Privacyverklaring en - beleid Stichting Sensire

Datum	15 april 2024
Versie	1.5

Inleiding
Voor u ligt de privacyverklaring, tevens het privacybeleid[1], van Stichting Sensire en haar bedrijfsonderdelen. Deze privacyverklaring heeft betrekking op alle verwerkingen van persoonsgegevens waaronder van onze klanten, sollicitanten en werknemers van Sensire. Deze privacyverklaring is van toepassing op zowel op papier als elektronische verwerking van persoonsgegevens en geeft inzicht in de bepalingen waar Sensire zich aan houdt in het kader van de verwerking van persoonsgegevens. Sensire verwerkt deze gegevens onder verantwoordelijkheid van haar Raad van Bestuur.

Handzame samenvatting

De belangrijkste onderwerpen hebben wij voor u op een rijtje gezet:

- Sensire bepaalt ‘waarom’ en ‘hoe’ persoonsgegevens moeten worden verwerkt ten behoeve van de zorg die zij levert. Sensire is daarom de Verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens.

- Sensire voldoet aan de eisen in de privacywet Algemene Verordening Gegevensbescherming (hierna: AVG). Een aantal van deze eisen zijn opgenomen in deze privacyverklaring. Tevens staat soms beschreven hoe Sensire daar invulling aan heeft gegeven.

- Als u een algemene vraag heeft kunt u met Sensire contact opnemen via de actuele contactgegevens op websites van Sensire zoals www.sensire.nl en www.werkenbijsensire.nl.

- U kunt met uw vragen over privacy allereerst terecht bij uw zorgverlener en de zorgteams. Zij zullen uw vraag beantwoorden of u verder helpen.

- Sensire heeft een Privacy Functionaris aangesteld voor de uitvoering van de werkzaamheden op het gebied van privacy. Daarnaast is een Functionaris voor de Gegevensbescherming aangesteld. Hij houdt binnen Sensire toezicht op de toepassing en naleving van de AVG. Als u vragen heeft over uw privacy en u komt er niet uit met uw zorgverlener, kunt u beide functionarissen bereiken via een email aan mijngegevens@sensire.nl of 0900-8856.

- Sensire verwerkt uw persoonsgegevens voor verschillende doeleinden waaronder:
    - het uitvoeren van overeenkomsten, zoals voor het leveren van zorg en

[1] Hierna te noemen ‘privacyverklaring’

de arbeidsovereenkomst;
    - het voldoen aan een wettelijke plicht, waaronder de WGBO en fiscale wetgeving;
    - het onderhouden van contact en toezending van informatie waar een betrokkene zelf om heeft gevraagd of toestemming voor heeft gegeven;
    - het verbeteren van (de kwaliteit van) producten en diensten.

- Een overzicht van de verwerkingen, doelen en grondslagen enz. wordt bijgehouden in het verwerkingsregister. Een belangrijke verwerking is bijvoorbeeld dat Sensire persoonsgegevens van haar klanten verwerkt ten behoeve van het leveren van zorg en alles wat daarmee samenhangt. En dat persoonsgegevens van medewerkers worden verwerkt ten behoeve van communicatie, personeelsadministratie en salarisbetalingen. Van sollicitanten bewaren we persoonsgegevens voor de afhandeling van de sollicitaties. Het verwerkingsregister is beschikbaar op de website van Sensire.

- Sensire heeft uw persoonsgegevens nodig, meestal omdat dit wettelijk verplicht is. Sensire heeft uw persoonsgegevens ook nodig om u de kwaliteit te kunnen leveren die u mag verwachten. Via overeenkomsten maken we afspraken over o.a. uw zorg of arbeidsovereenkomst en geeft u toestemming voor de verwerking van uw gegevens. Als u besluit uw persoonsgegevens niet meer met Sensire te delen zal dat waarschijnlijk gevolgen hebben voor aangegane overeenkomsten. Sollicitanten geven bij de sollicitatie toestemming voor de verwerking van persoonsgegevens.

- Sensire verwerkt niet meer persoonsgegevens dan nodig. Hiervoor voert Sensire voor, tijdens en na de gegevensverwerking een aantal activiteiten uit. Dit, en het voldoen aan andere privacy beginselen, staat hieronder bij paragraaf 2.2.1.

- Het kan zijn dat Sensire uw persoonsgegevens van andere zorginstellingen heeft gekregen. Bijvoorbeeld door een verwijzing van een huisarts of een ziekenhuis. Ook met deze gegevens gaat Sensire zeer zorgvuldig om. Sensire bewaart alleen de medische gegevens die relevant zijn voor uw zorgverlening. Sensire verzamelt geen persoonsgegevens uit openbare bronnen.

- De medewerkers van Sensire hebben allen een geheimhoudingsplicht en een (afgeleid) beroepsgeheim. Dat betekent vooral dat uw gegevens alleen met andere partijen worden gedeeld als Sensire dat wettelijk verplicht is of als u daar toestemming voor heeft gegeven.

- Sensire doet haar uiterste best om uw gegevens te beveiligen, zodat deze onder meer beschermd zijn tegen ongeoorloofde inzage en tegen verlies, vernietiging of beschadiging. Sensire voldoet op het gebied van informatiebeveiliging aan wet- en regelgeving waaronder de NEN 7510, de norm voor informatiebeveiliging in de zorg.

- De persoonsgegevens die Sensire verwerkt worden binnen de EU (en Europese Economische Ruimte) opgeslagen en verwerkt. Of in andere landen

(zogenaamde derde landen) als de AVG-regels dat toelaten. Wij letten daar op bij het aangaan van contracten met onze leveranciers.

