

Verwerkersovereenkomst zorgpost

DE PARTIJEN:

naam zorginstelling _____
gevestigd aan de adres, postcode te plaats _____
hierbij rechtsgeldig vertegenwoordigd door
de heer/mevrouw naam en functie _____
hierna ook te noemen: "Verantwoordelijke"
en
DMDR Medical Support B.V., gevestigd aan de Klompenmakerstraat 18-c, 2984 BB te Ridderkerk, en ingeschreven in het register van de Kamer van Koophandel onder nummer 24440010, in deze rechtsgeldig vertegenwoordigd door M. ten Cate, directeur, hierna ook te noemen "Verwerker".

Verantwoordelijke en Verwerker hierna gezamenlijk ook aan te duiden als: "Partijen" en afzonderlijk als "Partij".

KOMEN HIERBIJ HET VOLGENDE OVEREEN

Artikel 1. Onderwerp van de verwerkersovereenkomst

- 1.1 Verwerker zal op schriftelijke instructie van Verantwoordelijke (bijzondere) persoonsgegevens verwerken in het kader van een tussen partijen gesloten Hoofdovereenkomst met als doel het verzendklaar maken en versturen van zorgpost. Een overzicht van de categorieën persoonsgegevens, de doeleinden waarvoor de persoonsgegevens worden verwerkt en de duur van de opslag zijn opgenomen in [Bijlage 1](#) bij deze verwerkersovereenkomst.
- 1.2 Verwerker zal de persoonsgegevens niet voor enig ander doel verwerken dan zoals door Verantwoordelijke is vastgesteld en zal de persoonsgegevens niet verwerken voor eigen doeleinden.
- 1.3 Onverminderd enige andere contractuele geheimhoudingsverplichting die op Verwerker rust, garandeert Verwerker dat hij alle persoonsgegevens als strikt vertrouwelijk zal behandelen en dat hij al zijn werknemers, vertegenwoordigers en/of onderaannemers die betrokken zijn bij de verwerking van de persoonsgegevens van de vertrouwelijke aard van dergelijke persoonsgegevens op de hoogte zal stellen.
- 1.4 Verwerker kan voor het verwerken van deze gegevens gebruik maken van eveneens gecertificeerde subverwerkers: PostNL Holding B.V. gevestigd te Den Haag (ISO/IEC 27001: 2013 gecertificeerd) en Multipost B.V., gevestigd te Dordrecht (ISO/IEC 27001: 2017 gecertificeerd). Deze subverwerkers zijn ook gebonden aan deze verwerkingsbepalingen, waaronder een strikte geheimhoudingsplicht. Verwerker staat in voor de werkzaamheden van de subverwerkers.

Artikel 2. Beginselen voor aantoonbare beveiliging van informatie

- 2.1 Verwerker zal alle redelijke instructies van Verantwoordelijke in verband met de verwerking van persoonsgegevens opvolgen.
- 2.2 Verwerker zal de persoonsgegevens aantoonbaar, transparant en op behoorlijke en zorgvuldige wijze verwerken, in overeenstemming met de op hem als Verwerker rustende wettelijke en contractuele verplichtingen. Verantwoordelijke staat ervoor in dat de gegevens rechtmatig verkregen en juist zijn.
- 2.3 De in opdracht van Verantwoordelijke te verwerken persoonsgegevens blijven onder verantwoordelijkheid van en het eigendom van Verantwoordelijke en/of de betreffende betrokkenen.

