De AVG voor de zorg: 12 vragen en antwoorden

Deze whitepaper geeft op hoofdlijnen een toelichting op de Algemene verordening persoonsgegevens (AVG) voor de zorgsector.

1. Wat is de AVG?

De Algemene verordening gegevensbescherming (AVG) is een Europese verordening die betrekking heeft op de verwerking van persoonsgegevens van natuurlijke personen. Het regelt de privacyrechten van burgers en geeft verplichtingen voor overheden en bedrijven. De AVG vervangt de Wet bescherming persoonsgegevens (Wbp) en treedt per 25 mei 2018 in werking. Niet-naleving van de AVG kan leiden tot forse boetes (tot 20 miljoen euro of 4% van de wereldwijde jaaromzet) en aansprakelijkheid voor schade.

2. Is de AVG van toepassing op de zorgsector?

De AVG geldt ook voor de zorgsector. De AVG is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Gegevens over de gezondheid van een persoon worden onder de AVG als bijzondere persoonsgegevens aangemerkt. Het verwerken daarvan is -net als onder de Wbp- verboden, tenzij daarvoor een in de AVG vastgelegde grondslag bestaat.

3. Blijven zorgspecifieke privacyregels van kracht?

Zorgspecifieke privacyregels blijven naast de AVG van kracht, zoals die volgen uit de Wet op de geneeskundige behandelingsovereenkomst (WGBO), de Wet kwaliteit, klachten en geschillen zorg (Wkkgz), de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG), de Zorgverzekeringswet (Zvw), de Wet langdurige zorg (Wlz), de Wet marktordening gezondheidszorg (Wmg) en de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wagz). De AVG brengt ook geen veranderingen met zich mee voor het medisch beroepsgeheim.

4. Wanneer mogen patiëntgegevens onder de AVG worden verwerkt?

De AVG kent zes grondslagen voor de rechtmatige verwerking van persoonsgegevens: 1) toestemming van de betrokkene, of als verwerking *noodzakelijk* is voor 2) uitvoering van een overeenkomst, 3) voldoen aan een wettelijke verplichting, 4) bescherming van vitale belangen, 5) vervulling van een taak van algemeen belang of uitoefening van openbaar gezag of als sprake is van 6) een (zwaarwegender) gerechtvaardigd belang van de gegevensverantwoordelijke of een derde.

Verwerking van patiëntgegevens door een zorgaanbieder zal in de regel kunnen worden gebaseerd op de noodzaak van verwerking voor de uitvoering van de geneeskundige behandelingsovereenkomst en/of de toestemming van de patiënt (*informed consent*). Een schriftelijke (waaronder digitale) vastlegging van de toestemming van de patiënt (bijvoorbeeld in het medisch dossier) is noodzakelijk. Als de toestemming voor verwerking van patiëntgegevens reeds vóór inwerkingtreding van de AVG is verleend, dient binnen twee jaar vanaf inwerkingtreding van de AVG (25 mei 2018) te worden getoetst of die toestemming in overeenstemming met de strengere voorschriften van de AVG is verkregen. Alleen dan is het opnieuw vragen van toestemming niet vereist.

5. Staat de AVG in de weg aan verstrekking van patiëntgegevens aan een zorg- of ziektekostenverzekeraar?

De Wet marktordening gezondheidszorg (Wmg), de Zorgverzekeringswet (Zvw) en de Wet langdurige zorg (Wlz) regelen de verstrekking van gegevens van zorgaanbieders aan c.q. ten behoeve van zorg-/ziektekostenverzekeraars, voor zover dat voor uitvoering van de zorg-/ziektekostenverzekering of deze wetten noodzakelijk is (denk aan declaratie van zorgkosten of het uitvoeren van materiële controles). In de AVG is onder meer een uitzondering op het verbod tot het verwerken van persoonsgegevens bepaald, voor zover de verwerking noodzakelijk is voor '*doeleinden van het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten*'. De regelingen van de Wmg, Zvw en Wlz bieden een nationale rechtsbasis die onder de reikwijdte van deze uitzonderingsbepaling valt.

6. Wat zijn de rechten van de patiënt bij gegevensverwerking onder de AVG?

Een betrokkene heeft bij verwerking van zijn of haar persoonsgegevens recht op: 1) transparante informatie en communicatie, 2) inzage en rectificatie, 3) verwijdering ('recht op vergetelheid'), 4) beperking van de verwerking, 5) overdraagbaarheid van gegevens ('dataportabiliteit'), 6) het maken van bezwaar en 7) niet te worden onderworpen aan geautomatiseerde individuele besluitvorming, waaronder profilering.

