Privacybeleid

Inhoudsopgave

Privacyreglement

Dit reglement is is gebaseerd op het Model Privacyreglement van GGZ-Nederland en is van toepassing binnen Stichting Cosis, statutair gevestigd te Assen en heeft betrekking op de verwerkingen van gegevens binnen Cosis.

Dit reglement is van toepassing op zowel papier als elektronische verwerking van gegevens.

1. Definities

Algemene verordening gegevensbescherming (AVG): Europese privacywetgeving die 25 mei 2018 van kracht wordt en de huidige Wet bescherming persoonsgegevens vervangt.

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 medewerker, de cliënt, 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 Cosis 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"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Pseudonimisering: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkenen kunnen worden gekoppeld zonder dat aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en 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 externe hostingsfirma, saas-leverancier, kwaliteitsauditor of een extern salarisadministratiekantoor).

Verwerking van persoonsgegevens: alle 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 bestuurder van Cosis.

Werkgever/Zorgaanbieder: Stichting Cosis

2. Verwerking van persoonsgegevens in overeenstemming met de AVG

2.1. Beginselen inzake persoonsgegevens verwerking

Cosis is verantwoordelijk voor de naleving van onderstaande uitgangspunten bij de verwerking van persoonsgegevens en moet de naleving hiervan kunnen aantonen ("verantwoordingsplicht").

Binnen Cosis worden persoonsgegevens alleen verwerkt:

- als de verwerking mag volgens de wet, de verwerking op een goede manier gebeurd en de betrokkene weet welke gegevens van hem verwerkt worden, voor welk doel en hoe lang deze bewaard worden;
- voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen en mogen vervolgens niet verder worden verwerkt als dit niet met die doelen overeen komt; 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 ("doelbinding");

- voor zover zij toereikend zijn, daadwerkelijk voor het doel gebruikt kunnen worden en beperkt tot wat noodzakelijk is voor het doel waarvoor zij worden verwerkt (“minimale gegevensverwerking” ook wel “dataminimalisatie”);
- indien de persoonsgegevens juist zijn en zo nodig worden geactualiseerd. Alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doelen waarvoor zij worden verwerkt, onjuist zijn, onverwijld te verwijderen of aan te passen (“juistheid”)
- en bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doelen waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens alleen met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerk én de bij de AVG vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen (“opslagbeperking”);
- 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 (“integriteit en vertrouwelijkheid”).

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 gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, bijvoorbeeld de zorg- en dienstverleningsovereenkomst of arbeidsovereenkomst;
- de gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen, bijvoorbeeld de dossierplicht in de Wgbo, Wmo2015 en Jeugdwet of het bewaren van medewerkersgegevens op grond van de Wet op de Loonbelasting;
- de gegevensverwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of een ander natuurlijk persoon;
- 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 van de verwerkingsverantwoordelijke of van een derde én de belangen, grondrechten of fundamentele vrijheden van degene van wie de gegevens worden verwerkt niet prevaleren.;
- de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden; Cosis moet de toestemming kunnen aantonen en betrokkenen heeft het recht de toestemming te allen tijde in te trekken.

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

Let op: naast de opheffing van het verbod om bijzondere gezondheidsgegevens te verwerken zoals hierboven genoemd, moet ook nog een verwerkingsgrondslag aanwezig zijn om dergelijke gegevens te verwerken (zie ook 2.2).

2.4. Gegevensverwerking door verwerker

- Cosis kan de verwerking (extern) uitbesteden aan een verwerker en legt dan in een verwerkersovereenkomst de verplichtingen uit de AVG op aan de verwerker. Cosis doet uitsluitend een beroep op verwerkers die afdoende garanties met betrekking tot het toepassen van 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 Cosis 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 Cosis worden omschreven. Een dergelijke overeenkomst dient te voldoen aan de eisen die de AVG daaraan stelt. In BOZ[1]-verband is een dergelijke model verwerkersovereenkomst ontwikkeld, welke Cosis als standaard gebruikt.
- De verwerker en eenieder die onder het gezag van Cosis of van de verwerker handelt en toegang heeft tot persoonsgegevens, verwerkt deze uitsluitend in opdracht van Cosis, tenzij hij door wet- of regelgeving tot verwerking gehouden is.