- Sensire bewaart de persoonsgegevens in medische dossiers tenminste 20 jaar. Deze termijn is wettelijk bepaald. Na 20 jaar worden deze gegevens vernietigd, tenzij er een reden is om de persoonsgegevens langer te bewaren. Andere categorieën persoonsgegevens worden korter bewaard. Sensire heeft een uitgebreid overzicht met persoonsgegevens en bewaartermijnen opgesteld. Meer informatie hierover in het verwerkingsregister, te vinden op de website van Sensire.

- Alle klanten, medewerkers en andere betrokkenen waarvan Sensire persoonsgegevens verwerkt hebben privacyrechten zoals het recht op inzage, correctie of verwijdering van de gegevens die Sensire verwerkt. Zie paragraaf 2.3 voor een uitgebreide beschrijving. Als u een beroep doet op uw recht dan werken wij hier altijd aan mee, voor zover andere wet- en regelgeving dit toestaat.

- Als Sensire uw persoonsgegevens verwerkt op basis van uw toestemming dan heeft u altijd het recht om de toestemming weer in te trekken. Overlegt u met uw zorgverlener of onze Privacy Functionaris over hoe u dat kunt doen en wat dit voor u betekent

- Als u een klacht heeft over uw privacy kunt u terecht bij de klachtenfunctionaris van Sensire. De procedure en contactgegevens staan op de website www.sensire.nl. Ook kunt u terecht bij de Functionaris voor de Gegevensbescherming via een email aan mijngegevens@sensire.nl. Ook kunt u met uw klacht over privacy terecht bij de Autoriteit Persoonsgegevens.

- Sensire maakt geen gebruik van geautomatiseerd besluitvorming op basis van uw persoonsgegevens. Ook doen wij niet aan profilering.

Hieronder kunt u in detail lezen over belangrijke eisen uit de AVG waar Sensire aan voldoet, uw rechten en in sommige gevallen hoe Sensire daar invulling aan geeft.

1 Inhoudsopgave

Handzame samenvatting voor alle lezers 2

2 Beleid en uitgebreide Privacyverklaring 6

2.1 Definities

2.2 Verwerking van persoonsgegevens van klanten in overeenstemming met de AVG

2.2.1 Beginselen inzake persoonsgegevens verwerking

2.2.2 Rechtmatigheid van de verwerking

2.2.3 Voorwaarden voor het verwerken van gezondheidsgegevens

2.2.4 Gegevensverwerking door verwerker

2.2.5 Wanneer mogen andere bijzondere gegevens worden verwerkt?

2.2.6 Geheimhoudingsplicht en verstrekking aan derden

2.2.7 Bewaren van persoonsgegevens

2.3 Rechten van de betrokkenen 12

2.3.1 Voorwaarden m.b.t. de uitvoering van de rechten van de betrokkenen

2.3.2 Informatie

2.3.3 Te verstrekken informatie indien persoonsgegevens niet van de betrokkene zijn verkregen

2.3.4 Inzage en afschrift

2.3.5 Rectificatie (verbetering) of aanvulling van persoonsgegevens en beperking van de verwerking van persoonsgegevens

2.3.6 Recht op gegevenswissing (vergetelheid)

2.3.7 Recht van bezwaar

2.3.8 Recht op gegevensoverdraagbaarheid (dataportabiliteit)

2.3.9 Recht op elektronische afschrift van de logging

2.4 Veilige verwerking van persoonsgegevens 17

2.4.1 Verantwoordelijkheid van de verwerkingsverantwoordelijke

2.4.2 Gegevensbescherming door ontwerp en standaardinstellingen (Privacy by design en default)

2.4.3 Gezamenlijke verwerkingsverantwoordelijken

2.4.4 Register van verwerkingen

2.4.5 Medewerking verlenen aan/samenwerken met de Autoriteit Persoonsgegevens

2.4.6 Beveiliging van de verwerking

2.4.7 Melding van een inbreuk in verband met persoonsgegevens aan de Autoriteit Persoonsgegevens (datalekken melden aan de AP) en datalekkenregister

2.4.8 Melding van een inbreuk in verband met persoonsgegevens aan de betrokkenen (datalekken melden aan de betrokkene)

2.4.9 Gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment, DPIA)

2.5 Functionaris voor gegevensbescherming (FG) 20

2.5.1 Aanwijzing van een FG

2.5.2 Positie van de FG

2.5.3 Taken van de FG

2.5.4 Bij een klacht

Versies
Van deze privacyverklaring zijn de volgende versies uitgebracht

Versie	Datum	Omschrijving	Auteur
1.0	06-08-2018	Nieuw beleid n.a.v. de AVG	M. Dwarswaard
1.1	18-12-2018	Reglement nu ook van toepassing op werknemers en NAAST	M. Dwarswaard, G. van den Berg
1.2	24-07-2020	Aanpassingen vanwege Wabvpz en Wzd	L. Scholten G. van den Berg
1.3	25-06-2021	Diverse correcties, samenvatting toegevoegd	L. Scholten G. van den Berg
1.4	21–11-2022	Beknopte correcties n.a.v. periodieke controle	G. van den Berg
1.5	15-4- 2024	Uitbreiding met beleidsuitgangspunten en privacy functionaris	Th. Frits G. van den Berg

sensire
leven zoals u wilt

2 Beleid en uitgebreide Privacyverklaring

2.1 Definities

Autoriteit Persoonsgegevens (AP): de toezichthoudende autoriteit, de onafhankelijke instantie die erover waakt dat persoonsgegevens zorgvuldig en veilig worden verwerkt en zo nodig sancties kan opleggen als dat niet gebeurt.

Bestand: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn.

Betrokkene: degene op wie een persoonsgegeven betrekking heeft, meestal de klant of medewerker, of zijn (wettelijk) vertegenwoordiger.

Bijzondere categorieën persoonsgegevens: persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en 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.

Derde: elke persoon of instantie die geen betrokkene, verwerkingsverantwoordelijke, verwerker, of een persoon is die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd is persoonsgegevens te verwerken.

