Verwerkersovereenkomst



DE ONDERGETEKENDEN:

1. [Naam Verwerkingsverantwoordelijke], gevestigd aan de [adres] te [plaats] en ingeschreven in het register van de Kamer van Koophandel onder nummer [KvK-nummer], in deze rechtsgeldig vertegenwoordigd door [titel, naam en functie] (hierna: "**Verwerkingsverantwoordelijke**"); en

2. [Naam Verwerker], gevestigd aan de [adres] te [plaats] en ingeschreven in het register van de Kamer van Koophandel onder nummer [KvK-nummer], in deze rechtsgeldig vertegenwoordigd door [titel, naam en functie] (hierna: "**Verwerker**");

Hierna gezamenlijk ook aan te duiden als: "Partijen" en afzonderlijk als "Partij".

OVERWEGENDE DAT:

(a) Verwerkingsverantwoordelijke maakt gebruik van [vul in: systeem, applicatie etc.] van Verwerker. Verwerkingsverantwoordelijke en Verwerker hebben hiertoe een Overeenkomst gesloten: <naam hoofdovereenkomst> afgesloten op <datum afsluiten hoofdovereenkomst> , hierna Hoofdovereenkomst. Deze Verwerkersovereenkomst is als bijlage onlosmakelijk verbonden met genoemde Overeenkomst. Voor zover het bepaalde in de Verwerkersovereenkomst strijdig is met het bepaalde in de Overeenkomst, prevaleert het bepaalde in de Verwerkersovereenkomst. Verwerker verricht diensten ten behoeve van Verwerkingsverantwoordelijke, zoals beschreven in de Hoofdovereenkomst.

(b) De diensten meebrengen dat Persoonsgegevens worden verwerkt.

(c) Verwerker de betreffende gegevens louter overeenkomstig schriftelijke instructies van Verwerkingsverantwoordelijke verwerkt en niet voor eigen doeleinden.

(d) Op de verwerking van Persoonsgegevens door Verwerker zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) van toepassing.

(e) Partijen in deze Verwerkersovereenkomst de afspraken met betrekking tot de verwerking van Persoonsgegevens in het kader van de diensten wensen vast te leggen.

(f) Deze Verwerkersovereenkomst, indien van toepassing, alle eerdere Verwerkersovereenkomst(en) van gelijke strekking tussen Partijen vervangt.

VERKLAREN TE ZIJN OVEREENGEKOMEN ALS VOLGT:

Artikel 1. Definities

1.1. Termen met een hoofdletter die in deze Verwerkersovereenkomst worden gebruikt en die hierin niet worden gedefinieerd, hebben de betekenis die is uiteengezet in de AVG (waaronder Persoonsgegevens, Betrokkene, Verwerkingsverantwoordelijke en Verwerker).

In deze Verwerkersovereenkomst wordt onder de volgende met een hoofdletter aangeduide begrippen het volgende verstaan:

***Betrokkene*:**
Degene op wie een (bijzonder) persoonsgegeven betrekking heeft.

***Verwerkersovereenkomst**:*
Deze Verwerkersovereenkomst;
Inbreuk in verband met (bijzondere) Persoonsgegevens:
Een inbreuk op de beveiliging, in de zin van artikel 32 AVG, 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 persoonsgegevens.
(Bijzondere) persoonsgegevens:
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon die Verwerker in het kader van de Overeenkomst ten behoeve van Verwerkingsverantwoordelijke verwerkt.
Verwerken:
Elke handeling of geheel van handelingen met betrekking tot (bijzondere) persoonsgegevens, al dan niet met elektronische middelen, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, evenals het afschermen, uitwissen of vernietigen van (bijzondere) persoonsgegevens.
Inbreuk:
Een Inbreuk in verband met Persoonsgegevens als bedoeld in artikel 4 onder 12 AVG en/of een onderzoek naar of beslaglegging door overheidsfunctionarissen op de Persoonsgegevens of een vermoeden dat dit gaat plaatsvinden.
Medewerker:
Een bij de uitvoering van deze Verwerkersovereenkomst betrokken natuurlijke persoon die werkzaam is bij of voor een van de Partijen.
Hoofdovereenkomst:
De Hoofdovereenkomst(en) betreffende de levering van producten en/of diensten. Waarvan deze Verwerkersovereenkomst als Bijlage onlosmakelijk onderdeel van uitmaakt.
Verzoek van Betrokken:
Een klacht over de verwerking dan wel een verzoek tot uitoefening van de rechten van Betrokkene zoals omschreven in Hoofdstuk III van de AVG.
Algoritme:
Een set regels en instructies die een computer uitvoert, met als doel: problemen oplossen, vragen beantwoorden, taken of processen uitvoeren en/of besluiten nemen. Dit kunnen simpele rekenregels zijn. Of zelflerende algoritmes en AI-systemen.
Ai-systeem:
Een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te werken en dat na het inzetten ervan aanpassingsvermogen kan vertonen, en dat, voor expliciete of impliciete doelstellingen, uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die van invloed kunnen zijn op fysieke of virtuele omgevingen.