2.5. Gegevensuitwisseling met andere verantwoordelijke

- Cosis kan gegevens uitwisselen met een andere verantwoordelijke, bijvoorbeeld in het kader van onderzoek of uitbesteden van zorg, en legt de afspraken vast in een uitwisselovereenkomst.
- De uitwisselovereenkomst regelt 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 wederzijdse rechten en verplichtingen van de verantwoordelijken (o.a. met betrekking tot beveiliging van gegevens en het melden en afhandelen van een datalek).

2.6. Aansprakelijkheid verwerkingsverantwoordelijke en/of verwerker

1. Cosis (verwerkingsverantwoordelijke) is verantwoordelijk en aansprakelijk voor schade die voortvloeit uit het toerekenbaar tekortschieten of niet voldoende naleven van de AVG, waaronder het wel/niet naleven van de beveiligingseisen.
2. De verwerker, waaraan Cosis (een deel van) gegevensverwerking heeft uitbesteed, kan daarnaast zelfstandig aansprakelijk zijn voor schade of een deel van de schade die voortvloeit uit zijn werkzaamheden. Hoe die aansprakelijkheid wordt verdeeld, wordt beoordeeld door de schadeverzekeraar of de rechter. Van belang is dat Cosis goede afspraken maakt met de verwerker en deze vastlegt in een verwerkersovereenkomst.

[1] Brancheorganisaties zorg, waar ook GGZ-Nederland en VGN onderdeel van uitmaken.

2.7. Wanneer mogen andere bijzondere gegevens dan de gezondheidsgegevens worden verwerkt?

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

2.8. Geheimhoudingsplicht en verstrekking aan derden

1. Persoonsgegevens verkregen in de uitoefening van een beroep in de gezondheidszorg vallen onder de geheimhoudingsplicht van de hulpverlener. Deze geheimhoudingsplicht is o.a. vastgelegd in de Wgbo en/of Jeugdwet en de wet BIG en in verschillende beroepscodes.
2. Persoonsgegevens verkregen in het kader van de arbeidsovereenkomst vallen onder de geheimhouding van de werkgever op grond van het goed werkgeverschap.
3. Bij de verstrekking van gegevens aan derden wordt de wet nageleefd en dienen de handreikingen van de brancheorganisaties GGZ Nederland en VGN ter ondersteuning.

2.9. Wanneer mogen gegevens aan een ander worden verstrekt voor wetenschappelijk onderzoek en statistiek op het gebied van de volksgezondheid?

De gegevensverwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden is onderworpen aan passende waarborgen in overeenstemming met de AVG voor de rechten en vrijheden van de betrokkene. De waarborgen zorgen ervoor dat er technische en organisatorische maatregelen zijn getroffen om de inachtneming van het beginsel van minimale gegevensverwerking te garanderen. Deze maatregelen kunnen pseudonimisering omvatten, mits aldus die doeleinden in kwestie kunnen worden verwezenlijkt. Wanneer die doeleinden kunnen worden verwezenlijkt door verdere verwerking die de identificatie van betrokkenen niet of niet langer toelaat, moeten zij aldus worden verwezenlijkt. Tevens kan er in nationale wetgeving worden afgeweken van bepaalde rechten van betrokkenen uit de AVG voor zover die rechten de verwezenlijking van de specifieke doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren, en dergelijke afwijkingen noodzakelijk zijn om die doeleinden te bereiken.

