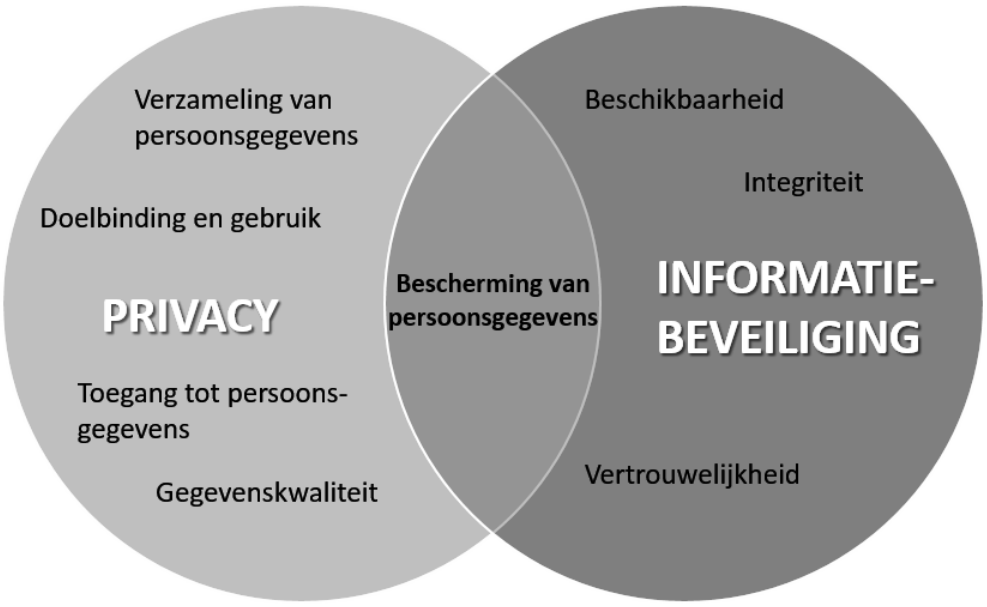
9.2

Gegevensbeschermingsbeleid

Inrichting Privacy & Informatiebeveiliging GGD Zeeland



Goes, 15 november 2020

Inhoudsopgave

1. Samenvatting

De GGD Zeeland (hierna: "GGD") verwerkt dagelijks veel gegevens en informatie over veel personen. Bescherming van deze zogenaamde persoonsgegevens tegen oneigenlijk gebruik is noodzakelijk en evident maar tegelijkertijd niet altijd eenvoudig.

Met dit beleid vult de werkgroep Gegevensbescherming van de GGD nader in hoe zij uitvoering wenst te geven aan gegevensbescherming. Het document is koersbepalend, en helpt om af te bakenen en te zien of er voldoende maatregelen zijn genomen om de persoonsgegevens te beschermen. Daarnaast wordt met naleving van dit beleid voldaan aan een wettelijke plicht en is het een manier waarmee de GGD aan zowel betrokkenen als de Autoriteit Persoonsgegevens toont dat de ze de Algemene Verordening Gegevensbescherming ("AVG") naleeft.

Een beleid voor gegevensbescherming is niet nieuw, maar is sinds de AVG een aangescherpte wettelijke verplichting voor organisaties die veel (bijzondere) persoonsgegevens verwerken, zoals de GGD.

Typisch vangt een gegevensbeschermingsbeleid aan met een antwoord op de vraag: 'Wat weet een organisatie allemaal over mensen en waarom?'. In dit geval is er voor gekozen om voor dit onderdeel te verwijzen naar het 'register van verwerkingen' van de GGD als apart document. Zie het intranet BAS/Insite van de GGD. Dit document vangt aan met de wijze waarop mensen invloed kunnen uitoefenen of grip kunnen krijgen op (verwerking van) hun persoonsgegevens bij de GGD. Dit wordt ook wel 'de rechten van betrokkenen' genoemd. Dit vindt plaats conform de privacyverklaring van de GGD. Voorts worden de (verplichte) procedures en maatregelen beschreven die de GGD hanteert om invulling te geven aan de plichten uit de AVG. Hierbij wordt achtereenvolgens stilgestaan bij:

- bewustwording van het personeel;
- (contractuele) afspraken bij (het inschakelen van) andere partijen;
- de (verplicht) aan te leggen documentatie;
- (technische én organisatorische) beveiliging van persoonsgegevens;
- (het melden van) datalekken;
- het uitvoeren van risicoanalyses bij verwerking van persoonsgegevens (DPIA's) en
- het beheer van persoonsgegevens.

Dit beleid is onderdeel van de governancestructuur van de GGD, zie rapport 'Governance IV GGD Zeeland' Hierbij worden de rollen, taken en verantwoordelijkheden die betrekking hebben op de naleving van de bepalingen uit dit beleid nader uitgewerkt.

2. Inleiding

Op 25 mei 2018 trad de Algemene Verordening Gegevensbescherming (hierna: "AVG") in werking. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de gehele Europese Unie. Lidstaten hebben slechts zeer beperkte vrijheid om aanvullende regelgeving vast te stellen. De Nederlandse wetgever bereidde daarvoor de Uitvoeringswet AVG (hierna: "UAVG") voor. Feitelijk gaat het om modernisering van de wetgeving, die een kans biedt om maatschappelijk vertrouwen in technologie te versterken. Ook stelt het organisaties in de gelegenheid om de beveiliging van waardevolle gegevens te verbeteren en zo te komen tot een 'AVG- proof' werkomgeving.

De AVG is dus een verplichting en wel één die ons in positieve zin uitdaagt om een stevige ambitie uit te spreken over het gegevensbeschermingsniveau van zowel cliënten, medewerkers als (keten)partners. Betrokkenen moeten er te allen tijde op kunnen vertrouwen dat hun gegevens bij ons in veilige handen zijn. Daarnaast is ook de samenleving kritischer en veeleisender geworden ten aanzien van de wijze waarop met gevoelige informatie wordt omgegaan.

Het beschermen van privacybelangen wordt vaak gezien als obstakel bij het uitvoeren van 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 de GGD behoorlijk en zorgvuldig omgaat met persoonsgegevens in verband met de privacy van betrokkenen.

Deze ambitie heeft een vertaalslag gekregen in dit beleid en is nader uitgewerkt in onze strategische (beleids)uitgangspunten, een governancestructuur en onderliggende protocollen en werkafspraken.