1.2. Waar in deze Verwerkersovereenkomst naar bepaalde normen wordt verwezen (zoals NEN 7510) wordt daarmee steeds gedoeld op de meest actuele versie daarvan. Voor zover de betreffende norm niet meer wordt onderhouden, dient in de plaats daarvan de meest actuele versie van de logische opvolger van de betreffende norm gelezen te worden.

Artikel 2. Onderwerp van deze Verwerkersovereenkomst en beschrijving Bijlagen

2.1. Deze Verwerkersovereenkomst betreft de verwerking van Persoonsgegevens door Verwerker in opdracht van de Verwerkingsverantwoordelijke in het kader van de uitvoering van de Hoofdovereenkomst.

2.2. Onderdeel van deze Verwerkersovereenkomst zijn de volgende Bijlagen:

a) Bijlage 1: Omschrijving van de verwerking
b) Bijlage 2: Beveiliging Persoonsgegevens
c) Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens

d) Bijlage 4:

Artikel 3. Uitvoering verwerking

3.1. Verwerker garandeert dat hij ten behoeve van Verwerkingsverantwoordelijke uitsluitend Persoonsgegevens zal verwerken voor zover:

a) dit noodzakelijk is voor de uitvoering van de Hoofdovereenkomst (binnen de gespecificeerde omschrijving in Bijlage 1); of
b) Verwerkingsverantwoordelijke daartoe uitdrukkelijk schriftelijke instructies heeft gegeven.

3.2. Verwerker zal alle redelijke instructies van Verwerkingsverantwoordelijke in verband met de verwerking van de Persoonsgegevens opvolgen. Verwerker stelt Verwerkingsverantwoordelijke onmiddellijk op de hoogte indien naar zijn oordeel instructies in strijd zijn met de toepasselijke wetgeving met betrekking tot de verwerking van Persoonsgegevens.

3.3. Onverminderd het bepaalde in het eerste lid van dit artikel 3, is het Verwerker toegestaan om Persoonsgegevens te verwerken indien een wettelijk voorschrift (waaronder begrepen daarop gebaseerde rechterlijke of bestuurlijke bevelen) hem tot een verwerking verplicht. In dat geval stelt de Verwerker voorafgaand aan de verwerking Verwerkingsverantwoordelijke schriftelijk in kennis van de beoogde verwerking en het wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt. Verwerker zal Verwerkingsverantwoordelijke, waar mogelijk, in staat stellen zich te verweren tegen deze verplichte verwerking en ook overigens de verplichte verwerking beperken tot het strikt noodzakelijke.

3.4. Verwerker zal de Persoonsgegevens aantoonbaar op behoorlijke en zorgvuldige wijze verwerken en in overeenstemming met de op hem als Verwerker rustende verplichtingen op grond van de AVG en overige wet- en regelgeving.

3.5. Het is Verwerker niet toegestaan om persoonsgegevens buiten de Europese Economische Ruimte (EER) te verwerken, tenzij verwerkingsverantwoordelijke hiervoor uitdrukkelijk voorafgaande schriftelijke toestemming heeft gegeven.