De Wgbo geeft onderstaande afwijkende bepalingen voor wetenschappelijk onderzoek op het gebied de van gezondheidszorg. Het uitgangspunt is dat voor het verstrekken van gepseudonimiseerde gegevens[2] en andere gegevens die niet geanonimiseerd zijn toestemming van de cliënt is vereist. In afwijking van dit uitgangspunt kan ook zonder toestemming van de cliënt ten behoeve van statistiek of wetenschappelijk onderzoek op het gebied van de volksgezondheid aan een ander desgevraagd inlichtingen over de cliënt of inzage in de bescheiden, worden verstrekt indien:

1. het vragen van toestemming in redelijkheid niet mogelijk is en bij de uitvoering van het onderzoek zodanige waarborgen gelden, dat de persoonlijke levenssfeer van de cliënt niet onevenredig wordt geschaad, of
2. het vragen van toestemming, gelet op de aard en het doel van het onderzoek, in redelijkheid niet kan worden verlangd en de hulpverlener ervoor zorgt dat gegevens in zodanige vorm worden verstrekt dat herleiding tot individuele natuurlijke personen redelijkerwijs wordt voorkomen.

Verder moet:

a) het onderzoek een algemeen belang dienen;

[2] Pseudonimisering is een beveiligingsmaatregel (versleuteling of apart opslaan van identificerende gegevens los van de inhoudelijke) die direct herleiden tot een natuurlijke persoon onmogelijk maakt, maar indirecte herleiding (bijvoorbeeld door koppeling aan andere reeds bekende gegevens) blijft mogelijk. Daarom blijven gepseudonimiseerde gegevens persoonsgegevens en blijven de AVG-bepalingen en die uit de sectorspecifieke wetten over privacy van toepassing.

b) aangetoond zijn dat het onderzoek niet zonder de gegevens kan worden uitgevoerd; en
c) de betrokken cliënt tegen een verstrekking niet uitdrukkelijk bezwaar hebben gemaakt.

Belangrijk om te beseffen is dat bovenstaande voorwaarden cumulatief werken; verstrekking is pas mogelijk indien aan alle voorwaarden is voldaan.

2.10. Bewaren van persoonsgegevens

Cosis 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 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.

Cosis stelt vast hoelang de vastgelegde/geregistreerde persoonsgegevens bewaard blijven in overeenstemming met de geldende wet- en regelgeving. Indien nog geen specifieke termijn kan worden genoemd: de criteria voor het vaststellen van de bewaartermijn.
Voor gezondheidsgegevens die binnen de zorgrelatie worden verwerkt, zoals het dossier van de cliënt, gelden verschillende bewaartermijnen.

3. Rechten van de betrokkenen

3.1. Voorwaarden met betrekking tot de **uitvoering** van de rechten van de betrokkenen

1. Het verstrekken van de in dit hoofdstuk bedoelde informatie, het verstrekken van de communicatie en het treffen van de maatregelen gebeuren kosteloos. Indien het verzoek kennelijk ongegrond of buitensporig is, met name vanwege het rherhaadelijke karakter, mag Cosis:
    a) een redelijke vergoeding in rekening brengen 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 te voldoen aan het verzoek.

    Het is aan Cosis om de kennelijk ongegronde of buitensporige aard van het verzoek aan te tonen.
2. De in dit hoofdstuk onder 3.4 t/m 3.8 beschreven rechten kunnen door cliënten worden uitgeoefend door het verzoek schriftelijk in te dienen bij het hoofd. Indien een cliënt niet meer bij Cosis in zorg is kan dit verzoek schriftelijk worden gericht aan de Raad van Bestuur.
3. De in dit hoofdstuk onder 3.4 t/m 3.8 beschreven rechten kunnen door medewerkers worden uitgeoefend door dit verzoek schriftelijk in te dienen bij de leidinggevende. Indien een medewerker niet meer bij Cosis in dienst is kan dit verzoek schriftelijk worden gericht aan de Raad van Bestuur.
4. Cosis verstrekt de betrokkene zo snel mogelijk en in ieder geval binnen een maand na ontvangst van het verzoek informatie over het voldoen aan of weigeren van het verzoek. Afhankelijk van de complexiteit van het verzoek en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. Cosis 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 verzoekt de informatie anders te ontvangen.