2.1. Aard en positie van dit document

Dit beleid stelt de algemene kaders vast waarbinnen de GGD gegevensbescherming regelt. Het is een kapstokbeleid dat de basis is voor de uitwerking van alle aspecten van onze bedrijfsvoering, zowel binnen als buiten de organisatie, voor zover daarbij sprake is van de verwerking van persoonsgegevens. Onderstaande tabel toont de relatie van dit beleid met andere documenten.

Governance Informatieveiligheid & gegevensbeschermingsbeleid:

Register van verwerkingen
Privacyverklaringen
Administratie van incidenten
Protocol meldplicht datalekken
Administratie van (D)PIA's
Procedure rechten van betrokkenen
Procedure nieuwe verplichtingen t.o.v. de oude wet bescherming persoonsgegevens
Procedure toestemming
Procedure bescherming persoonsgegevens conform AVG (voorheen WBP)

3. Uitgangspunten

3.1. Aanleiding, ambitie en doelstellingen van het beleid

Binnen de GGD werken we veel met persoonsgegevens: van burgers, medewerkers en (keten)partners. Deze verzamelen we voornamelijk voor het goed uitvoeren van onze taak zoals opgenomen in de Wet publieke gezondheid (hierna: "WPG") of de Wet maatschappelijke ondersteuning 2015 (hierna: "Wmo"). Men moet er op kunnen vertrouwen dat wij zorgvuldig en veilig met persoonsgegevens omgaan.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De GGD is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen te treffen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Directe aanleiding voor dit beleid is de inwerkingtreding van de AVG. De AVG staat voor een versterking en uitbreiding van privacyrechten en meer verantwoordelijkheden voor organisaties. De bevoegdheden van de Europese toezichthouders, voor Nederland de Autoriteit Persoonsgegevens (hierna: "AP"), zijn uitgebreid.

De GGD heeft de ambitie, maar ook de wettelijke verplichting om te voldoen aan de (kwaliteits)eisen voor gegevensbescherming uit de AVG. Wij stellen burgers, medewerkers en (keten)partners centraal en vinden dat ze moeten kunnen vertrouwen op een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens. Niet alleen vanwege de wettelijke verplichting en het risico op handhaving, maar juist omdat de GGD veel waarde hecht aan de bescherming van de persoonlijke levenssfeer van betrokkenen.
Daarnaast zet de GGD in op een actief gegevensbeschermingsbeleid, dat vooral gericht is op bewustwording, een transparante en kritische cultuur en kennisoverdracht. Daarbij willen wij medewerkers en klanten zoveel mogelijk betrekken bij het onderwerp gegevensbescherming en de bijbehorende dilemma's. Goede, transparante communicatie met alle belanghebbenden is van groot belang.
De GGD geeft met dit beleid duidelijk richting aan hoe er moet worden omgegaan met privacy en laat zien dat zij de bescherming van persoonsgegevens waarborgt en handhaaft. De GGD wil hiermee onder andere bereiken dat:

- de basis voor een goed geïmplementeerd beleid op het gebied van gegevensbescherming 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 zorg en overheid niet wordt beschaamd;
- uitvoering van dit beleid binnen de GGD gericht wordt opgepakt, zodat de wettelijke eisen goed geïmplementeerd zijn;
- het onderwerp zowel op bestuurlijk- als medewerkersniveau breed wordt gedragen, als onderdeel van zowel uitvoering van de wettelijke opgave, goed werkgeverschap, opdrachtnemer- en opdrachtgeverschap;
- de kans op financiële schade door het oplopen van boetes en reputatieschade voor de GGD wordt geminimaliseerd en bijbehorende risico's worden beheerst.

3.2. Begripsbepalingen

Accountability (verantwoordingsplicht)
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 voorkomende gevallen: het uitvoeren van een Data Protection Impact Assessment ("DPIA");
- het treffen van passende technische en organisatorische maatregelen, waaronder juridische en beveiligingsmaatregelen;
- het opstellen van een procedure om beveiligingsincidenten en datalekken te documenteren, alsmede een procedure voor het melden van een datalek aan AP;
- het aanstellen van een Functionaris Gegevensbescherming.

Anonimiseren
Persoonsgegevens die voor een taakuitvoering niet meer noodzakelijk zijn, worden verwijderd uit een dataset. De dataset bevat dan enkel geanonimiseerde gegevens, die wel worden bewaard voor bijvoorbeeld onderzoeksdoeleinden of om te gebruiken als open data.
Geanonimiseerde gegevens zijn geen persoonsgegevens en vallen niet onder dit beleid.

Autoriteit Persoonsgegevens
De Autoriteit Persoonsgegevens ("AP") staat voor het grondrecht op bescherming van persoonsgegevens. De AP is de toezichthoudende autoriteit verantwoordelijk voor het toezicht op de toepassing van de Verordening teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met de verwerking van hun persoonsgegevens te beschermen en het vrije verkeer van persoonsgegevens binnen de Unie te vergemakkelijken.

Betrokkene
Degene op wie de persoonsgegevens betrekking hebben.

Big data
Een of meer datasets, zowel ongestructureerd als gestructureerd, die door middel van koppeling of hergebruik geschikt zijn voor analyse doeleinden, zoals bijvoorbeeld beleidsonderzoek, gedragsonderzoek, of (medisch) wetenschappelijk onderzoek.

Dataminimalisatie
Bij het verzamelen en verwerken van persoonsgegevens mogen niet meer gegevens worden gebruikt dan nodig is om het doel waarvoor ze gebruikt zullen worden te bereiken.

DB
Het Dagelijks Bestuur van de GGD.

Derde
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.

Functionaris gegevensbescherming
De functionaris gegevensbescherming (hierna: "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 bij de meldingen van datalekken. Hij functioneert als tussenpersoon tussen verschillende belanghebbenden en is daarmee ook verlengstuk van de AP.

Geautomatiseerde (individuele) besluitvorming en profilering
Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Gegevensbescherming
Bescherming van persoonsgegevens tegen oneigenlijk gebruik.

Gegevensbeschermingseffectbeoordeling (Data protection impact assessment/DPIA)
Een instrument waarmee het effect van beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens op een gestructureerde en heldere manier in kaart wordt gebracht om vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een analyse van de gevolgen voor gegevensbescherming als een project, beleid, dienst, product of ander initiatief wordt gestart of ingevoerd en het nemen van eventueel noodzakelijke mitigerende acties om een negatieve impact te voorkomen dan wel te verkleinen.

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 (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

Een verzameling van processen die zijn ingericht om de betrouwbaarheid van informatie te beschermen. Informatiebeveiliging heeft betrekking op (BIV):

- Beschikbaarheid: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- Vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Persoonsgegevens
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Bij de GGD worden onder andere de volgende categorieën persoonsgegevens verwerkt:

- Personalia en identificatiegegevens

Persoonsgegevens, die betrekking hebben op persoonlijke bijzonderheden van betrokkene (naam, adres, woonplaats e.d.) om een persoon te kunnen identificeren.