Functionaris voor gegevensbescherming (FG): functionaris die door de zorgaanbieder moet of kan worden aangesteld voor het informeren en adviseren over en het toezicht houden op de toepassing en naleving van de AVG en andere gegevensbeschermingsbepalingen.

Gezondheidsgegevens: gegevens over de lichamelijke of geestelijke gezondheid van een persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.

Inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of 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 gegevens. Onder een ‘datalek’ valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”).

Pseudonimisering: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat aanvullende gegevens worden gebruikt, mits technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

Toestemming van de betrokkene: door betrokkene, op goede informatie berustende, specifieke, in vrijheid en ondubbelzinnig gegeven toestemming waarbij betrokkene hem betreffende verwerking van persoonsgegevens aanvaardt. Dat kan door middel van een schriftelijke of mondelinge verklaring of een ondubbelzinnige actieve handeling (zoals het elektronisch aanvinken van een hokje).

Verwerker: degene die in opdracht van en voor de verwerkingsverantwoordelijke persoonsgegevens verwerkt (bijvoorbeeld een saas-leverancier).

Verwerking van persoonsgegevens: 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 in een andere vorm beschikbaar stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Verwerkingsverantwoordelijke: degene die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; meestal de zorgaanbieder.

Zorgaanbieder: Stichting Sensire en alle bijbehorende bedrijfsonderdelen.

Bij discussie over een definitie geldt de definitie zoals deze is opgenomen in de AVG.

2.2 Verwerking van persoonsgegevens van klanten in overeenstemming met de AVG

2.2.1 Beginselen inzake persoonsgegevens verwerking

De zorgaanbieder is verantwoordelijk voor de naleving van onderstaande beginselen bij de verwerking van persoonsgegevens en moet de naleving van deze beginselen kunnen aantonen (“verantwoordingsplicht”).

Binnen Sensire worden persoonsgegevens alleen verwerkt:

- op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is;
- voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd;
- voor zover zij toereikend zijn en ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt;
- indien de persoonsgegevens juist zijn en zo nodig worden geactualiseerd. Redelijke maatregelen worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren;
- en bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is voor zover de wetgeving dit toelaat. Persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen;
- door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Om te borgen dat voldaan wordt aan de hiervoor genoemde beginselen heeft Sensire onder meer een privacyfunctionaris en functionaris gegevensbescherming aangesteld. Daarnaast worden voor, tijdens en na de gegevensverwerking diverse activiteiten uitgevoerd. Dit betreft (niet limitatief):

- Leveranciers- en pakketselectie via een programma van eisen waarin privacy en informatiebeveiliging is opgenomen.
- Beoordeling van de verwerkersovereenkomsten.
- Het uitvoeren van een verkorte data protection impact assessment bij nieuwe verwerkingen.
- Het uitvoeren van een uitgebreide data protection impact assessment indien er sprake is van een hoog risico voor de vrijheden en rechten van betrokkenen.
- Het monitoren en periodiek beoordelen van leveranciers, soms ook verplicht vanwege

de jaarlijkse accountantscontrole.
- Het periodiek beoordelen van verantwoordings- en beleidsdocumenten zoals het verwerkingsregister en de privacyverklaring.
- Het periodiek uitvoeren van risicoanalyses.
- Een onafhankelijke beoordeling van privacy door middel van een privacy audit.
- Het onafhankelijk beoordelen van informatiebeveiliging door middel van een audit op informatiebeveiliging.

2.2.2 Rechtmatigheid van de verwerking

De verwerking is alleen rechtmatig indien en voor zover aan ten minste één van de onderstaande voorwaarden, rechtsgrond voor de verwerking, is voldaan:

- de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden; de zorgaanbieder moet de toestemming kunnen aantonen en betrokkenen heeft het recht de toestemming te allen tijde in te trekken;
- de gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, bijvoorbeeld de behandelingsovereenkomst;
- de gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen, bijvoorbeeld de dossierplicht in de Wgbo;
- de gegevensverwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of een ander natuurlijk persoon[2];
- de gegevensverwerking noodzakelijk is voor de goede vervulling van een taak van algemeen belang, dat elders in een wet is vastgelegd met eventuele nadere bepalingen;
- de gegevensverwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen[3] van de verwerkingsverantwoordelijke of van een derde én de belangen, grondrechten of fundamentele vrijheden van degene van wie de gegevens worden verwerkt niet prevaleren.

2.2.3 Voorwaarden voor het verwerken van gezondheidsgegevens

Gezondheidsgegevens zijn één van de categorieën bijzondere persoonsgegevens. Het is in de AVG verboden bijzondere categorieën persoonsgegevens te verwerken, tenzij voldaan wordt aan één van de onderstaande voorwaarden:

- Als de verwerking noodzakelijk is voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, voor zover dit is toegestaan in nationale wetgeving.
- Zo mogen gegevens over gezondheid worden verwerkt met het doel gezondheidszorg te leveren, onder de verantwoordelijkheid van een beroepsbeoefenaar die aan het

[2] De AVG geeft in overweging (46) aan dat de verwerking van persoonsgegevens ook als rechtmatig wordt beschouwd indien zij noodzakelijk is voor de bescherming dat voor het leven van de betrokkene of dat van een ander persoon essentieel is. Deze grond voor verwerking is slechts toegestaan als de verwerking kennelijk niet op een andere rechtsgrond kan worden gebaseerd.
[3] In overweging (47) en (49) AVG: een gerechtvaardigd belang kan aanwezig zijn wanneer sprake is van een relevante en passende verhouding tussen de betrokkene en de verwerkingsverantwoordelijke, in situaties waarin de betrokkene een klant is of in dienst is van de verwerkingsverantwoordelijke. In elk geval is een zorgvuldige beoordeling geboden om te bepalen of er sprake is van een gerechtvaardigd belang. De belangen en de grondrechten van de betrokkene kunnen met name zwaarder wegen wanneer persoonsgegevens worden verwerkt in omstandigheden waarin de betrokkenen redelijkerwijs geen verdere verwerking verwachten. De verwerking van persoonsgegevens voor zover die strikt noodzakelijk en evenredig is met het oog op netwerk- en informatiebeveiliging vormt een gerechtvaardigd belang van de verwerkingsverantwoordelijke in kwestie.

beroepsgeheim gebonden is of door een ander persoon die op grond van de wet of overeenkomst tot geheimhouding is gehouden.