Artikel 3. Technische en organisatorische maatregelen en ISO/NEN

- 3.1 Verwerker is ISO/IEC 27001: 2013 en NEN 7510: 2017 gecertificeerd.
- 3.2 Verwerker garandeert dat de beveiliging van de persoonsgegevens onder alle omstandigheden doeltreffend is. Verwerker garandeert voldoende technische en organisatorische maatregelen te nemen tegen verlies of tegen enige vorm van onrechtmatige verwerking (zoals onbevoegde kennisname, aantasting, wijziging of verstrekking van de persoonsgegevens).
- 3.3 In [Bijlage 2](#) zijn de beveiligingsmaatregelen beschreven die de Verwerker in ieder geval zal toepassen.
- 3.4 Verwerker stelt aan Verantwoordelijke op verzoek daartoe alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit artikel 28 jo 32 AVG worden nagekomen.
- 3.5 Verwerker zal de persoonsgegevens betreffende Verantwoordelijke gescheiden opslaan en verwerken van de persoonsgegevens die hij voor zichzelf of namens derde partijen verwerkt.

Artikel 4. Aansprakelijkheid

- 4.1 Indien de Verwerker tekortschiet in de nakoming van een van de verplichtingen uit deze Verwerkersovereenkomst kan Verantwoordelijke hem in gebreke stellen. Verwerker is echter onmiddellijk in gebreke als de nakoming van desbetreffende verplichting anders dan door overmacht binnen de overeengekomen termijn, reeds blijvend onmogelijk is.

- 4.2 Ingebrekestelling vindt schriftelijk plaats, waarbij aan de Verwerker een redelijke termijn wordt gegund om alsnog zijn verplichtingen na te komen. Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is Verwerker in verzuim.
- 4.3 Verwerker vrijwaart Verantwoordelijke voor schade of nadeel, voor zover ontstaan door werkzaamheden van de Verwerker.
- 4.4 Indien Verwerker de in deze Verwerkersovereenkomst neergelegde verplichtingen niet of niet-tijdig nakomt en de toezichthouder de Verantwoordelijke dientengevolge een boete oplegt, is Verwerker aansprakelijk en zal Verantwoordelijke een (contractuele) boete ter hoogte van hetzelfde bedrag opleggen aan Verwerker.
Deze boete is niet vatbaar voor verrekening en opschorting en laat de rechten van Verantwoordelijke op nakoming en schadevergoeding onverlet.
- 4.5 Indien Verantwoordelijke de te verwerken informatie niet veilig aanlevert (bijv. via de beveiligde portal SecuDoc/Zivver via <https://portal.dmdr.nl>, via secure mail (safe relay, S/MIME) of rechtstreeks via SFTP-bestandsoverdracht met PharmaPartners) en de aanlevermethode die verantwoordelijke kiest als onveilig - of niet veilig genoeg – kan worden beschouwd in het licht van de heersende best-practices informatiebeveiliging, hetgeen in strijd is met het veiligheidsbeleid van Verwerker, blijft Verantwoordelijke drie werkdagen alleen verantwoordelijk voor de informatie, zodat Verwerker de aangeleverde informatie alsnog kan veiligstellen in een beveiligde omgeving en de oorspronkelijke aangeleverde gegevens kan verwijderen. Mocht in dit soort situaties blijken dat een informatielek is opgetreden, waarbij niet onomstotelijk kan worden aangetoond dat deze door toedoen van Verwerker is opgetreden, is het de Verwerker vrij om de verantwoordelijkheid voor het lek geheel of gedeeltelijk neer te leggen bij de Verantwoordelijke in gevallen waar geldt dat lekken door tussentijdse onderschepping tijdens transport van Verantwoordelijke naar Verwerker en/of opslag bij Verwerker of Derden niet volledig zijn uit te sluiten.

Artikel 5. Meldplicht datalekken

- 5.1 Partijen zullen elkaar onverwijld informeren indien blijkt dat er een inbreuk op de beveiliging is (geweest) die waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van een individu. Verwerker garandeert dat de verstrekte informatie in de melding zoals genoemd in het volgende lid, volledig, correct en accuraat is.
- 5.2 De meldplicht behelst in ieder geval alle informatie zoals omschreven in [Bijlage 3](#).
- 5.3 Verantwoordelijke beoordeelt of zij de betrokkene(n) en/of de relevante toezichthouder(s) zal informeren of niet.
- 5.4 Verwerker zal op verzoek van Verantwoordelijke meewerken aan het informeren van de bevoegde autoriteiten en Betrokkene(n).

