Omgevingsdienst Zuid-Holland Zuid

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 549
12 april
2018

Officiële uitgave van de gemeenschappelijke regeling Omgevingsdienst Zuid-Holland Zuid

Privacy- en informatiebeveiligingsbeleid Omgevingsdienst Zuid-Holland Zuid

Inhoudsopgave

1. Inleiding

Gemeenten en gemeentelijke organisaties, waaronder de Omgevingsdienst Zuid-Holland Zuid (OZHZ), verwerken persoonsgegevens om een dienst te verlenen, een product te leveren of om andere doelen te bereiken. Het belang van de gemeenten en gemeentelijke 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 overheidsorganisaties binnen de regio Drechtsteden, waaronder OZHZ, hebben het derhalve hoog op de agenda staan om zo goed mogelijk de Europese Algemene Verordening Gegevensbescherming (AVG) na te leven en 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 is het gezamenlijke privacybeleid geformuleerd, waarin beschreven staat hoe om te gaan met de verwerking van persoonsgegevens. OZHZ heeft er daarbij voor gekozen de tekst van het beleid toe te spitsen op de eigen organisatie, en het informatiebeveiligingsbeleid en privacybeleid in één beleidskader te combineren. 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 een goede toepassing van het informatiebeveiligingsbeleid van cruciaal belang.

In het privacybeleid staan de kaders beschreven voor het verwerken van privacygevoelige informatie oftewel persoonsgegevens, de bescherming van deze gegevens en omgang met deze gegevens. Dit beleid dient als kapstok, waarbij ervoor kan worden gekozen voor een specifiek vakgebied een beheerplan of privacyprotocol op te stellen. In het verlengde daarvan is informatie één van de belangrijkste bedrijfsmiddelen van OZHZ, met als uitgangspunt dat OZHZ digitaal betrouwbaar werkt, de gebruikte informatie klopt en ook veilig wordt verwerkt. Goede informatiebeveiliging is dus van belang. Informatiebeveiliging gaat echter niet alleen over digitaal werken, maar om alle uitingsvormen van informatie (analoog, digitaal, gesproken, enzovoort), alle mogelijke informatiedragers (papier, elektronisch, foto, etc.) en alle informatieverwerkende systemen. Het gaat dus over meer dan ICT-systemen, en het gaat zeker ook over mensen en processen. Een betrouwbare informatievoorziening is noodzakelijk voor goede taakuitvoering en dienstverlening. Dit vereist een integrale aanpak en risicobewustzijn binnen de hele organisatie. OZHZ heeft de informatiebeveiliging daarom verankerd in de bedrijfsvoering.

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) is verantwoordelijk voor een juiste verwerking van persoonsgegevens.

2. Uitgangspunten

2.1 Doelstellingen van het beleid

Doelstelling van het beleid is dat op een verantwoordelijke wijze en binnen wettelijke kaders met privacygevoelige gegevens wordt omgegaan. Het wettelijk kader voor bescherming van persoonsgegevens wordt - naast vele specifieke wetten - gegeven door de AVG. De eisen die de AVG stelt aan het verwerken van persoonsgegevens zijn dan ook zorgvuldig geïmplementeerd binnen OZHZ, waarbij deels wordt aangesloten bij de Drechtsteden. Als startpunt is het verplichte bewustwordingsprogramma voor alle medewerkers opgezet. De privacybescherming kan zo stapsgewijs worden verhoogd en vormt de basis voor de vergroting van het bewustzijn over privacy en informatieveiligheid en de verdere professionalisering binnen alle lokale organisaties. Alle units binnen OZHZ zijn bovendien in de aanloop naar 25 mei 2018 betrokken geweest bij de implementatie van de AVG, en hebben daarvoor waardevolle input geleverd. Zij zijn het immers die hun processen het beste kennen.

OZHZ wil hiermee onder andere bereiken dat:

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

2.2 Begrippenkader

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

Accountability: Het kunnen aantonen op welke manier de persoonsgegevens worden verwerkt conform de AVG. Hiertoe dienen passende en effectieve maatregelen te worden genomen, zoals:
- documentatieplicht: het bijhouden van een register van verwerkingen;
- het beschermen van gegevens door 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, alsmede een procedure voor het melden van een datalek aan AP;
- het aanstellen van een Functionaris Gegevensbescherming.

Betrokkene: De natuurlijke persoon van wie de gegevens worden verwerkt.

BIG Baseline Informatiebeveiliging Nederlandse Gemeenten, het normenkader informatiebeveiliging dat geldt voor gemeenten.

DB: Het dagelijks bestuur van OZHZ.

Functionaris Gegevensbescherming (FG): De FG is de interne toezichthouder op de verwerking van persoonsgegevens. De FG dient in alle onafhankelijkheid zijn werkzaamheden te kunnen uitvoeren en ontvangt daarbij geen instructies van opdrachtgevers of verwerkers. Hij is aangemeld bij de AP als contactpersoon en aanspreekpunt voor de meldingen van datalekken. Hij functioneert als tussenpersoon tussen verschillende belanghebbenden en is daarmee ook verlengstuk van de Autoriteit Persoonsgegevens (AP). De FG van de Drechtsteden is tevens FG van OZHZ.