2.2.4 Gegevensverwerking door verwerker

- De zorgaanbieder kan de verwerking (extern) uitbesteden aan een verwerker en legt dan in een verwerkersovereenkomst de verplichtingen uit de AVG op aan de verwerker. De zorgaanbieder doet uitsluitend een beroep op verwerkers die afdoende passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.
- De verwerking door een verwerker wordt geregeld in een (verwerkers)overeenkomst die de verwerker ten aanzien van de zorgaanbieder bindt en waarin het onderwerp, de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen en de rechten en verplichtingen van de zorgaanbieder worden omschreven. Een dergelijke overeenkomst dient te voldoen aan de eisen die de AVG daaraan stelt[4].
- De verwerker en eenieder die onder het gezag van de zorgaanbieder of van de verwerker handelt en toegang heeft tot persoonsgegevens, verwerkt deze uitsluitend in opdracht van de zorgaanbieder, tenzij hij door wet- of regelgeving tot verwerking gehouden is.
- Bij het opstellen van de verwerkersovereenkomst wordt vastgesteld dat de gegevensverwerking plaatsvindt binnen de Europese Economische Ruimte (EER). Dit heeft namelijk onze sterke voorkeur. Indien dat niet het geval is moet die verwerking vallen onder afspraken zoals in de AVG aangegeven.

2.2.5 Wanneer mogen andere bijzondere gegevens worden verwerkt?

Andere bijzondere gegevens, bijvoorbeeld gegevens met betrekking tot ras/etniciteit of godsdienst/ levensovertuiging mogen alleen als aanvulling op gezondheidsgegevens worden verwerkt als dat nodig is voor een goede behandeling of verzorging van de betrokkene en dus niet systematisch bij elke klant. Bijvoorbeeld voor de inschakeling van een tolk/vertaler als dat voor de uitleg van de behandeling aan klant nodig is.

2.2.6 Geheimhoudingsplicht en verstrekking aan derden

1. Persoonsgegevens verkregen in de uitoefening van een beroep in de (geestelijke) gezondheidszorg vallen onder de geheimhoudingsplicht van de hulpverlener. Deze geheimhoudingsplicht is o.a. vastgelegd in wettelijke regelingen zoals de Wet BIG en in verschillende beroepscodes of in een (arbeids)overeenkomst.
2. Bij de verstrekking van gegevens aan derden wordt de wet nageleefd en wordt voor zover nodig toestemming gevraagd aan de klant.

2.2.7 Bewaren van persoonsgegevens

De zorgaanbieder dient de papieren en elektronische persoonsgegevens op een veilige wijze te bewaren, die in overeenstemming is met de geldende wet- en regelgeving. Persoonsgegevens worden niet langer bewaard dan noodzakelijk is om de doelen te bereiken waarvoor de gegevens worden verwerkt, tenzij de gegevens worden geanonimiseerd of indien het noodzakelijk is voor de uitoefening van het recht op vrijheid van meningsuiting en van informatie, voor de nakoming van een wettelijke verplichting, voor de uitvoering van een taak in het algemeen belang of in het kader van de uitoefening van het openbaar gezag dat aan de

[4] Actiz heeft in BOZ-verband een dergelijke model verwerkersovereenkomst ontwikkeld.

verwerkingsverantwoordelijke is verleend, om redenen van algemeen belang op het vlak van volksgezondheid, met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden of voor de vaststelling, uitoefening of onderbouwing van een rechtsvordering.

De zorgaanbieder stelt vast hoelang de vastgelegde/geregistreerde persoonsgegevens bewaard blijven in overeenstemming met de geldende wet- en regelgeving. Voor gezondheidsgegevens die binnen de zorgrelatie worden verwerkt, zoals het dossier van de klant, gelden verschillende bewaartermijnen.

De gegevens van klanten van Sensire worden 20 jaar bewaard na afronden van de zorg, conform de bewaartermijnen die opgenomen zijn in de Wet op de Geneeskundige Behandel Overeenkomst (WGBO). Na deze termijn worden de gegevens vernietigd. Dit gebeurt eenmaal per jaar. Verder is voor ieder (persoons)gegeven bepaald hoelang deze bewaard dienen te worden. Meer informatie over bewaartermijnen is opgenomen in het verwerkingsregister.

2.3 Rechten van de betrokkenen

2.3.1 Voorwaarden m.b.t. de uitvoering van de rechten van de betrokkenen

1. De betrokkene kan de in deze paragraaf 2.3 genoemde verzoeken richten tot de FG via een e-mail aan mijngegevens@sensire.nl of via 0900-8856.
2. Het verstrekken van de in deze paragraaf 2.3 bedoelde informatie, het verstrekken van de communicatie en het treffen van de maatregelen geschieden kosteloos. Indien het verzoek kennelijk ongegrond of buitensporig is, met name vanwege het repetitieve karakter, mag de zorgaanbieder:
    a) een redelijke vergoeding aanrekenen in het licht van de administratieve kosten waarmee het verstrekken van de gevraagde informatie of communicatie en het treffen van de gevraagde maatregelen gepaard gaan; ofwel
    b) weigeren gevolg te geven aan het verzoek.

   Het is aan de zorgaanbieder om de kennelijk ongegronde of buitensporige aard van het verzoek aan te tonen.[5]
3. De zorgaanbieder verstrekt de betrokkene onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek krachtens deze paragraaf informatie over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van het verzoek en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De zorgaanbieder stelt de betrokkene binnen één maand, na ontvangst van het verzoek, in kennis van een dergelijke verlenging. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

   Sensire heeft een procedure opgesteld en ingericht om een verzoek van een betrokkene adequaat en tijdig af te handelen.