3.6. Verwerker waarborgt dat Medewerkers een geheimhoudingsovereenkomst hebben getekend dan wel garandeert dat Medewerkers en ingeschakelde subverwerkers geheimhouding zullen betrachten ten aanzien van de verwerking van de Persoonsgegevens.

Artikel 4. Beveiliging Persoonsgegevens en controle

4.1. Verwerker zal aantoonbaar passende en doeltreffende technische en organisatorische beveiligingsmaatregelen nemen die, gezien de huidige stand der techniek en de daarmee gemoeide kosten, afgestemd zijn op de (in Bijlage 1 gespecificeerde) aard van de te verwerken Persoonsgegevens, ter bescherming van de Persoonsgegevens tegen verlies, onbevoegde kennisname, verminking of enige vorm van onrechtmatige verwerking, alsmede om de (tijdige) beschikbaarheid en integriteit van de gegevens te garanderen. In deze beveiligingsmaatregelen zijn de mogelijk in de Hoofdovereenkomst reeds beschreven maatregelen ook inbegrepen.

4.2. In Bijlage 2 geeft gebruiker aan welke standaarden en aanvullend getroffen technische en/of organisatorische maatregelen relevant zijn om de bescherming van Persoonsgegevens van de Betrokkenen te waarborgen ten aanzien van de onderhavige samenwerking.

Artikel 5. Monitoring, informatieplichten en incidentenmanagement

5.1. Verwerker zal actief monitoren op Inbreuken op de beveiliging en over de resultaten van de monitoring in overeenstemming met dit artikel rapporteren aan verwerkingsverantwoordelijke.

5.2. Wanneer zich een Inbreuk voordoet of heeft voorgedaan, is Verwerker verplicht de afspraken betreffende Inbreuken in verband met Persoonsgegevens, zoals vastgelegd in bijlage 3 na te leven.

Artikel 6. Medewerkingsverplichtingen

6.1. De AVG en overige wetgeving kent aan de Betrokkene bepaalde rechten toe. Verwerker zal zijn volledige en tijdige medewerking verlenen aan Verwerkingsverantwoordelijke bij de nakoming van de op Verwerkingsverantwoordelijke rustende verplichtingen voortvloeiend uit deze rechten.

6.2. Een door Verwerker ontvangen Verzoek van een Betrokkene met betrekking tot verwerking van Persoonsgegevens wordt door Verwerker zo snel als mogelijk, doch binnen 24 uur, doorgestuurd naar Verwerkingsverantwoordelijke.

6.3. Op het eerste daartoe strekkende verzoek van Verwerkingsverantwoordelijke zal Verwerker aan Verwerkingsverantwoordelijke alle relevante informatie verstrekken betreffende de aspecten van de door hem verrichte verwerking van Persoonsgegevens zodat Verwerkingsverantwoordelijke, mede aan de hand van die informatie, aan kan tonen dat zij de toepasselijke (privacy) wetgeving naleeft.

6.4. Verwerker zal voorts op verzoek van Verwerkingsverantwoordelijke alle noodzakelijke bijstand verlenen bij de nakoming van de op grond van de toepasselijke privacywetgeving op Verwerkingsverantwoordelijke rustende wettelijke verplichtingen, zoals het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA).

6.5. Verwerker verleent alle benodigde medewerking aan audits uitgevoerd door een gecertificeerde auditor over de nakoming van de afspraken binnen deze Verwerkersovereenkomst en Bijlagen, tenzij Verwerker door middel van een geldige certificering, die periodiek door een geaccrediteerde instelling wordt getoetst, heeft aangetoond dat Verwerker de gemaakte afspraken nakomt. De kosten van deze audit worden gedragen door Verwerkingsverantwoordelijke (zowel eigen kosten als kosten van Verwerker),

tenzij de auditor één of meer tekortkomingen van niet ondergeschikte aard van Verwerker constateert die ten nadele zijn van Verwerkingsverantwoordelijke

