December 2022

Toelichting Verwerkersovereenkomst Brancheorganisaties Zorg

Verenigd in

boz Brancheorganisaties Zorg

December 2022

Inleiding

ActiZ, De Nederlandse GGZ, NFU, NVZ en VGN verenigd in de Brancheorganisaties Zorg (BoZ) hebben eind 2017 in het kader van de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) een modelverwerkersovereenkomst ontwikkeld. Anno eind 2022 werd het hoog tijd voor een update daarvan. In deze toelichting leest u de belangrijkste uitgangspunten van de BoZ verwerkersovereenkomst en welke belangrijke wijzigingen zijn doorgevoerd.

Om goede zorg te kunnen verlenen is het in de gezondheidszorg noodzakelijk dat dossiers van cliënten worden aangelegd. Die bevatten daardoor zeer gevoelige gegevens. Het recht op privacy en de daarop gebaseerde wetgeving brengt mee dat degenen die deze persoonsgegevens verwerken daar heel zorgvuldig mee omgaan. Daarom is het essentieel om daarover goede afspraken te maken met partijen die in opdracht van zorginstellingen met deze bijzondere persoonsgegevens te maken krijgen, zodat die gegevens te allen tijde veilig en verantwoord worden verwerkt. Met een zogeheten verwerkersovereenkomst kunnen (en moeten) daarover met de opdrachtnemer afspraken worden gemaakt.

Wettelijk verplicht

Het sluiten van een verwerkersovereenkomst is wettelijk verplicht indien een zorgaanbieder een derde inschakelt die persoonsgegevens verwerkt namens u, bijvoorbeeld een leverancier van een cliëntendossier.

Een verwerkersovereenkomst wordt gesloten tussen een verwerkingsverantwoordelijke en de verwerker. Een *verwerkingsverantwoordelijke* is degene die op grond van de wet, als gevolg van afspraken of door de omstandigheid de verantwoordelijkheid over de verwerking heeft en het doel en de middelen voor de verwerking vaststelt. De verwerkersverantwoordelijke in de gezondheidszorg is meestal degene die de zorgovereenkomst met de cliënt heeft en dus om die reden een zorgdossier over die cliënt bijhoudt. De verwerkingsverantwoordelijke bepaalt welke gegevens worden verwerkt en het 'hoe en waarom' van de gegevensverwerking. Een *verwerker* is degene die persoonsgegevens verwerkt *uitsluitend* ten behoeve van en in opdracht van de verwerkingsverantwoordelijke. De verwerker mag de persoonsgegevens niet voor eigen doeleinden gebruiken.

Verwerkingsverantwoordelijke of verwerker?

Het is niet altijd eenvoudig om vast te stellen wie in een concreet geval verwerkingsverantwoordelijke is en wie verwerker. Hierbij een aantal aandachtspunten om dit te kunnen bepalen:

De verwerker mag geen zelfstandige beslissingen nemen over het doel van de verwerking indien de wederpartij alleen mag handelen onder de verantwoordelijkheid van de verwerkingsverantwoordelijke en diens instructies. Als de verwerker wel zelfstandig beslissingen neemt over het doel van de verwerking en de middelen voor de gegevensverwerking wordt de wederpartij aangemerkt als verwerkingsverantwoordelijke. De verwerker heeft met andere woorden geen zeggenschap over de persoonsgegevens.

De verwerker verwerkt gegevens ten behoeve van de verwerkingsverantwoordelijke als primaire opdracht: de dienstverlening van de verwerker moet gericht zijn op het verwerken van persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke. Wanneer de verwerking van persoonsgegevens niet de primaire opdracht is van de verwerker maar het een uitvloeisel is van een andere vorm van dienstverlening, dan is de wederpartij zelf de verwerkingsverantwoordelijke voor deze verwerking. Oftewel, het enkele feit dat u een opdracht krijgt van of dienst verleent aan de verwerkingsverantwoordelijke is niet voldoende om te kunnen spreken van