Gegevensbeschermingseffectbeoordeling, 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.

IB-functionaris (functionaris informatiebeveiligingsbeleid) De functionaris informatiebeveiliging adviseert binnen OZHZ over informatiebeveiliging en coördineert en monitort de uitvoering van de maatregelen. De IB-functionaris rapporteert rechtstreeks aan de directie.

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.

Informatiebeveiliging: Informatiebeveiliging gaat over alle uitingsvormen van informatie (analoog, digitaal, gesproken, etc.), alle mogelijke informatie¬dragers (papier, elektronisch, foto, etc.) en alle informatie verwerkende processen en systemen. Daarbij wordt gekeken naar vier aspecten:
- Beschikbaarheid / continuïteit van data en systemen: OZHZ kan de taken uitvoeren als dat nodig is en continuïteit is gegarandeerd.
- Integriteit / betrouwbaarheid: informatie is juist en kan niet worden gewijzigd, achtergehouden of verwijderd door onbevoegden.
- Vertrouwelijkheid: data is alleen toegankelijk voor mensen die daarvoor bevoegd zijn.
- Controleerbaarheid: de bovenstaande criteria kunnen worden getoetst, en worden periodiek getoetst.

In privacywetgeving gespecialiseerde juridische adviseur: De in privacywetgeving gespecialiseerde juridisch adviseurs van het 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. Het JKC voert deze werkzaamheden ook uit voor OZHZ.

Persoonsgegevens: Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene) als bedoeld in de AVG of daarvoor in de plaats tredende wetgeving. Naast gewone persoonsgegevens, zoals naam en adresgegevens, zijn er ook bijzondere persoonsgegevens, zoals etnische achtergrond, politieke voorkeur, gezondheid en strafrechtelijke gegevens. In de Uitvoeringswet AVG is bovendien opgenomen dat speciale regels gelden voor verwerking van een nationaal identificatienummer (BSN).

Privacybescherming: Het omgaan met persoonsgegevens conform de eisen in de AVG.

Privacycoördinatoren: Medewerkers binnen OZHZ die worden getraind door de in privacywetgeving gespecialiseerde adviseurs. Zij zijn het interne aanspreekpunt voor de organisatie en communiceren en rapporteren met/aan de FG.

Proceseigenaren: Degenen die binnen de organisatie zijn aangewezen als verantwoordelijke voor een proces. Binnen OZHZ zijn dit de managers van de units.

Verwerking: Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedures, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens. Ook het publiceren van informatie op het internet kan zo'n verwerking zijn.

Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die of dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. OZHZ heeft in de praktijk te maken met meerdere verwerkers waarmee verwerkersovereenkomsten zijn afgesloten.

Verwerkingsverantwoordelijke Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst die of een ander orgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In de relatie met de deelnemers in de gemeenschappelijke regeling van OZHZ dient OZHZ te worden beschouwd als verwerkingsverantwoordelijke. Dat betekent dat OZHZ zelf verantwoordelijk is voor de naleving van de AVG en daarop aanspreekbaar is.

2.3 Juridisch kader – basiseisen uit de AVG

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

De AVG is de hoogste wetgeving voor privacybescherming en fungeert als een parapluwet die van toepassing is voor alle verwerkingen van persoonsgegevens door organisaties, zowel bedrijven als overheden. De uitgangspunten van de AVG zijn:

- 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 de sluiting van een overeenkomst maatregelen te nemen;
- de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
- verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
- de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen.

Vervolgens moet worden vastgesteld dat de verwerkte persoonsgegevens proportioneel zijn (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 strafrechtelijke gegevens, 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). In de Uitvoeringswet AVG is bovendien opgenomen dat speciale regels gelden voor verwerking van een nationaal identificatienummer (BSN). Veelal wordt het BSN aangeduid als een 'gevoelig persoonsge-

geven'. Het verwerken van bijzondere (artikel 9 AVG) en gevoelige persoonsgegevens 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 vragen. Om het proces van gegevensverwerking ordelijk te laten verlopen en betrokkenen (burgers) makkelijk toegang te geven tot OZHZ is een FG (artikel 37 AVG) aangesteld.

OZHZ heeft de wettelijke verplichting om gegevensbescherming te borgen. Dit moet hij doen door technische en organisatorische maatregelen te treffen (artikel 15 VG). Informatieveiligheid is hiervan een belangrijk onderdeel. Samen met onder andere informatiebeheer, het juridisch kader en privacybewustzijn zorgt informatieveiligheid voor de borging van bescherming van privacygevoelige gegevens.

Het voorliggende privacy- en informatiebeveiligingsbeleid van OZHZ gaat uit van het voldoen aan de eisen van de AVG en de Uitvoeringswet AVG. Daarnaast zijn er diverse specifieke wetten, zoals de BRP, WMO, Jeugdwet, Politiewet, die aanvullende eisen stellen aan privacybescherming. OZHZ heeft niet met al deze wetten te maken. In de context van de Drechtsteden worden deze wetten later meegenomen in de uitwerking van het privacybeleid, omdat deze wetten vanzelfsprekend van belang zijn voor de medewerkers die op basis van deze wetten taken uitvoeren.

