Privacy in de zorg en de rol van de cliëntenraad

Met de inwerkingtreding van de Algemene verordening gegevensbescherming (AVG) op 25 mei jl. is de privacywetgeving in de hele Europese Unie hetzelfde. De Wet bescherming persoonsgegevens (Wbp) wordt daarmee buiten werking gesteld.

Deze whitepaper van auteur Yvonne Nijhuis (Advocaat Kienhuis Hoving) in samenwerking met NCZ, geeft, op hoofdlijnen, de gevolgen van de AVG en andere zorgspecifieke wet- en regelgeving betreffende privacy voor de zorgsector weer en licht daarbij de rol van de toezichthouders en de cliëntenraad (CR) toe.

Wat blijft hetzelfde door de AVG?

Met de AVG blijft de (inhoud van de) reeds bestaande zorgspecifieke wet- en regelgeving ongewijzigd. Dit betekent onder meer dat de Wet op de geneeskundige behandelingsovereenkomst (WGBO), de Wet kwaliteit, klachten en geschillen zorg (Wkkgz), Wet op de beroepen in de individuele gezondheidszorg (Wet BIG), Zorgverzekeringswet (Zvw) en de Wet marktordening gezondheidszorg (Wmg) van kracht zijn naast de AVG.

De AVG is voor zorgaanbieders op onderdelen vooral een aanscherping en aanvulling op de Wbp. Daarom eerst een uiteenzetting van verplichtingen voor zorgaanbieders die hetzelfde blijven of minimaal worden aangescherpt in de AVG:

- De zorgaanbieder informeert patiënten over de persoonsgegevens die hij verwerkt. Patiënten hebben daarnaast het recht op inzage in hun persoonsgegevens, deze te laten aanvullen, corrigeren of af te schermen. Daarnaast hebben patiënten het recht bezwaar te maken tegen de verwerking van (bepaalde) persoonsgegevens.

- Inbreuken op de beveiliging van persoonsgegevens (datalekken) meldt de zorgaanbieder bij de Autoriteit Persoonsgegevens (AP) en bij de patiënt. Er is sprake van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens. Het gaat om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een zorgaanbieder zonder dat dit de bedoeling was van deze zorgaanbieder.

- Tenslotte behoudt de AP de mogelijkheid om boetes op te leggen indien de AVG wordt overtreden door de zorgaanbieder.

Wat verandert er door de AVG?

De AVG legt in de zorgsector aan zorgaanbieders ook een aantal extra verplichtingen op. Omdat zorgaanbieders met 'bijzondere persoonsgegevens' werken, zijn die regels strikt. Het gaat om de volgende verplichtingen:

- De zorgaanbieder ziet erop toe dat bij de ontwikkeling van nieuwe verwerkingssystemen bewust omgegaan moet worden met privacyrisico's. Deze privacyrisicobeheersing wordt ook wel als 'privacy by design' en 'privacy by default' aangeduid. 'Privacy by design' houdt in dat privacywaarborgen al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) aandacht krijgen. 'Privacy by default' zorgt dat applicaties die om persoonlijke gegevens vragen automatisch staan ingesteld op de meest privacyvriendelijke stand.

- Een zorgaanbieder moet een register van gegevensverwerkingen aanleggen, waarin bijgehouden wordt welke gegevens worden verwerkt, met welk doel en aan wie deze gegevens worden verstrekt door de zorgaanbieder. In het register staat ook steeds vermeld waarom de zorgaanbieder de gegevens mag gebruiken op grond van de AVG (bijvoorbeeld omdat de zorgaanbieder wettelijk verplicht is de gegevens te verwerken of omdat de verwerking noodzakelijk is met het oog op de behandeling van de patiënt).

- Wanneer een verwerking gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen c.q. patiënten voert de zorgaanbieder een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens (zogenoemde 'Data Protection Impact Assessments' (DPIA)). De AP heeft een lijst met voorbeelden van soorten verwerkingen opgesteld waarvoor het uitvoeren van een DPIA verplicht is.[1] De lijst is niet uitputtend.

- Wanneer de zorgaanbieder persoonsgegevens laat verwerken door andere verwerkers, moet de zorgaanbieder hierover afspraken vastleggen in een verwerkersovereenkomst. Denk bijvoorbeeld aan de salarisadministratie, indien deze is uitbesteed aan een derde partij. Dus met een ieder, anders dan de medewerkers of ingehuurd personeel, die toegang heeft tot de persoonsgegevens.

