Toelichting Verwerkersovereenkomst Brancheorganisaties Zorg

Versie Maastricht UMC+

Verenigd in

December 2023

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. Eind 2022 werd het hoog tijd voor een update daarvan. Deze toelichting beschrijft 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.

De verwerkersovereenkomst
Een verwerkersovereenkomst wordt gesloten tussen een verwerkingsverantwoordelijke en een verwerker. Een *verwerkingsverantwoordelijke* is degene die op grond van de wet, als gevolg van afspraken of feitelijk de verantwoordelijkheid over de verwerking heeft en het doel en de middelen (verwerkingsmethoden) 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. Een belangrijk criterium is dat de verwerker geen zelfstandige beslissingen mag nemen over het doel van de verwerking en alleen mag handelen onder de verantwoordelijkheid van de verwerkingsverantwoordelijke en diens instructies. De verwerker heeft met andere woorden geen zeggenschap over de persoonsgegevens.

Samenwerken met een andere verwerkingsverantwoordelijke (gezamenlijke verwerkingsverantwoordelijken)?
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 verwerkingsverantwoordelijken.

Van gezamenlijke verwerkingsverantwoordelijkheid is sprake wanneer voor een specifieke gegevensverwerking twee of meer partijen gezamenlijk het doel voor en de middelen (verwerkingsmethoden) van deze gegevensverwerking bepalen. Dit houdt in dat meer dan één partij beslissende invloed heeft op de vraag of en hoe de gegevensverwerking plaatsvindt. Met andere woorden: de verwerking zou niet mogelijk zijn zonder de deelname van de partijen, in die zin dat de verwerking door elke partij onscheidbaar/onlosmakelijk met de verwerking van de andere partij verbonden is (denk bijvoorbeeld aan een situatie waarbij zorgverlener en universiteit besluiten om samen een klinische proef met hetzelfde doel te starten en zij samen het onderzoeksprotocol opstellen. Zij kunnen als gezamenlijke verwerkingsverantwoordelijke worden gezien aangezien zij samen hetzelfde doel en de wezenlijke middelen voor de verwerking vaststellen).

Bij gezamenlijke verantwoordelijkheid moet op grond van de AVG óók altijd een overeenkomst worden gesloten waarin afspraken worden gemaakt over het verwerken van persoonsgegevens. Hiervoor kan

het model gegevensuitwisselingsovereenkomst gezamenlijke verwerkingsverantwoordelijken van het MUMC+ worden gebruikt.

Gegevensuitwisseling tussen zelfstandige verwerkingsverantwoordelijken?

Als een organisatie persoonsgegevens verwerkt voor haar eigen doeleinden en middelen (verwerkingsmethoden) en deze gegevens vervolgens deelt met een andere organisatie die de persoonsgegevens voor haar eigen doelen gebruikt, dan is er sprake van twee zelfstandige verwerkingsverantwoordelijken. Er kunnen zich ook situaties voordoen waarin verschillende partijen achtereenvolgens dezelfde persoonsgegevens verwerken in een keten van verwerkingen, maar waarbij elke partij wel onafhankelijk doel en middelen in haar deel van de keten bepaalt. Indien niet gezamenlijk het doel en de middelen van dezelfde gegevensverwerking of reeks gegevensverwerkingen wordt bepaald, kwalificeren partijen als opeenvolgende 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.

Ondanks dat de AVG geen formele eisen stelt aan hoe zelfstandige verwerkingsverantwoordelijken afspraken over de gegevensverwerking moeten maken, beveelt de European Data Protection Board (EDPB) wel aan om de afspraken vast te leggen in een *binding* document. Een voorbeeld van zo'n document is een gegevensuitwisselingsovereenkomst. Binnen het MUMC+ wordt het volgende beleid gehanteerd voor het afsluiten van een gegevensuitwisselingsovereenkomst tussen twee zelfstandige verwerkingsverantwoordelijken:

