axians

Verwerkersovereenkomst

DATUM: 6 september 2022

AUTEURS: Rob Smit / Ad Schaafsma / Roxane Leijgraaf

SUB-AUTEUR: Bert Wijnholds

CLASSIFICATIE: Vertrouwelijk

VERSIENUMMER: HS-20210317-2.8

VINCI ENERGIES

axians

DE ONDERGETEKENDEN:

1. Praktijk voor Psychotherapie B.H. Plaggo (statutair) gevestigd en kantoorhoudende te Oosterbeek op het adres Veritasweg 5a met postcode 6861 XT en KvK nr. 09207393 hierna te noemen 'Verwerkingsverantwoordelijke', bevoegd vertegenwoordigd door B.H. Plaggo ____.

en

2. **VCD Healthcare B.V. h.o.d.n. Axians**, statutair gevestigd en kantoorhoudende te **Groningen** op het adres **Eemsgolaan 15** met postcode **9727 DW** en KvK nr. **01101645**, hierna te noemen 'Verwerker', bevoegd vertegenwoordigd door **de heer B. Wijnholds**.

- Verwerkingsverantwoordelijke en **Verwerker** hierna ook individueel respectievelijk gezamenlijk te noemen: **Partij** respectievelijk **Partijen** -

IN AANMERKING NEMENDE DAT:

A. tussen Verwerkingsverantwoordelijke en Verwerker zijn Overeenkomsten gesloten met betrekking tot ondersteunende dienstverlening op en het beschikbaar stellen van de online applicatie Zorg GGZ (en Online-DBC indien van toepassing) inclusief aanpalende services waaronder facturatieservices en het vanuit de verplichting van Verwerkingsverantwoordelijke aanleveren van persoonsgegevens van diens cliënten aan diverse landelijke systemen en dat Partijen voor alle daaruit voortvloeiende Verwerkingen deze Verwerkersovereenkomst willen aangaan;

B. Verwerker in het kader van de uitvoering van zijn verplichtingen voortvloeiend uit de Overeenkomst Persoonsgegevens ten behoeve van Verwerkingsverantwoordelijke zal verwerken;

C. VCD Healthcare B.V. h.o.d.n. Axians zoals hierboven opgenomen als ondergetekende 2 in het kader van de uitvoering van de Overeenkomst Verwerker is en de relatie zoals hierboven opgenomen als ondergetekende 1 de Verwerkingsverantwoordelijke is;

D. Partijen, mede gelet op het bepaalde in artikel 28 lid 3 Avg, in deze Verwerkersovereenkomst hun wederzijdse rechten en verplichtingen op basis van de Avg en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens willen vastleggen.

VERKLAREN TE ZIJN OVEREENGEKOMEN ALS VOLGT:

Artikel 1 Definities

De in deze Verwerkersovereenkomst met een hoofdletter geschreven begrippen hebben de volgende betekenis:

1.1	Autoriteit Persoonsgegevens (AP):	Toezichthoudende autoriteit, zoals bedoeld in artikel 4 sub 21 Avg.

1.2	Avg:	Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) inclusief de Uitvoeringswet Algemene verordening gegevensbescherming (UAvg).
1.3	Betrokkene:	De geïdentificeerde of identificeerbare natuurlijke persoon op wie de Persoonsgegevens betrekking hebben, zoals bedoeld in artikel 4 sub 1 Avg.
1.4	Bijlage(n):	Aanhangsel(s) bij deze Verwerkersovereenkomst, die daarvan een onverbrekelijk onderdeel uitmaken.
1.5	Bijzondere categorieën van persoonsgegevens:	Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, zoals bedoeld in artikel 9 Avg.
1.6	Data Privacy Impact Assessment (DPIA)	De gegevensbeschermingseffectbeoordeling die vóór de Verwerking ten aanzien van het effect van de beoogde verwerkingsactiviteiten op de bescherming van Persoonsgegevens wordt uitgevoerd, zoals bedoeld in artikel 35 Avg.
1.7	Gevoelige gegevens:	Gegevens over de financiële of economische situatie van Betrokkene (schulden-salaris- en betalingsgegevens), gegevens die kunnen leiden tot stigmatisering of uitsluiting van de Betrokkene (gokverslaving, prestatie op school, werkproblemen, relatieproblemen), gebruikersnamen, wachtwoorden en andere inloggegevens en gegevens die kunnen worden gebruikt voor identiteitsfraude (biometrische gegevens, kopieën van identiteitsbewijzen en BSN-nummers).
1.8	Inbreuk in verband met Persoonsgegevens (Datalek):	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, zoals bedoeld in artikel 4 sub 12 Avg.
1.9	Overeenkomst(en):	De tussen Partijen geldende Overeenkomst of Overeenkomsten waaruit voortvloeit dat Verwerker voor Verwerkingsverantwoordelijke ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt.

1.10	Persoonsgegevens:	Alle informatie over een 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, zoals bedoeld in artikel 4 sub 1 Avg.
1.11	Sub-verwerker:	Een andere verwerker die door Verwerker wordt ingezet om ten behoeve van de Verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten.
1.12	Toepasselijke wet- en regelgeving:	Toepasselijke wet- en regelgeving en/of (nadere) verdragen, verordeningen, richtlijnen, besluiten, beleidsregels, instructies en/of aanbevelingen van een bevoegde overheidsinstantie betreffende de Verwerking van Persoonsgegevens, tevens omvattende toekomstige wijziging hiervan en/of aanvulling hierop, inclusief andere lidstaatrechtelijke uitvoeringswetten van de Avg.
1.13	Verwerker:	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke persoonsgegevens verwerkt, zoals bedoeld in artikel 4 sub 8 Avg.
1.14	Verwerkersovereenkomst:	Deze overeenkomst inclusief de daaraan gehechte Bijlagen, zoals bedoeld in artikel 28 lid 3 Avg.
1.15	Verwerking:	Een bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens, zoals bedoeld in artikel 4 sub 2 Avg.
1.16	Verwerkingsverantwoordelijke:	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt, zoals bedoeld in artikel 4 sub 7 Avg.

Artikel 2. Onderwerp van de Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst is van toepassing op alle Verwerkingen van Persoonsgegevens die Verwerker doet in het kader van de Overeenkomst.