3.2. Te verstrekken informatie

1. Als Cosis gegevens bij de betrokkene zelf opvraagt om te verwerken, informeert hij de betrokkene in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm over:
   a) de identiteit en de contactgegevens van Cosis;
   b) de contactgegevens van de functionaris voor gegevensbescherming;
   c) de verwerkingsdoelen waarvoor de gegevens zijn bestemd en de wettelijke grondslag voor de verwerking;
   d) indien van toepassing, de ontvangers of categorieën van ontvangers van de persoonsgegevens.
2. Daarnaast wordt onderstaande aanvullende informatie verstrekt om behoorlijke en transparante verwerking te waarborgen:
   a) de periode gedurende welke de persoonsgegevens zullen worden opgeslagen of indien dat niet mogelijk is, de criteria ter bepaling van die termijn;
   b) de mogelijkheden die de betrokkene heeft om een verzoek om inzage, rectificatie of wissing van de persoonsgegevens in te dienen, het verzoek om beperking van de verwerking die hem betreft in te dienen, het recht om tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid;
   c) Indien de gegevensverwerking op toestemming is gebaseerd, dient de betrokkene geïnformeerd te worden over het recht om te allen tijde die toestemming in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking die op basis van de toestemming voor de intrekking daarvan is uitgevoerd.
   d) het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens en op welke wijze de betrokkene deze rechten kan inroepen.
   e) of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt.
3. Wanneer Cosis de persoonsgegevens verder wil verwerken voor een ander doel dan waarvoor de persoonsgegevens zijn verzameld, verstrekt Cosis de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie zoals genoemd in het tweede lid van dit artikel.
4. De leden 1, 2 en 3 van dit artikel zijn niet van toepassing wanneer en voor zover de betrokkene reeds over de informatie beschikt.

3.3. Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen

1. Wanneer persoonsgegevens niet van de betrokkene zijn verkregen, verstrekt Cosis de betrokkene alle informatie zoals hierboven (artikel 3.2) onder lid 1 en 2 genoemd, de betrokken categorieën van persoonsgegevens en de bron waar de persoonsgegevens vandaan komen.
2. Cosis verstrekt de hiervoor genoemde 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 Cosis de persoonsgegevens verder wil verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verkregen, verstrekt Cosis 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. Cosis 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. In het bijzonder bij verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, behoudens de in artikel 89, lid 1, bedoelde voorwaarden en waarborgen, of voor zover de in lid 1 van dit artikel bedoelde verplichting de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen. In dergelijke gevallen neemt Cosis passende maatregelen om de rechten, de vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van de informatie;
   c) het verkrijgen of verstrekken van informatie (zoals hiervoor genoemd) op grond van wet- en regelgeving verplicht is voor Cosis 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.

3.4. Inzage en afschrift/kopie

1. De betrokkene van twaalf jaar of ouder heeft het recht op inzage en een kopie van de op hem betrekking hebbende verwerkte gegevens. De inzage of verstrekking van het afschrift gebeurt alleen voor zover daarbij de privacy 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 persoon verstrekt.
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 voor zover van die vertegenwoordigers toestemming voor de behandeling is vereist en met dezelfde uitzondering voor informatie over of verstrekt door derden (de andere ouder, familie, naastbetrokkenen en omstanders), zoals hiervoor genoemd. De vertegenwoordiger krijgt alleen die informatie die noodzakelijk is voor het uitoefenen van zijn taken als vertegenwoordiger.
3. De hulpverlener gaat niet over tot het verstrekken van inlichtingen over de cliënt dan wel inzage in of afschrift van de gegevens aan de (wettelijk) vertegenwoordiger te verstrekken als dit in strijd is met de zorg van een goed hulpverlener. 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. Het kan voorkomen dat 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 Cosis van mening is dat de gevraagde inzage en/of de kopieën moeten worden verstrekt, dient dat 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. Cosis 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 verzoekt de informatie anders te ontvangen.