- Tot slot moet een zorgaanbieder (in beginsel) een functionaris gegevensbescherming (FG) aanstellen. Deze plicht geldt al voor de meeste zorgaanbieders onder de bestaande regelgeving sinds januari 2018.[2]

[1] De lijst is te vinden in de volgende link; https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-ap-voor-een-verplichte-dpia-6667.
[2] Zie voor meer informatie over de positie van de FG onder meer pagina 27 en verder in de volgende link: https://www.zorgictzorgen.nl/wp-content/uploads/2018/03/Model_privacyreglement_ggz_januari_2018.pdf.

Toezicht op privacy

De AP ziet toe op, kort gezegd, de verwerking en beveiliging van persoonsgegevens. Met name daar waar privacy-aangelegenheden effect hebben op de kwaliteit van zorg en vice versa werkt de AP samen met de Inspectie voor de Gezondheidszorg en Jeugd (IGJ). De IGJ ziet toe op de kwaliteit van zorg. De wijze van omgang met persoonsgegevens is hier onderdeel van voor zover deze de kwaliteit en veiligheid van de zorgverlening raakt.

Een voorbeeld van inspectietoezicht in dit kader vond eind 2017 plaats, toen de IGJ is gestart met verkennende inspectiebezoeken op het gebied van e-health bij zorgaanbieders. De IGJ onderzocht of e-health veilig wordt ingezet. De conclusies op basis van dit inspectietoezicht zijn onder meer dat elektronische gegevensuitwisseling en informatiebeveiliging van e-health voor verbetering vatbaar zijn.

Elektronische gegevensuitwisseling en informatiebeveiliging

De conclusies van het inspectietoezicht eind 2017 zijn terug te voeren op twee, recent ingevoerde, zorgspecifieke regelingen. Ten aanzien van elektronische gegevensuitwisseling geldt allereerst de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabv). De Wabv vormt een aanvulling op de AVG en de WGBO en geeft weer welke extra rechten en waarborgen patiënten hebben wat betreft hun privacy bij elektronische gegevensuitwisseling. Met een elektronische uitwisselingssysteem wordt bedoeld:

> *"een systeem waarmee zorgaanbieders op elektronische wijze, dossiers, gedeelten van dossiers of gegevens uit dossiers voor andere zorgaanbieders raadpleegbaar kunnen maken, waaronder niet begrepen een systeem binnen een zorgaanbieder, voor het bijhouden van een elektronisch dossier".*

Niet alle bepalingen uit de Wabv zijn gelijktijdig in werking getreden. Sommige wettelijke bepalingen gelden per 1 juli 2017 en andere per 1 juli 2020.

Per 1 juli 2017:

- Moet de patiënt op grond van de Wabv door de zorgaanbieder worden geïnformeerd over zijn rechten bij elektronische gegevensuitwisseling, de wijze waarop hij zijn rechten kan uitoefenen, de werking van het elektronische uitwisselingssysteem en welke zorgaanbieders zijn aangesloten op het systeem. Ook zal de zorgaanbieder de patiënt moeten informeren als er een nieuwe categorie zorgaanbieder(s) gebruik maakt van het door de zorgaanbieder gebruikte elektronische uitwisselingssysteem.

- Een zorgaanbieder mag slechts gegevens van een patiënt beschikbaar stellen via een elektronisch uitwisselingssysteem voor zover de cliënt daartoe uitdrukkelijk toestemming heeft gegeven.

Per 1 juli 2020:

- De zorgaanbieder moet gespecificeerde toestemming van de patiënt verkrijgen voordat gegevens elektronisch worden uitgewisseld.

- De zorgaanbieder dient een registratie bij te houden van de door zijn patiënten verleende toestemmingen.

- De patiënt heeft recht op het (kosteloos) verkrijgen van een elektronische inzage en afschrift van het eigen medisch dossier.