2.3.2 Informatie

1. Als de zorgaanbieder gegevens bij de betrokkene zelf opvraagt om te verwerken, informeert hij de betrokkene in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm, voorafgaand aan het verkrijgen van zijn persoonsgegevens, over:
    a) de identiteit en de contactgegevens van de zorgaanbieder;
    b) de verwerkingsdoelen waarvoor de gegevens zijn bestemd, alsook de rechtsgrond voor de verwerking;
    c) in voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens.
    Sensire heeft deze informatie opgenomen in het verwerkingsregister, te vinden op de website van Sensire.
2. Daarnaast heeft betrokkene recht om:
    a) inzage, rectificatie of wissing van de persoonsgegevens of beperking van de hem betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid;
    b) Indien de gegevensverwerking op toestemming is gebaseerd, om te allen tijde die toestemming in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming voor de intrekking daarvan;
    c) een klacht in te dienen bij de Zorgaanbieder;
3. De betrokkene kan voor de rechten in lid 2 zich wenden tot zijn contactpersoon van de

[5] Artikel 12 AVG.

zorgaanbieder.

4. Indien de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde is om een overeenkomst te sluiten, wordt de betrokkene geïnformeerd wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt.
5. Wanneer de zorgaanbieder voornemens heeft de persoonsgegevens verder te verwerken voor een ander doel dan waarvoor de persoonsgegevens zijn verzameld, verstrekt de zorgaanbieder de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie.

2.3.3 Te verstrekken informatie indien persoonsgegevens niet van de betrokkene zijn verkregen

1. Wanneer persoonsgegevens niet van de betrokkene zijn verkregen, verstrekt de zorgaanbieder de betrokkene alle informatie en bovendien de betrokken categorieën van persoonsgegevens alsmede de bron waar de persoonsgegevens vandaan komen.
2. De zorgaanbieder verstrekt de in het eerste lid van dit artikel bedoelde informatie:
    a) binnen een redelijke termijn, maar uiterlijk binnen één maand na de verkrijging van de persoonsgegevens, afhankelijk van de concrete omstandigheden waarin de persoonsgegevens worden verwerkt;
    b) indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met de betrokkene; of
    c) indien verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt.
    d) Wanneer de zorgaanbieder voornemens heeft om de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verkregen, verstrekt de zorgaanbieder de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als bedoeld in het eerste lid van dit artikel.
3. De zorgaanbieder hoeft de betrokkene niet te informeren over de hiervoor genoemde informatie indien:
    a) de betrokkene al over de informatie beschikt;
    b) het informeren van betrokkene onmogelijk blijkt of een onevenredige inspanning kost;
    c) het verkrijgen of verstrekken van informatie (zoals hiervoor genoemd) op grond van wet- en regelgeving verplicht is voor de zorgaanbieder en die wet- en regelgeving voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen; of
    d) de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim in het kader van wet- en regelgeving, waaronder een statutaire geheimhoudingsplicht.

2.3.4 Inzage en afschrift[6]

1. De betrokkene heeft het recht op kosteloze elektronische inzage en een elektronische afschrift van de op zijn persoon betrekking hebbende verwerkte gegevens. De inzage of afschrift verstrekking vindt plaats voor zover daarbij de persoonlijke levenssfeer van een ander niet wordt geschaad. Bijvoorbeeld: informatie over of verstrekt door derden (niet-professionals), zoals familie en naastbetrokkenen of omstanders, wordt niet zonder voorafgaande toestemming van die derde verstrekt. Daarnaast heeft de betrokkene recht

[6] Artikel 7:456, 7:457 BW (Wgbo).

op kosteloze elektronische inzage en afschrift van zijn of haar gegevens die de zorgaanbieder via een elektronisch uitwisselingssysteem beschikbaar stelt.
2. Een wettelijk vertegenwoordiger van jongeren onder de 16 jaar of van een wilsonbekwame volwassene, heeft recht op inzage in of afschrift van het dossier met dezelfde uitzondering voor informatie over of verstrekt door derden (de andere ouder, familie, naastbetrokkenen en omstanders) voor zover van die vertegenwoordigers toestemming voor de behandeling is vereist.[7] De vertegenwoordiger krijgt alleen die informatie die noodzakelijk is voor het uitoefenen van zijn taken als vertegenwoordiger.
3. Indien de hulpverlener door inlichtingen over de klant dan wel inzage in of afschrift van de bescheiden aan de (wettelijk) vertegenwoordiger te verstrekken niet geacht kan worden de zorg van een goed hulpverlener in acht te nemen, laat hij zulks achterwege[8]. Bijvoorbeeld als een minderjarige bezwaar maakt tegen het verstrekken van (bepaalde) informatie aan de ouders of bij een vermoeden van kindermishandeling. In dat geval kan een ouder inzage in het dossier van de minderjarige worden geweigerd. Onder omstandigheden kan de hulpverlener in dat geval feitelijk worden belemmerd om de wettelijk vertegenwoordigers voldoende te informeren om hun toestemming voor de behandeling van de minderjarige te verkrijgen.
4. Indien de zorgaanbieder van mening is dat de gevraagde inzage en/of de kopieën moeten worden verstrekt, dient dit zo spoedig mogelijk plaats te vinden/te worden verstrekt, doch uiterlijk binnen één maand. Afhankelijk van de complexiteit van het verzoek/de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De zorgaanbieder stelt de betrokkene binnen één maand, na ontvangst van het verzoek, in kennis van een dergelijke verlenging. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

