per 25 mei 2018 in werking.

3 Rechten van betrokkenen

Binnen de AVG krijgen betrokkenen nieuwe privacyrechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt, meer dan onder de 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, oftewel recht op 'vergetelheid' (artikel 17 AVG);
- beperking van de verwerking (artikel 18 AVG);
- kennisgevingplicht inzake rectificatie, wissing of beperking (artikel 19 AVG);
- overdraagbaarheid van gegevens, 'dataportabiliteit' (artikel 20 AVG).

3.1 Recht op inzage van gegevens, artikel 15 AVG

De betrokkene heeft het recht om van de DG&J als verwerkingsverantwoordelijke uitsluitsel te krijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens.

De betrokkene heeft het recht om te informeren of zijn persoonsgegevens worden verwerkt. Als dat het geval blijkt heeft hij recht op uitleg over het wat en het hoe, als ook op inzage en een kopie van zijn persoonsgegevens (zie nader artikel 20 AVG).
De DG&J als 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

De betrokkene heeft het recht om van de DG&J als verwerkingsverantwoordelijke onverwijld een rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen, met in achtneming van de doeleinden van de verwerking.

Wanneer verwerkte persoonsgegevens onjuist of onvolledig zijn, heeft de betrokkene het recht deze te laten corrigeren of aanvullen. Dit artikel is een uitwerking van het beginsel van juistheid van persoonsgegevens (artikel 5, lid 1, onder d, AVG).
De DG&J en de eventuele verwerker moeten alle redelijke maatregelen nemen om er voor te zorgen dat onjuiste persoonsgegevens worden gerectificeerd. Het is daarbij niet relevant of de onjuistheden berusten op een fout van de DG&J of van een verwerker.

3.3 Recht op gegevenswissing, recht op 'vergetelheid', artikel 17 AVG

De betrokkene heeft het recht van de DG&J als verwerkingsverantwoordelijke zonder onredelijke vertraging, wissing van hem betreffende persoonsgegevens te verkrijgen.
De DG&J is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer dit van toepassing is. Op grond van de beginselen van juistheid en opslagbeperking (artikel 5 AVG) mogen persoonsgegevens niet langer worden bewaard dan nodig is voor het doel van hun verwerking. Het recht van gegevenswissing werkt dit nader uit tot een recht voor de betrokkene om overtollige persoonsgegevens gewist te krijgen met corresponderende plicht voor de verwerkingsverantwoordelijke en eventuele verwerkers.

3.4 Recht op beperking van de verwerking, artikel 18 AVG

De betrokkene heeft het recht van de DG&J als verwerkingsverantwoordelijke de beperking van de verwerking te verkrijgen.

Beperking is enigszins circulair gedefinieerd (artikel 4 AVG) 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 Kennisgeving inzake rectificatie, wissing of beperking, artikel 19 AVG

De DG&J als verwerkingsverantwoordelijke stelt iedere ontvanger (niet zijnde betrokkene zelf) 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 DG&J verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.

Wanneer DG&J een rectificatie (artikel16 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 beperking ook doorvoeren.

3.6 Recht op overdraagbaarheid gegevens, dataportabiliteit, artikel 20 AVG

Naast het al bekende recht van inzage in persoonsgegevens (artikel 15 AVG) introduceert de AVG het recht van 'dataportabiliteit', oftewel overdraagbaarheid van persoonsgegevens.

De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en machinaal leesbare vorm te verkrijgen en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt.

4 Werkprocessen

4.1 Omgaan met persoonsgegevens

DG&J verwerkt persoonsgegevens alleen indien het doel van de verwerking kan worden gebaseerd op één van de zes grondslagen van artikel 6 AVG (zie paragraaf 2.3).