2.2 Verwerker verwerkt Persoonsgegevens namens en in opdracht van Verwerkingsverantwoordelijke overeenkomstig de schriftelijke instructies van Verwerkingsverantwoordelijke die met Verwerker zijn overeengekomen, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht. In dat geval stelt Verwerker Verwerkingsverantwoordelijke, voorafgaand aan de Verwerking, schriftelijk in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

2.3 Verwerker verwerkt Persoonsgegevens uitsluitend ten behoeve van en binnen het kader van de Overeenkomst, in overeenstemming met de door Verwerkingsverantwoordelijke bepaalde doeleinden en met inachtneming van de door Verwerkingsverantwoordelijke vastgestelde bewaartermijnen.

2.4 Een overzicht van onder meer de categorieën Persoonsgegevens en de doeleinden waarvoor de Persoonsgegevens worden verwerkt, is uiteengezet in Bijlage 1.

2.5 Verwerkingsverantwoordelijke heeft de zeggenschap over de Verwerking van Persoonsgegevens en heeft het doel van en de middelen voor de Verwerking van Persoonsgegevens vastgesteld.

2.6 Verwerker heeft geen zeggenschap over het doel van en de middelen voor de Verwerking van Persoonsgegevens en neemt derhalve geen beslissingen over bijvoorbeeld het gebruik van Persoonsgegevens, de verstrekking aan derden en de duur van de opslag van Persoonsgegevens. De zeggenschap over Persoonsgegevens komt nimmer bij Verwerker te rusten.

2.7 Partijen verplichten zich over en weer conform de Avg en Toepasselijke wet- en regelgeving te handelen.

Artikel 3. Gebruik Persoonsgegevens

3.1 Verwerker zal de van Verwerkingsverantwoordelijke verkregen Persoonsgegevens niet voor andere doeleinden of op andere wijze te gebruiken dan voor het doel/de doeleinden waarvoor de gegevens aan Verwerker zijn verstrekt of aan hem bekend zijn geworden. Verwerker zal geen andere gegevensverwerkingen uitvoeren dan door Verwerkingsverantwoordelijke (schriftelijk dan wel elektronisch) aan Verwerker zijn opgedragen. Het voorgaande geldt zowel gedurende de looptijd van deze Verwerkersovereenkomst als na afloop daarvan.

3.2 Verwerker verschaft uitsluitend toegang tot de Persoonsgegevens aan zijn medewerkers voor zover dit noodzakelijk is voor de uitvoering van zijn verplichtingen voortvloeiend uit de Overeenkomst.

3.3 Verwerker zal Persoonsgegevens binnen de EU/EER (doen) verwerken. Verwerking van Persoonsgegevens buiten de EU/EER is slechts mogelijk na voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke (Bijlage 1).

3.4 Verwerker zal geen Persoonsgegevens aan een derde verstrekken, tenzij de verstrekking plaatsvindt op grond van deze Verwerkersovereenkomst, op grond van een uitdrukkelijke schriftelijke opdracht van Verwerkingsverantwoordelijke of noodzakelijk is om te voldoen aan een op Verwerker rustende wettelijke verplichting, zoals Unierechtelijke of lidstaatrechtelijke

bepalingen op grond waarvan Verwerker tot verstrekken verplicht is. Verwerker zal, indien sprake is van een wettelijke verplichting, voorafgaand aan de verstrekking de grondslag van het verzoek en de identiteit van de verzoeker verifiëren. Verwerker stelt voor zover mogelijk voorafgaand aan de verstrekking Verwerkingsverantwoordelijke daarvan in kennis, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

3.5 Verwerkingsverantwoordelijke staat er tegenover Verwerker voor in dat hij zijn systemen en infrastructuur te allen tijde adequaat beveiligt en dat de inhoud, het gebruik en/of de Verwerking van Persoonsgegevens niet onrechtmatig zijn en geen inbreuk maken op enig recht van een derde. Daarnaast dient de Verwerkingsverantwoordelijke vast te stellen dat sprake is van een rechtmatige grondslag voor de Verwerking van Persoonsgegevens.

Artikel 4 Beveiliging

4.1 Verwerker treft passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen. De tussen Partijen overeengekomen en door Verwerker te treffen technische en organisatorische maatregelen zijn vastgelegd in Bijlage 2. Bij het treffen van technische en organisatorische maatregelen heeft Verwerker rekening gehouden met de stand van de techniek, de uitvoeringskosten van de maatregelen, 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 Betrokkenen.

4.2 De maatregelen zoals genoemd in artikel 4.1 omvatten, waar passend, onder meer:

a. de pseudonimisering en versleuteling van Persoonsgegevens;
b. het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen 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;
e. het hanteren van een passend informatiebeveiligingsbeleid voor de Verwerking van Persoonsgegevens;
f. certificering ISO 9001:2015, ISO 27001:2013, NEN 7510:2011.

Een overzicht op hoofdlijnen van de door Verwerker op het moment van aangaan van deze Verwerkersovereenkomst toegepaste maatregelen is weergegeven in Bijlage 2.

4.3 Bij de beoordeling van het passend beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

4.4 De door Verwerker omschreven beveiligingsmaatregelen bieden naar de mening van Verwerkingsverantwoordelijke, rekening houdend met de in artikel 4.1 genoemde factoren, een op het risico van de Verwerking van de door hem gebruikte of verstrekte Persoonsgegevens afgestemd beveiligingsniveau.

4.5 Verwerker zal de door hem getroffen beveiligingsmaatregelen periodiek evalueren en verscherpen, aanvullen of verbeteren voor zover de eisen of (technologische) ontwikkelingen daartoe aanleiding geven. Op verzoek van Verwerkingsverantwoordelijke rapporteert Verwerker eenmaal per jaar over de door hem getroffen beveiligingsmaatregelen.

4.6 Verwerker staat er niet voor in dat de door hem getroffen beveiligingsmaatregelen onder alle omstandigheden doeltreffend zijn.

4.7 Indien Verwerkingsverantwoordelijke nadere c.q. zwaardere beveiligingsmaatregelen wenst, dan zal Verwerker zo mogelijk aan deze wens tegemoetkomen. De hiermee verband houdende extra kosten komen voor rekening van Verwerkingsverantwoordelijke.

Artikel 5 Inbreuk in verband met Persoonsgegevens

5.1 Verwerker informeert Verwerkingsverantwoordelijke zonder onredelijke vertraging en uiterlijk binnen 48 uur, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens.

