Checklist verwerkersovereenkomst voor zorgaanbieders

Veel zorgaanbieders nemen externe diensten af die gepaard gaan met de verwerking van persoonsgegevens van betrokkenen, gezondheidsgegevens van patiënten in het bijzonder. Hierbij kan worden gedacht aan het gebruik van een patiënteninformatiesysteem (zoals een HIS voor huisartsen en een ZIS voor een ziekenhuis), e-healthapplicaties en oplossingen voor veilig e-mailen en het veilig delen van bestanden.

Bij het afnemen van dit soort diensten dient ervoor te worden gewaakt dat de omgang met persoonsgegevens met voldoende veiligheidswaarborgen is omkleed. Zorgaanbieder en dienstverlener zijn op grond van de Algemene verordening gegevensbescherming (AVG) dan ook verplicht schriftelijke afspraken met elkaar te maken over de voorwaarden voor de verwerking van persoonsgegevens. In het kader van de AVG kwalificeert de zorgaanbieder als 'verwerkingsverantwoordelijke' en de dienstverlener als 'verwerker'.

De afspraken tussen zorgaanbieder en dienstverlener worden doorgaans vastgelegd in een verwerkersovereenkomst, veelal separaat van de dienstverleningsovereenkomst zelf. In een verwerkersovereenkomst zijn onderwerpen geregeld zoals de beveiliging van de persoonsgegevens, incidentenmanagement, medewerkingsverplichtingen en het inschakelen van subverwerkers. Ook kunnen aansprakelijkheidsbeperkingen (in het voordeel van de verwerker) zijn opgenomen, in aanvulling op de beperkingen uit de dienstverleningsovereenkomst.

Meestal zal de dienstverlener de zorgaanbieder een (model) verwerkersovereenkomst aanbieden. Het is in dat geval van belang te beoordelen of de inhoud aan de voorschriften van de AVG voldoet, ofwel of de verwerking met voldoende veiligheidswaarborgen is omkleed. Onderstaande checklist omvat een toelichting op onderdelen van de verwerkersovereenkomst. Zorgaanbieders kunnen deze checklist gebruiken bij een eerste beoordeling van een verwerkersovereenkomst, in die zin dat onderstaande onderwerpen in overeenstemming met de AVG in de overeenkomst zijn uitgewerkt. Hierbij geldt dat deze checklist geen juridisch advies vervangt. Raadpleeg dan ook zo nodig een ter zake kundig advocaat of jurist.

Garanties

1. Een zorgaanbieder mag uitsluitend dienstverleners inschakelen die afdoende garanderen dat de verwerking met 'passende technische en organisatorische maatregelen' gepaard gaat, zodat de verwerking aan de vereisten van de AVG voldoet en de bescherming van de rechten van betrokkenen (wiens persoonsgegevens worden verwerkt) is gewaarborgd. Voor zorgaanbieders is in het bijzonder van belang dat een dienstverlener de NEN-normen voor informatiebeveiliging in de zorg in acht neemt (NEN 7510, NEN 7512 en NEN 7513), als deze normen op de dienstverlening van toepassing zijn. Het is aan te raden om beveiligingsmaatregelen concreet in de overeenkomst te benoemen.

Schriftelijke instructies

2. De dienstverlener mag de persoonsgegevens alleen verwerken op basis van schriftelijke instructies van de zorgaanbieder, behoudens wettelijke

verplichtingen van de dienstverlener. Over wettelijke verplichtingen dient de dienstverlener de zorgaanbieder op voorhand te informeren, tenzij wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt. Schriftelijke instructies kunnen in (een bijlage bij) de overeenkomst worden omschreven. Deze instructies hebben ook betrekking op doorgiften van persoonsgegevens buiten de Europese Economische Ruimte (EER) (zie ook onderdeel 15).

Inschakelen subverwerkers

3. De dienstverlener mag geen subverwerkers inschakelen zonder voorafgaande specifieke of algemene schriftelijke toestemming van de zorgaanbieder. Bij algemene schriftelijke toestemming dient de dienstverlener de zorgaanbieder over beoogde veranderingen ten aanzien van de toevoeging of vervanging van andere verwerkers te informeren, waarbij de zorgaanbieder de mogelijkheid wordt geboden daartegen bezwaar te maken.

Subverwerkers: verplichtingen en aansprakelijkheid

4. Wanneer de dienstverlener een andere verwerker inschakelt om voor rekening van de zorgaanbieder specifieke verwerkingsactiviteiten te verrichten, dient de dienstverlener deze andere dienstverlener dezelfde verplichtingen met betrekking tot gegevensbescherming op te leggen als die voor de dienstverlener zelf gelden. Als de andere dienstverlener die verplichtingen niet nakomt, blijft de eerste dienstverlener tegenover de zorgaanbieder volledig aansprakelijk voor het nakomen van de verplichtingen.

Vertrouwelijkheid

5. De dienstverlener, zijn medewerkers, door hem ingeschakelde derden en subverwerkers dienen vertrouwelijkheid ten aanzien van persoonsgegevens te betrachten, op grond van een wettelijke geheimhoudingsverplichting dan wel een contractueel geheimhoudingsbeding.

