

Checklist AVG voor zorgaanbieders

Met ingang van 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) rechtstreeks van toepassing in alle EU-lidstaten. In Nederland is deze verordening in de plaats gekomen van de Wet bescherming persoonsgegevens (Wbp). Op grond van de AVG is elke organisatie die persoonsgegevens verwerkt, verplicht zorgvuldig met persoonsgegevens om te gaan. Schending van voorschriften van de AVG kan leiden tot sancties van de Autoriteit Persoonsgegevens (AP) (waaronder boetes tot maximaal 20 miljoen euro of 4% van de wereldwijde jaaromzet) en schadeclaims van gedupeerde betrokkenen.

Bij uitstek voor de zorgsector is een hoog beschermingsniveau van persoonsgegevens aangewezen. Zorgaanbieders verwerken structureel gezondheidsgegevens van patiënten. Gezondheidsgegevens worden aangemerkt als bijzondere persoonsgegevens. De verwerking van dergelijke gevoelige(r) gegevens is aan strenge(re) voorschriften onderworpen.

Hoewel het materieel toepassingsgebied van de AVG niet van dat van de Wbp verschilt, zijn in de AVG wel verdergaande verplichtingen opgenomen voor organisaties die gegevens verwerken ('verwerkingsverantwoordelijken' en 'verwerkers'). Daarbij is meer de nadruk komen te liggen op het registreren van verwerkingen en het documenteren van maatregelen, met als doel dat kan worden aangetoond dat persoonsgegevens in overeenstemming met de AVG worden verwerkt. Welke documenten zorgaanbieders op orde dienen te hebben om aan deze 'verantwoordingsplicht' te kunnen voldoen, lichten wij hieronder toe.

Privacybeleidsdocument

In een privacybeleidsdocument wordt het beleid voor de omgang met persoonsgegevens beschreven. Onder meer wordt daarin uiteengezet welke organisatorische en technische maatregelen zijn getroffen om de privacy van betrokkenen (personen wiens gegevens worden verwerkt) te waarborgen.

Verwerkingsregister

Elke zorgaanbieder is verplicht een register van verwerkingsactiviteiten bij te houden, omdat op structurele basis gezondheidsgegevens (bijzondere persoonsgegevens) worden verwerkt. Het verwerkingsregister is overigens bij uitstek het hulpmiddel om de gegevensstromen voor specifiek persoonsgegevens binnen een organisatie in kaart te brengen.

Datalekkenregister

Een registratie in het datalekkenregister dient plaats te vinden als er een beveiligingsincident heeft plaatsgevonden, bijv. als een medisch dossier is kwijtgeraakt of als een brief met gezondheidsgegevens aan een ander dan de beoogd geadresseerde is verzonden.

Verwerkersovereenkomst

Als een zorgaanbieder gebruik maakt van de diensten van een verwerker, rust op beide partijen de verplichting met elkaar een verwerkersovereenkomst te sluiten. Voorbeelden van verwerkers zijn een administratiekantoor, de beheerder van een huisartsen- of ziekenhuisinformatiesysteem (HIS respectievelijk ZIS) en een aanbieder van diensten voor veilig e-mailen en het veilig delen van bestanden.

Dergelijke partijen kwalificeren als 'verwerker' omdat zij op instructie van de zorgaanbieder persoonsgegevens verwerken.

Overeenkomst verwerkingsverantwoordelijken

Niet alleen afspraken tussen verwerkingsverantwoordelijken en verwerkers zijn verplicht. Ook als verwerkingsverantwoordelijken onderling samenwerken en die samenwerking gepaard gaat met de verwerking van persoonsgegevens dienen afspraken over de omgang met persoonsgegevens en de verdeling van verantwoordelijkheden te worden vastgelegd. Een typisch voorbeeld hiervan is de samenwerking tussen het Medisch Specialistisch Bedrijf (MSB) en het ziekenhuis.

Privacyprotocol

Een zorgaanbieder dient haar medewerkers te instrueren over hoe zij met persoonsgegevens dienen om te gaan. Hoewel niet verplicht, is het raadzaam om daarvoor praktische instructies te formuleren en die op te nemen in een intern protocol. Uitgangspunt voor het privacyprotocol is het hiervoor genoemde privacybeleidsdocument.

Privacyverklaring

Betrokkenen dienen te worden geïnformeerd over hoe met hun persoonsgegevens binnen de organisatie van een zorgaanbieder wordt omgegaan. Aan deze verplichting kan worden voldaan door publicatie van een privacyverklaring op de eigen website. In deze verklaring wordt ook beschreven op welke wijze betrokkenen verzoeken ter uitoefening van hun rechten kunnen uitoefenen, zoals het recht op inzage of het recht op vernietiging van gegevens.

Advies?

Voor advies over 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).