Artikel 7. Inschakeling subverwerkers

7.1. Verwerker zal zijn activiteiten die bestaan uit het verwerken van Persoonsgegevens of vereisen dat Persoonsgegevens verwerkt worden, niet uitbesteden aan een subverwerker zonder drie maanden van te voren dat mede te delen aan Verwerkingsverantwoordelijke en de Verwerkingsverantwoordelijke de gelegenheid te geven om eventuele bezwaren aan de Verwerker kenbaar te maken. Indien Verwerkingsverantwoordelijke bezwaren heeft, zal Verwerker redelijke inspanningen leveren om de bezwaren van de Verwerkingsverantwoordelijke op te lossen of om de levering van de diensten zoals genoemd in de Hoofdovereenkomst - zonder daaraan afbreuk te doen - aan te passen om verwerking van Persoonsgegevens door de voorgestelde (nieuwe) subverwerker te voorkomen.

7.2. Indien de Verwerker de bezwaren van de Verwerkingsverantwoordelijke niet kan oplossen of de levering van de diensten niet kan aanpassen om de verwerking van Persoonsgegevens door de voorgestelde subverwerker te voorkomen, kan de Verwerkingsverantwoordelijke de Hoofdovereenkomst opschorten of geheel of gedeeltelijk beëindigen, met inachtneming van een opzegtermijn van zes maanden, gerekend vanaf de einddatum van de bezwaartermijn. Gedurende een schorsing van de Hoofdovereenkomst vanwege bezwaar tegen een (nieuwe) subverwerker en vanaf de einddatum van de Hoofdovereenkomst is de Verwerkingsverantwoordelijke niet verplicht om de Verwerker enige vergoeding op grond van de Hoofdovereenkomst of anderszins of enige schadevergoeding te betalen.

7.3. Artikel 7.1 is niet van toepassing op de in Bijlage 1 vermelde subverwerkers.

7.4. Verwerker zal aan deze subverwerker minstens dezelfde verplichtingen opleggen als voor hemzelf uit deze Verwerkersovereenkomst en de wet voortvloeien. Verwerker zal deze afspraken schriftelijk vastleggen en zal toezien op de naleving daarvan door de subverwerker. Verwerker zal Verwerkingsverantwoordelijke op verzoek afschrift verstrekken van de met de subverwerker gesloten verwerkersovereenkomst.

7.5. Verwerker blijft volledig aansprakelijk jegens Verwerkingsverantwoordelijke voor de gevolgen van het uitbesteden van werkzaamheden aan een subverwerker. Voor de inzet van subverwerkers buiten de EER is schriftelijke toestemming vereist in overeenstemming met artikel 3.5 van deze Verwerkersovereenkomst.

Artikel 8. Kosten

8.1. De kosten voor de verwerking van gegevens die inherent zijn aan de normale uitvoering van de Verwerkersovereenkomst en de uitoefening van rechten van Betrokkenen, worden geacht besloten te liggen in de op grond van de Hoofdovereenkomst reeds verschuldigde vergoedingen.

Artikel 9. Duur en beëindiging

9.1. Deze Verwerkersovereenkomst gaat in op de datum van ondertekening en de duur van deze Verwerkersovereenkomst is gelijk aan de duur van de Hoofdovereenkomst inclusief eventuele verlengingen daarvan.

9.2. De Verwerkersovereenkomst maakt na ondertekening ervan door beide Partijen integraal en onverbrekelijk deel uit van de Hoofdovereenkomst. Beëindiging van de Hoofdovereenkomst,

op welke grond dan ook, heeft tot gevolg dat de Verwerkersovereenkomst eveneens op dezelfde grond beëindigd wordt, tenzij Partijen in voorkomend geval anders overeenkomen.

9.3. 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 bijvoorbeeld die welke voortvloeien uit de bepalingen betreffende geheimhouding, aansprakelijkheid, geschillenbeslechting en toepasselijk recht.

9.4. Ieder der Partijen is gerechtigd, onverminderd hetgeen daartoe bepaald is in de Hoofdovereenkomst, de uitvoering van deze Verwerkersovereenkomst en de daarmee samenhangende Hoofdovereenkomst op te schorten, dan wel deze Verwerkersovereenkomst [en de daarmee samenhangende Hoofdovereenkomst] zonder rechterlijke tussenkomst met onmiddellijke ingang te beëindigen indien:

a) de andere Partij wordt ontbonden of anderszins ophoudt te bestaan;
b) de andere Partij aantoonbaar ernstig tekortschiet in de nakoming van de verplichtingen die voortvloeien uit deze Verwerkersovereenkomst en die toerekenbare tekortkoming niet binnen 30 dagen is hersteld na een daartoe strekkende schriftelijke ingebrekestelling;
c) een Partij in staat van faillissement wordt verklaard of surseance van betaling aanvraagt.