2.4 Wijze van inrichten van de gegevensverwerking

Door het cyclische karakter van de aangegeven maatregelen en door de bescherming van persoonsgegevens onderdeel te laten zijn van het kwaliteitsmanagementsysteem van OZHZ en daarmee vast op de verschillende agenda's te plaatsen, ontstaat een continue proces van veranderen en verbeteren. De kwaliteit van het omgaan met privacyvraagstukken wordt immers verhoogd door op verschillende niveaus en vanuit verschillende rollen telkens weer de Deming-cyclus van plan-do-check-act te doorlopen. Hierdoor ontstaat een evenwichtig privacy- beheersingssysteem. Organisaties werken zo actief aan privacybewustzijn, het opbouwen van kennis bij medewerkers en aan verantwoorde procesuitvoering.

Het borgen van de privacy is onlosmakelijk verbonden met informatiebeveiliging. In dat kader werkt OZHZ nauw samen met het Servicecentrum Drechtsteden (SCD).

2.5 Informatiebeveiliging

Doel van het informatiebeveiligingsbeleid is dat informatie van OZHZ beschikbaar en integer is, alleen toegankelijk is voor mensen die daarvoor bevoegd zijn en dat dit beleid controleerbaar wordt uitgevoerd. Het beleid geeft het kader voor passende technische en organisatorische maatregelen om informatie te beschermen en te waarborgen dat OZHZ voldoet aan relevante wet- en regelgeving. Dit informatiebeveiligingsbeleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten en informatiesystemen.

OZHZ gaat als volgt om met informatiebeveiliging:

- OZHZ hanteert als normenkader de BIG, het gemeenschappelijk normenkader voor gemeenten.
- OZHZ gaat uit van een risicobenadering op basis van het ‘pas toe of leg uit’ principe.
- De directie benoemt de verantwoordelijkheden voor informatiebeveiliging in algemene uitvoeringsmaatregelen. Deze sluiten aan op bestaande taken en bevoegdheden en de mandaatregeling.
- OZHZ heeft een PDCA-cyclus, met een jaarlijks werkplan voor informatiebeveiliging en een jaarlijkse rapportage over de uitvoering en incidenten. Het beleid wordt periodiek geëvalueerd.
- OZHZ heeft een functionaris informatiebeveiliging voor de coördinatie, monitoring en advisering. Deze rapporteert rechtstreeks aan de directie.

Op basis van deze uitgangspunten stelt de directie uitvoeringsmaatregelen vast voor het informatiebeveiligingsbeleid.

2.6 Doelgroep

Het beleid is van toepassing op alle taken en processen waarvoor OZHZ verantwoordelijk is. Dit betreft zowel de taken die OZHZ op grond van de gemeenschappelijke regeling, al dan niet in mandaat, uitvoert voor de bestuursorganen van de gemeenten en de provincie Zuid-Holland, alsmede de taken die OZHZ uitvoert als openbaar lichaam in het kader van de Wet gemeenschappelijke regelingen (Wgr) en als werkgever. OZHZ geldt hierbij als verwerkingsverantwoordelijke in de zin van de AVG.

Dit privacy- en informatiebeveiligingsbeleid 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. Bestuur en mana-

gement spelen een belangrijke rol bij de besluitvorming over dit onderwerp en de sturing ervan in de planning- en controlcyclus.

2.7 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 beleid 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 namelijk recht op:

- inzage van gegevens (artikel 15 AVG);
- rectificatie van gegevens (artikel 16 AVG);
- gegevenswissing, oftewel 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);
- het niet onderworpen worden aan geautomatiseerde besluitvorming (artikel 22 AVG).

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

3.1 Recht op inzage van gegevens (artikel 15 AVG)

De betrokkene heeft het recht om van OZHZ 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). OZHZ kan verlangen dat de betrokkene zich op adequate wijze identificeert. Het is immers belangrijk dat de gevraagde persoonsgegevens bij de juiste persoon terecht komen. Het recht van inzage is mede bedoeld om uitoefening van de rechten van een rectificatie (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 OZHZ 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 artikel 5, eerste lid onder d, AVG, het beginsel van juistheid van persoonsgegevens. OZHZ en een eventuele verwerker van de persoonsgegevens moeten alle redelijke maatregelen nemen om er voor te zorgen dat onjuiste persoonsgegevens worden gerectificeerd. Het is daarbij irrelevant of de onjuistheden berusten op een fout van OZHZ of een verwerker.

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

De betrokkene heeft het recht van OZHZ zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen. OZHZ is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer dit van toepassing is.

Op grond van de beginselen van juistheid en opslagbeperking (beide geregeld in artikel 5 AVG) mogen persoonsgegevens niet langer worden bewaard dan nodig is voor het doel van hun verwerking. Het recht van gegevenswissing werkt dit nader uit tot een recht voor de betrokkene om overtollige persoonsgegevens gewist te krijgen met corresponderende plicht voor OZHZ en een eventuele verwerker.