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

1. De betrokkene kan Cosis vragen om rectificatie (verbetering) van hem of haar betreffende persoonsgegevens als die onjuist zijn of Cosis verzoeken om aanvulling 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. Cosis informeert de verzoeker zo snel mogelijk maar uiterlijk 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. Cosis 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 Cosis het verzoek van betrokkene afwijst, geeft hij daarvan schriftelijk de reden. Cosis deelt een afwijzing van het verzoek zo snel mogelijk en uiterlijk binnen één maand na ontvangst van het verzoek aan de verzoeker mee. Ook informeert Cosis 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 Cosis vragen om bepaalde gegevens voor bepaalde personen af te schermen en hen de toegang tot die gegevens te laten blokkeren.
5. Het verzoek van een betrokkene en beslissing van Cosis tot rectificatie (verbetering), wissing of aanvulling van gegevens blijft bewaard in het dossier van de betrokkene.

3.6. Recht op gegevenswissing (vergetelheid)

1. De betrokkene heeft het recht van Cosis zonder onredelijke vertraging de gegevens die op hem betrekking hebben te laten en Cosis 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 doelen 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 Cosis rust, de persoonsgegevens moeten worden gewist.
2. Cosis 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. Cosis verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.
3. Wanneer Cosis de persoonsgegevens openbaar heeft gemaakt en op grond van 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. Indien het gezondheidsgegevens betreft, wist Cosis de gegevens zonder onredelijke vertraging en verstrekt de betrokkene in ieder geval binnen een maand na ontvangst van het verzoek informatie over de uitvoering van het verzoek. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. Cosis stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van een dergelijke verlenging.
5. Een verzoek tot gegevenswissing mag alleen worden geweigerd als:
    a) de wet zich tegen de vernietiging verzet;
    Bijvoorbeeld: de gegevens moeten bewaard worden op grond van fiscale wetgeving.
    b) een derde een aanmerkelijk belang heeft bij bewaring van die gegevens.
    Bijvoorbeeld: een kind van een cliënt heeft een erfelijke ziekte;
    c) de betrokkene heeft een procedure tegen Cosis 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) Cosis de gegevens nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering;

f) om redenen van algemeen belang op het gebied van volksgezondheid.

6. Het verzoek tot wissing van gegevens en de reactie daarop worden bewaard door Cosis.

3.7. Recht van bezwaar

1. De betrokkene heeft te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van gegevens die op hem betrekking hebben indien die verwerking op basis van de noodzakelijkheid voor de vervulling van een taak van algemeen belang of op basis van de noodzakelijkheid voor de behartiging van de gerechtvaardigde belangen van Cosis of van een derde plaats vindt;
2. Cosis beoordeelt zo snel mogelijk en uiterlijk binnen één maand na ontvangst van het bezwaar of het bezwaar gerechtvaardigd is. Indien het bezwaar gerechtvaardigd is, beëindigt Cosis 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.

3.8. Recht op gegevensoverdraagbaarheid (dataportabiliteit)

1. De betrokkene heeft het recht de gegevens die op hem betrekking hebben en die hij aan Cosis 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 degene aan wie de persoonsgegevens waren verstrekt. Dit geldt alleen indien de verwerking berust op toestemming van de betrokkene 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 verantwoordelijke naar de andere worden doorgezonden.
3. Bij de uitoefening van dit recht mag dit geen afbreuk doen aan de rechten en vrijheden van anderen.