Beveiliging

6. De dienstverlener dient passende technische en organisatorische maatregelen te treffen om een bepaald beveiligingsniveau te waarborgen, om persoonsgegevens die worden verwerkt te beschermen tegen vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig. Welke precieze maatregelen zijn aangewezen, is afhankelijk van de aard van de verwerking. In zijn algemeenheid geldt: hoe gevoeliger de persoonsgegevens, des te verstrekkender maatregelen benodigd zijn. De dienstverlener doet van deze maatregelen schriftelijk opgave aan de zorgaanbieder, bijv. in of als bijlage bij de overeenkomst. Voor zorgaanbieders is van belang dat een dienstverlener de NEN-normen voor informatiebeveiliging in de zorg in acht neemt (NEN 7510, NEN 7512 en NEN 7513), als deze op de dienstverlening van toepassing zijn.

Ondersteuning beantwoording verzoeken betrokkenen

7. De dienstverlener dient de zorgaanbieder te ondersteunen bij het vervullen van haar plicht om verzoeken van betrokkenen (zoals patiënten) ter uitoefening van hun rechten (op inzage, rectificatie, vernietiging, beperking, bezwaar, overdracht) te beantwoorden.

Ondersteuning nakoming specifieke verplichtingen

8. De dienstverlener dient de zorgaanbieder te ondersteunen bij het nakomen van zijn verplichtingen om zorg te dragen voor een passend beschermingsniveau van de beveiliging, melding van datalekken aan de Autoriteit Persoonsgegevens (AP) en betrokkenen, het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) en, als dat in het kader van een DPIA is aangewezen, om de AP voorafgaand te raadplegen.

Medewerking inzage toezichthouders

9. De dienstverlener dient medewerking te verlenen aan verzoeken (tot inzage) van toezichthoudende instanties, zoals de AP.

Vernietiging of retournering bij einde overeenkomst

10. De dienstverlener dient bij het einde van de dienstverlening, naargelang de keuze van de zorgaanbieder, alle persoonsgegevens te wissen of deze aan de zorgaanbieder terug te bezorgen, en bestaande kopieën te verwijderen, tenzij opslag van de persoonsgegevens uit hoofde van wet- of regelgeving is verplicht.

Informatieverstrekking en audits

11. De dienstverlener dient alle informatie aan de zorgaanbieder ter beschikking te stellen die nodig is om de nakoming van de verplichtingen als dienstverlener aan te tonen en maakt audits, waaronder inspecties, door de zorgaanbieder of een door de zorgaanbieder gemachtigde controleur mogelijk en draagt er aan bij.

Beveiligingsincidenten

12. De dienstverlener dient zonder onredelijke vertraging (suggestie: in elk geval binnen 24 uur) aan de zorgaanbieder melding te doen van beveiligingsincidenten die betrekking hebben op de verwerking van de persoonsgegevens. De zorgaanbieder heeft 72 uur om een datalek aan de AP te melden en dient dus voldoende tijd te hebben om te beoordelen of een incident bij de dienstverlener een datalek is of niet.

Algemene voorwaarden, offerte, overeenkomst

13. Algemene voorwaarden, een offerte en de dienstverleningsovereenkomst van/met de dienstverlener kunnen bepalingen inhouden die ook gelden voor de verwerkersovereenkomst, bijv. bepalingen over de beëindiging van de verwerkersovereenkomst of over de aansprakelijkheid van de dienstverlener. Beoordeeld dient te worden of daarvan sprake is.

Aansprakelijkheid

14. In veel verwerkersovereenkomsten is aansprakelijkheid van de dienstverlener voor schade beperkt of uitgesloten. Daarbij wordt veelal verwezen naar clausules uit de dienstverleningsovereenkomst (ook wel 'hoofdovereenkomst' genoemd) die de zorgaanbieder (vaak eerder of tegelijkertijd) met de dienstverlener heeft gesloten. Van belang is om te beoordelen of die clausules zich zonder meer lenen voor toepassing op de verwerkersovereenkomst en wat de gevolgen zijn als de dienstverlener zich op een dergelijke clausule kan beroepen. Is het bijv. mogelijk schade en/of een boete die de AP aan de zorgaanbieder heeft opgelegd op de dienstverlener te verhalen, als een handelen of nalaten van de dienstverlener daarvan de oorzaak is? Is schade

geheel van vergoeding uitgesloten of is de vergoeding beperkt tot de verzekeringsdekking van de dienstverlener of een optelsom van bepaalde factuurbedragen? Als uitgangspunt kan worden genomen dat de beperkingen van aansprakelijkheid verenigbaar dienen te zijn met de verantwoordelijkheden van partijen.

Doorgifte aan derde landen

15. Voor doorgifte van persoonsgegevens vanuit Nederland naar landen buiten de Europese Economische Ruimte ('EER', ofwel de lidstaten van de EU tezamen met Noorwegen, Liechtenstein en IJsland) gelden andere regels. Van doorgifte aan derde landen is bijv. sprake als persoonsgegevens worden opgeslagen op een server buiten de EER. De hoofdregel is dat een organisatie persoonsgegevens alleen mag doorgeven aan derde landen met een passend beschermingsniveau.

Advies?

Voor advies over verwerkersovereenkomsten of andere privacyvraagstukken in de zorg kunt u contact opnemen met mr. E. Luijendijk of mr. N. van den Burg, telefonisch (030-2122800) of per e-mail (e.luijendijk@kbsadvocaten.nl; n.vandenburg@kbsadvocaten.nl).