5.2 De melding van de Verwerker aan de Verwerkingsverantwoordelijke omvat in ieder geval informatie met betrekking tot:

a. de aard en - bij benadering - omvang van de inbreuk;
b. de contactpersoon waar meer informatie over de inbreuk kan worden verkregen;
c. de waarschijnlijke gevolgen van de inbreuk;
d. de door Verwerker voorgestelde of genomen maatregelen om de eventuele negatieve gevolgen van de inbreuk te beperken
e. andere noodzakelijke informatie die nodig is om Verwerkingsverantwoordelijke in staat te stellen om tijdig en volledig te voldoen aan voor Verwerkingsverantwoordelijke geldende meldingsverplichtingen ingevolge artikel 33 en 34 Avg (Bijlage 1).

5.3 Indien het voor Verwerker niet mogelijk is om alle informatie gelijktijdig te verstrekken, zal Verwerker de informatie zonder onredelijke vertraging in stappen verstrekken.

5.4 Verwerkingsverantwoordelijke dient te beoordelen of de Inbreuk in verband met Persoonsgegevens waarover Verwerker hem heeft geïnformeerd, gemeld moet worden aan de AP of de Betrokkene. Het melden van een Inbreuk in verband met Persoonsgegevens die op grond van artikel 33 en 34 Avg moet worden gemeld aan de AP en/of de Betrokkene blijft te allen tijde de verantwoordelijkheid van de Verwerkingsverantwoordelijke. Verwerker is niet verplicht tot het melden van een Inbreuk in verband met Persoonsgegevens aan de AP en/of Betrokkene.

Artikel 6 Vertrouwelijkheid

6.1 Verwerker waarborgt dat de medewerkers die onder zijn verantwoordelijkheid Persoonsgegevens verwerken zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen.

6.2 De in artikel 6.1 opgenomen geheimhoudingsplicht geldt niet indien:

a. Verwerkingsverantwoordelijke schriftelijk toestemming aan Verwerker heeft gegeven om de Persoonsgegevens aan een derde, Verwerker daaronder begrepen, te verstrekken;
b. het verstrekken van Persoonsgegevens aan een derde noodzakelijk is in het kader van de uitvoering van de Overeenkomst of Verwerkersovereenkomst;
c. een dwingendrechtelijk wettelijk voorschrift of rechterlijke uitspraak Verwerker tot bekendmaking en/of verstrekking van die Persoonsgegevens verplicht, zoals Unierechtelijke of lidstaatrechtelijke bepalingen op grond waarvan Verwerker tot het verstrekken verplicht is.

6.3 Alle door Verwerker aan Verwerkingsverantwoordelijke verstrekte toegangs- en/of identificatiecodes, certificaten, informatie omtrent toegangs- en/of wachtwoordenbeleid, de inhoud van de Bijlagen en alle door Verwerker aan Verwerkingsverantwoordelijke verstrekte informatie die invulling geeft aan de in Bijlage 2 opgenomen technische en organisatorische beveiligingsmaatregelen zijn vertrouwelijk en zullen door Verwerkingsverantwoordelijke als zodanig worden behandeld en slechts aan geautoriseerde medewerkers van Verwerkingsverantwoordelijke kenbaar worden gemaakt. Verwerkingsverantwoordelijke ziet erop toe dat zijn medewerkers de verplichtingen uit dit artikel naleven.

Artikel 7 Sub-verwerkers

7.1 In Bijlage 1 is opgenomen of Verwerker voor de Verwerking van Persoonsgegevens in het kader van de uitvoering van de Overeenkomst gebruik maakt van diensten van een of meerdere Sub-verwerkers. Met deze Sub-verwerker(s) zal Verwerker een sub-verwerkersovereenkomst afsluiten, welke zoveel als mogelijk een afspiegeling is van de in deze Verwerkersovereenkomst vastgelegde afspraken. Door ondertekening van deze Verwerkersovereenkomst geeft Verwerkingsverantwoordelijke aan Verwerker toestemming voor het inschakelen van Sub-verwerker(s).

7.2 Verwerker zal Verwerkingsverantwoordelijke informeren over wijzigingen in de door Verwerker ingeschakelde Sub-verwerker(s). Verwerkingsverantwoordelijke zal zijn toestemming hiervoor niet op onredelijke gronden onthouden. Indien Verwerkingsverantwoordelijke bezwaar heeft tegen deze wijzigingen, zullen Partijen in overleg treden teneinde een voor beide Partijen aanvaardbare oplossing te vinden.

7.3 Verwerker zal ervoor zorgen dat de door hem inschakelde Sub-verwerker(s) zich aan hetzelfde beveiligingsniveau in het kader van de bescherming van Persoonsgegevens houden waaraan Verwerker is gebonden op basis van deze Verwerkersovereenkomst.

Artikel 8 Looptijd en beëindiging

8.1 Deze Verwerkersovereenkomst treedt in werking op het moment van ondertekening daarvan door beide Partijen en wordt gesloten voor onbepaalde tijd.

8.2 Deze Verwerkersovereenkomst eindigt van rechtswege bij de beëindiging van de Overeenkomst en in geval van feitelijke en permanente beëindiging van de Verwerking van Persoonsgegevens.

8.3 Bij beëindiging van de Verwerkersovereenkomst zal Verwerker alle onder zich zijnde en van Verwerkingsverantwoordelijke ontvangen Persoonsgegevens binnen de in Bijlage 1 opgenomen termijn verwijderen op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn, of indien overeengekomen, in een algemeen gangbaar, gestructureerd gegevensformaat langs elektronische weg worden teruggeven aan Verwerkingsverantwoordelijke.

8.4 Verwerker kan eventuele redelijke kosten die hij maakt in het kader van lid 3 van dit artikel bij Verwerkingsverantwoordelijke in rekening brengen.

8.5 Het bepaalde in lid 3 van dit artikel is niet van toepassing indien een wettelijke regeling het geheel of gedeeltelijk teruggeven, vernietigen of verwijderen van Persoonsgegevens door Verwerker belet. In een dergelijk geval zal Verwerker de Persoonsgegevens enkel blijven verwerken voor zover noodzakelijk uit hoofde van zijn wettelijke verplichtingen. Het bepaalde in lid 3 van dit artikel geldt eveneens niet indien Verwerker ten aanzien van de Persoonsgegevens 'Verwerkingsverantwoordelijke' in de zin van de Avg zou zijn.