4. Vertegenwoordiging cliënten

1. Bij een jeugdige jonger dan twaalf jaar en bij een wilsonbekwame jeugdige van twaalf tot achttien jaar, oefent (oefenen) de ouder(s) met gezag of de voogd de rechten van de jeugdige uit, tenzij dit niet verenigbaar is met de zorg van een goed hulpverlener.
2. De ouder die geen gezag heeft krijgt desgevraagd belangrijke, algemene en feitelijke informatie over de gezondheidstoestand van de jeugdige, tenzij:
   a. de hulpverlener de informatie ook niet aan de ouder met gezag heeft verstrekt/ verstrekt;
   b. niet in niet verenigbaar is met de zorg van een goed hulpverlener.
3. De wilsbekwame jeugdige van twaalf jaar of ouder oefent zelfstandig zijn rechten over zijn persoons- en gezondheidsgegevens uit. Vernietiging van gegevens over (vermoedens van) kindermishandeling vindt uitsluitend plaats met toestemming van een wilsbekwame jeugdige van zestien jaar en ouder.
4. Is de betrokkene ouder dan achttien jaar en wilsonbekwaam ter zake, dan treedt als vertegenwoordiger voor hem op:
   a) een (toegewezen) curator of mentor;
   b) indien er geen curator of mentor is, de persoon die de cliënt schriftelijk heeft

gemachtigd;

c) indien de persoonlijk gemachtigde ontbreekt of niet optreedt; de echtgenoot of levensgezel van de betrokkene;
d) indien de echtgenoot of levensgezel ontbreekt of niet optreedt: een kind, broer of zus van de betrokkene.

5. In het uiterste geval treedt Cosis op als goed hulpverlener; hij zorgt er voor dat er zo snel mogelijk een wettelijk vertegenwoordiger voor betrokkene optreedt. Zo nodig, als familie of naaste dat niet kan of wil, verzoekt hij de rechter om een vertegenwoordiger te benoemen.

5. Veilige verwerking van persoonsgegevens

5.1. 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 Cosis 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 Cosis wordt uitgevoerd.
3. Het aansluiten bij goedgekeurde gedragscodes of goedgekeurde certificeringsmechanismen kan worden gebruikt als element om aan te tonen dat de verplichtingen van Cosis zijn nagekomen.

5.2. 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 Cosis, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, 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. Cosis 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.

   Praktische uitwerking:

   a) Cosis baseert haar verwerking van zorggegevens op de normen van de NEN 7510, 7512 en 7513 .
   b) Voor de verstrekking van gegevens via e-mail wordt gebruik gemaakt van de beveiligde e-mailverbinding <evt. naam>.
   c) Cosis werkt volgens de ‘Richtsnoeren beveiliging persoonsgegevens’ van de Autoriteit Persoonsgegevens en de ‘Praktijkgids patiëntgegevens in de cloud’ van de Autoriteit Persoonsgegevens.
   d) De identificerende gegevens zijn zoveel als mogelijk gescheiden opgeslagen van de inhoudelijke gegevens, gepseudonimiseerd of versleuteld.
   e) De standaardinstellingen zijn nee, tenzij (opt-in) in plaats van ja, mits (opt-out), tenzij

de wetgeving opt-out toelaatbaar stelt.

f) Cosis hanteert per verwerking een autorisatieprotocol. Daarin staat welke gegevens door wie/welke (groepen) medewerkers verwerkt kunnen worden en waarom en welke bevoegdheden zij hebben ten aanzien van welke gegevens (inzage, toevoegen, wijzigen, verwijderen).

5.3. 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.

5.4. Register van verwerkingen

1. Zorgaanbieder dient een register bij te houden van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden. Dat register bevat in ieder geval de volgende gegevens:
   a) de naam en de contactgegevens van Cosis en eventuele gezamenlijke verwerkingsverantwoordelijken, en van de functionaris voor gegevensbescherming;
   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, onder meer ontvangers in derde landen of internationale organisaties;
   e) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, van de AVG bedoelde doorgiften, de documenten inzake de passende waarborgen;
   f) indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
   g) 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 functionaris voor gegevensbescherming;
   b) de categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke zijn uitgevoerd;
   c) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, onder vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, eerste lid, tweede alinea, van de AVG bedoelde doorgiften, de documenten inzake de passende waarborgen;

d) 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 .

5.5. Medewerking verlenen aan/samenwerken met de Autoriteit persoonsgegevens

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

5.6. 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 Cosis 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 pseudonimisering en 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. Cosis en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van Cosis of van de verwerker en toegang heeft tot persoonsgegevens, deze slechts in opdracht van Cosis verwerkt, tenzij hij daartoe volgens wet- en regelgeving is gehouden.