- Een gegevensuitwisselingsovereenkomst tussen twee zelfstandige verwerkingsverantwoordelijken is niet nodig wanneer er gegevens worden uitgewisseld tussen zorgaanbieders/zorgverleners onderling
- In alle andere gevallen dan hierboven genoemd, dient er in beginsel wel een gegevensuitwisselingsovereenkomst te worden afgesloten (denk bijvoorbeeld aan commerciële partijen, (zorg)verzekeraars, etc.). In deze gevallen kan het model gegevensuitwisselingsovereenkomst zelfstandige verwerkingsverantwoordelijken van het MUMC+ worden gebruikt.
- Wanneer er persoonsgegevens worden uitgewisseld in het kader van wetenschappelijk onderzoek, kan er gebruik worden gemaakt van de Data Transfer Agreement (ook wel Data Sharing Agreement genoemd) die is opgesteld door de NFU. Deze is te raadplegen op de website van ELSI Health-RI via Wat voor soort overeenkomst heb ik nodig voor het uitwisselen van gegevens of lichaamsmaterialen voor wetenschappelijk onderzoek? | Elsi Servicedesk (health-ri.nl) (onder het kopje 'Meer lezen').

Bijlage bij deze toelichting

Algemeen

De Ondergetekenden

Voor ondertekening van de verwerkersovereenkomst en de gegevensuitwisselingsovereenkomsten is de hoofdovereenkomst leidend. De hoofdovereenkomst dient ondertekend te worden conform de bevoegdhedenregeling. De verwerkersovereenkomst en gegevensuitwisselingsovereenkomsten volgen de hoofdovereenkomst. Kan de hoofdovereenkomst op basis van de bevoegdhedenregeling getekend worden door de centrumdirecteur (medisch of bedrijfskundig) of het medisch afdelingshoofd, dan kan de bijbehorende verwerkersovereenkomst of gegevensuitwisselingsovereenkomst eveneens door hen getekend worden. De ondertekenaar is ook verantwoordelijk voor het opnemen van de nieuwe gegevensverwerking in de Registratie van verwerkingen van persoonsgegevens.

Verwerkersovereenkomst

Doorgevoerde wijzigingen nieuwe versie BoZ-verwerkersovereenkomst

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

Artikel 4 Beveiliging persoonsgegevens en controle

Artikel 4 is geschreven voor twee situaties: de situatie waarin medische gegevens door de verwerker worden verwerkt en de situatie waarin door de verwerker persoonsgegevens worden verwerkt die niet medisch zijn. 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 ISO 27001 en daarnaast in het geval van medische gegevens ook aan NEN 7510 en wanneer van toepassing NEN 7512 en NEN 7513. Om die reden geldt in het geval dat er door de verwerker medische gegevens worden verwerkt het extra artikellid 4.3. **LET OP!** Wanneer er geen medische gegevens worden verwerkt, moet het artikellid 4.3. worden doorgehaald in de verwerkersovereenkomst.

De AVG vraagt daarnaast 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 ISO 27001- en een NEN 7510-certificaat aan 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. Om die reden dient de verwerker in alle gevallen, dus zowel bij aanwezigheid van een certificaat of TPM alsook bij het ontbreken hiervan, de tabel in Bijlage 2 volledig in te vullen. In deze tabel dient de verwerker inzichtelijk te maken welke concrete technische en organisatorische beveiligingsmaatregelen er zijn getroffen om de bescherming van de persoonsgegevens te garanderen.

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 verwerkingsverantwoordelijke 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 de verwerkingsverantwoordelijke bezwaar heeft tegen de nieuwe subverwerker dan gaan partijen 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

De aansprakelijkheidsbepaling is aanvullend aan die in de Hoofdovereenkomst en regelt eventuele aansprakelijkheid als de verwerker zich bij de verwerking niet aan de regels van de AVG houdt. Er is gekozen om voor de maximum bedragen voor aansprakelijkheid (1,25 miljoen per gebeurtenis respectievelijk 2,5 miljoen per kalenderjaar) aan te sluiten bij de NFU-inkoopvoorwaarden, aangezien de aanbestedingswet zich verzet tegen ongelimiteerde aansprakelijkheid. De opgenomen beperkingen zijn goed te verzekeren door partijen.