2.3.5 Rectificatie (verbetering) of aanvulling van persoonsgegevens en beperking van de verwerking van persoonsgegevens

1. De betrokkene kan de zorgaanbieder vragen om rectificatie (verbetering) van hem of haar betreffende persoonsgegevens als die onjuist zijn of de zorgaanbieder verzoeken om vervollediging van zijn persoonsgegevens, met in acht neming van het doel van de verwerking, onder meer door een eigen aanvullende verklaring toe te voegen aan zijn dossier.
2. De zorgaanbieder informeert de verzoeker onverwijld en ten laatste binnen één maand na ontvangst van een verzoek tot aanvulling, rectificatie of wissing (verwijdering) van gegevens of en op welke manier aan het verzoek wordt voldaan. De zorgaanbieder heeft de mogelijkheid om de termijn van één maand te verlengen met nog eens twee maanden afhankelijk van de complexiteit van het verzoek. In dat geval dient de betrokkene wel binnen één maand van die verlenging in kennis te worden gesteld.
3. Als de zorgaanbieder het verzoek van betrokkene afwijst, geeft hij daarvan de reden. De zorgaanbieder deelt een afwijzing van het verzoek onverwijld en uiterlijk binnen één maand ontvangst van het verzoek aan de verzoeker mee. Ook informeert de zorgaanbieder de verzoeker over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens en de mogelijkheid om beroep in te stellen bij de rechter.
4. De betrokkene kan de zorgaanbieder vragen om bepaalde gegevens voor bepaalde personen af te schermen en hen de toegang tot die gegevens te laten blokkeren.

[7] In de Wgbo wordt de minderjarigheidsgrens verlaagd van 18 jaar naar 16 jaar. Bij jongeren die de leeftijd van 16 jaar hebben bereikt, is toestemming van de ouders (wettelijk vertegenwoordigers) en het verstrekken van de nodige informatie om toestemming te geven daarom niet nodig, tenzij de betrokkene ter zake wilsonbekwaam is.
[8] Artikel 7:457, derde lid, BW (Wgbo).

5. Het verzoek van een klant en beslissing van de zorgaanbieder tot rectificatie (verbetering), wissing of aanvulling van gegevens blijft bewaard in het dossier van de klant.

2.3.6 Recht op gegevenswissing (vergetelheid)

1. De betrokkene heeft het recht van de zorgaanbieder zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen en de zorgaanbieder is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer een van de volgende gevallen van toepassing is:
    a) de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
    b) de betrokkene trekt de toestemming waarop de verwerking berust in en er geen andere rechtsgrond is voor de verwerking;
    c) de persoonsgegevens zijn onrechtmatig verwerkt;
    d) op basis van een wettelijke verplichting, die op de zorgaanbieder rust, de persoonsgegevens moeten worden gewist.
2. De zorgaanbieder stelt iedere ontvanger aan wie persoonsgegevens zijn verstrekt, in kennis van de wissing (verwijdering) van persoonsgegevens tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. De zorgaanbieder verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.
3. Wanneer de zorgaanbieder de persoonsgegevens openbaar heeft gemaakt en overeenkomstig lid 1 verplicht is de persoonsgegevens te wissen, neemt hij, rekening houdend met de beschikbare technologie en de uitvoeringskosten, redelijke maatregelen, waaronder technische maatregelen, om verwerkingsverantwoordelijken die de persoonsgegevens verwerken, ervan op de hoogte te stellen dat de betrokkene de verwerkingsverantwoordelijken heeft verzocht om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen.
4. Een verzoek tot gegevenswissing mag alleen worden geweigerd als:
    a) de wet zich tegen de vernietiging verzet;
    b) een derde een aanmerkelijk belang heeft bij bewaring van die gegevens. Bijvoorbeeld: een kind van een klant heeft een erfelijke ziekte;
    c) de klant heeft een procedure tegen de hulpverlener aangespannen of het is waarschijnlijk dat hij dit zal doen;
    d) in het dossier gegevens over (vermoedens van) kindermishandeling staan dan kunnen deze gegevens op grond van de Meldcode Huiselijk Geweld en Kindermishandeling alleen op verzoek van het kind zelf worden vernietigd en uitsluitend als het kind de leeftijd van 16 jaar heeft bereikt en wilsbekwaam ter zake kan worden geacht;
    e) de zorgaanbieder de gegevens nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering, waaronder voor de betaling van de verleende zorg;
    f) om redenen van algemeen belang op het gebied van volksgezondheid.
5. Het verzoek tot wissing van gezondheidsgegevens en de reactie daarop worden bewaard door de zorgaanbieder.

2.3.7 Recht van bezwaar

1. Indien betrokkene het niet eens is met de verwerking van de gegevens of bezwaar wil maken kan deze contact opnemen met de Functionaris Gegevensbescherming via mijngegevens@sensire.nl. Mocht dit niet leiden tot een oplossing dan heeft betrokkene het

recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens.
2. De betrokkene heeft te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens op basis van de noodzakelijkheid 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 zorgaanbieder is opgedragen of op basis van de noodzakelijkheid voor de behartiging van de gerechtvaardigde belangen van de zorgaanbieder of van een derde;
3. De zorgaanbieder beoordeelt onverwijld en in ieder geval binnen één maand na ontvangst van het bezwaar of het bezwaar gerechtvaardigd is. Indien het bezwaar gerechtvaardigd is, beëindigt hij onmiddellijk de verwerking, tenzij er sprake is van dwingende gerechtvaardigde gronden voor de verwerking die zwaarder wegen dan de belangen, vrijheden en rechten van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.