In het merendeel van de gevallen worden persoonsgegevens door de betrokkene zelf verstrekt. Veel gebruikte gegevens of al bekende gegevens die zijn opgenomen in basisregistraties of andere authentieke bronnen, worden daaruit opgevraagd voor zover DG&J daartoe gerechtigd is. Dit is in overeenstemming met het principe van 'eenmalige uitvraag en meervoudig gebruik' dat door de overheid wordt voorgestaan.
Meestal worden gegevens in informatiesystemen opgenomen waar ze alleen toegankelijk zijn voor de medewerkers die belast zijn met het uitvoeren van de taak.
Informatiesystemen moeten voldoen aan de eisen van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

4.2 Bewustwording

Zorgvuldig omgaan met persoonsgegevens is enerzijds een kwestie van het organiseren van een goede Informatieveiligheid en het zorgvuldig inrichten van werkprocessen, anderzijds is het een zaak van bewustwording en communicatie. Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het bewustzijn wordt voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.
De bedrijfscultuur in zijn geheel moet op een 'bewust bekwaam' niveau van omgaan met persoonsgegevens worden gebracht. Er moet een constante afweging worden gemaakt tussen 'need to know' en 'nice to know', waarbij in de laatste categorie geen persoons-gegevens worden verwerkt.

Het is van belang dat medewerkers die daadwerkelijk werken met persoonsgegevens weten wat hun verantwoordelijkheid is en hoe zij zorgvuldig moeten omgaan met persoonsgegevens. Zij moeten in staat zijn om te beoordelen welke gegevens nodig zijn voor het uitvoeren van de werkprocessen. Er mogen niet te weinig maar ook niet te veel gegevens te worden verwerkt (artikel 5.1c AVG). De FG zorgt er samen met de CISO van het SCD voor dat informatie over gegevensbescherming en informatieveiligheid herhaaldelijk onder de aandacht wordt gebracht van leidinggevenden en medewerkers. Medewerkers worden getraind in privacybewust functioneren door middel van presentaties, workshops en trainingen, door de leermodules in de e-learningomgeving en het altijd voor handen hebben van een vraagbaak in de vorm van het SCD-JKC.

4.3 Verplichte maatregelen en procedures

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

- In het Informatiebeveiligingsbeleid zijn op basis van de BIG richtlijnen beschreven waaraan processen en informatiesystemen moeten voldoen om gegevensbescherming te borgen. Deze richtlijnen gelden voor proceseigenaren die nieuwe en bestaande processen en informatiesystemen beheren;
- Er is een procedure vastgesteld voor standaard incidentbeheer en er is een privacy-incidentprocedure. Deze procedures vormen de basis voor het *'Register van inbreuk op persoonsgegevens (datalekken)*';

- Er is een procedure vastgesteld waarin is vastgelegd hoe betrokkenen worden geïnformeerd bij een datalek;
- Alle gegevensverwerkingen waar persoonsgegevens worden verwerkt zijn in beeld gebracht en vastgelegd. Voor interne gegevensverwerkingen worden de gegevens opgeslagen en bijgehouden in het *'Register van verwerkingen, met aantekeningen van PIA's'*;
- Voor verwerkers worden de gegevens opgeslagen en bijgehouden in het *'Register van verwerkersovereenkomsten, convenanten en privacy protocollen'*;
- In het *'Register voor aanvragen van betrokkenen'* wordt bijgehouden welke aanvragen er zijn vanuit betrokkenen en het afhandelingstraject van de aanvraag.

4.4 Dataclassificatie

Met dataclassificatie wordt de uitvoering van het privacybeleid ondersteund op gebied van informatiebeveiliging. De maatregelen die getroffen moeten worden op gebied van informatiebeveiliging om de gegevensbescherming te kunnen borgen, zijn niet voor elk proces en informatiesysteem hetzelfde. Om die reden is het nodig dat alle processen en informatiesystemen die gegevens verwerken een eigen dataclassificatie ontvangen.

Dataclassificatie heeft als doel om de *beschikbaarheid, integriteit en vertrouwelijkheid* van het proces en het informatiesysteem formeel te benoemen. Dit maakt inzichtelijk waarom maatregelen genomen moeten worden om de gegevens die verwerkt worden te beschermen. Elke proceseigenaar voorziet elk proces en informatiesysteem van een dataclassificatie, zoals dat voor gemeenten in VNG-verband is voorgeschreven door de Informatiebeveiligingsdienst Gemeenten (IBD).