8.6 Verplichtingen welke naar hun aard bestemd zijn om ook na beëindiging van deze Verwerkersovereenkomst voort te duren, blijven na beëindiging van deze Verwerkersovereenkomst gelden. Tot deze verplichtingen behoren onder meer welke voortvloeien uit de bepalingen betreffende vertrouwelijkheid (artikel 6), aansprakelijkheid en vrijwaring (artikel 11) en toepasselijk recht en bevoegde rechter (artikel 12).

Artikel 9 Rechten Betrokkene(n)

9.1 Verwerker zal, voor zover mogelijk, zijn medewerking verlenen aan redelijke verzoeken van Verwerkingsverantwoordelijke die voortvloeien uit de op Verwerkingsverantwoordelijke rustende verplichting om verzoeken van Betrokkene(n) om uitoefening van hun rechten te beantwoorden.

9.2 Indien Verwerker rechtstreeks van een Betrokkene een verzoek ontvangt om uitoefening van zijn rechten, zoals inzage, wijzing of verwijdering van zijn Persoonsgegevens, zal Verwerker het verzoek van Betrokkene onverwijld doorsturen naar Verwerkingsverantwoordelijke. De Verwerkingsverantwoordelijk handelt deze verzoeken vervolgens zelf af.

Artikel 10 Auditrechten en DPIA

10.1 Verwerker kan de nakoming van de in deze Verwerkersovereenkomst vastgelegde afspraken aantonen door middel van een certificaat vergelijkbaar met het ISO27001 certificaat, beveiligingsrapport of een auditrapport (Third Party Memorandum) van een onafhankelijke deskundige.

10.2 Verwerker zal verder op verzoek van Verwerkingsverantwoordelijke alle informatie aan Verwerkingsverantwoordelijke ter beschikking stellen die nodig is om de nakoming van de in deze Verwerkersovereenkomst vastgelegde afspraken aan te tonen.

10.3 Verwerkingsverantwoordelijke kan maximaal éénmaal per jaar een audit door een onafhankelijke, gecertificeerde externe deskundig – hierna ook te noemen: deskundige – die aantoonbaar ervaring heeft met de onderhavige Verwerkingen van Persoonsgegevens laten uitvoeren indien Verwerker geen certificaat of rapport, zoals bedoeld in artikel 10.1 kan overleggen. De met de audit verband houdende kosten komen voor rekening van Verwerkingsverantwoordelijke.

10.4 Indien Verwerkingsverantwoordelijke reden heeft aan te nemen dat de Verwerking van Persoonsgegevens niet overeenkomstig de Verwerkersovereenkomst plaatsvindt, zal Verwerker Verwerkingsverantwoordelijke in de gelegenheid stellen om een tussentijdse audit uit te voeren. Deze audit wordt voor zover mogelijk conform artikel 10.3 uitgevoerd. De met deze audit verband houdende kosten komen voor rekening van Verwerkingsverantwoordelijke tenzij de audit daadwerkelijke toerekenbare tekortkomingen aan de zijde van Verwerker in de nakoming van deze Verwerkersovereenkomst aantoont.

10.5 De inhoud en omvang van de audit is beperkt tot het controleren van het nakomen van de afspraken inzake de Verwerking van Persoonsgegevens, zoals vastgelegd in deze Verwerkersovereenkomst. Verwerkingsverantwoordelijke zal de audit minimaal veertien dagen voor aanvang daarvan schriftelijk aankondigen aan Verwerker. Een audit mag de bedrijfsactiviteiten van Verwerker niet onnodig verstoren. Verwerker heeft het recht een audit of instructie van de deskundige te weigeren indien deze in strijd is met de wet- of regelgeving of een ontoelaatbare inbreuk vormt op de door Verwerker getroffen beveiligingsmaatregelen.

10.6 Voorafgaand aan de audit zal de deskundige een door Verwerker voorgelegde geheimhoudingsverklaring ondertekenen.

10.7 De deskundige zal een kopie van zijn rapport aan Verwerker verstrekken. Partijen zullen vervolgens in overleg treden over de uitkomsten van het rapport. Indien uit het rapport verbetermaatregelen blijken, zal Verwerker deze voorstellen doorvoeren voor zover deze naar zijn oordeel passend zijn, rekening houdend met de stand van de techniek, de uitvoeringskosten van de maatregelen, de verwerkingsrisico's verbonden aan zijn product of dienst, de markt waarin hij opereert en het beoogd gebruik van zijn producten en diensten.

10.8 Indien Verwerkingsverantwoordelijke van mening is dat een gegevensbeschermingseffectbeoordeling (DPIA) dient plaats te vinden, zal Verwerker na verzoek daartoe van Verwerkingsverantwoordelijke en rekening houdend met de aard van de Verwerking en de hem ter beschikking staande informatie, Verwerkingsverantwoordelijke bijstand verlenen. Verwerkingsverantwoordelijke draagt hiervoor de redelijke kosten aan de zijde van Verwerker.

Artikel 11 Overige bepalingen

11.1 Waar in deze Verwerkersovereenkomst wordt gesproken over Verwerkersovereenkomst, zijn daaronder de aan deze Verwerkersovereenkomst gehechte Bijlagen mede begrepen.

11.2 Het bepaalde in de considerans van deze Verwerkersovereenkomst maakt integraal onderdeel uit van deze Verwerkersovereenkomst.

11.3 Indien één der Partijen tekort schiet in de nakoming van (één van) zijn verplichting(en) uit de Verwerkersovereenkomst, zal de andere Partij hem deswege in gebreke stellen, tenzij nakoming van de betreffende verplichting(en) reeds blijvend onmogelijk is, in welk geval de nalatige Partij onmiddellijk in gebreke is. De ingebrekestelling dient een zo gedetailleerd en volledig mogelijke omschrijving van de tekortkoming te bevatten, zal schriftelijk geschieden en aangetekend worden verzonden waarbij aan de nalatige Partij een redelijke termijn zal worden gegund om alsnog zijn verplichtingen na te komen.

11.4 Deze Verwerkersovereenkomst vormt een integraal onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst, waaronder begrepen beperkingen van aansprakelijkheid voor schade, zijn derhalve ook van toepassing op deze Verwerkersovereenkomst.

11.5 Bij strijdigheid tussen bepalingen in de Verwerkersovereenkomst en bepalingen in de Overeenkomst, prevaleren uitsluitend die bepalingen in de Verwerkersovereenkomst die zien op de Verwerking van Persoonsgegevens. Voor wat betreft de bepalingen inzake aansprakelijkheid voor schade prevaleren de bepalingen uit de Overeenkomst.