- Medische gegevens

Persoonsgegevens, direct of indirect betrekking hebbend op de lichamelijke of geestelijke gesteldheid van betrokkene, verzameld door een beroepsbeoefenaar op het gebied van de (publieke) gezondheidszorg in het kader van zijn beroepsuitoefening.

- Financiële en administratieve gegevens

Gegevens die in de administratie van de GGD en de persoonsdossiers zijn opgenomen, niet zijnde personalia, identificatie-, medische of psychologische gegevens, die noodzakelijk zijn voor de financiering en/of administratieve afhandeling van de zorgverlening.

Toestemming van betrokkene
Elke vrije, specifieke en op informatie berustende ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling aanvaardt dat zijn persoonsgegevens worden verwerkt.

Tracking
Het volgen van mobiele datadragers zoals telefoons, bijvoorbeeld door Wifi- of bluetooth apparatuur waarbij (persoons)gegevens worden verzameld uit die datadragers.

Verwerker
Een verwerker is een persoons of organisatie die op basis van een opdracht van de verwerkingsverantwoordelijke en conform de aanwijzingen van deze verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Verwerking van persoonsgegevens
Elke handeling of geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Verwerkingsverantwoordelijke

Een persoon of instantie die, alleen of samen met een ander, het doel en de middelen voor de verwerking van de persoonsgegevens vaststelt. Binnen de GGD is het DB de verwerkingsverantwoordelijke. Het DB stelt het doel en de middelen vast voor de verwerking van persoonsgegevens. Het bestuur kan bepaalde taken overdragen aan de directeur publieke gezondheid (hierna: "DPG") die hiermee de bevoegdheid krijgt om in naam van het bestuur besluiten te nemen.

3.3. Juridisch kader

Bij dit beleid wordt in aanmerking genomen:

- Burgerlijk Wetboek, Boek 7 (Wet op de geneeskundige behandelingsovereenkomst, ”WGBO”);
- Wet op de Beroepen in de individuele gezondheidszorg (Wet Big);
- Wet kwaliteit, klachten en geschillen zorg (“Wkkgz”);
- Algemene Verordening Gegevensbescherming (“AVG”);
- Uitvoeringswet Algemene Verordening Gegevensbescherming (“UAVG”);
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (“Wabvpz”);
- Besluit elektronische gegevensverwerking door zorgaanbieders (Besluit egz);
- Wet en besluit publieke gezondheid (“Wpg”);
- Burgerlijk Wetboek, Boek 1; Jeugdwet (“Jw”);
- Wet maatschappelijke ondersteuning 2015 (“Wmo”);
- Wet verplichte meldcode huiselijk geweld en kindermishandeling;
- Wet op de lijkbezorging;
- Wet toetsing levensbeëindiging op verzoek en hulp bij zelfdoding;
- Vreemdelingenwet in verband met de Regeling verstrekkingen asielzoekers en andere categorieën vreemdelingen 2005;
- Wet op het bevolkingsonderzoek;
- KNMG-richtlijn Omgaan met medische gegevens;
- KNMG-meldcode Kindermishandeling en huiselijk geweld;
- KNMG/GGD GHOR NL/GGZ NL-handreiking Gegevensuitwisseling in de bemoeizorg;
- KNCV-richtlijn Archivering tuberculosegegevens (Commissie voor Praktische Tuberculosebestrijding);
- GGD NL-handreiking Privacybescherming epidemiologie;
- FMWV-gedragscode Gezondheidsonderzoek (Federatie Medisch Wetenschappelijke Verenigingen);

3.4. Doelgroep en toepassingsbereik

Dit beleid is van toepassing op de gehele organisatie en op alle processen, onderdelen, objecten en gegevensverzamelingen van de GGD waarin persoonsgegevens worden verwerkt. Dit betreft zowel de taken die GGD op grond van de gemeenschappelijke regeling, al dan niet in mandaat, uitvoert voor de bestuursorganen van de gemeenten, alsmede de taken die de GGD uitvoert als openbaar lichaam in het kader van de Wet gemeenschappelijke regelingen ("Wgr") en als werkgever. De GGD geldt hierbij als verwerkingsverantwoordelijke in de zin van de AVG.

Dit gegevensbeschermingsbeleid 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.

Het beleid heeft betrekking op de hele "data levenscyclus": van het genereren of verzamelen van persoonsgegevens, het dagelijkse gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging ervan.

Het gegevensbeschermingsbeleid staat niet op zichzelf. Het heeft raakvlakken of vertoont overlap met andere beleidsthema's als informatiebeveiliging, integriteit, kwaliteitszorg, personeel en organisatie en communicatie.

3.5. Inrichtingswijze gegevensverwerking

Door het cyclische karakter van de aangegeven maatregelen en door de bescherming van persoonsgegevens onderdeel te laten zijn van het managementsysteem van de GGD ontstaat een continu proces van veranderen en verbeteren. De kwaliteit van het omgaan met gegevensbeschermingsvraagstukken wordt immers verhoogd door op verschillende niveaus en vanuit verschillende rollen telkens weer de cyclus van plan-do-check-act ("PDCA") te doorlopen. Hierdoor ontstaat een evenwichtig beheersingssysteem. De GGD werkt zo actief aan bewustzijn, het opbouwen van kennis bij medewerkers en aan verantwoorde procesuitvoering op het gebied van gegevensbescherming.

Het borgen van de gegevensbescherming is onlosmakelijk verbonden met informatiebeveiliging. Informatieveiligheid en Privacy wordt bewaakt door de werkgroep Gegevensbescherming in samenwerking met alle verantwoordelijken, zie rapport Governance Informatieveiligheid GGD Zeeland.

4. Rechten van betrokkenen

4.1. Rechten van betrokkenen

- De AVG brengt betrokkenen sterkere en nieuwe privacyrechten. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt op de 'accountability', ofwel de verantwoordelijkheid van de GGD om te kunnen aantonen of de organisatie zich aan de wet houdt.

- De rechten van de betrokkenen zijn binnen de GGD transparant ingericht. Betrokkenen hebben recht op:

    - informatie en toegang tot gegevens (artikel 13 AVG en 14 AVG);
    - 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).