verwerkerschap, de opdracht moet gericht zijn op het verwerken van persoonsgegevens. Volledige controle door de leverancier over de gegevens, zoals bij SaaS oplossingen en bij zelfstandig beheer bij data die zich bij verwerkingsverantwoordelijke bevindt, geldt als primaire opdracht. De opdracht van de leverancier is namelijk gericht op de gegevens. Wanneer de leverancier onder regie van de verwerkingsverantwoordelijke remote support biedt en daarmee alleen toegang heeft tot de data op het moment dat de verwerkingsverantwoordelijke dit openstelt voor remote support (via een beveiligde VPN-verbinding), is deze dienst niet gericht op de gegevensverwerking maar op het technisch oplossen van het probleem en is de verwerking van gegevens niet de primaire opdracht. In de Hoofdovereenkomst dienen wel adequate afspraken gemaakt te worden over de toegang tot en omgang met die gegevens, gericht op het verwerken van de gegevens alleen ter uitvoering van de remote controle. Daarnaast moeten afspraken worden gemaakt over geheimhoudingsplicht, het uitsluiten van aanvullende verwerkingshandelingen met de data, controel op de logging en het monitoren van de logging.

Samenwerken met een andere verwerkingsverantwoordelijke?

In de zorg komt het ook voor dat er gezamenlijke verantwoordelijkheid bestaat voor de gegevensverwerkingen, bijvoorbeeld bij ketenzorg of in de samenwerking tussen zorgaanbieder en gemeenten. Ook als een zorgaanbieder delen van de zorg door een onderaannemer laat uitvoeren zal er in de regel eerder een samenwerking bestaan tussen twee verwerkersverantwoordelijken en niet tussen een verwerkingsverantwoordelijke en een verwerker.

Als er veel samenwerkende verwerkingsverantwoordelijken zijn kan het soms raadzaam zijn om één juridische verwerkingsverantwoordelijke aan te wijzen, omdat dan voor iedereen duidelijk is wie het aanspreekpunt is en wie (formeel) de beslissingen neemt. Bij het landelijk schakelpunt (LSP), waarvan feitelijk alle zorgaanbieders verantwoordelijke zijn is hiervoor gekozen. Niet in alle gevallen waarin er een gezamenlijke verwerkingsverantwoordelijkheid bestaat hoeft er een juridisch verwerkingsverantwoordelijke te worden aangewezen. Wel moet er bij gezamenlijke verantwoordelijkheid op grond van de AVG altijd óók een overeenkomst worden gesloten waarin afspraken worden gemaakt over het verwerken van persoonsgegevens. Deze overeenkomst heeft echter een ander karakter dan deze verwerkersovereenkomst en valt daarom ook buiten dit kader.

Gegevensuitwisseling tussen verwerkingsverantwoordelijken?

<u>Data Transfer Agreement (DTA) (of "gegevensuitwisselingsovereenkomst")</u>

Als een organisatie persoonsgegevens verwerkt voor haar eigen doeleinden en deze gegevens deelt met een andere organisatie die de persoonsgegevens voor haar eigen doelen gebruikt, dan is sprake van twee zelfstandige verwerkingsverantwoordelijken. Iedere organisatie moet zelf doel en middelen vastleggen voor het eigen proces. Hier is dus géén sprake van gezamenlijke verwerkingsverantwoordelijkheid in de zin van de AVG. Wel is het van belang dat voor deze gegevensuitwisseling tussen twee verwerkingsverantwoordelijken een Gegevensuitwisselingsovereenkomst wordt opgesteld.

De European Data Protection Board (EDPB) heeft guidelines uitgebracht over de begrippen 'verwerkingsverantwoordelijke' en 'verwerker'. Ondanks dat de AVG geen formele eisen stelt aan hoe de verwerkingsverantwoordelijken dergelijke afspraken moeten maken, beveelt de EDPB wel aan om de afspraken vast te leggen in een *binding* document. Een voorbeeld van zo'n document is de data-uitwisselingsovereenkomst.

Wat regel je in een data-uitwisselingsovereenkomst?
Eigenlijk verschilt een verwerkersovereenkomst niet zo heel erg veel van een data-uitwisselingsovereenkomst. In een data-uitwisselingsovereenkomst wil je ook vastleggen welke persoonsgegevens worden verwerkt en voor welke doeleinden dit gebeurt. Denk verder aan afspraken over welke partij vragen en/of verzoeken van betrokkenen afhandelt,

en hoe de beveiligingsmaatregelen zijn ingericht en geregeld. De gegevensuitwisselingsovereenkomst valt buiten de scope van de verwerkersovereenkomst en daarmee is dit kader niet van toepassing.