11.6 Enkel indien en voor zover in de Overeenkomst *geen* bepaling is opgenomen inzake de beperking van aansprakelijkheid voor schade zal de volgende beperking van aansprakelijkheid gelden: De totale aansprakelijkheid van Verwerker wegens een toerekenbare tekortkoming in de nakoming van de Verwerkersovereenkomst of uit enige andere hoofde, waaronder nadrukkelijk begrepen eventuele garantie- en/of vrijwaringsverplichtingen, is beperkt tot vergoeding van directe schade tot maximaal het netto factuurbedrag corresponderende met de door Verwerker aan Verwerkingsverantwoordelijke gezonden c.q. te zenden factuur met betrekking tot de verrichte werkzaamheden waarmee de betreffende aansprakelijkheid verband houdt c.q. waaruit de betreffende aansprakelijkheid voortvloeit. Indien de Overeenkomst hoofdzakelijk een duurovereenkomst is met een looptijd van meer dan één jaar, wordt de voor de Overeenkomst bedongen prijs gesteld op het totaal van de vergoedingen bedongen voor één jaar. In geen geval zal de totale aansprakelijkheid van Verwerker voor directe schade uit welke hoofde dan ook meer bedragen dan € 500.000,= (vijfhonderdduizend Euro).

11.7 De aansprakelijkheid van Verwerker voor indirecte schade, gevolgschade, gederfde winst, gemiste besparingen, geleden verlies, verminderde goodwill, schade door bedrijfsstagnatie en schade verband houdende met de inschakeling van door Verwerkingsverantwoordelijke aan Verwerker voorgeschreven toeleveranciers en/of derde-leveranciers is uitgesloten. Eveneens is uitgesloten de aansprakelijkheid van Verwerker wegens verminking, vernietiging of verlies van gegevens of documenten en eventueel daarmee verband houdende schade.

11.8 De in de leden 6 en 7 van dit artikel bepaalde beperkingen gelden niet indien de schade het gevolg is van opzet of bewuste roekeloosheid van Verwerker.

11.9 Partijen kunnen jegens elkaar geen beroep doen op een aansprakelijkheidsbeperking, die is opgenomen in de Overeenkomst en/of in deze Verwerkersovereenkomst, ten aanzien van een door de andere Partij toerekenbaar tekortkoming op grond van artikel 82 lid 5 AVG. Iedere Partij is verplicht de andere Partij onverwijld schriftelijk in kennis te stellen van een (dreigende) aansprakelijkstelling. Iedere Partij is in redelijkheid verplicht de andere Partij informatie te verschaffen en/of ondersteuning te verlenen ten behoeve van het voeren van verweer tegen een (mogelijke) aansprakelijkstelling. De Partij die informatie verstrekt en/of ondersteuning verleent, is gerechtigd om eventuele redelijke kosten dienaangaande in rekening te brengen bij de andere Partij. Een (mogelijke) aansprakelijkheidstelling kan in geen geval worden verhaald, zolang hiertegen gewone rechtsmiddelen openstaan. Verwerkingsverantwoordelijke is in redelijkheid gehouden deze rechtsmiddelen aan te wenden.

11.10 Verwerker behoudt zich het recht voor instructies van Verwerkingsverantwoordelijke die kennelijk strijdig zijn met Toepasselijke wet- en regelgeving of de openbare orde onder opgaaf van redenen te weigeren.

11.11 Indien Verwerkingsverantwoordelijke in instructies aan Verwerker of in de door Verwerkingsverantwoordelijke zelf te treffen beveiligingsmaatregelen te kort schiet en blijft schieten nadat Verwerker Verwerkingsverantwoordelijke schriftelijk op de tekortkoming(en) heeft gewezen, is Verwerker gerechtigd de Verwerking te beperken of op te schorten, onverminderd de aansprakelijkheid voor schade van Verwerkingsverantwoordelijke jegens Verwerker.

11.12 Een aan Verwerkingsverantwoordelijke opgelegde bestuurlijke boete kan niet worden verhaald op Verwerker, tenzij er sprake is van opzet of bewuste roekeloosheid aan de zijde van Verwerker. Een bestuurlijke boete kan in geen geval worden verhaald, zolang hiertegen gewone rechtsmiddelen openstaan. Verwerkingsverantwoordelijke is in redelijkheid gehouden deze rechtsmiddelen aan te wenden.

11.13 Aanvullingen en andere wijzigingen van deze Verwerkersovereenkomst dienen schriftelijk door Partijen te worden overeengekomen en te worden ondertekend door de daartoe bevoegde vertegenwoordigers. Op de gewijzigde verwerkersovereenkomst zullen de bepalingen van deze Verwerkersovereenkomst van overeenkomstige toepassing zijn.

11.14 Kennisgevingen die Partijen op grond van deze Verwerkersovereenkomst aan elkaar zullen doen, vinden schriftelijk plaats. Mondelinge mededelingen, toezeggingen of afspraken hebben geen rechtskracht tenzij deze schriftelijk zijn bevestigd.

11.15 Indien één of meerdere bedingen van deze Verwerkersovereenkomst nietig of onverbindend is/zijn of blijft/blijven, blijven de overige bepalingen van deze Verwerkersovereenkomst van kracht. Partijen verbinden zich om de nietige of niet-verbindende bepalingen te vervangen door bepalingen die wel verbindend zijn en die zo min mogelijk - gelet op het doel en de strekking van de Verwerkersovereenkomst - afwijken van nietige of niet-verbindende bepalingen.

Artikel 12. Toepasselijk recht en bevoegde rechter

12.1 Op deze Verwerkersovereenkomst en de uitvoering daarvan is uitsluitend Nederlands recht van toepassing.

12.2 Alle geschillen, waaronder geschillen betreffende de uitleg van deze Verwerkersovereenkomst, zullen bij uitsluiting worden beslecht door de rechter of instantie die bevoegd is kennis te nemen van geschillen betreffende de Overeenkomst. Indien in de Overeenkomst geen bevoegde rechter of instantie is opgenomen, is de rechter te Rotterdam bevoegd, tenzij Verwerker verkiest de rechter te adiëren welke de wet aanwijst.

Aldus overeengekomen, opgemaakt in tweevoud, ondertekend almede per pagina geparafeerd.