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

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

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

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

Wanneer OZHZ een rectificatie (artikel16 AVG), gegevenswissing (artikel 17 AVG) of beperking (artikel 18 AVG) van persoonsgegevens van betrokkene uitvoert, worden alle ontvangers van die persoonsgegevens hierover ingelicht. Doel van deze kennisgeving is dat deze ontvangers de betreffende rectificatie, wissing of betrekking ook doorvoeren.

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

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

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

3.7 Recht om niet onderworpen te worden aan geautomatiseerde besluitvorming (artikel 22 AVG)

Bij geautomatiseerde individuele besluitvorming is geen sprake van (noemenswaardige) menselijke tussenkomst zodat eventuele uitkomst kunnen worden gecorrigeerd. Het is uitsluitend gebaseerd op geautomatiseerde verwerking van persoonsgegevens. OZHZ zal geen persoonsgegevens verwerken op een manier die onder dit artikel valt.

4. Werkprocessen

4.1 Omgaan met persoonsgegevens

OZHZ verwerkt persoonsgegevens alleen indien het doel van de verwerking kan worden gebaseerd op één van de zes rechtsgrondslagen van artikel 6 AVG. In het merendeel van de gevallen worden persoonsgegevens door de betrokkene zelf verstrekt. Veel gebruikte gegevens of al bekende gegevens die zijn opgenomen in basisregistraties of andere authentieke bronnen, worden daaruit opgevraagd indien OZHZ daartoe toegang heeft. 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 conform de categorisering van de gegevens zoals vastgelegd in de dataclassificatie. Informatiesystemen moeten voldoen aan de eisen van de 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 persoonsgegevens worden verwerkt.

Het is van groot belang dat medewerkers die daadwerkelijk werken met persoonsgegevens weten wat hun verantwoordelijkheid is en hoe zij zorgvuldig om dienen te gaan met persoonsgegevens. Zij dienen in staat te zijn om te beoordelen welke gegevens nodig zijn voor het uitvoeren van de werkprocessen. Er dienen niet te weinig, maar ook niet te veel gegevens te worden verwerkt (artikel 5.1c AVG). De FG zorgt er samen met IB-functionaris voor dat informatie over gegevensbescherming en informatieveilig-

heid herhaaldelijk onder de aandacht wordt gebracht van leidinggevenden en medewerkers. Medewerkers worden getraind in privacy- bewust 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 de privacycoördinator (zowel juridisch als voor informatiebeveiliging). Op de achterhand kan via de privacycoördinator gebruik worden gemaakt van de ondersteuning door het JKC.

4.3 Verplichte maatregelen en procedures

Om te voldoen aan de eisen van de AVG is een aantal maatregelen getroffen en zijn procedures ingericht:

- Alle bij OZHZ gangbare processen waarin persoonsgegevens worden verwerkt zijn in beeld gebracht en vastgelegd in het Register van verwerkingen. Voor de primaire processen geldt de Product Diensten Catalogus (PDC) van OZHZ als basis. Daarnaast is ook van alle overige processen in beeld gebracht welke persoonsgegevens worden verwerkt. Naast de vanuit de AVG verplichte onderdelen van de registratie is in het register tevens vastgelegd of er extra maatregelen nodig zijn ten opzichte van de standaard van de BIG. Dit register is openbaar beschikbaar op de website van OZHZ.

- Met externe verwerkers van persoonsgegevens zijn verwerkersovereenkomsten afgesloten. Indien van toepassing wordt in het zakensysteem van OZHZ bij elk contract een verwerkersovereenkomst gevoegd. Een overzicht van verwerkersovereenkomsten is opgenomen in een Register van verwerkersovereenkomsten.

- OZHZ werkt met meerdere geautomatiseerde systemen, zowel voor de primaire als voor de overige processen. Er is daarom een Register van informatiesystemen opgesteld. Hierin is per systeem vastgelegd welke niveaus van integriteit en vertrouwelijkheid gelden en welke (inrichtings) maatregelen daarbij passen.

- Er is een dienstverleningsovereenkomst afgesloten met het JKC/SCD ten behoeve van de ondersteuning bij het invullen van de verplichte functie van Functionaris Gegevens-bescherming op grond van artikel 37, eerste lid, en 6 AVG, advisering in privacy-vraagstukken, juridische begeleiding van datalekken en de juridische advisering daarover (maatregelen treft OZHZ zelf), het verzorgen van meldingen van datalekken bij de Autoriteit Persoonsgegevens, het bijhouden van het register datalekken, het uitvoeren van privacyaudits in het kader van de PDCA-cyclus en training ten behoeve van privacy compliance.

- In het verlengde van de dienstverleningsovereenkomst is ook het mandaatbesluit van het DB OZHZ aan het DB van de Gemeenschappelijke regeling Drechtsteden (GRD) dienovereenkomstig aangepast.