2.3.8 Recht op gegevensoverdraagbaarheid (dataportabiliteit)

1. De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan een zorgaanbieder heeft verstrekt, in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen en heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke (bijvoorbeeld andere zorgaanbieder) over te dragen, zonder daarbij te worden gehinderd door de zorgaanbieder aan wie de persoonsgegevens waren verstrekt, indien de verwerking berust op toestemming of op uitvoering van een overeenkomst en de verwerking geautomatiseerd wordt verricht.
2. Bij de uitoefening van het recht op gegevensoverdraagbaarheid heeft de betrokkene het recht dat de persoonsgegevens, indien dit technisch mogelijk is, rechtstreeks van de ene zorgaanbieder naar de andere worden doorgezonden.
3. Bij de uitoefening van dit recht mag dit geen afbreuk doen aan de rechten en vrijheden van anderen.

2.3.9 Recht op elektronische afschrift van de logging

1. De betrokkene heeft het recht op een elektronisch afschrift van de logging. In het afschrift wordt informatie opgenomen wie bepaalde informatie via het elektronisch uitwisselingssysteem beschikbaar heeft gesteld en op welke datum en/of wie bepaalde informatie heeft ingezien of opgevraagd en op welke datum.

2.4 Veilige verwerking van persoonsgegevens

2.4.1 Verantwoordelijkheid van de verwerkingsverantwoordelijke

1. Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de zorgaanbieder passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.
2. Wanneer zulks in verhouding staat tot de verwerkingsactiviteiten, omvatten de hierboven bedoelde maatregelen een passend gegevensbeschermingsbeleid dat door de zorgaanbieder wordt uitgevoerd.
3. Het aansluiten bij goedgekeurde gedragscodes of certificeringsmechanismen kan worden gebruikt als element om aan te tonen dat de verplichtingen van de zorgaanbieder zijn nagekomen.

2.4.2 Gegevensbescherming door ontwerp en standaardinstellingen (Privacy by design en default)

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de zorgaanbieder, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen.
2. De zorgaanbieder treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.
3. Een goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat aan de voorschriften is voldaan.

2.4.3 Gezamenlijke verwerkingsverantwoordelijken

1. Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze AVG vast, met name met betrekking tot de uitoefening van de rechten van de betrokkene en hun respectieve verplichtingen om de verplichte informatie te verstrekken, door middel van een onderlinge regeling. In de regeling kan een contactpunt voor betrokkenen worden aangewezen.
2. Uit de bedoelde regeling blijkt duidelijk welke rol de gezamenlijke

verwerkingsverantwoordelijken respectievelijk vervullen, en wat hun respectieve verhouding met de betrokkenen is. De wezenlijke inhoud van de regeling wordt aan de betrokkene beschikbaar gesteld.
3. Ongeacht een dergelijke regeling kan een betrokkene zijn rechten uit de AVG met betrekking tot en jegens iedere verwerkingsverantwoordelijke uitoefenen.

2.4.4 Register van verwerkingen

1. Zorgaanbieder dient een register bij te houden van de verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden. Dat register bevat in ieder geval de volgende gegevens:
   a) de naam en de contactgegevens van de zorgaanbieder en van de FG;
   b) de verwerkingsdoeleinden;
   c) een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
   d) de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
   e) indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
   f) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.
2. De verwerker en, in voorkomend geval, de vertegenwoordiger van de verwerker houdt een register van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht. Dit register bevat de volgende gegevens:
   a) de naam en de contactgegevens van de verwerkers en van iedere verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke of de verwerker en van de FG;
   b) de categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke zijn uitgevoerd;
   c) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.
3. Het register is in schriftelijke vorm, waaronder in elektronische vorm, opgesteld.
4. Desgevraagd stellen de verwerkingsverantwoordelijke of de verwerker het register ter beschikking van de Autoriteit Persoonsgegevens.

Sensire beperkt de gegevensverwerking tot deze gegevens die minimaal noodzakelijk zijn voor het uitvoeren van de overeenkomst en het leveren van kwalitatieve hoogwaardige zorg. Dat betekent onder meer dat de volgende categorieën persoonsgegevens verwerkt worden:

a) NAW gegevens.
b) Identificerende gegevens, waaronder geboortedatum.
c) Contactgegevens.
d) (contact-) Gegevens van mantelzorgers.
e) BSN nummer.
f) Verzekeringsgegevens.
g) Medische gegevens.

2.4.5 Medewerking verlenen aan/samenwerken met de Autoriteit Persoonsgegevens

De zorgaanbieder en de verwerker en, in voorkomend geval, hun vertegenwoordigers, werken desgevraagd samen met de Autoriteit Persoonsgegevens bij het vervullen van haar taken.

2.4.6 Beveiliging van de verwerking

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de zorgaanbieder en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:
   a) de versleuteling van persoonsgegevens;
   b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
   c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
   d) 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.
2. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, met name als gevolg van vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.
3. Het aansluiten bij een goedgekeurde gedragscode of een goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat de in lid 1 van dit artikel bedoelde vereisten worden nageleefd.
4. De zorgaanbieder en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van de zorgaanbieder of van de verwerker en toegang heeft tot persoonsgegevens, deze slechts in opdracht van de zorgaanbieder verwerkt, tenzij hij daartoe volgens wet- en regelgeving is gehouden.

Meer informatie over technische en organisatorische maatregelen die Sensire neemt ter bescherming van haar gegevens is opgenomen in het verwerkingsregister. Deze is te vinden op de website van Sensire, www.sensire.nl/privacy/

2.4.7 Melding van een inbreuk in verband met persoonsgegevens aan de Autoriteit Persoonsgegevens (datalekken melden aan de AP) en datalekkenregister

1. Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de zorgaanbieder dit zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de Autoriteit Persoonsgegevens niet binnen 72 uur plaatsvindt, wordt de vertraging toegelicht (gemotiveerd).
2. De verwerker informeert de zorgaanbieder zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.
3. In de melding aan de Autoriteit Persoonsgegevens wordt ten minste het volgende omschreven of meegedeeld:
   a) de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder

vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
   b) de naam en de contactgegevens van de FG of een ander contactpunt waar meer informatie kan worden verkregen;
   c) de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
   d) de maatregelen die de zorgaanbieder heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.
4. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.
5. De zorgaanbieder houdt alle inbreuken in verband met persoonsgegevens bij in een overzicht, met inbegrip van de feiten omtrent die inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de Autoriteit Persoonsgegevens in staat de naleving van dit artikel te controleren.