Artikel 6. Afhandeling verzoeken van betrokkenen¹

- 6.1 Betrokkenen hebben het recht op transparantie aangaande de (medische) gegevens die worden verwerkt. Hiertoe wordt aan hen toegang verleend tot de opgeslagen gegevens. Betrokkenen kunnen gegevens onder andere: inzien, corrigeren en laten rectificeren. Nu de Verantwoordelijke de contactpartij van de betrokkenen is, worden deze rechten door Verantwoordelijke kenbaar gemaakt aan betrokkenen.
- 6.2 Verwerker zal volledige medewerking verlenen opdat Verantwoordelijke kan voldoen aan de op haar rustende wettelijke verplichtingen voortvloeiend uit de situatie waarin een Betrokkene de rechten uitoefent zoals bedoeld in lid 1.
- 6.3 Indien een Betrokkene met betrekking tot de uitvoering van zijn rechten contact opneemt met Verwerker, dan gaat Verwerker hier - behoudens uitdrukkelijke andersluidende instructie van Verantwoordelijke - in eerste instantie niet (inhoudelijk) op in, maar bericht hij dit onverwijld aan Verantwoordelijke, met een verzoek om nadere instructies.

Artikel 7. Audit

- 7.1 Verwerker toont aan de hand van de Verklaring van Toepasselijkheid en het doorlopen van het (jaarlijks) verplichte externe audittraject afdoende aan dat hij voldoet aan de wettelijke en overige vereisten.
- 7.2 Verantwoordelijke heeft het recht om bij een aantoonbaar vermoeden van misbruik van persoonsgegevens een audit uit te (laten) voeren door een onafhankelijke derde die aan geheimhouding is gebonden, ter controle van naleving van alle bepalingen uit deze Verwerkersovereenkomst, en al datgene dat daarmee verband houdt.
- 7.3 Verwerker zal aan genoemde audit meewerken en alle voor de audit redelijkerwijs relevante informatie, inclusief ondersteunende gegevens zoals systeemlogs, en betrokken medewerkers zo tijdig mogelijk ter beschikking stellen.

Artikel 8. Duur en beëindiging

- 8.1 Deze Verwerkersovereenkomst wordt ingegaan op de datum van de laatste ondertekening en de duur van deze Verwerkersovereenkomst eindigt in principe een maand na de in artikel 1 van deze Verwerkersovereenkomst genoemde Hoofdovereenkomst.
- 8.2 De Verwerkersovereenkomst en de Hoofdovereenkomst zijn accessoir, dat wil zeggen dat beëindiging van de Verwerkersovereenkomst, op welke grond dan ook (opzegging/ontbinding), tot gevolg heeft dat de Hoofdovereenkomst ook op dezelfde grond beëindigd wordt (en omgekeerd), tenzij partijen schriftelijk anders overeenkomen.

¹ De betrokkene is degene van wie DMDR persoonsgegevens verwerkt. Dit is dus degene op wie de persoonsgegevens betrekking hebben.

- 8.3 Verplichtingen die naar hun aard bestemd zijn om ook na beëindiging van deze Verwerkersovereenkomst voort te duren, blijven na beëindiging van de Verwerkersovereenkomst gelden. Tot deze bepalingen behoren onder andere de bepalingen over geheimhouding, aansprakelijkheid en toepasselijk recht.
- 8.4 Ieder van de partijen is gerechtigd, naast wat daarover bepaald is in de Hoofdovereenkomst, de uitvoering van deze Verwerkersovereenkomst en de daarmee samenhangende Hoofdovereenkomst op te schorten, dan wel zonder rechterlijke tussenkomst met onmiddellijke ingang te ontbinden, indien:
- (a) de andere partij wordt ontbonden of anderszins ophoudt te bestaan;
 - (b) de andere partij aantoonbaar tekortschiet in de nakoming van de verplichtingen die voortvloeien uit deze Verwerkersovereenkomst en die ernstige toerekenbare tekortkoming niet binnen 30 dagen is hersteld na een schriftelijke ingebrekestelling;
 - (c) een partij in staat van faillissement wordt verklaard of surséance van betaling aanvraagt.
- 8.5 Verantwoordelijke 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 ontwikkelingen in de wet en/of de rechtspraak aan de verwerking van de persoonsgegevens worden gesteld. Artikel 9.2 is van overeenkomstige toepassing.