4.5 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, neemt het dagelijks bestuur van de DG&J een besluit over de bewaartermijn. Daarnaast geldt de Archiefwet voor het bewaren van papieren en elektronische documenten.

4.6 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, dat dit gepaard gaat met verwerking van zijn of haar gegevens. Het is hierom van belang dat de DG&J betrokkene informeert hoe zijn of haar gegevens worden verwerkt.

In sommige situaties kan het nodig zijn dat gegevens worden gedeeld met andere organisaties. Het delen van deze gegevens wordt niet uitgevoerd zonder de expliciete toestemming van betrokkenen of wettelijke grondslag. In welke gevallen gegevens worden gedeeld is vermeld in het *'Register van verwerkingen'.*

4.7 Open communicatie

Betrokkenen moeten erop kunnen vertrouwen dat zijn of haar persoonsgegevens zorgvuldig worden verwerkt. DG&J maakt daarom inzichtelijk, door middel van verschillende communicatie kanalen, op welke wijze persoonsgegevens worden verwerkt en beheerd. In uitzonderingsgevallen kan worden besloten om bepaalde persoonsgegevens niet te verstrekken (artikel 23 AVG).

In privacy-protocollen worden aanleidingen gedocumenteerd en wordt inzichtelijk:

- welke gegevens worden verzameld;
- waarom deze gegevens worden verzameld;
- hoe deze gegevens worden verzameld en bewaard:
- wanneer en wat er vervolgens met deze gegevens gebeurt;
- wie toegang heeft tot deze gegevens;
- welke rechten betrokkenen hebben.

De bovenstaande lijst is niet uitputtend. Hiertoe zijn heldere, laagdrempelige procedures ingericht. Deze procedures worden, evenals de contactgegevens van de FG, gecommuniceerd naar betrokkenen. Betrokkenen worden zo gefaciliteerd in het doen van een beroep op één of meerdere van hun rechten. Processen en informatiesystemen die door de DG&J worden gebruikt, zijn zodanig ingericht dat aan de vraag van betrokkenen kan worden voldaan (artikel 12 AVG).

4.8 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 die niet voor de ontvanger is bestemd (brief of e-mail), het in de post zoekraken van een dossier, enzovoort. Ook het intern verwerken van te veel bijzondere persoonsgegevens is een datalek.

Wanneer er sprake blijkt van een inbreuk in verband met persoonsgegevens of te wel een datalek, moet dit datalek door de FG zonder onnodige vertraging worden gemeld aan de AP. Een melding moet indien van toepassing ook onverwijld aan betrokkenen worden gedaan (artikel 33 AVG). Het SCD hanteert een procedure voor standaard incidentbeheer, de privacy-incidentprocedure welke hier goed op aansluit. Hierbij vormt de basis het verplichte *'Register van inbreuken op persoonsgegevens (datalekken)'*.

Organisaties die persoonsgegevens verwerken zijn verplicht om datalekken binnen 72 uur na het ontdekken daarvan te melden bij de AP. Het gaat hier om datalekken waarvoor de DG&J verantwoordelijk is. Daaronder vallen ook datalekken die ontstaan bij een derde partij die werkzaamheden uitvoert voor de DG&J. Het SCD is door het dagelijks bestuur van de DG&J gemandateerd voor het aan de AP melden van datalekken die onder verantwoordelijkheid van de DG&J vallen. Hoe een betrokkene een (vermoedelijk) datalek kan melden is te lezen op de website van de DG&J. Ook deze meldingen worden door de DG&J gemeld bij de AP, door tussenkomst van het JKC/SCD.