De standaard kernelementen die in ieder geval hierin kunnen worden opgenomen zijn:
- Duur van de overeenkomst
- Doel en grondslag gegevensuitwisseling
- Verplichtingen partijen
- Geheimhouding
- Beveiliging
- Datalekken
- Rechten van betrokkenen
- Aansprakelijkheid.

Doorgevoerde wijzigingen nieuwe versie BoZ verwerkersovereenkomst

Vanuit de BoZ zijn de ervaringen met het vorige model geïnventariseerd om zo tot een verbetering te kunnen komen. De teksten zijn hier en daar vereenvoudigd, overbodige definities en overbodige artikelen en bepalingen zijn verwijderd. Een aantal gewijzigde artikelen worden hieronder nader toegelicht:

Artikel 4 Beveiliging persoonsgegevens en controle

Artikel 4 is er in twee versies: één voor wanneer het medische gegevens betreft die door de verwerker worden verwerkt en één voor wanneer het persoonsgegevens betreft die niet medisch zijn. Verwijder de artikel 4-optie die niet van toepassing is. Wanneer er medische gegevens worden verwerkt is er sprake van bijzondere persoonsgegevens die een hogere beveiliging nodig hebben. De Autoriteit Persoonsgegevens (AP) heeft aangegeven dat onder een passende beveiliging voor persoonsgegevens wordt verstaan het voldoen aan de ISO27001 en daarnaast in het geval van medische gegevens ook aan de NEN7510 en wanneer van toepassing de NEN7512 en NEN7513.

De AVG vraagt van verwerkers dat het hebben van voldoende beveiliging aangetoond kan worden. Uitgangspunt in de BoZ verwerkersovereenkomst is dat de verwerker dit kan aantonen door een certificaat van de ISO27001 en de NEN7510 in Bijlage 2 toe te voegen. Wanneer er geen certificaat aanwezig is kan een Third Party Memorandum (TPM) worden toegevoegd. Een TPM is een verklaring van een onafhankelijke derde partij die kan beoordelen of in overeenstemming wordt gewerkt met de ISO- en NEN-normen. Het is voor de verwerkingsverantwoordelijke van belang om inzichtelijk te hebben waarop de dienst is gecertificeerd (scope en inhoud) en indien mogelijk ook een rapport van een onafhankelijk auditor te ontvangen.

Voorbeelden van maatregelen die verwerker dient te nemen zijn:

a) maatregelen om te waarborgen dat enkel bevoegde medewerkers toegang hebben tot de persoonsgegevens voor de doeleinden die zijn uiteengezet;

b) maatregelen waarbij de verwerker zijn medewerkers en subverwerkers uitsluitend toegang geeft tot persoonsgegevens via op naam gestelde accounts, waarbij het gebruik van die accounts adequaat gelogd wordt en waarbij de betreffende accounts alleen toegang geven tot die Persoonsgegevens waartoe de toegang voor de betreffende (rechts)persoon noodzakelijk is;

c) maatregelen om de persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, verwerking, toegang of openbaarmaking;

d) maatregelen om zwakke plekken te identificeren ten aanzien van de verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan verwerkingsverantwoordelijke;

e) maatregelen om de tijdige beschikbaarheid van de persoonsgegevens te garanderen;

f) maatregelen om te waarborgen dat persoonsgegevens logisch gescheiden worden verwerkt van de persoonsgegevens die hij voor zichzelf of namens derde partijen verwerkt.

Artikel 7 Inschakeling subverwerkers

Er is voor gekozen om de voorafgaande schriftelijke toestemming voor iedere nieuwe subverwerker te vervangen door een meldingsplicht van de verwerker aan de Verwerkersverantwoordelijke en de mogelijkheid daar als Verwerkingsverantwoordelijke bezwaar tegen te maken. Hierdoor hoeft de Verwerker niet voor iedere nieuwe subverwerker toestemming te vragen aan de Verwerkingsverantwoordelijke. Wanneer Verwerkingsverantwoordelijke bezwaar heeft tegen de nieuwe subverwerker dan gaan partijen in eerste instantie met elkaar in overleg over hoe het bezwaar kan worden weggenomen of hoe de afgenomen diensten toch doorgang kunnen vinden. Let op, bij verwerkingen buiten de EER is toestemming van de Verwerkingsverantwoordelijke wel vereist, ook bij subverwerkers.