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

    - Om gebruik te maken van hun rechten kunnen de betrokkenen een verzoek indienen. Iemand kan een verzoek tot uitoefening van zijn of haar rechten via de website van de GGD of via andere gangbare publieksdienstverleningskanalen van de GGD doen. Dit verzoek is geldig ongeacht het middel waarmee het verzoek wordt gedaan onder voorwaarde van een deugdelijke identiteitsvaststelling.

    - Een beslissing op een verzoek wordt behandeld als een besluit in de zin van de Algemene wet bestuursrecht ("Awb"). Hiertegen kan bezwaar worden gemaakt.

4.2. Recht op informatie en toegang tot gegevens

- Tijdens het eerste contact met een cliënt informeert de hulpverlener betrokkenen over de wijze waarop zijn persoonsgegevens worden verwerkt. Er wordt dan informatie verstrekt over het (a) doel van de gegevensverwerking, (b) de aard van de gegevens die worden verwerkt, (c) de grondslag van de verwerking, (d) de rechten die ten aanzien van de gegevensverwerking kunnen worden ingeroepen en (e) de identiteit van de verantwoordelijke.

- Als het niet mogelijk is om de betrokkene tijdens het eerste contact te informeren, dan zorgt de hulpverlener dat de betrokkene zo spoedig als de situatie toe laat, alsnog over de gegevensverwerking wordt geïnformeerd.

- Van het (uitstellen of niet) informeren van de betrokkene kan een aantekening worden gemaakt in het dossier.

- De GGD verzamelt gegevens om haar taken te kunnen uitvoeren. Indien dit persoonsgegevens betreft en indien betrokkenen hiervan niet op de hoogte zijn informeert de GGD hen actief over de verwerking van hun persoonsgegevens zoals het doel daarvan, welke persoonsgegevens worden verwerkt, wie daarvoor verantwoordelijk is en of de gegevens aan anderen worden verstrekt.

- De GGD informeert betrokkene, uiterlijk binnen vier weken na de verzameling van persoonsgegevens, indien de persoonsgegevens van derden afkomstig zijn.

4.3. Recht op inzage en afschrift van gegevens

- Patiënten, medewerkers en andere betrokkenen kunnen altijd hun persoonsgegevens inzien wanneer zij hier om vragen en kunnen er op vertrouwen dat deze gegevens correct zijn dan wel worden aangepast wanneer noodzakelijk of door de betrokkene is aangegeven dat deze aangepast dienen te worden, voor zover een (wettelijke) verplichting dit niet onmogelijk maakt.

- Betrokkenen hebben de mogelijkheid om te controleren of en op welke manier hun gegevens worden verzameld en verwerkt en het recht op inzage en afschrift van zijn dossier [1]. Uitzondering op deze regel is als de persoonlijke levenssfeer van een ander daardoor wordt geschaad. Bijvoorbeeld informatie die een partner aan een hulpverlener heeft verstrekt in het vertrouwen dat betrokkene deze informatie niet te zien krijgt.

1 Artikel 7:456 BW en artikel 15 van de AVG

- De GGD verstrekt de betrokkene, binnen vier weken na ontvangst van het verzoek, kosteloos een kopie van de persoonsgegevens die worden verwerkt.

- Indien de termijn van vier weken onhaalbaar blijkt, verlengt de GGD de termijn met twee maanden en brengt de betrokkene hier schriftelijk van op de hoogte.

- Indien de betrokkene om bijkomende kopieën vraagt, kan de GGD een vergoeding rekenen niet hoger dan de kostprijs.

4.4. Recht op rectificatie (correctie, aanvulling) van gegevens

- Als de GGD persoonsgegevens van betrokkenen verwerkt die naar hun oordeel onjuist zijn, kunnen zij een verzoek indienen bij de GGD om feitelijke onjuistheden in het dossier te corrigeren. Het gaat dan bijvoorbeeld om onjuiste adresgegevens. Niet wordt bedoeld dat de bijvoorbeeld de diagnose mag worden gewijzigd.

- Er kan ook een verklaring aan het medisch dossier worden toegevoegd, bijvoorbeeld eigen visie van de betrokkene, ook als de hulpverlener het niet eens is met de verklaring moet deze worden opgenomen.

4.5. Recht op gegevenswissing

- Betrokkenen hebben het recht persoonsgegevens te laten verwijderen indien de GGD niet langer een goede grond heeft voor het gebruik hiervan, bijvoorbeeld indien betrokkenen een gegeven toestemming intrekken, indien de gegevens onjuist zijn of de gegevens niet langer nodig zijn.

- Het AVG recht op gegevenswissing geldt in principe niet voor medische dossiers. De betrokkene heeft het recht om op hem betrekking hebbende gegevens te laten verwijderen en op grond van de Wgbo heeft hij bovendien het recht dossiergegevens te laten vernietigen ongeacht of dit relevante gegevens zijn[2].

- Het recht op vernietiging geldt alleen voor gegevens die de hulpverlener in het kader van zijn dossierplicht heeft opgeslagen. Het geldt niet voor andere gegevens, zoals financiële gegevens die de hulpverlener op andere gronden moet bewaren.

2 Artikel 7: 455 BW

- De GGD hanteert drie uitzonderingen op het recht op vernietiging:
  (1) Een andere wet schrijft een afwijkende bewaartermijn voor waarbinnen de gegevens niet vernietigd mogen worden;
  (2) Een ander dan de betrokkene heeft een aanmerkelijk belang bij het bewaren van de gegevens;
  (3) 'Goed hulpverlenerschap' staat vernietiging in de weg.

4.6. Recht op beperking van de verwerking

- Het recht op beperking van de verwerking van persoonsgegevens houdt in dat de gegevens wel beschikbaar blijven in het medisch dossier, maar dat ze tijdelijk niet gebruikt mogen worden. De persoonsgegevens mogen dan alleen nog worden gebruikt met toestemming van de betrokkene, of als dat nodig is voor het instellen, uitoefenen of onderbouwen van een rechtsvordering of ter bescherming van de rechten van andere natuurlijke personen of rechtspersonen. Voorbeeld: als de juistheid van de persoonsgegevens worden betwist en voor een periode die de verwerkingsverantwoordelijke in staat stelt om de juistheid van die persoonsgegevens te controleren.

4.7. Recht op overdraagbaarheid van gegevens (dataportabiliteit)

- De GGD is vanuit de AVG niet verplicht invulling te geven aan overdraagbaarheid van gegevens voor zover het werkzaamheden betreft in het kader van algemeen belang, op basis van een wettelijke verplichting of het verstrekken van gezondheidszorg.