9.5. Gelet op de grote afhankelijkheid van Verwerkingsverantwoordelijke van Verwerker alsmede het continuïteitsrisico bij incidenten en calamiteiten (zoals faillissement), verklaart Verwerker zich reeds nu voor alsdan bereid op eerste verzoek van Verwerkingsverantwoordelijke aanvullende afspraken met Verwerkingsverantwoordelijke te maken teneinde voornoemde risico's te verkleinen.

9.6. Verwerkingsverantwoordelijke is gerechtigd deze Verwerkersovereenkomst en de Hoofdovereenkomst per direct te ontbinden indien Verwerker te kennen geeft niet (langer) te kunnen voldoen aan de betrouwbaarheidseisen die op grond van de wet en/of de rechtspraak aan de verwerking van de Persoonsgegevens worden gesteld.

9.7. Verwerker dient Verwerkingsverantwoordelijke zo spoedig mogelijk te informeren over een voorgenomen overname of eigendomsoverdracht. Verwerkingsverantwoordelijke heeft het recht bij zwaarwegende bezwaren tegen de verandering van eigenaar de Hoofdovereenkomst te beëindigen zonder schadeplichtig te zijn.

9.8. Het is Verwerker niet toegestaan om zonder uitdrukkelijke en schriftelijke toestemming van Verwerkingsverantwoordelijke deze Verwerkersovereenkomst en de rechten en plichten die samenhangen met deze Verwerkersovereenkomst over te dragen aan een derde partij.

9.9. De verplichtingen uit deze Verwerkersovereenkomst duren voort zolang de Verwerker Persoonsgegevens van Verwerkingsverantwoordelijke verwerkt, ook nadat de Verwerker is opgehouden de in de Hoofdovereenkomst opgedragen zorg, diensten en/of faciliteiten ten behoeve van Verwerkingsverantwoordelijke te verlenen.

Artikel 10. Bewaartermijnen, teruggave en vernietiging van Persoonsgegevens

10.1. Verwerker bewaart de Persoonsgegevens niet langer dan strikt noodzakelijk, waaronder begrepen de wettelijke bewaartermijnen of een eventueel tussen Partijen gemaakte afspraak over bewaartermijnen zoals vastgelegd in Bijlage 1. In geen geval bewaart Verwerker de Persoonsgegevens langer dan tot het einde van deze Verwerkersovereenkomst. Verwerkingsverantwoordelijke bepaalt of en zo ja hoe lang gegevens bewaard moeten blijven.

10.2. Bij beëindiging van de Verwerkersovereenkomst, of indien van toepassing aan het einde van de overeengekomen bewaartermijnen, of op schriftelijk verzoek van Verwerkingsverantwoordelijke zal Verwerker, tegen redelijke kosten, naar keuze van Verwerkingsverantwoordelijke, de Persoonsgegevens definitief (doen) vernietigen of teruggeven aan Verwerkingsverantwoordelijke. Op verzoek van Verwerkingsverantwoordelijke verstrekt Verwerker bewijs van het feit dat de gegevens onherroepelijk zijn vernietigd of verwijderd. Eventuele teruggave van de gegevens zal in een algemeen gangbaar, gestructureerd en gedocumenteerd gegevensformaat langs elektronische weg plaatsvinden. Indien teruggave, definitieve vernietiging of verwijdering niet mogelijk is, stelt Verwerker Verwerkingsverantwoordelijke daarvan onmiddellijk op de hoogte. In dat geval garandeert Verwerker dat hij de Persoonsgegevens vertrouwelijk zal behandelen en niet langer zal verwerken.