Artikel 9. Bewaartermijnen, teruggave en vernietiging van persoonsgegevens

- 9.1 Verwerker bewaart de persoonsgegevens niet langer dan strikt noodzakelijk en in geen geval langer dan tot het einde van deze Verwerkersovereenkomst of, indien tussen partijen een bewaartermijn is overeengekomen, niet langer dan deze termijn.
- 9.2 Bij beëindiging van de Verwerkersovereenkomst, of indien van toepassing aan het einde van de overeengekomen bewaartermijnen, of op schriftelijk verzoek van Verantwoordelijke zal Verwerker, kosteloos, naar keuze van Verantwoordelijke, de persoonsgegevens vernietigen of teruggeven aan Verantwoordelijke. Op verzoek van Verantwoordelijke verstrekt Verwerker bewijs van het feit dat de gegevens vernietigd of verwijderd zijn. Indien teruggave, vernietiging of verwijdering niet mogelijk is, stelt Verwerker Verantwoordelijke daarvan onmiddellijk op de hoogte. In dat geval garandeert Verwerker dat hij de persoonsgegevens vertrouwelijk zal behandelen en niet langer zal verwerken.
- 9.3 Bij het einde van de Verwerkersovereenkomst zal Verwerker alle derden die betrokken zijn bij het verwerken van persoonsgegevens op de hoogte stellen van de beëindiging van de Verwerkersovereenkomst. De verplichtingen uit artikel 9.2 zijn van overeenkomstige toepassing op deze derden. Verwerker zal waarborgen dat alle betrokken derden hieraan uitvoering zullen geven.

Artikel 10. Voorrang Verwerkersovereenkomst

In geval van strijdigheid tussen de bepalingen uit deze Verwerkersovereenkomst en de bepalingen uit de in artikel 1 genoemde Hoofdovereenkomst, zullen de bepalingen van de Verwerkersovereenkomst voorgaan.

Artikel 11. Toepasselijk recht en bevoegde rechter

- 11.1 Deze Verwerkersovereenkomst en de uitvoering daarvan worden beheerst door Nederlands recht.
- 11.2 Eventuele conflicten zullen eerst met elkaar besproken worden waarbij beide partijen zich inspannen om deze in goed overleg met elkaar op te lossen.
- 11.3 Geschillen die tussen partijen mochten ontstaan in verband met de Verwerkersovereenkomst, zullen worden voorgelegd aan de bevoegde rechter in het arrondissement waar Verwerker is gevestigd.
- 11.4 In alle gevallen waarin deze verwerkersovereenkomst niet voorziet beslissen partijen in onderling overleg.

Voor akkoord (of overeengekomen als gevolg van het aanvinken van "Ik heb de verwerkersovereenkomst gelezen en ga akkoord").

Namens Verantwoordelijke

Plaats:

Datum:

Naam:
Functie:

Namens Verwerker

Plaats: Ridderkerk

Datum:


M. ten Cate
Directeur

BIJLAGE 1: Te verwerken persoonsgegevens en doeleinden

Een, door Verantwoordelijke aangeleverde, extractie van het digitaal adressenbestand (bestaande uit NAW-gegevens, geslacht en geboortedatum) van de voor de zorgpost geselecteerden uit het huisartsinformatiesysteem zal door Verwerker worden verwerkt teneinde, de door Verantwoordelijke aangeleverde, brieftekst te personaliseren, te printen, te vouwen, in een envelop te stoppen en dicht te plakken. Opdrachtnemer zorgt voor het papier, de enveloppen en de aanlevering bij PostNL die hierna zorgdraagt voor bezorging in de af te spreken periode.