- Het recht om gegevens te mogen meenemen geldt voor een deel van de gegevens van medische dossiers. Persoonsgegevens die de cliënt zelf actief en bewust heeft verstrekt (eigen data) vallen onder het recht op dataportabiliteit. Dit geldt ook voor de gegevens die de betrokkene indirect heeft verstrekt door het gebruik van een dienst of een apparaat. Gegevens die niet (in)direct door het gebruik van een dienst of een apparaat door de betrokkene zijn verstrekt vallen hier niet onder. Bijvoorbeeld conclusies, diagnoses, vermoedens of behandelplannen die de hulpverlener op basis van de door de betrokkene verstrekte gegevens vaststelt.

- De GGD treft voorzieningen in het kader van dataportabiliteit.

4.8. Recht van bezwaar tegen verwerking

- Betrokkenen hebben het recht aan de GGD te vragen hun persoonsgegevens niet meer te gebruiken en bezwaar te maken tegen de verwerking van hun persoonsgegevens. De GGD moet hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

4.9. Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming waaronder profilering

- 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.

- De GGD past geen geautomatiseerde individuele besluitvorming, waaronder profilering, toe als daaraan rechtsgevolgen voor de betrokkene (degene wiens persoonsgegevens het betreft) aan zijn verbonden of het besluit hem/haar in aanmerkelijke mate treft. Daarbij kan gedacht worden aan een indicatie van een medisch oordeel op basis van karakteristieken uit het digitaal dossier of het verwerken van sollicitaties via internet zonder menselijke tussenkomst.

4.10. Klachten en vragen

- Onverminderd de rechten die de betrokkenen worden toegekend in de WGBO en de AVG, kan iedere klant schriftelijk een klacht indienen bij de GGD indien hij meent dat door (een hulpverlener van) de GGD persoonsgegevens worden verwerkt op een wijze die in strijd is met de wet of met dit beleid.

- Binnen vier weken beoordeelt de GGD of het verzoek ontvankelijk is. De GGD laat binnen die termijn weten wat er met het verzoek gaat gebeuren, waaronder of de GGD de behandeling van het verzoek met twee maanden verlengt. De GGD behandelt het verzoek volgens de daarvoor door haar vastgestelde en bekendgemaakte procedure, te weten de Klachtenregeling GGD Zeeland.

- Als het verzoek niet tijdig kan worden opgevolgd, deelt de GGD uiterlijk binnen vier weken mee waarom het verzoek zonder gevolg is gebleven. De betrokkene heeft dan de mogelijkheid om bezwaar te maken bij de GGD of een klacht in te dienen bij de Autoriteit Persoonsgegevens.

- Indien naar de mening van de klant de beslissing op een klacht niet tot het gewenste resultaat heeft geleid, wordt gewezen op de mogelijkheid om diens klacht voor te leggen aan de Autoriteit Persoonsgegevens, Postbus 93374, 2509 AJ Den Haag.

4.11. Informeren van (keten)partners

- De GGD informeert relevante ketenpartners indien het verzoek wordt ingewilligd. Dit betreft o.a. organisaties met wie een verwerkersovereenkomst dan wel een gebruiksovereenkomst of een overeenkomst tot derde verstrekking is afgesloten. Indien relevant vraagt de GGD actief om bevestiging van de betreffende ketenpartner(s) dat aan het betreffende verzoek is voldaan.

4.12. Rechten en plichten aangaande het medisch dossier

- De Wet op de geneeskundige behandelingsovereenkomst ("WGBO") verplicht de hulpverlener van de GGD om een medisch dossier in te richten. In het medisch dossier neemt de hulpverlener alle gegevens op over de gezondheid van de betrokkene en over de uitgevoerde verrichtingen, voor zover dit voor een goede hulpverlening noodzakelijk is.

- De betrokkene kan de hulpverlener niet van deze verplichting ontheffen. De gegevens vallen onder het medisch beroepsgeheim: de hulpverlener heeft een geheimhoudingsplicht.

- Een hulpverlener kan alleen gegevens aan een derde verstrekken als dat mag op basis van de AVG én als er een grond is om het medisch beroepsgeheim te doorbreken. Doorbreking van deze zwijgplicht is toegestaan op grond van:

  (1) expliciete toestemming van de betrokkene;
  (2) een wettelijke bepaling;
  (3) (noodtoestand in de zin van) conflict van plichten;
  (4) zwaarwegend belang;
  (5) zeer uitzonderlijke omstandigheden.

- Ieder heeft het recht om zijn (medisch)dossier in te zien, gegevens te laten corrigeren c.q. te verwijderen. In de WGBO is bepaald dat wanneer een kind jonger dan 12 jaar is de ouder(s)/wettelijk vertegenwoordiger(s) bevoegd zijn en het dossier van het kind mogen inzien.

- Jeugdigen van 12,13,14 of 15 jaar kunnen zelfstandig deze rechten uitoefenen en moeten toestemming verlenen aan de ouder(s). Jeugdigen van 16 of 17 jaar oefenen

de rechten zelfstandig uit, ouders hebben geen recht op informatie zonder toestemming van de jeugdige.

- Een hulpverlener van de GGD mag uitsluitend een (medisch) dossier aanleggen in de hiervoor bestemde en door de GGD aangewezen (zorg)informatiesystemen.

5. Verplichte maatregelen en procedures

5.1. Bewustwording

- De GGD zorgt voor bewustzijn op het gebied van gegevensbescherming voor al haar medewerkers. Hierbij dienen zij minimaal op de hoogte te zijn van de voor hun relevante wet- en regelgeving en bepalingen zodat zij deze in hun dagelijkse werk kunnen toepassen. Hierbij kan gedacht worden aan regels over toegang tot medische gegevens, maatregelen ter bescherming van bijzondere persoonsgegevens, datalekken en zwijgplicht.

- Concreet kan de GGD bewustwording vormgeven door enerzijds te voorzien in algemene en op het thema afgestemde specifieke voorlichtingen op het gebied van gegevensbescherming. Anderzijds wil de GGD het bewustzijn op dit gebied door gegevensbescherming tot terugkerend agendapunt te maken van de verschillende overleggen. Daarmee worden dilemma's op het gebied van gegevensbescherming bespreekbaar en stimuleert de GGD medewerkers om beveiligingsincidenten en datalekken te melden. Tenslotte kan bewustwording bevorderd worden door bijvoorbeeld e-learning, nieuwsbrieven en informatie op het intranet, zie Governance Informatieveiligheid GGD Zeeland.