4.9 Verwerkersovereenkomst

Bij veel processen worden gegevens verwerkt door derden (zie artikel 4 AVG). Hierbij kan onder andere worden gedacht aan de werkzaamheden die medewerkers van de DG&J uitvoeren via een applicatie in de Cloud. Ook het SCD, in de hoedanigheid van leverancier van de ICT-infrastructuur van de DG&J, is te beschouwen als een verwerker.

Het verlenen van opdrachten aan derden (verwerkers) brengt risico's met zich mee op het gebied van gegevensverwerking en informatieveiligheid. De DG&J blijft echter verantwoordelijk voor de verwerking van de persoonsgegevens. Het afsluiten van verwerkersovereenkomsten geeft de mogelijkheid erop toe te zien dat ook door verwerkers gegevens juist worden beschermd en juist worden verwerkt (zie artikel 32 AVG).

Bij contracten waar persoonsgegevens door verwerkers worden verwerkt sluit de DG&J verwerkersovereenkomsten af, waarin minimaal afspraken worden gemaakt over:

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

Ten einde te borgen dat er verwerkersovereenkomsten worden gesloten, vormt dit een vast onderdeel in het inkoopproces. De verwerkersovereenkomsten worden opgenomen in het *'Register voor Verwerkersovereenkomsten'*.

5 Governance

5.1 Verantwoordelijken voor uitvoering en naleving AVG

Het dagelijks bestuur van de DG&J is verantwoordelijk voor de juiste uitvoering van de AVG en naleving van het privacybeleid. Het dagelijks bestuur is verantwoordelijk voor het verwerken van persoonsgegevens door de eigen organisatie en voor de taken die met toepassing van de gemeenschappelijke regeling en eventuele mandaatbesluiten voor de deelnemende gemeenten of de rijksoverheid worden uitgevoerd.

De door de Drechtsteden aangestelde FG zorgt voor onafhankelijk toezicht en controle op de kwaliteit van de uitvoering van het privacybeleid.

5.2 Verantwoording aan het algemeen bestuur

Het dagelijks bestuur van de DG&J informeert binnen de jaarlijkse planning & control cyclus respectievelijk het algemeen bestuur van de DG&J over de risico's en over de getroffen beheersmaatregelen op het gebied van privacy, binnen de processen waarvoor de DG&J verantwoordelijk is.

Op grond van de AVG wordt de uitvoering van het privacybeleid elk jaar door de FG geauditeerd. De FG rapporteert aan het dagelijks bestuur van de DG&J. Het afleggen van jaarlijkse verantwoording door de FG doet overigens niet af aan de algemene informatieplicht die het dagelijks bestuur heeft in de Wet gemeenschappelijke regelingen.

Het dagelijks bestuur meldt bijzonderheden ten aanzien van gegevensverwerking, te denken valt aan ernstige inbreuk op of verlies van persoonsgegevens, afzonderlijk en proactief aan het algemeen bestuur, en indien nodig aan één of meer colleges van de deelnemende gemeenten. Het dagelijks bestuur wijst een portefeuillehouder aan voor informatiebeveiliging en privacy.

5.3 Functionaris Gegevensbescherming (FG)

Voor onafhankelijk toezicht en controle op de kwaliteit van de uitvoering van het privacybeleid hebben de Drechtsteden één of meerdere personen aangesteld voor de functie van Functionaris Gegevensbescherming (FG) (artikel 37 AVG). De functie van FG wordt gepositioneerd binnen het SCD. De FG heeft een onafhankelijke positie in de organisatie. De werkzaamheden die een FG uitvoert hebben een wettelijke grondslag (artikelen 37 t/m 39 AVG).

De interne verantwoording is gewaarborgd door proceseigenaren binnen de individuele organisaties (i.c. de DG&J), die rapporteren aan de FG over de realisatie van passende privacywaarborgen. Zij rapporteren onverwijld bij privacyincidenten conform de vastgestelde privacyincidentprocedure.[1] Ook afwijkingen van de uitvoering van het privacybeleid worden direct gerapporteerd.