Artikel 8 Aansprakelijkheid

Dit artikel uit is geschrapt. Deze aansprakelijkheid is specifiek bedoeld voor de privacy risico's van de gegevensverwerking en is een andere dan in de hoofdovereenkomst over het algemeen wordt overeengekomen. De aansprakelijkheids- bepalingen en beperkingen in de hoofdovereenkomst hebben vaak alleen betrekking op de contractwaarde. Wanneer de contractwaarde laag is staat dit niet in verhouding tot de privacy risico's van de gegevensverwerking. Aan de andere kant is onbeperkte aansprakelijkheid voor de verwerker niet acceptabel en ook niet verzekerbaar.

Voortvloeiend uit mogelijk hoge risico's voor de verwerkingsverantwoordelijke kan in de hoofdovereenkomst de volgende aanvullende bepalingen worden opgenomen die specifiek zien op de aansprakelijkheid van boetes door AP:

-Verwerker is aansprakelijk voor alle schade die Verwerkingsverantwoordelijke lijdt, waaronder in elk geval maar niet uitsluitend door de Autoriteit Persoonsgegevens of andere bevoegde autoriteit opgelegde boetes en/of dwangsommen en aanspraken van betrokkenen als gevolg van enige tekortkoming in de nakoming van deze verwerkersovereenkomst en/of overtreding van de AVG.
-Verwerker vrijwaart Verwerkingsverantwoordelijke voor alle (financiële) schade en kosten die de Verwerkingsverantwoordelijke dientengevolge lijdt, tenzij verwerker aantoont dat deze schade en kosten niet aan verwerker kunnen worden toegerekend.

Artikel 9 Duur en beëindiging

In artikel 9.5 wordt aangegeven dat er nadere afspraken kunnen worden gemaakt om continuïteitsrisico's te verkleinen in het geval van incidenten en calamiteiten, zoals een faillissement. Voorbeelden van deze aanvullende afspraken zijn:

a) het maken van afspraken over het periodiek terug of aan een derde partij leveren van de door Verwerker verwerkte gegevens; en/of

b) het met een derde partij sluiten van een overeenkomst die ertoe strekt dat de betreffende derde partij zich hoofdelijk verbindt tot of borg staat voor de nakoming van de Overeenkomst; en/of

c) het met een derde partij sluiten van een (tripartite) overeenkomst die ertoe strekt dat de betreffende derde partij (voortdurend) over alle benodigde gegevens komt te

beschikken om in voorkomend geval (een deel van) de op grond van de Overeenkomst te verrichten prestaties – al dan niet op basis van een nieuwe overeenkomst – in plaats van of parallel aan Verwerker te kunnen (gaan) verrichten.

Bijlagen:

- Bijlage 1 is uitgebreid met een lijst voor de subverwerkers.
- In Bijlage 2 is verduidelijkt hoe de Verwerker kan aantonen dat wordt voldaan aan de eisen van de AVG ten aanzien van de beveiliging van de persoonsgegevens. Het uitgangspunt is dat de Verwerker het ISO27001 certificaat en, wanneer van toepassing, het NEN7510 certificaat toevoegt. Wanneer dit er niet is kan er een verklaring van een onafhankelijke derde worden verlangd. Advies is om niet met minder genoegen te nemen, maar dit is uiteraard aan de Verwerkingsverantwoordelijke. Wanneer bovengenoemd geen optie is dan kunnen de minimale eisen zoals in deze toelichting is opgenomen bij artikel 4 worden toegevoegd.
- Bij Bijlage 3 kan de contactinformatie worden opgenomen van de relevante contactpersoon, dit zal meestal de Functionaris Gegevensbescherming zijn.
- Bijlage 4 is geheel verwijderd, omdat de BoZ uit wil gaan van een standaard die niet gewijzigd wordt. Uiteraard blijft het mogelijk wijzigingen af te spreken en daarvoor een Bijlage 4 toe te voegen aan de Verwerkersovereenkomsten met daarin een overzicht van de overeengekomen aanpassingen.