5.2. Verwerking van persoonsgegevens door derden

Verwerkers en verwerkersovereenkomst(en)

- Wanneer de GGD een externe partij of (keten)partner inschakelt om ten behoeve van de GGD persoonsgegevens te verwerken en het verwerken van de persoonsgegevens een hoofdzaak is van deze partij, kan deze partij worden beschouwd als verwerker.

- De GGD schakelt enkel verwerkers in die afdoende garanties bieden met betrekking tot het toepassen van passende technische, procesmatige, communicatieve en organisatorische maatregelen[4].

- De instructies omtrent verwerking(en) door een verwerker worden schriftelijk vastgelegd in een verwerkersovereenkomst[5] voordat de dienstverlening aanvangt.

- De belangrijkste verwerkers zullen minstens eens per jaar door de GGD, middels de leveranciersbeoordeling, gecontroleerd worden op borging en naleving van de

verplichtingen uit de verwerkersovereenkomst. Een dergelijke controle kan o.a. bestaan uit het opvragen van relevante certificeringen. Minder kritische verwerkers worden periodiek gecontroleerd.

- De GGD hanteert als modelovereenkomst: de standaard model verwerkersovereenkomst voor de zorgsector[6].

- Verwerkingen mogen niet plaatsvinden in landen die geen passend beveiligingsniveau kunnen bieden. Hiervan kan worden afgeweken met uitdrukkelijke toestemming van de betrokkenen of andere waarborgen die de autoriteiten hebben goedgekeurd. Een lijst met landen met een passend beveiligingsniveau is te vinden op: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data- protection/adequacy-decisions_en

[4] Artikel 28 lid 1 van de AVG

[5] Artikel 28 lid 3 van de AVG

[6] Zie: https://www.vgn.nl/nieuws/standaard-model-verwerkersovereenkomst-voor-de-zorgsector

De GGD als verwerker

- In voorkomende gevallen treedt de GGD op als verwerker voor derden. Hierbij zijn derden verwerkingsverantwoordelijk.

- De GGD streeft na om voor deze verwerkingen heldere en eenduidige voorwaarden op te stellen die ook toepasbaar zijn voor gelijksoortige verwerkingen.

- De GGD biedt daarbij aan de verwerkingsverantwoordelijke voldoende garanties voor het zorgvuldig verwerken van gegevens door het toepassen van passende technische en organisatorische maatregelen.

- De afspraken omtrent de verwerking worden schriftelijk vastgelegd in een verwerkersovereenkomst, voordat de dienstverlening door de GGD aanvangt.

De GGD als gezamenlijke verwerkingsverantwoordelijke

- Indien de GGD met een andere partij samenwerkt, die geen verwerker is, maar waarmee wel persoonsgegevens worden uitgewisseld waarbij een gezamenlijke verwerkingsverantwoordelijkheid bestaat maakt de GGD passende afspraken. In dat geval zal de GGD een regeling[8] sluiten omtrent de verwerking van persoonsgegevens, of samen met de andere partij een regeling vaststellen, waarin de respectievelijke verantwoordelijkheden worden vastgelegd.

- De GGD plaatst genoemde regeling op haar website[9].

5.3. Documentatie over verwerking van persoonsgegevens

- De werkgroep Gegevensbescherming documenteert namens de GGD de verwerkingen van persoonsgegevens waarvoor meld- of registratieplicht geldt bij in het daartoe bestemde register van verwerkingen, daarin bijgestaan door de ambassadeurs zorg voor beveiligde informatie (zie rapport Governance informatieveiligheid GGD Zeeland) namens het verantwoordelijke team.

- Alle nieuwe of niet geregistreerde verwerkingen worden actief door de betreffende medewerker(s) (daar waar de verwerking plaatsvindt) aangemeld bij de Functionaris Gegevensbescherming dan wel de werkgroep Gegevensbescherming.

- Bij de inschrijving worden in ieder geval de volgende gegevens[10] vermeld:

  a. de naam van de verwerking;
  b. wie de verantwoordelijke is voor de verwerking;
  c. het doel van de verwerking;
  d. de groep van personen van wie persoonsgegevens worden verwerkt (betrokkenen);
  e. de categorie persoonsgegevens die bij de verwerking worden gebruikt;
  f. de ontvangers van de gegevens;
  g. de rechtmatige grondslag voor de verwerking van de persoonsgegevens;
  h. eventuele verstrekkingen aan andere landen buiten de Europese Economische Ruimte;
  i. de verwijderingstermijnen die in acht genomen worden;

- De FG houdt toezicht op de volledigheid, juistheid en rechtmatigheid van de in het register ingeschreven verwerkingen van persoonsgegevens.

- Bij wijzigingen van de bij de inschrijving opgenomen gegevens draagt de ambassadeur zorg voor beveiligde informatie van het verantwoordelijke team voor wijziging hiervan in het register via de FG.

- De GGD maakt het register van verwerkingsactiviteiten niet openbaar op de website.

---

[8] Artikel 26 lid 1 van de AVG

[9] Artikel 26 lid 2 van de AVG

[10] Artikel 30 lid 1 van de AVG

5.4. Informatiebeveiliging

- Het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens is een voorwaarde om te garanderen dat betrokkenen hun rechten op adequate wijze kunnen uitoefenen.

- De GGD streeft de bepalingen uit de NEN 7510, NEN 7512, NEN 7513 en NTA 7516 normen na, ter bescherming van de verwerking van medische gegevens.

- De GGD controleert steekproefsgewijs op toegang tot persoonsgegevens door onbevoegden.

Passende beschermende technische en organisatorische maatregelen

- Wanneer de GGD persoonsgegevens verwerkt of laat verwerken door een derde, zorgt de GGD ervoor dat passende beveiligingsmaatregelen worden getroffen om de betreffende persoonsgegevens te beschermen tegen de verschillende risico's.

- De GGD slaat gegevens zo op dat voldaan kan worden aan de wettelijke kaders van de AVG, dit betekent in verband met de doelbinding vaak gescheiden opslag. Concreet betekent dit bijvoorbeeld dat medische gegevens van klanten nooit worden opgeslagen in een boekhoudkundig systeem.

- De GGD houdt actief, per informatiesysteem, een autorisatiemix bij en controleert steekproefsgewijze achteraf op (eventueel ongeautoriseerde) toegang.

- De GGD beperkt de toegang tot inzage en wijzigen van gegevens tot degenen die dit vanuit hun functie nodig hebben; medewerkers worden actief aangesproken in geval van overschrijding van toegangsbevoegdheden.

- De GGD beschermt persoonsgegevens onder andere door het aggregeren, versleutelen en anonimiseren van deze gegevens. Hierdoor wordt de mate waarin de verwerkte persoonsgegevens kunnen worden herleid tot een individu verminderd.