De DG&J maakt afspraken met de FG over een privacy-auditplan. De FG houdt toezicht op het uitvoeren van het auditplan en voert daarnaast zelfstandig controles uit. Het is de verantwoordelijkheid van de FG dat de bestuursorganen in de Drechtsteden, waaronder het dagelijks bestuur van de DG&J, in control zijn en dat de registers op orde zijn.

[1] Zie de procedure in Mozaïek: http://as-g-1mozaiekweb.sc.grid.internal/pls/dmoz/mozaiek/5406591

Ook in geval van calamiteiten moeten de procedures goed werken en dienen organisaties in control te zijn. Het is de FG die toeziet op de prioritering van de processen en de wijze van implementatie van maatregelen.

De AVG verplicht tot het bijhouden van registers. Deze taken behoren toe aan de FG, bijgestaan door proceseigenaren en verantwoordelijke portefeuillehouders in de regio. De FG beheert de volgende verplichte registers:

- Register van verwerkingen, met aantekeningen van PIA's;
- Register van verwerkersovereenkomsten, convenanten en privacy protocollen;
- Register van inbreuken op persoonsgegevens, datalekken;
- Register voor aanvragen van betrokkenen.

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

5.4 Adviseur Gegevensbescherming (AG)

De Adviseur Gegevensbescherming (AG) ondersteunt de FG bij het uitvoeren van de wettelijke taken omschreven in artikel 38 en 39 van de AVG. De voornaamste taak bestaat uit het onder toezicht van de FG leveren van inhoudelijke en procesmatige bijdragen aan het onafhankelijk toezicht en de controle op de kwaliteit van de uitvoering van het privacy-beleid van de DG&J.

De AG adviseert organisaties in afstemming met de FG over het implementeren van de AVG en het opstellen van een strategie omtrent het gebruik van persoonsgegevens. Belangrijk zijn daarbij zowel juridische als technische aspecten met betrekking tot de bescherming van persoonsgegevens.

De AG ziet mede toe op, en adviseert in concrete situaties over, het toewijzen van verantwoordelijkheden, privacy-awareness en draagt zorg voor het opleiden van collega’s. In overleg met de FG adviseert de AG over het uitvoeren van Privacy Impact Assessments (PIA) en houdt mede toezicht op de uitvoering.

Onder aansturing van de FG heeft de AG onder meer de volgende taken:

- Het Register van Verwerkingen te controleren en beheren;
- Het Register voor het melden van inbreuken op de persoonsgegevens (datalekken) te maken en bijhouden;
- Toe te zien op invulling, door afdeling contractmanagement, van het Register van verwerkingsovereenkomsten;
- Het Register van rechten betrokkenen te controleren en beheren;
- Dossiervorming van de achterliggende stukken.

5.5 Privacycoördinatoren

Privacycoördinatoren zijn medewerkers binnen de individuele organisaties (i.c. de DG&J) die worden getraind door de AG. Zij zijn het interne aanspreekpunt voor de organisatie en communiceren met, en rapporteren aan, de FG. Zij zijn in dienst van de afzonderlijke organisaties. Gezien de aard en de hoeveelheid van de werkzaamheden kunnen de rollen en de taken van de Privacycoördinatoren bij verschillende personen met aanverwante werkzaamheden in de organisatie worden belegd.

De Privacycoördinator krijgt van een proceseigenaar het verzoek om voor elk proces met behulp van de procesrisicoanalyse vast te stellen of er sprake is van privacygevoelige gegevens. Indien geconstateerd is dat er sprake is van persoonsgegevens met een groot risico, dient in samenwerking met CIO-Office van het SCD een PIA te worden uitgevoerd naar de risico's van het betreffende proces. Over alle naar aanleiding van de uitkomst van de PIA genomen maatregelen wordt door de Privacycoördinator advies gevraagd aan de FG. De processen waar PIA's voor zijn uitgevoerd, worden periodiek geëvalueerd en de status wordt bijgewerkt in het register van verwerkingen van de FG.