- Er is een procedure vastgesteld voor de afhandeling van incidenten en datalekken, het informeren van betrokkenen in geval van een datalek, voor het afhandelen van verzoeken van burgers op grond van de AVG (de rechten van betrokkenen) en voor de organisatie van de informatiebeveiliging. Met het JKC/SCD is een dienstverleningsovereenkomst gesloten voor de uitvoering van een deel van de taken (zie hierboven).

- In het Register voor aanvragen van betrokkenen wordt bijgehouden welke aanvragen er zijn gedaan door betrokkenen en het afhandelingstraject van de aanvraag. Het zaaksysteem van OZHZ fungeert als zodanig.

- Voor de rechten van betrokkenen zijn werkprocessen opgesteld.

De genoemde procedures en met het JKC/SCD gemaakte afspraken maken onderdeel uit van het kwaliteitmanagementsysteem van OZHZ.

4.4 Dataclassificatie

Voor de aspecten beschikbaarheid, integriteit en vertrouwelijkheid hanteert OZHZ een classificatie met een basisniveau van beveiliging. Het uitgangspunt is 'basisniveau, tenzij'. Dat wil zeggen dat het basisniveau voldoende, tenzij uit een analyse blijkt dat een lager niveau mag, of een hoger niveau moet worden toegepast. Deze analyse wordt voor ieder proces gemaakt en vastgelegd in het Register van verwerkingen. De proceseigenaar is hiervoor verantwoordelijk. Dit betreft zowel de technische maatregelen (inrichting van systemen) als gedragsmaatregelen (beschrijving van het proces in het kader van het kwaliteitsbeleid).

Veel processen worden echter met algemene systemen uitgevoerd. Voor die systemen wordt voor alle processen één basisniveau vastgesteld met de bijbehorende technische maatregelen. De systeemeigenaar is hiervoor verantwoordelijk. Vervolgens wordt voor afzonderlijke processen gekeken of er nog een

hoger niveau nodig is. Dat wordt bepaald door de proceseigenaar. Een en ander wordt vastgelegd in het Register van informatiesystemen.

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. Daarnaast geldt de Archiefwet voor het bewaren van papieren en elektronische documenten en past OZHZ de selectielijsten voor de archiefbescheiden van gemeentelijke en intergemeentelijke organen en voor provinciale organen toe. Daar waar er geen wettelijke bepaling is die voorziet in een verplichte bewaartermijn, neemt OZHZ een eigen besluit over de bewaartermijn.

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 bijvoorbeeld een melding of aanvraag gedaan wordt, dit gepaard gaat met verwerking van zijn of haar gegevens. Het is hierom van belang dat OZHZ de betrokkene informeert hoe zijn of haar gegevens worden verwerkt. OZHZ doet dit in eerste instantie door betrokkenen hierover op de website te informeren en daar ook het Register van verwerkingen beschikbaar te stellen, derhalve ook in de gevallen waarin de gegevens niet van een betrokkene zijn verkregen. Betrokkenen ontvangen in individuele gevallen ook een ontvangstbevestiging van hun melding of aanvraag.

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

4.7 Open communicatie

Betrokkenen moeten erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. OZHZ maakt daarom inzichtelijk, door middel van verschillende communicatiekanalen, op welke wijze persoonsgegevens worden verwerkt en beheerd. Onder meer door het Register van verwerkingen, informatie over de rechten van betrokkenen en contactgegevens van de FG te publiceren op de website. Betrokkenen worden zo gefaciliteerd in het doen van een beroep op één of meerdere van hun rechten. Processen en informatiesystemen die door OZHZ 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 persoonsgegevens, inbraak door een hacker, maar ook aan onbevoegde autorisaties in een informatiesysteem of aan het toegestuurd krijgen van informatie met bijzondere persoonsgegevens die niet voor de ontvanger is bestemd (brief of e-mail), het in de post zoekraken van een dossier, enzovoort. Ook het intern verwerken van te veel bijzondere persoonsgegevens is een datalek.

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

Een melding moet indien van toepassing ook onverwijld aan betrokkenen worden gedaan (artikel 34 AVG). Om aan de wet te kunnen voldoen hanteert OZHZ, met tussenkomst van het JKC/SCD, een procedure voor standaard incidentbeheer: de privacyincidentprocedure die hier goed op aansluit. Het vormt de basis van het Register van inbreuken op persoonsgegevens/datalekken.

Hoe een betrokkene een (vermoedelijk) datalek kan melden is te lezen op de website van OZHZ. Ook deze meldingen worden door OZHZ, via het JKC/SCD, gemeld bij de AP.

4.9 Verwerkersovereenkomst

Bij veel processen worden gegevens verwerkt door derden. Zie hierover artikel 4 AVG. Hierbij kan onder andere worden gedacht aan de werkzaamheden die medewerkers van OZHZ uitvoeren via een applicatie

in de Cloud. Ook de GRD, in haar hoedanigheid als leverancier van de ICT-infrastructuur van OZHZ, is in die zin te beschouwen als een verwerker.