- In beginsel, in het bijzonder bij gegevens aangaande de gezondheid, worden alle gegevensdragers en alle communicatie tussen de GGD en haar klanten en/of (keten)partners voorzien van encryptie (versleuteling).

- Als uitgangspunt kiest de GGD voor technische maatregelen om ‘gegevensbescherming door ontwerp’ te waarborgen. Daar waar de technische mogelijkheden ontbreken of disproportioneel hoge kosten met zich meebrengen, zoekt de GGD naar organisatorische en of procesmatige maatregelen als alternatief voor of als aanvulling op de technische maatregelen. Dit wordt uiteraard samen en in overleg met informatiebeveiliging uitgewerkt.

- Deze (technische, procesmatige, communicatie en organisatorische) maatregelen omvatten bij de verwerking van persoonsgegevens een op het risico afgestemd beveiligingsniveau. Hierbij wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, en ook met de aard, de omvang, de context en de verwerkingsdoeleinden etc. Tevens wordt rekening gehouden met de, qua waarschijnlijkheid en ernst, uiteenlopende risico’s voor de rechten en vrijheden van personen.

Waar wenselijk omvatten de maatregelen onder meer het volgende:

- De pseudonimisering en versleuteling van persoonsgegevens;
- Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

5.5. Meldplicht voor inbreuken in verband met persoonsgegevens (zie procedure datalekken GGD Zeeland)

- Indien zich een informatiebeveiligingsincident voordoet, waarbij bijvoorbeeld gegevens van personen in verkeerde handen kunnen komen of zijn gekomen, handelt de GGD in overeenstemming met de vastgestelde werkwijze in de procedure datalekken. Deze procedure bevat een vastgesteld proces van te doorlopen stappen om de eventuele schade of de kans hierop, bij een ‘datalek’ te beperken en de getroffen perso(o)n(en) te beschermen.

- Het gaat bij een ‘datalek’ om situaties waarbij een onrechtmatige verwerking van persoonsgegevens heeft plaatsgevonden of kan plaatsvinden, waarbij beveiligingsmaatregelen (on)bewust zijn omzeild of doorbroken of dat geen of onvoldoende beveiligingsmaatregelen zijn genomen. Het gaat ook om situaties waarbij

persoonsgegevens verloren zijn gegaan, waardoor ze niet meer beschikbaar zijn, en om situaties waarin gegevens in handen kunnen komen of zijn gekomen van derden die geen toegang tot die gegevens mogen hebben.

- De plicht tot het melden van een (vermoeden van een) 'datalek' geldt als er sprake is van een aanzienlijke kans op ernstige nadelige gevolgen voor betrokkene, dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Het betreft situaties van het (mogelijk) lekken van persoonsgegevens uit GGD bestanden en/of gegevens waarvoor de GGD verantwoordelijkheid draagt.

- Wanneer er een dergelijk 'datalek' heeft plaatsgevonden, wordt dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, gemeld aan de AP. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd.

- Indien de inbreuk een hoog risico voor de rechten en vrijheden van de betrokkenen met zich meebrengt, word de inbreuk ook in eenvoudige en duidelijke taal aan de betrokkenen gemeld.

- De GGD maakt de afweging of het informeren van de betrokkene in diens belang is of dat dit beter achterwege kan blijven om de betrokkene zelf of anderen te beschermen. Indien van informeren wordt afgezien zal de GGD dit besluit registreren en duidelijk motiveren.

- De FG houdt namens de GGD een logboek bij waarin alle meldingsplichtige en niet-meldingsplichtige datalekken zijn opgenomen.

- In het logboek worden in ieder geval de volgende gegevens vermeld:

  a. Het onderwerp van het 'datalek'.
  b. De datum van het 'datalek';
  c. De duur van het 'datalek';
  d. de aard van de inbreuk;
  e. de instanties waar meer informatie over de inbreuk kan worden verkregen;
  f. de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk gevolgen te beperken.
  g. een beschrijving van de gevolgen voor de verwerkte persoonsgegevens;
  h. de maatregelen die de GGD heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen;
  i. de kennisgeving aan betrokkenen.

- De GGD maakt haar register van informatiebeveiligingsincidenten niet openbaar.

- Jaarlijks legt de werkgroep Gegevensbescherming in haar rapportage verantwoording af over naleving van de AVG. In betreffende verantwoording zijn ten minste de volgende onderdelen opgenomen:

- Het aantal geregistreerde datalekken en de opvolging hiervan, incl. resultaat;
- Het aantal medewerkers dat heeft deelgenomen aan het bewustwordingstraject;
- Gesignaleerde knelpunten en geplande/voorgestelde aanpak incl. tijdspad van implementatie.

5.6. DPIA's (Data Protection Impact Assessments)

- Voor de GGD is een DPIA een instrument waarmee het effect van beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens op een gestructureerde en heldere manier in beeld in kaart wordt gebracht om vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

- De GGD voert DPIA's uit voor nieuwe maar ook bestaande verwerkingen van persoonsgegevens die een hoog privacyrisico opleveren voor de betrokkenen. De GGD volgt hierbij de lijst van de AP[12].

- Indien naar oordeel van de FG sprake is van een verwerking, die gelet op de aard en de omvang, de context en de doeleinden een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen dan wordt door middel van een DPIA aangetoond dat de privacy voldoende is gewaarborgd en worden de al dan niet te nemen maatregelen gemotiveerd.

- De GGD neemt het initiatief tot het uitvoeren van een DPIA en betrekt relevante medewerkers bij het proces wat gecoördineerd wordt door de adviseur gegevensbescherming.

- Voor nieuwe verwerkingen vindt een DPIA plaats voordat met de betreffende verwerking wordt gestart.

- Ten aanzien van bestaande verwerkingen voert de GGD een DPIA uit indien de betreffende verwerkingen hier aan onderworpen dient te worden maar deze nog niet heeft plaatsgevonden.

- Een DPIA wordt periodiek herhaald ter evaluatie, alsmede bij wijzigingen waardoor de risico's van de verwerking toenemen.

- Bij het uitvoeren van een DPIA wordt de FG altijd vooraf geïnformeerd.

- De ambassadeur zorg voor beveiligde informatie van een team ziet toe op het nemen van maatregelen die blijkens de DPIA nodig zijn om de risico's te verkleinen.

- Het resultaat van de DPIA en de genomen maatregelen om het risico te beperken worden aan de FG voorgelegd ter toetsing en opneming in het register van verwerkingen.