Bij het in ontvangst nemen, en het eventueel voor advies doorzenden van verzoeken om inzage en informatie van betrokkenen aan Privacyadviseurs van het JKC, speelt de Privacycoördinator een coördinerende rol. Daarnaast bewaakt hij de inzageprocessen en zal indien nodig opschalen naar de klachtenprocedure.
De Privacycoördinator zorgt ervoor dat betrokkenen met de FG contact kunnen opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten uit hoofde van deze verordening.

5.6 Privacyadviseurs

De Privacyadviseurs zijn gepositioneerd bij het SCD/JKC. Hun belangrijkste taak is het adviseren van de (medewerkers in de) organisaties over vragen op het gebied van het toepassen van de privacywetgeving in de praktijk.

5.7 Sturing en monitoring

Proceseigenaren zijn de eerstverantwoordelijke voor de zorgvuldige verwerking van persoonsgegevens die binnen een organisatieonderdeel plaatsvindt. Zij zijn daarom ook verantwoordelijk om te monitoren of persoonsgegevens zorgvuldig worden verwerkt, en zij moeten dit zo nodig bijsturen. In de praktijk wordt deze monitoring gedaan door de privacycoördinator, in samenwerking met o.a. de kwaliteitsmedewerkers.

Een belangrijk uitgangspunt in de AVG, waarop de AP zal gaan handhaven, is Accountability: de verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van art. 5.1a AVG en kan deze aantonen (verantwoordingsplicht op grond van artikel. 5.2 AVG).

5.8 Overzicht verantwoordlijkheden en verantwoordelijken

In de tabel op de bladzijden 17 t/m 19 staat een overzicht (op hoofdlijnen) van de verantwoordelijkheden en bijbehorende verantwoordelijken betreffende uitvoering en invulling van de AVG het privacybeleid binnen de DG&J.

Dordrecht, 24 mei 2018

Het dagelijks bestuur van de Dienst Gezondheid & Jeugd,
de secretaris, de voorzitter,