Onder het recht van inzage is ook het recht op afgifte van een kopie geschaard. Nieuw is dat een eerste kopie kosteloos dient te worden verstrekt. Daar waar onder de huidige wetgeving voor afgifte van een kopie van een medisch dossier kosten in rekening mochten worden gebracht, kan dat onder de AVG bij een eerste kopie dus niet meer. Voor elke volgende kopie mag wel een redelijke vergoeding worden gerekend.

Dataportabiliteit houdt in dat de patiënt het recht heeft om geautomatiseerde verwerkte gegevens in een '*gestructureerde, gangbare en machineleesbare vorm*' te verkrijgen en het recht om de gegevens (rechtstreeks, indien technisch mogelijk) zonder verhindering aan een andere verwerkingsverantwoordelijke over te laten dragen. Met name bij de overstap naar een andere zorgaanbieder zal een beroep op dit recht relevant zijn, indien gegevens in een digitaal patiëntinformatiesysteem zijn geregistreerd.

7. Welke verplichtingen heeft de zorgaanbieder onder de AVG?

De verplichtingen van een zorgaanbieder bestaan uit 1) het treffen van passende technische en organisatorische maatregelen om naleving van de AVG te waarborgen, 2) gegevensbescherming 'door ontwerp en standaardinstellingen', 3) het sluiten van overeenkomst met een verwerker, 4) het bijhouden van een register van verwerkingsactiviteiten, 5) het zorgdragen voor persoonsgegevensbeveiliging, 6) het melden van datalekken aan de toezichthoudende autoriteit en betrokkene, 7) het uitvoeren van een gegevensbeschermingseffectbeoordeling en 8) het aanstellen van een functionaris voor de gegevensbescherming. Verplichtingen 2 t/m 8 worden in de volgende onderdelen toegelicht.

8. Wat is gegevensbescherming 'door ontwerp en standaardinstellingen'?

Gegevensbescherming door ontwerp en door standaardinstellingen (*privacy by design & privacy by default*) betekent dat bij het ontwikkelen en bij de (technische en organisatorische) instellingen van een programma, app, website of dienst maximale privacy wordt betracht. Kortom: niet méér verzamelen en bewaren van gegevens dan nodig is.

Voor zorgaanbieders is deze verplichting van belang met het oog op het ontwerp en gebruik van bijvoorbeeld websites (geen vakjes vooraf aanvinken; geen *opt-out*, maar *opt-in*), *social media* en *e-health*-applicaties (bijv. niet onnodig de locatie van gebruikers registreren). Het gaat echter niet alleen om (ICT-)opties, maar ook om het gebruik van privacyvriendelijke algemene voorwaarden. Privacyonderwerpen mogen niet in lange documenten worden 'weggestopt'. Transparantie staat voorop.

9. Wat is een verwerkersovereenkomst en wanneer is deze verplicht?

Het gebruik van een digitaal patiëntinformatiesysteem, *cloudservices* (voor e-mail), *e-health*-applicaties, de uitbesteding van de personeelsadministratie aan een administratiekantoor en het overlaten van de declaratie van zorg aan een factoringmaatschappij; allemaal voorbeelden van externe dienstverlening die gepaard gaan met externe verwerking van (bijzondere) persoonsgegevens ten behoeve van de zorginstelling. In zulke gevallen zijn de zorginstelling (als gegevensverantwoordelijke) en de leverancier/dienstverlener (als verwerker) verplicht een verwerkersovereenkomst ('bewerkersovereenkomst' onder de Wbp) te sluiten. In de verwerkersovereenkomst worden afspraken vastgelegd met het oog op naleving van de AVG, zoals over het doel van de verwerking, de beveiliging van gegevens, incidentenmanagement, het uitvoeren van audits en de voorwaarden voor inschakeling van subverwerkers.

10. Wat is het register van verwerkingsactiviteiten? Geldt deze verplichting voor alle zorgaanbieders?

De AVG bevat de verplichting voor verwerkingsverantwoordelijken en verwerkers om een register bij te houden van activiteiten waarbij persoonsgegevens worden verwerkt. In het register dienen onder meer te worden opgenomen 1) de contactgegevens van de verantwoordelijke (en haar eventuele vertegenwoordiger en functionaris voor de gegevensbescherming, 2) de verwerkingsdoeleinden, 3) de categorieën van betrokkenen en persoonsgegevens, 4) de categorieën van partijen aan wie de gegevens zullen worden verstrekt, 5) indien gegevens aan derde landen (buiten de EU) worden verstrekt: vermelding van het derde land en waar nodig documentatie omtrent de genomen passende waarborgen voor de bescherming van persoonsgegevens in dit derde land, 6) de beoogde bewaartermijnen, en 7) een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Deze verplichting geldt onder meer voor ondernemingen of organisaties die 250 of meer personen in dienst hebben of -ongeacht het aantal werknemers- als sprake is van stelselmatige verwerking van (bijzondere) persoonsgegevens en/of als die verwerking een hoog risico voor rechten en vrijheden van de betrokkene inhoudt. Ook (kleine) zorgaanbieders met minder dan 250 werknemers zullen dus een register moeten

bijhouden, aangezien zij doorgaans structureel bijzondere persoonsgegevens (medische gegevens) van patiënten verwerken.