VCD Healthcare B.V. h.o.d.n. Axians

B. Wijnholds
Business Unit Director
Datum: 1 november 2021

Klantnaam:
Handtekening

Voorletter(s) en achternaam:
Functie: Klinisch psycholoog
Datum: 25.10.2022

Bijlagen:

- Bijlage 1: Verwerkingen, Persoonsgegevens, contactgegevens, datalekprotocol etc.
- Bijlage 2: Beveiligingsbeleid

Bijlage 1 Verwerkingen, Persoonsgegevens, contactgegevens, datalekprotocol, etc.

1. Omschrijving van de Verwerkingen van Persoonsgegevens

Verwerker verricht voor Verwerkingsverantwoordelijke de Verwerkingen van Persoonsgegevens zoals contractueel overeengekomen in de 'Overeenkomsten' inclusief addenda.

De feitelijke verwerking van gegevens binnen de online applicaties Zorg GGZ en Online-DBC geschiedt door Verwerkingsverantwoordelijke zelf. Het hoofddoel van de verwerking door Verwerker ten behoeve van Verwerkingsverantwoordelijke is het beheer inclusief ondersteunende dienstverlening en support van de door Verwerkingsverantwoordelijke bij Axians afgenomen Zorg GGZ en Online-DBC software. De software heeft tot doel het zorginhoudelijke en zorgadministratieve proces vanuit de geestelijke gezondheidszorg te ondersteunen waarbij de software op basis van Software-as-a-Service (SaaS) online beschikbaar wordt gesteld aan Verwerkingsverantwoordelijke en waartoe Verwerker in opdracht van Verwerkingsverantwoordelijke diverse aanpalende werkzaamheden op het gebied van Services volvoert zoals facturatie- en inningservices.

2. Aard van de Persoonsgegevens die partijen verwachten te verwerken (categorieën)

Verwerkingsverantwoordelijke heeft aangegeven dat Verwerker de volgende Persoonsgegevens ten behoeve van Verwerkingsverantwoordelijke zal verwerken:

Voor zowel de gewone Persoonsgegevens, de Bijzondere Persoonsgegevens als de Gevoelige Persoonsgegevens geldt conform het vorige artikel dat de feitelijke verwerking van gegevens binnen de applicaties Zorg GGZ en Online-DBC geschiedt door Verwerkingsverantwoordelijke zelf.

De volgende (gewone) Persoonsgegevens worden door Verwerker ten behoeve van Verwerkingsverantwoordelijke verwerkt:

☒ Naam	☐ KvK nummer	☐ Beeld- en geluidsopnamen
☒ Adres (zakelijk)	☒ Adres (privé)	☒ Geslacht
☒ Woonplaats (zakelijk)	☒ Woonplaats (privé)	☒ Geboortedatum
☒ Telefoonnummer (zakelijk)	☒ Telefoonnummer (privé)	☐ Beroep
☒ E-mailadres (zakelijk)	☒ E-mailadres (privé)	☐ Bankrekeningnummer
☐ Anders, nl. _____	☐ Anders, nl. _____	☐ Anders, nl. _____

EN

De volgende Bijzondere persoonsgegevens worden door Verwerker ten behoeve van Verwerkingsverantwoordelijke verwerkt:

☒ Gezondheid	☐ Partner status / seksuele geaardheid	☐ Biometrische gegevens
☐ Godsdienst of levensovertuiging	☐ Politieke voorkeur	☐ Genetische gegevens
☐ Lidmaatschap vakbond	☐ Anders, nl. _____	☐ Anders, nl. _____

EN

De volgende Gevoelige persoonsgegevens worden door Verwerker ten behoeve van Verwerkingsverantwoordelijke verwerkt:

☒ BSN-nummer	☐ Salarisgegevens	☐ Financiële data (o.a. creditcardnummer)
☐ Kopie van een ID-bewijs	☐ Loonbeslag / schulden	☒ Nationaliteit
☐ Afgeleide financiële data (inkomenscategorie, huizenbezit, autobezit, waarde van vermogensbestanddelen, ondernemingen, aandelen, etc.)	☐ Gegevens met betrekking tot transacties, donaties, aankoopgeschiedenis, betalingen	☐ Lifestylekenmerken (o.a. gezinssamenstelling, woonsituatie, interesses, demografische kenmerken)
☒ Zorgverzekeraar gerelateerde gegevens	☐ Anders, nl. _____	☐ Anders, nl. _____

3. Verwerking Persoonsgegevens binnen de EU/EER

De door Verwerker te verwerken Persoonsgegevens zullen worden verwerkt in:

- Nederland

4. Sub-verwerkers

Toegestane Sub-verwerkers zijn, zonder dat daarvoor toestemming van Verwerkingsverantwoordelijke zoals bedoeld in artikel 7 noodzakelijk is, de ondernemingen waarvan VINCI Energies Netherlands BV (mede) bestuurder is en/of de ondernemingen waarin VINCI Energies Netherlands BV een belang van 50% of meer heeft.

Verwerker maakt voor de overeengekomen verwerking(en) gebruik van de volgende Sub-verwerker(s):

a. **Microsoft Azure**
Microsoft Azure verricht de volgende Verwerkingen voor Verwerker:
Het beschikbaar stellen inclusief een in gezamenlijkheid uitgevoerd dagelijks operationeel beheer van de technische infrastructuur.
Microsoft is in Nederland gevestigd te Schiphol, 1118 CZ, huisnummer 354.
Enterprise agreement met Axians te Groningen, 9727 DW, huisnummer 15.

b. **VANAD Enovation**
VANAD Enovation verricht de volgende Verwerkingen voor Verwerker:
Zorgen voor de ontsluiting van ZorgMail communicatie.

c. **VECOZO**
VECOZO verricht de volgende Verwerkingen voor Verwerker:
Het via Vecozo verzorgen van veilige communicatie in de zorg tussen ketenpartijen ten behoeve van o.a. controle op verzekeringsrecht en het digitaal kunnen factureren/declareren.

d. **NZa**
NZa verricht de volgende Verwerkingen voor Verwerker:
Verwerkt de verplichte aanlevering zoals die door Verwerker voor Verwerkingsverantwoordelijke in het kader van de Aanlevering Zorgvraagtypering plaatsvindt ten behoeve van het beheren van gepseudonimiseerde informatie over (S-GGZ en B-GGZ) zorgtrajecten.