BIJLAGE 2: Beveiligingsmaatregelen

DMDR Medical Support B.V. heeft haar beleid ten aanzien van Informatiebeveiliging 'Beleid Informatiebeveiliging DMDR 14-10-2022' in- en extern gecommuniceerd en concreet geïmplementeerd in gedocumenteerde procedures. Ook is DMDR per 20 december 2022 houder van een ISO/IEC 27001 : 2017 en een NEN 7510 : 2020 certificaat. In 2022 heeft DMDR succesvol de transitie van NEN 7510 : 2017 naar NEN 7510 : 2020 uitgevoerd en is de her-certificeringsaudit, uitgevoerd door KIWA, met positief resultaat afgerond. DMDR onderhoudt een informatiebeveiligings-managementsysteem dat voldoet aan de daarin gestelde eisen en beveiligingsmaatregelen voor het volgende toepassingsgebied:

Het verzendklaar maken en versturen van zorgpost, zoals vastgesteld door het management en in overeenstemming met de Verklaring van Toepasselijkheid versie 1.0 d.d. 9 november 2022.

BIJLAGE 3: Informatie die moet worden verstrekt bij een beveiligingsinbreuk en contactgegevens

Het formulier om een beveiligingsinbreuk te melden (waar deze bijlage op is gebaseerd) is te vinden op de website van de Autoriteit Persoonsgegevens: <https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken>
In het geval van "incidenten"/datalekken dient contact te worden opgenomen met de functionaris voor de gegevensbescherming (FG), dhr. M. Baars telefoonnummer 078-6318919 en bij ontstentenis de Security & Privacy Officer (S&PO) S.Hofland, beiden van DMDR Medical Support B.V.

BIJLAGE 4: Derden binnen en buiten EER

Wij schakelen deze derden (Sub-verwerkers) binnen de EER in bij het uitvoeren van de onderliggende opdracht:

Sub-verwerker	Verwerking
PostNL	Bezorgen poststukken (brieven, pakketten e.d.)
Multipost B.V.	Printen en couverteren poststukken

De volgende verwerkingen worden buiten de EER verricht bij het uitvoeren van de onderliggende opdracht door:

Sub-verwerker	Verwerking

Toelichting:

Verwerking mogen alleen buiten de EER worden uitgevoerd als aan een van onderstaande condities is voldaan:

- het land van bestemming waarborgt een passend beschermingsniveau (adequaateitsbesluiten)
- er zijn passende waarborgen genomen
- er is sprake van een wettelijke uitzondering

Voor kleinere partijen bieden de passende waarborgen en wettelijke uitzonderingen doorgaans geen werkbare oplossing.

Met Noorwegen, Liechtenstein en IJsland mag u gegevens uitwisselen op grond van hun EER lidmaatschap. Daarnaast bieden de volgende landen buiten de EU een passend beschermingsniveau:

Andorra, Argentinië, Canada, Faeröer Eilanden, Guernsey, Israël, Isle of Man, Jersey, Nieuw Zeeland, Zwitserland en Uruguay.

De actuele lijst kunt u hier vinden: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

Verwerkingen mogen in de Verenigde Staten worden uitgevoerd indien de verwerker zich heeft geëncmitteerd aan het EU-US Privacy Shield afsprakenstelsel. U kunt dat hier controleren: <https://www.privacyshield.gov/list>.

Let op: Ook wanneer doorgifte op bovenstaande gronden is toegestaan dient nog steeds aan alle overige bepalingen van de AVG voldaan te worden.