

Leidraad voor de artsen inzake de Algemene Verordening Gegevensbescherming

Doc	a165001
Publicatiedatum	27/04/2019
Origine	NR
	Persoonlijke levenssfeer
Thema's	Beroepsgeheim
	GDPR

Leidraad voor de artsen inzake de Algemene Verordening Gegevensbescherming

Op 27 april 2016 heeft het Europees Parlement en de Europese Raad een nieuwe verordening inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens uitgebracht, de Algemene Verordening Gegevensbescherming (hierna "AVG"), die in werking trad op 25 mei 2018.

Omdat de arts bij de uitoefening van zijn beroep gezondheidsgegevens en andere gevoelige informatie van zijn patiënten verwerkt, is het aangewezen dat hij deze wetgeving incorporeert in zijn dagelijkse praktijk en de ontwikkelingen hiervan nauw opvolgt.

Aangezien verscheidene deontologische principes(1) zeer nauw samenhangen met het respect op privacy van de patiënt, heeft de nationale raad van de Orde der artsen dit advies opgesteld en een mogelijkheid tot vraagstelling voorzien via het e-mailadres : privacy@ordomedic.be.

1. Algemeen

De AVG is een uitdieping van de bestaande regels omtrent privacy. De arts die reeds de bestaande privacyregelgeving respecteerde, zal weinig nieuwe regels moeten implementeren.

Algemene principes van de regelgeving die nauw samenhangen met het recht op privacy, bijvoorbeeld bepaalde rechten van de patiënt(2) en het beroepsgeheim, blijven bestaan zoals voorheen.

Een individuele arts of een groepspraktijk hoeft voor de implementatie van de nieuwe regelgeving geen buitensporige uitgaven te doen. De nationale raad wenst zijn leden te waarschuwen voor bedrijven die buitensporige kosten aanrekenen voor de toepassing van de AVG in hun praktijk.

De nieuwe regelgeving kent evenwel enkele nieuwe begrippen, zoals een "functionaris gegevensbescherming(3)" of een "register van de verwerkingsactiviteiten". Deze begrippen zullen hierna aan bod komen.

2. Aanwijzing van een functionaris voor gegevensbescherming

Een functionaris voor gegevensbescherming (hierna "DPO") informeert en adviseert de

verwerkingsverantwoordelijke of de verwerker over hun verplichtingen uit hoofde van de AVG of andere gegevensbeschermingsbepalingen. Hij ziet toe op de naleving van de regelgeving en het beleid errond, zoals de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van de bij de verwerking van persoonsgegevens betrokken personen(4). Daarnaast werkt de DPO samen met de toezichthoudende autoriteit en treedt hij hiervoor op als contactpunt.(5)

Een individuele arts of een groepspraktijk hoeft geen DPO aan te wijzen. Slechts voor de verwerking van een groot aantal gezondheidsgegevens is de aanstelling verplicht. Dit is het geval bij ziekenhuizen of structuren waar minstens 250 werknemers aanwezig zijn.

3. Register van de verwerkingsactiviteiten

Elke arts moet een register van de verwerkingsactiviteiten bijhouden. Het is een bestand waarin de arts beschrijft welke persoonsgegevens hij verzamelt, hoe hij deze beveiligt, waarom hij deze verzamelt, waar hij deze bewaart, voor hoe lang hij deze bewaart en of hij deze doorstuurt.(6)

Het opmaken van dergelijk register is een proces waarbij de arts bewust gaat nadenken over hoe hij omgaat met persoonsgegevens van patiënten en/of personeel. Het is een aanzet tot een herstructurering van het datamanagement indien de arts vaststelt dat hij bijvoorbeeld bepaalde persoonsgegevens niet goed beveiligt of niet meer nodig heeft voor de uitoefening van zijn beroep van arts.

De nationale raad stelt binnenkort een voorbeeld ter beschikking van hoe een register van de verwerkingsactiviteiten er kan uitzien.

4. Andere personen dan de arts die toegang hebben tot de persoonsgegevens van de patiënt

De arts wijst de categorieën van personen aan die toegang hebben tot de persoonsgegevens van patiënten. Hierbij wordt hun hoedanigheid ten opzichte van de verwerking van de betrokken gegevens nauwkeurig omschreven en gedocumenteerd. (7) Dit wordt toegevoegd aan het register van de verwerkingsactiviteit.

De arts zorgt ervoor dat de aangewezen personen door een wettelijke of statutaire verplichting, of door een evenwaardige contractuele bepaling ertoe gehouden zijn het vertrouwelijk karakter van de betrokken gegevens in acht te nemen. Iedereen die toegang heeft tot de patiëntendossiers moet een vertrouwelijkheidsclausule hebben ondertekend in hun arbeids- of ander samenwerkingscontract.

Toegang betekent niet dat deze mensen ook effectief met de patiëntendossiers aan de slag gaan. Slechts de mogelijkheid om deze dossiers te consulteren is voldoende. De ondertekening van dit contract is een uitgelezen moment om deze medewerkers te informeren over de rechten en plichten bij het werken met persoonsgegevens.