- Waar het nieuwe verwerkingen betreft wordt - voorafgaand aan de verwerking- de AP om advies gevraagd indien de GGD niet in staat is om voldoende maatregelen te treffen om de risico's te beperken en er een hoog restrisico bestaat.

- DPIA's die binnen de GGD worden uitgevoerd vinden plaats volgens een bepaalde standaard.

- De FG geeft over de uitgevoerde DPIA een advies aan het MT.

- De GGD maakt de resultaten van uitgevoerde DPIA's niet openbaar. Deze dienen uitsluitend ter vaststelling van managementbeleid.

5.7. Beheer van persoonsgegevens

Big data en tracking

- Gegevens in big data en tracking mogen alleen worden verzameld, opgeslagen en gedeeld, als ze niet herleidbaar zijn tot een persoon en worden alleen verzameld voor onderzoek dat door of namens de GGD wordt uitgevoerd.

- Voor big data en tracking wordt uitsluitend gebruik gemaakt van brongegevens die door daartoe geautoriseerde personen zijn verzameld.

- Brongegevens die gebruikt worden voor big data toepassingen worden omgezet tot een dataset die geen persoonsgegevens bevat en dus geanonimiseerd is. Indien het noodzakelijk is om af te wijken wordt vooraf toestemming aangevraagd bij de FG die de aanvraag zal beoordelen in het kader van de rechtmatigheid en de doelmatigheid. Alleen bij een goedgekeurde aanvraag mogen de gegevens gepseudonimiseerd in plaats van geanonimiseerd worden.

Cameratoezicht, camerabewaking en overige inzet van camera's

- De GGD past op verschillende plekken binnen haar organisatie registratie van bewegende beelden toe. Voorbeelden hiervan zijn beelden van bewakingscamera's bij de frontoffice en parkeeringang op de hoofdlocatie. Bij elke registratie van camerabeelden bepaalt en documenteert de GGD of en hoe lang deze worden bewaard.

- De GGD plaatst de camera's niet zodanig dat deze uitsluitend of voornamelijk op de openbare ruimte zijn gericht.

- Camerabewaking kan door particuliere bedrijven worden uitgeoefend onder voorwaarde dat indien er camera's in de openbare ruimte worden geplaatst dan wel delen van de openbare ruimte in beeld worden gebracht, er een daartoe strekkend besluit door of namens het MT is genomen en er een overeenkomst met de verantwoordelijke is gesloten voorafgaande aan de verwerking. Deze overeenkomst gaat in ieder geval in op:

    - de grondslag voor de verwerking van persoonsgegevens;
    - het verzamel- en verwerkingsdoel;
    - de organisatorische en technische maatregelen die worden getroffen tegen verlies of onrechtmatige verwerking;

- de bewaartermijn;
- de wijze waarop voldaan wordt aan de meldplicht datalekken.

- Bij inzet van camera's voor andere doeleinden dient voorafgaand aan deze inzet advies te worden gevraagd aan de FG.

Cookies en soortgelijke technieken

- De GGD plaatst, indien noodzakelijk, alleen cookies die noodzakelijk zijn voor het correct functioneren van de website op de computers van betrokkenen en het analyseren hiervan, zgn. functionele en analytische cookies en maakt geen gebruik van tracking cookies.

Geheimhouding

- Persoonsgegevens worden in beginsel niet verwerkt door medewerkers zonder (medisch) beroepsgeheim of zonder ondertekende geheimhoudingsverklaring.

Minimaal gebruik van persoonsgegevens (dataminimalisatie)

- De GGD verzamelt (of vraagt om) niet meer gegevens dan strikt noodzakelijk.

- De GGD verwerkt alleen gegevens voor het doel waarvoor zij zijn verzameld en verwerkt deze verder alleen op een manier die verenigbaar is met dit doel.

- Bij configuratie van systemen kiest de GGD in voorkomende gevallen voor de privacy-vriendelijke variant (privacy by default).

- De informatie die de GGD verwerkt is in beginsel correct en actueel.

- De GGD maakt geen onnodige kopieën van verzamelingen van persoonsgegevens.

- De GGD voert actief beleid om alle overbodige gegevensverzameling (bijvoorbeeld op gestandaardiseerde- vragenlijsten en invulformulieren) te verwijderen.

- Per team zijn de wettelijk verplichte bewaartermijnen per categorie van persoonsgegevens vastgesteld. De GGD bewaart persoonsgegevens niet langer dan strikt noodzakelijk (bijvoorbeeld op basis van de Belastingwet, de Archiefwet etc.) en verwijdert actief wat niet meer nodig is.

- De GGD communiceert actief aan ketenpartners wanneer persoonsgegevens verwijderd dienen te worden waaronder begrepen het vragen van bevestiging dat betreffende persoonsgegevens door de ketenpartner zijn verwijderd.

Onderzoek

- De GGD ontdoet bij onderzoek alle persoonsgegevens van direct identificerende kenmerken (anonimiseren).

Privacy by design (privacy door ontwerp)

- De GGD hanteert achtereenvolgens de volgende acht data- en procesgeoriënteerde privacy strategieën om gegevensbescherming vanaf begin af aan mee te nemen bij het ontwerpen en bouwen van nieuwe systemen.

1. De verwerking van persoonsgegevens wordt zo veel mogelijk beperkt.
2. De verwerking van persoonsgegevens wordt zo veel mogelijk van elkaar gescheiden.
3. Het detail waarin persoonsgegevens worden verwerkt wordt zo veel mogelijk beperkt.
4. Persoonsgegevens worden afgeschermd of onherleidbaar. Er wordt voorkomen dat persoonsgegevens openbaar worden.
5. Klanten worden over de verwerking van hun persoonsgegevens geïnformeerd (voorafgaand aan de start van de nieuwe verwerking).
6. Klanten krijgen regie en invloed over de verwerking van hun persoonsgegevens.
7. Er wordt een privacy vriendelijke verwerking van persoonsgegevens afgedwongen.
8. Er wordt aangetoond dat persoonsgegevens op een privacy vriendelijke wijze zijn verwerkt

6. Slotbepalingen

De AVG is per 25 mei 2018 van toepassing. Dit beleid is opgesteld door de werkgroep Gegevensbescherming op basis van het door het MT vastgesteld rapport Governance Informatieveiligheid GGD Zeeland. Dit beleid treedt in werking na vaststelling door het MT van de GGD. Het DB wordt hiervan in kennis gesteld.

Het gegevensbeschermingsbeleid wordt elk jaar geëvalueerd en indien nodig herzien. Aanpassingen van dit beleid worden aangekondigd via het intranet.