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

1. Cosis heeft een proces voor het melden van het melden en afhandelen van (mogelijke) datalekken (Proces datalekken). Het gaat hierbij om het melden van (mogelijke) datalekken door medewerkers van Cosis maar ook om het melden door Bewerkers of andere mogelijke ontdekkers van een (mogelijk) datalek. Datalekken worden binnen Cosis centraal gemeld en van elk (mogelijk) datalek wordt beoordeelt of dit een inbreuk is die aan de AP gemeld moet worden, hiervan wordt een registratie bijgehouden in Planon.
2. Indien een inbreuk in verband met persoonsgegevens (datalek) heeft plaatsgevonden, meldt Cosis 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).
3. De verwerker informeert Cosis zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.

4. 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 functionaris voor gegevensbescherming 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 Cosis 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.
5. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.
6. Cosis 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.

5.8. 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 Cosis 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 (3.5.7, 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) Cosis 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) Cosis 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 Cosis 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, Cosis daartoe verplichten of besluiten dat aan een van de in lid 3 van dit artikel, bedoelde voorwaarden is voldaan.

5.9. 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 Cosis 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 functionaris voor gegevensbescherming is aangewezen, wint Cosis 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 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, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.
5. Bij het beoordelen van het effect van de door een zorgaanbieder of verwerker verrichte verwerkingen en met name ter wille van een gegevensbeschermingseffectbeoordeling, wordt de naleving van goedgekeurde gedragscodes naar behoren in aanmerking genomen.
6. Cosis vraagt in voorkomend geval de betrokkenen of hun vertegenwoordigers naar hun mening over de voorgenomen verwerking, met inachtneming van de bescherming van commerciële of algemene belangen of de beveiliging van verwerkingen.
7. Indien nodig verricht Cosis 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.

5.10. Voorafgaande raadpleging van de Autoriteit Persoonsgegevens

1. Wanneer uit een gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico zou opleveren indien Cosis geen maatregelen neemt om het risico te beperken, raadpleegt Cosis voorafgaand aan de verwerking de Autoriteit Persoonsgegevens.
2. Wanneer de Autoriteit Persoonsgegevens van oordeel is dat de bedoelde voorgenomen verwerking inbreuk zou maken op deze verordening, met name wanneer Cosis het risico onvoldoende heeft onderkend of beperkt, geeft de Autoriteit Persoonsgegevens binnen maximaal acht weken na de ontvangst van het verzoek om raadpleging schriftelijk advies aan Cosis en in voorkomend geval aan de verwerker, en mag zij al haar bevoegdheden uitoefenen. Die termijn kan, naargelang de complexiteit van de voorgenomen verwerking, met zes weken worden verlengd. Bij een dergelijke verlenging stelt de Autoriteit Persoonsgegevens Cosis en, in voorkomend geval, de verwerker binnen een maand na ontvangst van het verzoek om raadpleging in kennis van onder meer de redenen voor de vertraging. Die termijnen kunnen worden opgeschort totdat de Autoriteit Persoonsgegevens informatie heeft verkregen waarom zij met het oog op de raadpleging heeft verzocht.

3. Bij de raadpleging verstrekt Cosis de nodige informatie zoals benoemd in de AVG. In ieder geval dienen de volgende gegevens te worden verstrekt:
    a) indien van toepassing, de verantwoordelijkheden van Cosis, bij de verwerking betrokken gezamenlijke verwerkingsverantwoordelijken en verwerkers, in het bijzonder ten aanzien van een verwerking binnen een concern;
    b) de doeleinden en middelen van de voorgenomen verwerking;
    c) de maatregelen en waarborgen die worden geboden ter bescherming van de rechten en vrijheden van betrokkenen uit hoofde van de AVG;
    d) de contactgegevens van de functionaris voor gegevensbescherming;
    e) de gegevenseffectbeoordeling ten aanzien van die verwerking;
    f) alle andere informatie waar de Autoriteit Persoonsgegevens om verzoekt.