Artikel 11. Gebruik Algoritmes en AI

11.1. Het is verwerker niet toegestaan persoonsgegevens, die in het kader van de uitvoering van de Hoofdovereenkomst worden verwerkt, te verwerken middels een algoritme dat onder de definitie van artikel 1 valt zonder toestemming van Verwerkingsverantwoordelijke.

11.2. Het is verwerker verboden om persoonsgegevens, die in het kader van de uitvoering van de Hoofdovereenkomst worden verwerkt, op enige manier te verwerken in een AI-systeem, of (her) te gebruiken voor de training van een AI-model, zonder toestemming van Verwerkingsverantwoordelijke.

11.3. Indien Verwerker wil afwijken van het verbod van 11.2 vraagt hij hiervoor schriftelijke toestemming aan Verwerkersverantwoordelijke. Daarnaast is verwerker zelf verantwoordelijk om het AI-systeem vooraf te toetsen aan de geldende wet- en regelgeving en om hieraan te voldoen, in het bijzonder de Europese AI-act. Nalevingskosten zijn voor rekening van de verwerker.

11.4. Verwerker overlegt documenten t.a.v. de (technische) uitlegbaarheid aan verwerkersverantwoordelijke van AI of Algoritme en schriftelijk een onderbouwde risicoclassificatie van het AI systeem voor aan Verwerkingsverantwoordelijke.. Deze documenten maken integraal onderdeel uit van deze overeenkomst en worden tijdig vervangen door verwerker indien nieuwe ontwikkelingen optreden.

Artikel 12. Slotbepalingen

12.1. In geval van nietigheid c.q. vernietigbaarheid van een of meer bepalingen uit deze Verwerkersovereenkomst, blijven de overige bepalingen onverkort van kracht.

12.2. Op deze Verwerkersovereenkomst is Nederlands recht van toepassing.

12.3. Geschillen over of in verband met deze Verwerkersovereenkomst worden uitsluitend voorgelegd aan de daartoe in de Hoofdovereenkomst aangewezen rechtbank.

<Naam Verwerkingsverantwoordelijke>	<Naam Verwerker>
< Naam vertegenwoordiger Verwerkingsverantwoordelijke >	< Naam vertegenwoordiger Verwerker >
<Functie>	<Functie>

Plaats: _____

Datum:_____

Plaats: _____

Datum: _____

Bijlage 1: Omschrijving van de verwerking

Omschrijving van activiteiten en/of diensten, omvang en algemeen doel van de verwerking (benoem het aantal Persoonsgegevens/Betrokkenen):

Noem Hoofdovereenkomst: titel / kenmerk / ingangsdatum / partijen: Geef een omschrijving van activiteiten en/of diensten: Wat is het algemeen doel van de verwerking: Over hoeveel Persoonsgegevens/Betrokkenen gaat het:

Verwerking	Soort Persoonsgegevens	Categorieën van Betrokkenen	Doeleinden van de verwerking	Grondslag van de verwerking	Doorgifte buiten de EER	Afspraken bewaartermijnen	Afspraken verwijderprocedure
Noem de verwerking (bijvoorbeeld hosting, transfer, onderhoud, of naam van de applicatie).	Benoem de Persoonsgegevens (b.v. NAW, BSN, gegevens over gezondheid, etc.)	Benoem Betrokkenen (patiënten, Medewerkers, studenten, etc.)	Benoem het doel van de verwerking.	Benoem de grondslag waarop de verwerking plaatsvindt.	Indien ja, benoem opslag/ verwerking buiten de EER en vermeld land, instrument waaronder doorgifte kan plaatsvinden (hoofdstuk V AVG) en aanvullende maatregelen.	Benoem afspraken bewaartermijnen.	Benoem de verwijderprocedure.

Subverwerkers

Subverwerker	Beschrijving dienst en Persoonsgegevens	Gegevens buiten de EER	Verwerkers-overeenkomst
Naam en adres (incl. land)	Omschrijven	Ja/Nee (indien ja, vermeld land, instrument waaronder doorgifte kan plaatsvinden (hoofdstuk 5 AVG) en aanvullende maatregelen)	Ja/Nee

Toelichting:

Persoonsgegevens gaan over iemand (of zijn tot iemand te herleiden). Elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon is een persoonsgegeven. De identificatie kan bijvoorbeeld gebeuren aan de hand van een identificatiemiddel, zoals een naam, een identificatienummer, locatiegegevens, een online identificerende variabele of andere elementen die kenmerkend zijn. Hierbij kunt u denken aan fysieke, fysiologische, genetische, psychische, economische, culturele of sociale elementen.