e. **ROM-software, aan Zorg GGZ/Online-DBC gekoppeld**
De aan Zorg GGZ en Online-DBC gekoppelde ROM-software leveranciers verrichten de volgende Verwerkingen voor Verwerker:
Deze koppeling met ROM-leveranciers maakt het mogelijk om rechtstreeks toegang te krijgen vanuit Zorg GGZ en Online-DBC tot diverse ROM-pakketten waardoor de voor de ROM benodigde cliëntgegevens automatisch vanuit Zorg GGZ en Online-DBC in de ROM-applicatie van de leverancier van Verwerkingsverantwoordelijke terechtkomen.

f. **FarMedvisie**
FarMedvisie verricht de volgende Verwerkingen voor Verwerker:
FarMedvisie levert haar applicatie door middel van het door Verwerkingsverantwoordelijke in Zorg GGZ en Online-DBC kunnen aanroepen van FarmedZ om elektronisch medicatie te kunnen voorschrijven (EVS) aan patiënten die door Verwerkingsverantwoordelijke zijn geregistreerd in Zorg GGZ en Online-DBC.

g. **Bancaire relatie**
De bancaire relatie verricht de volgende Verwerkingen voor Verwerker:
Indien er een volmacht is afgegeven waarin de voorwaarden zijn neergelegd voor het door Verwerker kunnen inzien van rekeninginformatie betreffende de in de volmacht opgenomen rekening van Verwerkingsverantwoordelijke zal Verwerker informatie kunnen inzien van betalingen op de bankrekening ten behoeve van het kunnen uitvoeren van debiteurenbeheer.

h. **InfinitCare**
InfinitCare verricht de volgende Verwerkingen voor Verwerker:
Het zorgen voor de gegevensaanlevering van kwaliteitsinformatie aan Alliantie Kwaliteit in de geestelijke gezondheidszorg (AKWA) conform de specificaties van AKWA voor instellingen.
Het zorgen van de gegevensaanlevering van kwaliteitsaanlevering aan Stichting KiBG ten behoeve van het voldoen aan het keurmerk Basis GGZ.

5. Einde Overeenkomst / bewaartermijnen

Na beëindiging van de Overeenkomst zullen de data inclusief Persoonsgegevens die Verwerker voor Verwerkingsverantwoordelijke verwerkt en zoals aanwezig op de bij VCD Healthcare B.V. h.o.d.n.
Axians in beheer zijnde productieve Zorg GGZ en Online-DBC en facturatie-omgeving indien gewenst minimaal vijf (5) jaar door u als Verwerkingsverantwoordelijke benaderbaar zijn. Deze inzagemogelijkheid vindt

plaats vanuit de productieve Zorg GGZ en Online-DBC softwareomgeving waarin tot het moment van beëindiging door Verwerkingsverantwoordelijke is gewerkt met dien verstande dat er vanaf beëindiging enkele restricties van toepassing zijn waaronder het niet meer kunnen opvoeren van nieuwe patiënten/cliënten en het niet meer kunnen muteren van gegevens. Deze mogelijkheid wordt u kosteloos als extra service door Axians aangeboden teneinde u de mogelijkheid te bieden om bij vraagstukken vanuit bijvoorbeeld zorgverzekeraars en accountants gemakkelijk vanuit de bekende en vertrouwde vormgeving de gegevens te kunnen inzien. Anderzijds biedt Axians deze inzage om u als Verwerkingsverantwoordelijke in deze periode de mogelijkheid te bieden de door u geregistreerde gegevens veilig te stellen teneinde de op u van toepassing zijnde wet- en regelgeving op het gebied van bewaartermijnen te kunnen nakomen.

De bovenstaand beschreven inzagemogelijkheid bieden wij u standaard aan. Indien u dit niet wenst is het ook mogelijk om aan Axians het verzoek te doen om de productieve gegevens te ontvangen conform artikel 8.3 en 8.4. Daarbij is het mogelijk om het verzoek te doen om de door u in de productieve Zorg GGZ en Online-DBC omgeving geregistreerde data inclusief Persoonsgegevens binnen een termijn van drie (3) maanden door Axians als Verwerker te laten verwijderen op zodanige wijze dat de data inclusief Persoonsgegevens niet langer door u kunnen worden gebruikt en niet langer toegankelijk zijn.

6. Categorieën medewerkers

Ten behoeve van de Verwerking zijn de volgende categorieën medewerkers van Verwerker geautoriseerd;

- Support- en Service specialisten;
- Technische en Functionele Consultants;
- Developmentmedewerkers.

7. Contactgegevens

In geval van vragen, incidenten of datalekken wordt contact opgenomen met:

Primair aanspreekpunt Verwerkingsverantwoordelijke	
Functie	Klinisch psycholoog
Naam	B.H. Plagge
E-mailadres	bplagge@hotmail.com
Telefoon	0653741379
Mobiel	

Primair aanspreekpunt Verwerker	
Functie	Privacyfunctionaris
Naam	Aaltje Zijlstra – de Jong
E-mailadres	Binnendienst.hc.nl@axians.com
Telefoon	088-5975500
Mobiel	06-14990347

Zie volgende pagina voor de secundaire aanspreekpunten

Bij afwezigheid:

Secundair aanspreekpunt Verwerkingsverantwoordelijke	
Functie	idem als primair
Naam	
E-mailadres	
Telefoon	
Mobiel	

Secundair aanspreekpunt Verwerker	
Functie	Business Unit Director
Naam	De heer Bert Wijnholds
E-mailadres	bert.wijnholds@axians.com
Telefoon	088-5975500
Mobiel	

8. Datalekprotocol

Verwerker zal bij het doen van een datalekmelding aan Verwerkingsverantwoordelijke de volgende specifieke afspraken in acht nemen

- Dit zal via reguliere media als telefoon en/of mail verlopen en zal afhankelijk van de specifieke situatie worden opgepakt met de contactpersonen conform de afspraken zoals gemaakt in deze Verwerkersovereenkomst.

Standaard is opgenomen:
- Datum melding en de datum van moment waarop Verwerker op de hoogte is geraakt van het (potentiele) beveiligingsincident;
- Samenvatting van het (potentiele) beveiligingsincident;
- De beveiligingsmaatregel waarop zich een beveiligingsincident heeft voorgedaan;
- De aard van het beveiligingsincident, (betreft het lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van persoonsgegevens?);
- De oorzaak van het beveiligingsincident;
- Schade beperkende maatregelen welke zijn getroffen na constatering beveiligingsincident.