6. Functionaris voor gegevensbescherming (FG)

6.1. Aanwijzing van een functionaris voor gegevensverwerking

1. Cosis en de verwerker wijst een functionaris voor gegevensbescherming aan wanneer Cosis of de verwerker bijzondere categorieën van persoonsgegevens, zoals gezondheidsgegevens, verwerkt.
2. Een concern heeft de mogelijkheid om één functionaris voor gegevensbescherming benoemen, mits de functionaris voor gegevensbescherming vanuit elke vestiging makkelijk te contacteren is.
3. De functionaris voor gegevensbescherming 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 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 functionaris voor gegevensbescherming kan een personeelslid van Cosis of de verwerker zijn of kan de taken op grond van een dienstverleningsovereenkomst verrichten.
5. Cosis of de verwerker maakt de contactgegevens van de functionaris voor gegevensbescherming bekend en deelt die mee aan de Autoriteit Persoonsgegevens. Binnen Cosis is als functionaris voor gegevensbescherming werkzaam: Tanita Dijks, t.dijks@cosis.nu, 06 - 52870741

6.2. Positie van de functionaris voor gegevensbescherming

1. Cosis zorgt ervoor dat de functionaris voor gegevensbescherming naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. Concreet heeft een functionaris voor gegevensbescherming onder meer het volgende nodig om de functie in te vullen:
    a) de actieve steun vanuit het management;
    b) voldoende tijd om de taken uit te voeren;
    c) voldoende praktische ondersteuning (budget, faciliteiten en personeel);
    d) heldere communicatie aan al het personeel over de benoeming van de FG;
    e) scholing.
2. Cosis ondersteunt de functionaris voor gegevensbescherming 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.

3. Cosis zorgt ervoor dat de functionaris voor gegevensbescherming geen instructies ontvangt met betrekking tot de uitvoering van die taken; de functionaris voor gegevensbescherming werkt zelfstandig en onafhankelijk. De functionaris voor gegevensbescherming wordt door Cosis niet ontslagen of gestraft voor de uitvoering van zijn taken en ondervindt geen nadeel van de uitoefening van zijn taak. De functionaris voor gegevensbescherming brengt rechtstreeks verslag uit aan de hoogste leidinggevende, raad van bestuur of directie, van Cosis.
4. Betrokkenen kunnen met de functionaris voor gegevensbescherming contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun persoonsgegevens en met de uitoefening van hun rechten uit de AVG.
5. De functionaris voor gegevensbescherming is met betrekking tot de uitvoering van zijn taken tot geheimhouding of vertrouwelijkheid gehouden.
6. De functionaris voor gegevensbescherming kan andere taken en plichten vervullen. Cosis of zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden. Om belangenverstrengeling te voorkomen, mag de functionaris voor gegevensverwerking binnen de organisatie niet ook een functie hebben waarin hij het doel en de middelen van een gegevensverwerking bepaalt. Dit kan bijvoorbeeld zo zijn als de functionaris voor gegevensverwerking een managementpositie vervult, zoals hoofd financiën, strategie, marketing, IT of HRM.

6.3. Taken van de functionaris voor gegevensverwerking

1. De functionaris voor gegevensbescherming vervult ten minste de volgende taken:
   a) Cosis 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 gegevensbeschermingsbepalingen en van het beleid van Cosis 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) met de Autoriteit Persoonsgegevens samenwerken;
   e) 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 functionaris voor gegevensbescherming 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.

6.4. Bij een klacht

Bij een klacht over de naleving van dit reglement kan de betrokkene zich wenden tot:
De functionaris voor gegevensverwerking, via privacy@cosis.nu
De Autoriteit Persoonsgegevens, via www.autoriteitpersoonsgegevens.nl
Voor andere klachten raadpleegt de betrokkene de klachtenregeling van Cosis.

7. Wijzigingen en inzage van dit reglement

Dit reglement geldt per 8 augustus 2018 en is via intranet en www.cosis.nu in te zien.