5. Te nemen maatregelen (algemeen)

Voor de uitoefening van zijn beroep, verzamelt de arts gegevens over de gezondheid van zijn patiënten. Het betreft een bijzondere categorie van persoonsgegevens.(8) Gezondheidsgegevens zijn persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder ook wordt verstaan gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.(9)

De arts neemt alle nodige maatregelen om het recht op privacy van de patiënt te respecteren, de gevoelige data optimaal te beveiligen en een "gegevenslek" te

voorkomen.

6. Doorgifte van persoonsgegevens

Er zijn heel wat situaties denkbaar waarbij de arts de gezondheidsgegevens van zijn patiënten doorgeeft. Ofwel worden de persoonsgegevens doorgegeven aan de patiënt zelf(10), ofwel worden deze doorgegeven aan derden(11).

Bij een doorgifte van gezondheidsgegevens moet de arts zich steeds afvragen of hij de gegevens mag doorsturen naar een derde ontvanger. Het beroepsgeheim laat niet toe dat de arts medische gegevens van zijn patiënten aan derden verstrekt. De arts kan derhalve slechts gezondheidsgegevens doorgeven indien hiervoor een wettelijke basis bestaat.

Bij een doorgifte van gezondheidsgegevens aan derden, op vraag van de patiënt, dient de arts zich de vraag te stellen of de patiënt uit hoofde van zijn zelfbeschikkingsrecht niet zelf het beste is geplaatst om te bepalen met wie en welke informatie hij wenst te delen.

De doorgifte van gezondheidsgegevens zelf moet op een veilige manier gebeuren en vraagt extra veiligheidsmaatregelen. Gezondheidsgegevens mogen enkel digitaal worden doorgestuurd via systemen met een multi-factor authenticatie. De arts mag bijgevolg geen medische gegevens via onbeveiligde e-mail versturen, zelfs niet indien de patiënt hiervoor de toestemming geeft.

De arts dient beveiligde informatienetwerktoepassingen te gebruiken, met een beschermingsniveau volgens de huidig geldende regels.

7. Software

De arts die gebruik maakt van software of nieuwe software aankoopt voor het management van zijn praktijk of de beveiliging van persoonsgegevens, moet steeds navraag doen bij de leverancier over de privacy settings. De leverancier van de software moet de AVG respecteren en hierover transparant communiceren met de arts. De arts blijft evenwel medeverantwoordelijk mocht de software niet voldoen aan de wettelijke voorwaarden.

Bij het inschakelen van derden bij de verwerking van persoonsgegevens onder de verantwoordelijkheid van de arts, moet de samenwerking, de beveiliging en het verloop van de verwerking contractueel vastgelegd worden in een verwerkingsovereenkomst. Veel bedrijven hebben hier reeds modellen voor en pasten hun algemene voorwaarden aan. Het is aangewezen om na te gaan of deze bepalingen afdoende zijn.

8. Bewustmaking van de nieuwe regelgeving

De arts maakt de medewerkers in zijn praktijk bewust van de veiligheidsmaatregelen die de patiëntengegevens beschermen en bepaalt welke personen tot welke gegevens toegang hebben.

Indien er een onbevoegde persoon toegang kreeg tot gezondheidsgegevens van patiënten of andere gevoelige informatie die de arts in de context van zijn activiteit bijhoudt, is er sprake van een "gegevenslek"(12).

Gegevenslekken moeten geregistreerd worden en, afhankelijk van de ernst, binnen de 72 uren gemeld worden aan de gegevensbeschermingsautoriteit en de betrokkenen. (13)

9. Toekomst

Verschillende overheden, instellingen en andere betrokken actoren bij het verwerken van gezondheidsgegevens beraden zich over deze nieuwe Europese regelgeving. In de toekomst zullen Europese richtlijnen preciseren hoe actoren binnen de gezondheidszorg moeten omgaan met patiëntengegevens.

- (1) Het gaat voornamelijk om hoofdstuk 2, "Respect" van de Code voor Medische Deontologie
- (2) Artikel 9 en 10 van de Wet van 22 augustus 2002 betreffende de rechten van de patiënt (recht op een veilig bewaard patiëntendossier, recht op de bescherming van de persoonlijke levenssfeer)
- (3) De veelgebruikte Engelse benaming is "Data Protection Officer" of "DPO"
- (4) Bijvoorbeeld het secretariaat, het verplegend personeel die de arts bijstaat
- (5) Artikel 39 Algemene Verordening Gegevensbescherming
- (6) Artikel 30 Algemene Verordening Gegevensbescherming
- (7) Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens
- (8) Artikel 9 Algemene Verordening Gegevensbescherming
- (9) Artikel 4, 15 Algemene Verordening Gegevensbescherming
- (10) Bijvoorbeeld de resultaten van een onderzoek of bij de uitoefening van het recht op inzage in het patiëntendossier
- (11) Bijvoorbeeld aan collega-artsen die de patiënt behandelen in het kader van gedeeld beroepsgeheim, aan het RIZIV op basis van bijzondere wetgeving, etc.
- (12) Bijvoorbeeld inbraak, hacking, gezondheidsgegevens die worden verstuurd aan de verkeerde persoon, etc.
- (13) Artikel 33 Algemene Verordening Gegevensbescherming