2.4.8 Melding van een inbreuk in verband met persoonsgegevens aan de betrokkenen (datalekken melden aan de betrokkene)

1. Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de zorgaanbieder de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.
2. De bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in het vorige artikel (1.4.7, derde lid, onder b), c) en d), bedoelde gegevens en maatregelen.
3. De mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:
   a) de zorgaanbieder heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
   b) de zorgaanbieder heeft achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;
   c) de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.
4. Indien de zorgaanbieder de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan de Autoriteit Persoonsgegevens, na beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, de zorgaanbieder daartoe verplichten of besluiten dat aan een van de in lid 3 van dit artikel, bedoelde voorwaarden is voldaan.

2.4.9 Gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment, DPIA)

1. Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de zorgaanbieder vóór de verwerking een beoordeling uit van het effect van

de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.

2. Wanneer een FG is aangewezen, wint de zorgaanbieder bij het uitvoeren van een gegevensbeschermingseffectbeoordeling diens advies in.
3. Een gegevensbeschermingseffectbeoordeling als bedoeld in het eerste lid is met name vereist in de volgende gevallen:
    a) indien sprake is van de verwerking van persoonsgegevens met het oog op het nemen van besluiten met betrekking tot specifieke natuurlijke personen na een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;
    b) er sprake is van een grootschalige verwerking van bijzondere categorieën van persoonsgegevens, zoals gezondheidsgegevens;
    c) er sprake is van stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.
4. De beoordeling bevat ten minste:
    a) een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden;
    b) een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
    c) een beoordeling van het eerste lid van dit artikel bedoelde risico's voor de rechten en vrijheden van betrokkenen; en
    d) de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan.
5. Indien nodig verricht de zorgaanbieder een toetsing om te beoordelen of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling wordt uitgevoerd, zulks ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden.

2.5 Functionaris voor gegevensbescherming (FG)

2.5.1 Aanwijzing van een FG[9]

1. De zorgaanbieder en de verwerker wijst een FG (FG) aan wanneer de zorgaanbieder of de verwerker, hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens, namelijk voor zorgaanbieders: gezondheidsgegevens.
2. Een concern heeft de mogelijkheid om één FG benoemen, mits de FG vanuit elke vestiging makkelijk te contacteren is.
3. De FG wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de hieronder bedoelde taken te vervullen. De vereiste expertise en vaardigheden omvatten in ieder geval:
    a) kennis van nationale en Europese privacywet- en regelgeving over

[9] Artikel 37 AVG. Zie voor een model functieomschrijving FG http://www.ggznederland.nl/themas/privacywetgeving of rechtstreeks via www.ggzdocs.nl

gegevensbescherming;
   b) begrip van de gegevensverwerkingen die de organisatie uitvoert;
   c) begrip van IT en informatiebeveiliging;
   d) kennis van de organisatie en de sector waarin die actief is;
   e) vaardigheden om binnen de organisatie een cultuur van gegevensbescherming te ontwikkelen.
4. De FG kan een personeelslid van de zorgaanbieder of de verwerker zijn of kan de taken op grond van een dienstverleningsovereenkomst verrichten.
5. De zorgaanbieder of de verwerker maakt de contactgegevens van de FG bekend en deelt die mee aan de Autoriteit Persoonsgegevens. De contactgegevens van de Functionaris voor de Gegevensbescherming van Sensire zijn bekendgemaakt op de website van Sensire.

2.5.2 Positie van de FG

1. De zorgaanbieder en de verwerker ondersteunen de FG bij de vervulling van hieronder bedoelde taken door hem toegang te verschaffen tot persoonsgegevens en verwerkingsactiviteiten en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van deze taken en het in stand houden van zijn deskundigheid.
2. De zorgaanbieder en de verwerker zorgen ervoor dat de FG geen instructies ontvangt met betrekking tot de uitvoering van die taken; de FG werkt zelfstandig en onafhankelijk. De FG brengt rechtstreeks verslag uit aan de hoogste leidinggevende, raad van bestuur of directie, van de zorgaanbieder of de verwerker.
3. Betrokkenen kunnen met de FG contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun persoonsgegevens en met de uitoefening van hun rechten uit de AVG.
4. De FG is met betrekking tot de uitvoering van zijn taken tot geheimhouding of vertrouwelijkheid gehouden.
5. De FG kan andere taken en plichten vervullen. De zorgaanbieder of de verwerker zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden.

2.5.3 Taken van de FG

1. De FG vervult ten minste de volgende taken:
   a) de zorgaanbieder of de verwerker en de werknemers die verwerken, informeren en adviseren over hun verplichtingen uit hoofde van de privacywetgeving (de AVG en andere gegevensbeschermingsbepalingen zoals uit sectorspecifieke wet- en regelgeving);
   b) toezien op naleving van deze AVG, van andere gegevensbeschermingbepalingen en van het beleid van de zorgaanbieder of de verwerker met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
   c) desgevraagd advies verstrekken met betrekking tot de gegevensbeschermingseffect-beoordeling en toezien op de uitvoering daarvan;
   d) optreden als contactpunt voor de Autoriteit Persoonsgegevens inzake met verwerking verband houdende aangelegenheden, met inbegrip van de voorafgaande raadpleging, en, waar passend, overleg plegen over enige andere aangelegenheid.
2. De FG houdt bij de uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden.

2.5.4 Bij een klacht

Bij een klacht over de naleving van deze privacyverklaring kan de betrokkene zich wenden tot de klachtenfunctionaris. Meer informatie hierover op de website van Sensire. Ook kan betrokkene zich wenden tot de FG of tot de Autoriteit Persoonsgegevens.