K.J. van Hengel mw. C.M.L. Lambrechts

Verantwoordelijkheid	Wie & hoe
Actief privacybeleid jegens betrokkenen	Proceseigenaren zijn krachtens de organisatiestructuur van de DG&J, zoals de Mandaatregelingen, verantwoordelijk voor correcte en transparante afwikkeling van de verzoeken van betrokkenen. De privacycoördinator bereidt de besluitvorming hierover voor en rapporteert hierover per aanvraag over de aanvraag en de afhandeling aan de FG. De FG ondersteunt proceseigenaren hierin en neemt de aanvraag en afhandeling op in het hiervoor bestemde register.
Actief privacybeleid medewerkers	De FG verzorgt samen met de proceseigenaren training van en toezicht op privacybewustzijn van de medewerkers.
Actief privacybeleid jegens verwerkers	Daar waar verwerkingen uitbesteed worden aan derden zijn de proceseigenaren verantwoordelijk voor het sluiten van verwerkersovereenkomsten. De privacycoordinator faciliteert hierin. Proceseigenaren rapporteren hierover aan de FG door tussenkomst van de privacycoordinator. DG&J beheert de afgesloten verwerkersovereenkomsten in het verplichte register van verwerkersovereenkomsten.
Beheer van het beleid	De FG rapporteert aan het dagelijks bestuur en de directies over de voortgang en de kwaliteit van de uitvoering, en doet aanbevelingen voor verdere optimalisering. Waarborg voor optimalisering is het hanteren van de PDCA-cyclus.
Bestuurlijke verantwoording	Jaarlijks legt het dagelijks bestuur verantwoording af aan het algemeen bestuur.
Interne verantwoording	De FG rapporteert ieder kwartaal rechtstreeks aan de bestuursorganen van de Drechtsteden, waaronder het dagelijks bestuur DG&J. De per organisatie aangewezen proceseigenaren rapporteren ieder kwartaal aan de FG over de realisatie van passende privacy-waarborgen, en rapporteren onverwijld bij privacyincidenten conform de vastgestelde privacyincidentprocedure. Indien proceseigenaren verantwoordelijkheden hebben overgedragen, dragen zij zorg voor een gelijkwaardige vorm van verantwoording en voor kennisgeving hiervan aan de FG.
Ontwikkelen van thematisch beleid	De portefeuillehouders privacy in de Drechtsteden zien toe op de ontwikkeling van themagericht privacybeleid (BRP, Participatie, Jeugd). Afhankelijk van het thema besluit de DG&J of en hoe hierbij wordt aangesloten.
Praktische privacy waarborgen	Concretiseren van praktische privacy waarborgen gebeurt onder verantwoordelijkheid van de proceseigenaar.
Privacy-auditplan	De FG ziet er in afstemming met de DG&J op toe dat er een privacy-auditplan ontwikkeld wordt en dat dit wordt uitgevoerd door o.a. de Privacycoördinator. Dit plan wordt jaarlijks opgesteld en is in lijn met het Raamwerk privacy-audit van de AP. De PDCA-cyclus wordt hierop toegepast.
Risico gedreven aanpak	Vertrekpunt voor het maken van beleidskeuzes is de PIA. In samenwerking met JKC en na advies van de FG wordt de mate van persoonlijk- en bestuurlijk risico in kaart gebracht. De risico's worden door praktische-, organisatorische- en technische maatregelen beheerst en volgens de PDCA-cyclus geborgd.
Toezicht	De bestuursorganen van de Drechtsteden, waaronder de DG&J hebben gezamenlijk een Functionaris Gegevensbescherming (FG) voor de Drechtsteden aangesteld (artikelen 37 t/m 39 AVG). De FG rapporteert aan de bestuursorganen en onderhoudt de contacten met de AP.
Uitvoering van privacybeleid	De bestuursorganen hebben uit hun midden een Portefeuillehouder(s) privacy aangewezen. Deze is verantwoordelijk voor uitvoering van het beleid en voor controle op de naleving van het privacybeleid.
Vaststellen privacybeleid	Het dagelijks bestuur van de DG&J stelt het privacybeleid vast en bevorderen de beschikbaarheid van voldoende middelen om privacybescherming passend te waarborgen.
Verantwoording PIA's en verantwoordelijkheid voor audits	De FG ziet in overleg met de proceseigenaren toe op de controle van de uitvoering van de op basis van PIA's uitgevoerde maatregelen. Daarnaast ziet de FG toe op de ontwikkeling en uitvoering van een privacy-auditplan samen met de procesverantwoordelijken.

In onderstaand overzicht zijn de taken (op hoofdlijnen) beschreven van alle bij de privacybescherming betrokken functionarissen.