Het verlenen van opdrachten aan derden (verwerkers) brengt risico's met zich mee op het gebied van gegevensverwerking en informatieveiligheid. OZHZ 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 OZHZ dan ook verwerkersovereenkomsten af. In de verwerkersovereenkomsten worden minimaal afspraken gemaakt over:

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

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 DB OZHZ is verantwoordelijk voor de juiste uitvoering van de AVG en naleving van het privacybeleid. Het is zijn verantwoordelijk voor het verwerken van persoonsgegevens door de eigen organisatie en voor de taken die met toepassing van de gemeenschappelijke regeling en van de mandaatbesluiten van de bestuursorganen van gemeenten en provincie door OZHZ worden uitgevoerd. De FG zorgt voor onafhankelijk toezicht en controle op de kwaliteit van de uitvoering van het privacybeleid.

Het DB zal binnen de jaarlijkse planning- en controlcyclus het algemeen bestuur (AB) informeren over de risico's en over de getroffen beheersmaatregelen op het gebied van privacy en informatiebeveiliging binnen de processen waarvoor OZHZ verantwoordelijk is.

Op grond van de AVG wordt de uitvoering van het privacybeleid elk jaar door de FG geauditeerd. De FG rapporteert aan het DB. Het afleggen van jaarlijkse verantwoording door de FG doet overigens niet af aan de algemene informatieplicht van het DB aan het AB op grond van artikel 19a van de Wgr.

Het DB meldt bijzonderheden ten aanzien van gegevensverwerking, te denken valt aan ernstige inbreuk op of verlies van persoonsgegevens, afzonderlijk en proactief aan het AB.

5.2 Functionaris Gegevensbescherming

Voor onafhankelijk toezicht en controle op de kwaliteit van de uitvoering van het privacybeleid hebben de Drechtsteden op grond van artikel 37 AVG een FG aangesteld. Deze functie is gepositioneerd binnen het SCD. De FG heeft een onafhankelijke positie in de organisatie. De werkzaamheden die een FG uitvoert hebben een wettelijke grondslag in de artikelen 37 t/m 39 AVG. De FG van de Drechtsteden is mede namens het DB van OZHZ aangewezen.

De interne verantwoording is gewaarborgd door proceseigenaren binnen OZHZ, zijnde de unitmanagers, die rapporteren aan de privacycoördinator van OZHZ (zie hierna) over de realisatie van passende privacywaarborgen. Zij rapporteren onverwijld bij privacyincidenten conform de vastgestelde privacyincidentprocedure. Ook afwijkingen van de uitvoering van het privacybeleid worden direct gerapporteerd.

OZHZ maakt afspraken met de FG over een privacy-auditplan. Binnen OZHZ worden hierover afspraken gemaakt tussen de privacycoördinator en de kwaliteitscoördinator. De compliance van de AVG is onderdeel van het kwaliteitsmanagementsysteem. 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 OZHZ, in control zijn en dat de registers op orde zijn. Ook in geval van calamiteiten moeten de procedures goed werken en dienen organisaties in control te zijn. De FG ziet toe op de prioritering van de processen en de wijze van implementatie van maatregelen.

De AVG verplicht tot het bijhouden van registers:

- Register van verwerkingen, met aantekeningen van PIA's;
- Register van verwerkersovereenkomsten;
- Register van inbreuken op persoonsgegevens, datalekken;
- Register voor aanvragen van betrokkenen,

waarbij het Register van datalekken wordt bijgehouden door de FG. OZHZ houdt de overige registers bij. Het Register van verwerkingen is beschikbaar via de website van OZHZ.

De FG toetst de toepassing van het privacybeleid door OZHZ 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.

5.3 Adviseur gegevensbescherming

De adviseur gegevensbescherming ondersteunt de FG bij het uitvoeren van wettelijke taken zoals omschreven in artikel 38 en 39 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 privacybeleid van Drechtstedenorganisaties, waaronder OZHZ. De 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. Belangrijk zijn daarbij zowel juridische als technische aspecten met betrekking tot de bescherming van persoonsgegevens.

De adviseur gegevensbescherming ziet mede toe op en adviseert in concrete situaties over het toewijzen van verantwoordelijkheden, privacy-awareness en draagt zorg voor het opleiden van medewerkers. In overleg met de FG adviseert de adviseur gegevensbescherming over het uitvoeren van PIA's en houdt mede toezicht op de uitvoering.

Onder aansturing van de FG heeft de adviseur gegevensbescherming onder andere de volgende taken:

- Adviseren over het Register van verwerkingen;
- Maken en bijhouden van het Register voor het melden van inbreuken op de persoonsgegevens (datalekken);
- Adviseren over het afsluiten van verwerkersovereenkomsten en het Register van verwerkingsovereenkomsten;
- Beheren en controleren van het Register van de rechten van betrokkenen;
- Dossiervorming van de achterliggende stukken.

5.4 Privacycoördinatoren

Privacycoördinatoren zijn medewerkers binnen de organisaties van de Drechtsteden die worden getraind door de adviseurs gegevensbescherming. Zij zijn het interne aanspreekpunt voor de organisaties en communiceren en rapporteren aan en met de FG. Ook OZHZ werkt met een privacycoördinator.