Elke **verwerking** moet één of meerdere welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde **doeleinden** hebben. Het gaat hierbij om het doel of de doelen waarvoor de Persoonsgegevens zijn verkregen/verzameld. Maak het **verwerkingsdoel/**de **verwerkingsdoelen** zo concreet mogelijk.

Grondslagen voor verwerking Persoonsgegevens: Toestemming Betrokkene / Noodzakelijk voor uitvoering van een overeenkomst / Wettelijke verplichting / Beschermen van vitale belangen van de Betrokkene / Taak van algemeen belang of uitoefening van het openbaar gezag / Gerechtvaardigde belangen van de Verwerkingsverantwoordelijke of van een derde

Bijlage 2: Aantonen passend niveau van beveiliging[1]

In deze Bijlage geeft verwerker aan welke standaarden en aanvullend getroffen technische en/of organisatorische maatregelen relevant zijn om de bescherming van Persoonsgegevens van de Betrokkenen te waarborgen ten aanzien van de hoofdovereenkomst. Verwerker kan hierbij ook verwijzen naar documenten waarin standaarden en maatregelen zijn neergelegd.

Verwerker dient ten minste een beschrijving te geven van:
1. de maatregelen die zijn genomen om ervoor te zorgen dat uitsluitend bevoegd personeel toegang heeft tot de Persoonsgegevens;
2. de maatregelen die zijn genomen ter bescherming van Persoonsgegevens tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk(e) verlies of wijziging, onbevoegde of onrechtmatige opslag, Verwerking, toegang of bekendmaking;
3. de maatregelen die zijn genomen om kwetsbaarheden op het gebied van de Verwerking van Persoonsgegevens vast te stellen in de systemen die worden gebruikt voor het verlenen van diensten aan Gegevensverstrekker.

Normenstelsel

□ De verwerker werkt volgens een algemeen erkende norm voor informatiebeveiliging, te weten: ……. (Vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS) en is volgens deze norm wel/niet gecertificeerd.

□ De verwerker werkt volgens een algemeen erkende overheidsnorm zoals de BIO, of vergelijkbaar, te weten: ……..,

□ De verwerker werkt volgens een andere norm, te weten:
……

Toereikendheid

De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

□ Verwerker verstrekt een actueel en geldig certificaat en verklaring van toepasselijkheid (VVT);
□ Rapportages van periodieke externe controles zoals audits, pentesten of TPM's (bijv. ISAE3xxx SOC type II);
□ Een assurance rapport (TPM) van een auditor die is aangesloten bij NOREA;
□ Eigen controles of eigen mededelingen over de beveiligingsmaatregelen zoals hieronder beschreven (in lijn met de aanpak uit hoofdstuk 4.4 uit de BIO, een ICV):
……

Uit de certificering/periodieke externe controles/audits of uit de eigen controles/beschrijvingen blijkt of kan afgeleid worden dat de beveiliging passend is bij de verwerking(en) genoemd in Bijlage 1.

Aansluiting bij goedgekeurde gedragscode

□ Verwerker is aangesloten bij een door een toezichthoudende autoriteit goedgekeurde gedragscode, te weten …….

[1] De in deze bijlage genoemde standaarden en maatregelen zijn door Partijen afgestemd met de daarvoor verantwoordelijke Chief Information Security Officer (CISO).