Uitgangspunten BoZ verwerkersovereenkomst

De BoZ verwerkersovereenkomst heeft een aantal uitgangspunten:

i. De BoZ verwerkersovereenkomst dient als standaard voor de hele zorgsector. De verwerkersovereenkomst dient gebruikt te worden met kennis van (juridische) zaken. Indien gewenst kan er binnen de grenzen van de AVG van worden afgeweken. Het is aan te raden om zich in geval van afwijkingen van het model juridisch te laten adviseren over de consequenties daarvan. Tevens is het aan te raden om de tekst ongewijzigd te laten en eventuele wijzigingen inclusief motivering op te nemen in een toegevoegde bijlage 4 bij de verwerkersovereenkomst.

ii. De BoZ verwerkersovereenkomst maakt onverbrekelijk onderdeel uit van de overeenkomst van opdracht of dienstverleningsovereenkomst tussen partijen. De BoZ verwerkersovereenkomst regelt uitsluitend de verhouding tussen de verwerkingsverantwoordelijke en de verwerker met betrekking tot het verwerken van persoonsgegevens.

iii. De BoZ verwerkersovereenkomst kan letterlijk onderdeel worden van de overeenkomst van opdracht of dienstverleningsovereenkomst. In dat geval ontstaat er slechts één document en ontstaat er geen ruis. Het is ook mogelijk om de BoZ verwerkersovereenkomst te hanteren *naast* de overeenkomst van opdracht. Om te voorkomen dat dan ruis ontstaat, bevat de verwerkersovereenkomst een bepaling die de bepalingen van de verwerkersovereenkomst laat vóórgaan boven die van de overeenkomst van opdracht of dienstverleningsovereenkomst.

iv. In de BoZ verwerkersovereenkomst is niet gepoogd de wet over te schijven. Dit betekent dat zaken die al in de wet geregeld zijn niet nogmaals in de BoZ verwerkersovereenkomst zijn opgenomen. Alle artikelen die betrekking hebben op de wet- en regelgeving zijn beperkt tot het verwerken van persoonsgegevens.

v. Waar het gaat om de vraag welke persoonsgegevens een verwerker in het kader van de opdracht of dienstverlening mag verwerken en hoe, dient dit goed beschreven te worden. Dit omdat hiermee het werk van de verwerker met

betrekking tot persoonsgegevens afgebakend wordt. Door dit goed toe omschrijven houdt de verwerkingsverantwoordelijke met de overige bepalingen in de verwerkersovereenkomst optimaal controle. En dat is met name in de zorg waar het dikwijls om gevoelige persoonsgegevens gaat van wezenlijk belang. Dit is dan ook een belangrijk onderdeel van de verwerkersovereenkomst en is hierin niet uitgewerkt. Dit is niet gebeurd omdat dit niet mogelijk is, omdat dit afhangt van de omstandigheden van het geval.

vi. De Hoofdovereenkomst, meestal een overeenkomst van opdracht om bepaalde diensten te leveren aan de zorgaanbieder, bevat alle andere afspraken tussen de opdrachtgever (zorgaanbieder) en de opdrachtnemer (de Leverancier) over de dienst die de leverancier gaat leveren en waarvoor het nodig is dat (medische) persoonsgegevens worden verwerkt. Denk aan een opdrachtovereenkomst waarbij de leverancier een applicatie levert waarin patiënt- of medewerkersgegevens worden verwerkt, vaak in de vorm van software as a service en/of hosting en/of technisch beheer. In de overeenkomst van opdracht of dienstverleningsovereenkomst worden dus zaken geregeld zoals de kosten voor het leveren van de dienst, de technische voorwaarden voor het leveren van de dienst, de SLA-bepalingen, de communicatieafspraken in de DAP, de aansprakelijkheid als de leverancier die verplichtingen niet, niet geheel of niet tijdig nakomt en eventuele beperkingen op die aansprakelijkheid etc.

vii. Deze verwerkersovereenkomst is opgesteld op basis van het huidige inzicht op de AVG. Indien naar aanleiding van gewijzigde wetgeving, evaluaties en/of reacties uit het veld aanpassingen noodzakelijk zijn zal een volgende versie worden opgesteld.