Bij het in ontvangst nemen en, zo nodig, voor advies doorzenden aan het JKC van verzoeken om inzage en informatie van betrokkenen speelt de privacycoördinator een coördinerende rol Daarnaast bewaakt hij de inzageprocessen en zal, indien van toepassing, 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. OZHZ heeft dit ook op zijn website gecommuniceerd.

5.5 Taken en verantwoordelijkheden bij informatiebeveiliging

Algemeen uitgangspunt is dat de taken en verantwoordelijkheden voor het informatiebeveiligings-beleid binnen OZHZ zoveel mogelijk aansluiten bij de bestaande taken en verantwoordelijkheden van de units en daarin werkende functionarissen conform de geldende Organisatieregeling en (onder-) mandaatregelingen. De unitmanagers zijn verantwoordelijk voor het informatiebeveiligingsbeleid binnen hun unit.

De maatregelen over de hele organisatie zijn ingedeeld in deelgebieden. Voor ieder deelgebied is een unitmanager van OZHZ verantwoordelijk voor de risicobeoordeling en uitvoering van de maatregelen. Deze beoordeelt of een maatregel nodig is en bepaalt door wie en wanneer deze wordt uitgevoerd.

Ook houdt de unitmanager toezicht op de uitvoering. Indien daarvoor onderliggend beleid moet worden vastgesteld, gebeurt dat op het niveau dat daarvoor bevoegd is. Zo stelt het dagelijks bestuur het personeelsbeleid vast, liggen algemene maatregelen bij de directie en zal unitmanager het uitvoerend beleid vaststellen. De coördinerende rol ligt bij de functionaris van OZHZ die verantwoordelijk is voor de implementatie van het Informatiebeveiligingsbeleid (IB-functionaris).

Ieder informatiesysteem binnen OZHZ heeft een unitmanager als eigenaar toegewezen gekregen. Deze wijst voor het informatiesysteem een functioneel beheerder aan. Dit wordt vastgelegd in het Register voor informatiesystemen. Ieder informatiesysteem kent een basisinrichting voor de maatregelen op het gebied van informatiebeveiliging en privacy. Ook de maatregelen voor de basisinrichting zijn vastgelegd in dit register. De eigenaar is eindverantwoordelijk voor de uitvoering van de maatregelen en de periodieke beoordeling van de maatregelen.

Ook ieder proces heeft een unitmanager als eigenaar. In het Register van verwerkingen staat welke unitmanager eigenaar is van welk proces. De eigenaar bepaalt of er, naast het basisniveau van het gebruikte informatiesysteem, extra maatregelen nodig zijn voor informatiebeveiliging en privacy. Dat kan gaan om maatregelen in een informatiesysteem of om maatregelen daarbuiten.

De IB-functionaris coördineert de uitvoering van het informatiebeveiligingsbeleid en ondersteunt de unitmanagers, monitort de uitvoering van het werkplan en is verantwoordelijk voor de uitvoering van de jaarcyclus. De IB-functionaris adviseert gevraagd en ongevraagd rechtstreeks de directie en unitmanagers over maatregelen op het gebied van informatiebeveiliging. Daarnaast is de IB-functionaris verantwoordelijk voor de afhandeling van beveiligingsincidenten, tenzij dit expliciet elders is belegd (zoals bij de meldplicht datalekken).

Met het SCD als ICT-leverancier zijn afspraken gemaakt over de verantwoordelijkheden voor het nemen van maatregelen die betrekking hebben op de technische infrastructuur en over de uitvoering van de BIG. OZHZ toetst niet de uitvoering van iedere maatregel afzonderlijk, maar baseert zich op de rapportage en de audit van het SCD.

5.6 Sturing en monitoring

De proceseigenaren zijn verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens die binnen zijn of haar unit plaatsvindt. Zij zijn daarom ook verantwoordelijk om te monitoren of persoonsgegevens zorgvuldig worden verwerkt en dienen dit zo nodig bij te sturen. In de praktijk wordt deze monitoring gedaan door de privacycoördinator, in samenwerking met het kwaliteitsteam. De bijsturing vindt plaats door de verantwoordelijke unitmanager.

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

In het kwaliteitsbeleid wordt informatiebeveiliging als integraal aspect van de taakuitvoering meegenomen. Dit gebeurt door het opnemen van de (gedrags)maatregelen en controlestappen in de procesbeschrijvingen die in het kader van het kwaliteitsbeleid worden gemaakt, alsmede bij het toezicht op de uitvoering van de processen in het kader van de certificering op grond van ISO 9001:2015.

OZHZ werkt bij de voorbereiding en uitvoering samen met de GRD. Er wordt gebruik gemaakt van de expertise en advisering van de CIO van de Drechtsteden. Binnen de GRD is het SCD verantwoordelijk voor veel technische maatregelen. Afstemming vindt plaats in periodiek overleg dat specifiek is gericht op informatiebeveiliging.