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) afspraken over het periodiek aan verwerkingsverantwoordelijke of een derde partij leveren van de door verwerker verwerkte gegevens; en/of
b) afspraken over 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 deze overeenkomst; en/of
c) afspraken over het met een derde partij sluiten van een tripartiteovereenkomst 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 deze overeenkomst te verrichten prestaties – al dan niet op basis van een nieuwe overeenkomst – in plaats van of parallel aan verwerker te kunnen verrichten.

Bijlagen

In de bijlagen dient de verwerking van de persoonsgegevens nader gespecificeerd te worden. In Bijlage 1 wordt o.a. nader uitgewerkt waarom en welke persoonsgegevens worden verwerkt, van wie deze gegevens zijn en met wie ze worden gedeeld. In Bijlage 2 worden de technische en organisatorische beveiligingsmaatregelen uitgewerkt die zijn genomen om de beveiliging en vertrouwelijkheid van de persoonsgegevens te waarborgen. In Bijlage 3 worden de contactgegevens van partijen opgenomen en in Bijlage 4 kunnen eventuele wijzigingen ten opzichte van de standaardtekst worden toegevoegd.

LET OP! Alle bijlagen dienen volledig te worden ingevuld.

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. Bij wijzigingen dient de tekst ongewijzigd te blijven en eventuele wijzigingen inclusief motivering dienen opgenomen te worden in de toegevoegde bijlage 4 bij de verwerkersovereenkomst.
ii. De BoZ-verwerkersovereenkomst maakt onverbrekelijk onderdeel uit van de hoofdovereenkomst (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. In de BoZ-verwerkersovereenkomst is niet gepoogd de wet over te schrijven. Dit betekent dat zaken die al in de wet geregeld zijn niet nogmaals in de BoZ-verwerkersovereenkomst zijn opgenomen.
iv. 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 te 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. Deze beschrijving en afbakening is dan ook een belangrijk onderdeel van de verwerkersovereenkomst en dient verder uitgewerkt te worden. Dit is niet vooringevuld, omdat dit niet mogelijk is, omdat dit afhangt van de specifieke omstandigheden van de gegevensverwerking in relatie tot de contractafspraken.

v. 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 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 hoofdovereenkomst (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 verplichtingen niet, niet geheel of niet tijdig nakomt en eventuele beperkingen op de aansprakelijkheid etc.

vi. De BoZ-verwerkersovereenkomst is opgesteld op basis van de huidige inzichten ten aanzien van de AVG. Indien naar aanleiding van gewijzigde wetgeving, evaluaties en/of reacties uit het veld aanpassingen noodzakelijk zijn zal een volgende versie worden opgesteld.

Gegevensuitwisselingsovereenkomst

De opzet van beide gegevensuitwisselingsovereenkomsten is vergelijkbaar met de verwerkersovereenkomst. In deze overeenkomst maken partijen afspraken over de wijze waarop zij persoonsgegevens onderling gaan uitwisselen en welke verantwoordelijkheden en taken partijen ten aanzien van deze verwerking hebben. De volgende onderwerpen zijn opgenomen in de gegevensuitwisselingsovereenkomsten:

- Algemene bepalingen zoals definities, onderwerp van de overeenkomst, duur en beëindiging en overige bepalingen
- Verplichtingen van partijen ten aanzien van de gegevensverwerking
- Toegang tot persoonsgegevens
- Geheimhouding en vertrouwelijkheid
- Aansprakelijkheid
- Inbreuk in verband met persoonsgegevens (datalek)
- Bijlagen met de specificatie van de samenwerking en onderlinge verantwoordelijkheden en taakverdeling van partijen, specificatie van de gegevensverwerking, de technische en organisatorische beveiligingsmaatregelen en contactinformatie.