Indien bekend, wordt tevens aangegeven:
- Omschrijving van de Persoonsgegevens welke zijn betrokken bij het beveiligingsincident;
- Aantal personen getroffen door het beveiligingsincident;
- Type Persoonsgegevens (NAW, toegangs- of identificatiegegevens, financiële gegevens, bijzondere gegevens);
- Vervolgacties ter voorkoming en reparatie van het beveiligingsincident.

Bijlage 2 Beveiligingsbeleid

Het informatiebeveiligingsbeleid van Verwerker is gestructureerd op basis van de volgende norm:
- ISO/IEC 27001;
- NEN 7510, NEN 7512, NEN 7513 (voor de zorg sector).

Het kwaliteitsmanagementsysteem van Verwerker is gestructureerd op basis van de volgende norm:
- ISO/IEC 9001.

Verwerker heeft de volgende certificaten:
- ISO/IEC 9001;
- ISO/IEC 27001;
- NEN 7510.

Verwerker heeft waar van toepassing minimaal de volgende technische en organisatorische beveiligingsmaatregelen getroffen ter beveiliging van zijn product of dienst waarbij rekening is gehouden 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:

Algemeen

nr.	Maatregel Verwerker
1.1	De Verwerker heeft een eigen vastgesteld en gepubliceerd informatiebeveiligingsbeleid

Organisatie van informatiebeveiliging

2.1	Medewerkers die te maken hebben met Persoonsgegevens van de Verwerkingsverantwoordelijke hebben een geheimhoudingsverklaring ondertekend. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding.
2.2	Maatregelen uit de Verwerkersovereenkomst zijn geïmplementeerd.
2.3	Periodieke beveiligingsaudits worden uitgevoerd volgens afspraken met de verwerkingsverantwoordelijke.

Personele beveiliging

3.1	De Verwerker heeft maatregelen genomen zo dat niet-geautoriseerden geen toegang hebben tot of kennis kunnen nemen van Persoonsgegevens.
3.2	Het personeel van de Verwerker of derden moeten kennis hebben van de verantwoordelijkheden ten aanzien van de Verwerking van de Persoonsgegevens voor de Verwerkingsverantwoordelijke.
3.3	Als externe toegang nodig is tot de Persoonsgegevens van de Verwerkingsverantwoordelijke door eigen personeel, of personeel van de Verwerker, dienen geschikte authenticatie methodes te worden gebruikt.

Fysieke beveiliging

4.1 Papieren documenten en mobiele gegevensdragers die Persoonsgegevens of andere vertrouwelijke gegevens van de Verwerkingsverantwoordelijke bevatten worden beveiligd opgeslagen.

4.2 Toegang tot beveiligde zones of gebouwen waar Persoonsgegevens van de Verwerkingsverantwoordelijke zich bevinden is alleen mogelijk na autorisatie daartoe.

Beheer van communicatie en bedienprocessen

5.1 De ICT-voorzieningen voldoen aan het voor de dienst overeengekomen niveau van beschikbaarheid.

5.2 Bij transport van vertrouwelijke informatie over niet vertrouwde netwerken tussen de Verwerker en de Verwerkingsverantwoordelijke, zoals over het internet, dient altijd geschikte encryptie te worden toegepast. De cryptografische beveiligingsvoorzieningen en componenten voldoen aan algemeen gangbare beveiligingscriteria (zoals FIPS 140-2).

5.3 Beveiligingskenmerken, niveaus van dienstverlening en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten door een Verwerker.

5.4 Het verwijderen c.q. vernietigen van vertrouwelijke data en de vernietiging van verwijderbare media gebeurt conform geldende wet- en regelgeving.

5.5 Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, evenals procedures over melding van incidenten van de Verwerker naar de Verwerkingsverantwoordelijke.

Beheer, onderhoud en ontwikkeling

6.1 In projecten ten behoeve van systemen voor de Verwerkingsverantwoordelijke wordt een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen.

6.2 Er worden eisen en geschikte beheersmaatregelen vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.

6.3 Van aanpassingen (zoals updates) aan softwarematige componenten van de technische infrastructuur wordt vastgesteld dat deze de juiste werking van de technische componenten niet in gevaar brengen en de beveiliging te niet doen.

6.4 Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident.

6.5 Er is een proces ingericht voor het beheer van technische kwetsbaarheden. Dit omvat minimaal het melden van incidenten aan de Verwerkingsverantwoordelijke, het uitvoeren van

periodieke penetratietests, het uitvoeren van risicoanalyses van kwetsbaarheden en patching van systemen en hardware.

6.6 Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is, worden zo spoedig mogelijk doorgevoerd. Minder kritische beveiliging-updates/patches moeten worden ingepland bij de eerstvolgende onderhoudsronde.

Beheer van incidenten

7.1 Vermissing of diefstal van apparatuur of media die gegevens van de Verwerkingsverantwoordelijke kunnen bevatten, wordt altijd ook aangemerkt als informatiebeveiligingsincident.

7.2 De informatie verkregen uit het beoordelen van beveiligingsmeldingen wordt geëvalueerd met als doel beheersmaatregelen te verbeteren (PDCA-Cyclus).

Naleving

8.1 De bescherming van gegevens en privacy behoort te worden bewerkstelligd in overeenstemming met relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.

8.2 Informatiesystemen van de Verwerker ten behoeve van de Verwerkingsverantwoordelijke worden regelmatig gecontroleerd op naleving van beveiligingsnormen. Dit kan door bijvoorbeeld kwetsbaarheidsanalyses en penetratietesten.

8.3 De registraties van de Verwerkingsverantwoordelijke behoren te worden beschermd tegen verlies, vernietiging en vervalsing, in overeenstemming met wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.

Toegangsbeveiliging

9.1 Toegangsrechten van medewerkers van de Verwerker worden direct geblokkeerd als geen toegang voor de bewerking van de persoonsgegevens noodzakelijk is.

9.2 Aan de gebruikers is een set gedragsregels aangereikt met daarin minimaal het volgende:

- Wachtwoorden worden niet opgeschreven en niet gedeeld met anderen;
- Een wachtwoord dient minimaal te voldoen aan standaard complexiteitsregels;
- Inloggegevens tot omgeving van Verwerkingsverantwoordelijke worden opgeslagen in een daartoe bestemde applicatie.