5.7 Overzicht schema verantwoordelijkheden en borging privacybeleid

In onderstaande tabel staat een overzicht (op hoofdlijnen) van de verantwoordelijkheden en bijbehorende verantwoordelijken betreffende uitvoering en invulling van de borging van het privacy- en informatiebeveiligingsbeleid binnen de regio en OZHZ.

Actief privacybeleid jegens betrokkenen: Proceseigenaren zijn krachtens de ondermandaatregeling van OZHZ 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 privacycoördinator betrekt de FG bij de voorbereiding van de besluitvorming en zorgt ervoor dat de aanvraag en de afhandeling in het daarvoor bestemde register worden opgenomen.

Actief privacybeleid medewerkers: De FG verzorgt samen met de privacycoördinator en 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 privacycoördinator faciliteert hierin. Proceseigenaren rapporteren hierover aan de FG, door tussenkomst van de privacycoördinator.

OZHZ beheert de afgesloten verwerkersovereenkomsten in het verplichte register van verwerkersovereenkomsten en geeft de FG daarin inzicht.

Adviseren over informatiebeveiliging en coördineren en monitoren van de uitvoering van maatregelen: De IB-functionaris adviseert binnen OZHZ over informatiebeveiliging en coördineert en monitort de uitvoering van de maatregelen. De IB-functionaris rapporteert rechtstreeks aan de directie.

Advisering over informatiebeveiligingsbeleid in het kader van het Drechtstedenbeleid: Het CIO en de CISO van de Drechtsteden adviseren over het informatiebeveiligingsbeleid, onder meer via het Periodiek Overleg Informatiebeveiliging van de Drechtsteden (PIO-D).

Beheer van het beleid: De FG rapporteert aan het DB en de directie 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 DB verantwoording af aan het AB over de risico's en beheersmaatregelen.

Informatiebeveiliging binnen de unit, risicobeoordeling en uitvoering van de maatregelen op het taakgebied van de unit, eigenaarschap van processen en van informatiesystemen: Unitmanagers OZHZ

Informatiebeveiligingtechnisch beheer: SCD-ICT is verantwoordelijk voor de informatiebeveiliging van de technische infrastructuur. De SAAS-leverancier is verantwoordelijk voor het technisch beheer van de applicatie.

Interne verantwoording: De FG rapporteert ieder kwartaal rechtstreeks aan de bestuursorganen van de Drechtsteden en aan OZHZ. De proceseigenaren rapporteren, door tussenkomst van de privacycoördinator, periodiek aan de FG over de realisatie van passende privacywaarborgen, en onverwijld bij privacyincidenten conform de vastgestelde privacy- incidentprocedure.

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 OZHZ of en hoe hierbij wordt aangesloten.

Praktische privacywaarborgen Concretiseren van praktische privacywaarborgen gebeurt onder verantwoordelijkheid van de proceseigenaar.

Privacy auditplan: De FG ziet er in afstemming met OZHZ op toe dat er een privacy auditplan ontwikkeld wordt en dat dit wordt uitgevoerd. Dit plan wordt jaarlijks opgesteld en is in lijn met het Raamwerk privacy- audit van de AP. De PDCA-cyclus wordt hierop toegepast. OZHZ zorgt ervoor dat het auditplan aansluit bij het eigen kwaliteitmanagementsysteem.

Risico gedreven aanpak: OZHZ brengt van alle primaire en overige processen de mate van persoonlijk en bestuurlijk risico in beeld. De risico's worden door praktische, organisatorische en technische maatregelen beheerst en volgens de PDCA-cyclus geborgd. In het Register van verwerking wordt vastgelegd of extra maatregelen zijn genomen bovenop de standaard van de BIG.

Toezicht: OZHZ heeft een FG aangesteld en is hiertoe een dienstverleningsovereenkomst aangegaan met het JKC/SCD. Zie de artikelen 37 t/m 39 AVG. De FG rapporteert aan OZHZ en onderhoudt de contacten met de AP.

Uitvoering van privacybeleid: Het DB is eindverantwoordelijk voor uitvoering van het beleid en voor controle op de naleving van het privacybeleid.

Vaststellen privacybeleid: Het DB heeft het beleid vastgesteld en bevordert de beschikbaarheid van voldoende middelen om privacybescherming passend te waarborgen.

Verantwoordelijk voor de uitvoering van IB-beleid voor de betreffende applicatie: Functioneel beheerders informatiesystemen

Verantwoording PIA's en verantwoordelijkheid voor audits: De FG ziet in overleg met de IB-functionaris toe op de controle van de uitvoering van de maatregelen voor informatiebeveiliging gericht op privacy. Daarnaast ziet de FG toe op de ontwikkeling en uitvoering van een privacy-auditplan samen met de privacycoördinator, de kwaliteitsmanager en de procesverantwoordelijken van OZHZ. Aan de hand hiervan kan de PDCA-cyclus worden doorlopen waarmee continu verbeteren wordt geborgd.

Aldus vastgesteld door het dagelijks bestuur van de Omgevingsdienst Zuid-Holland Zuid op 11 april 2018.