Functie	**Taak**
Dagelijks bestuur DG&J	– Vaststellen privacybeleid; – Aanwijzen portefeuillehouder voor Privacy; – Aanstellen FG (via mandaat); – Jaarlijkse rapportage aan het algemeen bestuur
Portefeuillehouder	– Toezien op ontwikkeling van themagericht privacybeleid; – Toezien op ontwikkeling en uitvoering van privacy-auditplan.
Functionaris Gegevensbescherming	– Zorgdragen voor ontwikkeling en beheer van wettelijk verplichte registers; – Houdt toezicht op en coördineert de uitvoering van het auditplan en voert daarnaast zelf controles uit; – Ziet toe op het toewijzen van verantwoordelijkheden, privacy-awareness en het opleiden van collega's; – Adviseert over het uitvoeren van Privacy Impact Assessments (PIA) en houdt toezicht op de uitvoering; – Zorgdragen voor en toezicht houden op de training van medewerkers op het gebied van privacy-bewustzijn; – Adviseert organisaties hoe te handelen rond incidenten m.b.t. het privacybeleid (o.a. datalekken); – Zorgdragen voor verantwoordingsrapportages aan het bestuur per kwartaal; – Melden van datalekken bij AP.
Adviseur Gegevensbescherming	– Adviseert in afstemming met de FG organisaties over het implementeren van de AVG en het opstellen van een strategie omtrent het gebruik van persoonsgegevens; – Adviseert/ondersteunt bij het opstellen van verwerkingsovereenkomsten; – Controleert en beheert mede de rechtmatigheid van de gegevensverwerkingen; – De Adviseur Gegevensbescherming dient onder aansturing door de FG o.a.: o *Het Register van Verwerkingen te controleren en beheren;* o *Toe te zien op invulling, door afdeling contractmanagement, van het Register van verwerkingsovereenkomsten;* o *Het Register van Rechten betrokkenen te controleren en beheren;* o *Het Register voor het melden van inbreuken op de persoonsgegevens (datalekken)te maken en bijhouden;* o *Dossiervorming van de achterliggende stukken;* – Handelt in naam van de FG bezwaren af in het kader van verwerking persoonsgegevens; – Ziet mede toe op en adviseert in concrete situaties over het toewijzen van verantwoordelijkheden, privacy-awareness en draagt zorg voor het opleiden van collega's; – Adviseert in overleg met de FG over het uitvoeren van Privacy Impact Assessments (PIA) en houdt mede toezicht op de uitvoering.
Proceseigenaren	– Toezien op het in behandeling nemen en correct afhandelen van verzoeken om inzage en informatie van betrokkenen; – Training van en toezicht op privacy bewustzijn van medewerkers; – Kwartaalrapportages aan FG; – Melding van datalekken bij FG.
Privacyadviseurs JKC	– Het in behandeling nemen en afdoen van adviesvragen op het gebied van privacybescherming.
Privacycoördinatoren	– Opbouwen en onderhouden van privacy deskundigheid binnen de afdeling (structureel); – Adviseren over eenvoudige ad-hoc privacy vraagstukken die de afdeling betreffen; – Uitvoeren van het beleid binnen de organisatie c.q. afdeling;

	– Meewerken aan het opstellen en bewaken van afdelingsspecifieke werkinstructies; – Ontwikkelen van afdelingsspecifieke handreikingen voor professionals; – Eerste aanspreekpunt voor het afdelingshoofd betreffende privacy; – Ondersteuning bij het beantwoorden van vragen uit het bestuur; – Het in ontvangst nemen en, zo nodig, voor advies doorzenden aan de Privacyadviseurs JKC van verzoeken om inzage en informatie van betrokkenen; – Zorgt ervoor dat betrokkenen met de FG contact kunnen opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten uit hoofde van deze verordening; – Coördineert en bewaakt inzageprocessen, zo nodig, signaleren en opschalen naar klachtenprocedure (incidenteel); – Meewerken aan onderzoeken (incidenteel); – Verantwoordelijk voor het verzamelen van informatie ten behoeve van data-inventarisaties; – Voorbereiden van informatie voor meldingen van gegevensverwerking (melding wordt gedaan door FG); – Collega's actief wijzen op de meldplicht (kennissessies), signalen oppakken en doorzetten; – Informeert de FG naar behoren en tijdig bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. (structureel); – Informeert de Adviseur Gegevensbescherming over nieuwe projecten waarbij privacy een rol speelt (incidenteel); – Mee reviewen van externe communicatie over privacy en gezamenlijke belangen bewaken; – Controleren en aanvullen Register van verwerkingsactiviteiten; – Voorbereiding en eventueel opstellen van convenanten en verwerkersovereenkomsten; – Kennis nemen van relevante privacy-ontwikkelingen; – Autorisatie matrices mee beoordelen en controleren; – Signaleren van afwijkingen in de afspraken rondom gegevensverwerkingen in datasystemen; – Bijdrage leveren aan control van privacy; – Verantwoordelijk voor de informatieverstrekking in het kader van audits en mede aanspreekpunt voor de auditcommissie; – Voor zover er sprake is van een afdelingsspecifieke audit, deze uitvoeren en mee ontwikkelen; – Wint advies in bij de FG bij PIA's en beoordeling van het effect van gegevensbescherming – Uitvoeren van PIA's (privacy impact assessments) op bestaande werkprocessen.