- De patiënt heeft tot slot het recht op een elektronisch overzicht van wie bepaalde informatie in een elektronisch uitwisselingssysteem beschikbaar heeft gesteld en op welke datum ('logging').[3]

Naast de verplichtingen uit de AVG en de Wabv gelden vanaf 1 januari 2018 specifieke functionele, technische en organisatorische eisen voor een elektronisch gegevensuitwisselingssysteem en een intern zorginformatiesysteem die een zorgaanbieder gebruikt. Deze eisen zijn neergelegd in het Besluit elektronische gegevensverwerking door zorgaanbieders (Besluit). In dit Besluit is allereerst opgenomen dat de zorgaanbieder verplicht is tot benoeming van een functionaris voor de gegevensbescherming. Bovendien verplicht het Besluit dat over het gebruikte systeem beleid, procedures en verantwoordelijkheden zijn vastgelegd en tot slot dat de systemen voldoen aan NEN-7510, NEN-7512 en NEN-7513.

Wat is de rol van de cliëntenraad?

De CR kan een rol spelen in het verdere verloop van bovengenoemde privacywetgeving. Van groot gewicht voor de positie van de CR in zijn algemeenheid is dat de CR het recht heeft gevraagd en ongevraagd te adviseren over alle onderwerpen die voor patiënten van belang zijn op grond van de Wet medezeggenschap cliënten zorginstellingen (Wmcz). Op hoofdlijnen ziet de rol van de CR er als volgt uit:

- De wijze waarop de zorgaanbieder haar patiënten informeert over de wijze van verwerking van persoonsgegevens valt onder het verzwaard adviesrecht van de CR (artikel 3 lid 1 sub l Wmcz). Voorts kan de CR vragen aan de zorgaanbieder hoe ervoor wordt zorggedragen dat de medewerkers van de zorgaanbieder zich bewust zijn van de wijze waarop met informatie en persoonsgegevens moet worden omgegaan en hoe de zorgaanbieder hierop toeziet in zijn beleid en nadere uitvoering.

[3] Zie voor meer informatie de 'Juridische factsheet Wet cliëntenrechten bij elektronische verwerking van gegevens' van de Rijksoverheid.

- Ten aanzien van het bijhouden van verwerkingsactiviteiten in een register, is het ook belangrijk dat de CR zich kan vinden in welke (persoons)gegevens allemaal worden geregistreerd en verwerkt, en met welk doel dat gebeurt. Kan de CR zich in die verwerkingsactiviteiten niet vinden, dan kan de CR een (ongevraagd) advies geven aan de zorgaanbieder.

- De CR heeft het recht op informatie over de uitkomsten van de DPIA. Als er sprake is van een hoog privacyrisico bij de verwerking en bescherming van gegevens, kan het noodzakelijk zijn om maatregelen te treffen omdat de gegevens niet voldoende worden beschermd. De CR kan vervolgens adviseren over de uitvoering van deze getroffen maatregelen door de zorgaanbieder.

- Voor de CR is het bovendien van belang om te weten of de zorgaanbieder toestemming van patiënten voor de verwerking en het delen van gegevens heeft gevraagd, of dat er opnieuw toestemming gevraagd moet worden onder het strengere regime van de AVG. Mocht dat laatste aan de orde zijn, dan is het van belang om te weten hoe en wanneer het (opnieuw) vragen van toestemming geschiedt. Dit valt ook onder het verzwaard adviesrecht van de CR (artikel 3 lid 1 sub l Wmcz).

- Tot slot in zijn algemeenheid heeft de CR een adviesrecht in het kader van belangrijke wijzigingen binnen de organisatie van de zorgaanbieder en ten aanzien van de systematische bewaking, beheersing en/of verbetering van de kwaliteit van de aan de cliënten te verlenen zorg heeft de CR een verzwaard adviesrecht. In dat kader kan de CR bijvoorbeeld ook een adviesrecht hebben bij de ontwikkeling van nieuwe methodes, denk aan de invoering van nieuwe ICT-systemen of elektronisch patiëntendossiers (EPD).

Voor vragen over de whitepaper kunt u contact opnemen met:
Yvonne Nijhuis, Advocaat
Kienhuis Hoving, advocaten en notarissen
yvonne.nijhuis@kienhuishoving.nl
Of telefonisch via secretaresse Renée Middelveld: 053 480 4722

Voor vragen over cliëntenraden in de zorg kunt u contact opnemen met:
Marika Biacsics, Netwerkvoorzitter
Netwerk Cliëntenraden Zorg (NCZ)
marika@ncz.nl
Of telefonisch: 06 51 22 25 05