11. Wat is een gegevensbeschermingseffectbeoordeling? Welke zorginstellingen zijn verplicht zo'n beoordeling uit te voeren?

Een gegevensbeschermingseffectbeoordeling (*DPIA: Data Privacy Impact Assessment)* is het in kaart brengen van de privacygevolgen van gegevensverwerking. Deze beoordeling dient te worden verricht als de soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, omvang, context en doeleinden een 'hoog risico' voor de rechten en vrijheden van natuurlijke personen inhoudt.

Een beoordeling is onder meer verplicht in geval van '*grootschalige verwerking*' van bijzondere persoonsgegevens, zoals in de zorg bij de verwerking van patiëntgegevens het geval kan zijn. In dit verband vindt de Artikel 29-werkgroep (het advies -en overlegorgaan van Europese privacytoezichthouders) de volgende omstandigheden van belang: het aantal betrokkenen, de hoeveelheid gegevens, de duur van de gegevensverwerking en de geografische reikwijdte van de verwerking. Als voorbeeld van grootschalige gegevensverwerking heeft de werkgroep een ziekenhuis genoemd en als voorbeeld voor niet-grootschalige gegevensverwerking een individuele arts.

Voor beantwoording van de vraag of sprake is van een hoog risico heeft de Artikel 29-werkgroep negen criteria opgesteld. Voor de zorg relevante criteria zijn, naast de grootschaligheid van de verwerking, of sprake is van de verwerking van 1) gevoelige gegevens of gegevens met een hoog persoonlijk karakter en 2) gegevens die betrekking hebben op kwetsbare betrokkenen (zoals -volgens de werkgroep- patiënten). De werkgroep gaat ervan uit dat er sprake is van een hoog risico indien minstens twee van de negen criteria van toepassing zijn. Niettemin kan in sommige gevallen ook de toepasselijkheid van één van de criteria bepalend zijn.

Als uit de beoordeling volgt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken, is voorafgaande raadpleging van de Autoriteit Persoonsgegevens (AP) verplicht.

12. Wat is een functionaris voor de gegevensbescherming en (vanaf) wanneer is aanstelling verplicht?

Een functionaris voor de gegevensbescherming (FG) (*Data Protection Officer*) ziet toe op de rechtmatige verwerking van persoonsgegevens binnen een organisatie. Volgens de AVG is een FG verplicht voor organisaties die hoofdzakelijk zijn belast met 'grootschalige verwerking' van bijzondere categorieën persoonsgegevens (zoals patiëntgegevens).

Voor zorginstellingen is van belang dat de Nederlandse wetgever op de komst van de AVG vooruitloopt. Vanaf 1 januari 2018 is het Besluit elektronische gegevensverwerking door zorgaanbieders van kracht. In dit besluit is de benoeming van een FG voor 'instellingen' als bedoeld in de Wkkgz verplicht gesteld, voor het geval sprake is van verwerking van bijzondere persoonsgegevens 'op grote schaal'. Alleen solistisch werkende zorgverleners vallen niet onder de definitie van instelling.

Voor de uitleg van het begrip ‘op grote schaal’ sluit het Besluit aan bij het begrip ‘grootschalige verwerking’ uit de AVG. De Artikel 29-werkgroep heeft als voorbeeld voor grootschalige gegevensverwerking een ziekenhuis genoemd en als voorbeeld voor niet-grootschalige gegevensverwerking, een individuele arts.

Voor zorgaanbieders die niet solistisch werken, geldt dus in beginsel dat zij reeds per 1 januari 2018 over een FG dienen te beschikken.

Een organisatie kan kiezen voor een interne of externe FG. De functie van FG mag met een andere functie worden gecombineerd, maar mag daarmee niet conflicteren.

Meer weten?
Voor meer informatie of advies over privacyrecht kunt u contact opnemen met Niels van den Burg (n.vandenburg@kbsadvocaten.nl) of Erik Luijendijk (e.luijendijk@kbsadvocaten.nl).