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens

1. Verwerker zal Verwerkingsverantwoordelijke direct informeren over ieder beveiligingsincident[2] bij Verwerker en door haar ingeschakelde sub-Verwerker(s) of derde(n). Naar aanleiding van de informatie zal de Verwerkingsverantwoordelijke vaststellen of hij verplicht is dit beveiligingsincident onverwijld te melden als zijnde een datalek in het kader van artikelen 33 en 34 AVG en, in voorkomend geval, de betrokkene(n) informeren.
2. Verwerker informeert Verwerkingsverantwoordelijke uiterlijk binnen 24 uur nadat een beveiligingsincident is ontdekt door Verwerker of door haar ingeschakelde sub-Verwerker(s) of derde(n). Deze verplichting geldt gedurende 24 uur per dag en 7 dagen in de week.
3. Het informeren van Verwerkingsverantwoordelijke over het beveiligingsincident gebeurt door onderstaande tabel per email te versturen naar de contactpersoon (zie bijlage 1) met als onderwerp 'Beveiligingsincident'.
4. Verwerker informeert daarnaast de Verwerkingsverantwoordelijke uit eigen beweging over alle overige relevante ontwikkelingen over het beveiligingsincident die zich voordoen na het moment van verstrekken van de informatie genoemd in deze bijlage. Verwerker dient binnen redelijke termijn te reageren op aanvullende vragen van Verwerker met betrekking tot het beveiligingsincident.
5. Verwerker dient, zodra het beveiligingsincident is ontdekt, zo spoedig mogelijk voor eigen rekening en risico alle maatregelen te treffen die redelijkerwijs noodzakelijk zijn om de schadelijke gevolgen van het beveiligingsincident te beperken en herhaling te voorkomen.
6. Verwerker zal Verwerkingsverantwoordelijke alle medewerking en informatie verlenen die redelijkerwijs nodig is om de toezichthouder, en/of de betrokkenen adequaat in te lichten over de oorzaak en omvang het beveiligingsincident. Indien de omstandigheden daartoe aanleiding geven, verleent Verwerker aan Verwerkingsverantwoordelijke toegang tot het systeem van Verwerker en/of van door Verwerker ingeschakelde sub-Verwerkers.
7. Het is Verwerker niet toegestaan een (vermeend) datalek zelfstandig te melden bij de Autoriteit Persoonsgegevens (AP)
8. De Verwerker houdt een gedetailleerd logboek bij van alle (vermoedens van) inbreuken op de beveiliging, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen waarin minimaal de informatie zoals bedoeld in deze bijlage is opgenomen, en geeft daar op eerste verzoek van de Verwerkingsverantwoordelijke inzage in.

[2] Overal waar beveiligingsincident staat wordt een incident bedoeld waarbij inbreuk op (bijzondere) persoonsgegevens heeft plaatsgevonden.

Vraag	Antwoord
Geef een samenvatting van de gebeurtenissen omtrent het beveiligingsincident	
Vond het beveiligingsincident plaats bij u of een door u ingeschakelde sub-Verwerker	*[Indien het gaat om een ingeschakelde sub-Verwerker, geef dan ook de naam]*
Datum en tijd of periode waarin het beveiligingsincident is ontdekt en heeft plaatsgevonden.	
De (vermeende) oorzaak van het beveiligingsincident	
De aard van het beveiligingsincident	*[kies uit: lezen, kopiëren, veranderen, verwijderen, vernietigen of diefstal van persoonsgegevens]*
De categorieën persoonsgegevens die (mogelijk) zijn getroffen door het beveiligingsincident	*[bijv. NAW-gegevens, telefoonnummers, emailadressen, BSN, medische gegevens, strafrechtelijke gegevens etc.]*
Waarschijnlijke gevolgen van het beveiligingsincident	
De maatregelen die getroffen zijn of zullen worden om het incident op te lossen dan wel de gevolgen/schade zoveel mogelijk te beperken	
Contactgegevens van de persoon/personen bij wie meer informatie over het beveiligingsincident verkregen kan worden	*[Geef aan: naam, functie/afdeling, telefoonnummer, emailadres]*

Bijlage 4: Contactgegevens

Contactpersoon Verwerkingsverantwoordelijke (NB: Ook buiten kantooruren)	Naam: <contactpersoon> Functie: <functie> Telefoon: <telefoonnummer> Email: <emailadres>
Contactpersoon Verwerker (NB: Ook buiten kantooruren)	Naam: <contactpersoon> Functie: <functie> Telefoon: <telefoonnummer> Email: <emailadres>