AVG: impact op huisartsenpraktijken

Korte introductie op de impact van de AVG op huisartsenpraktijken,
wat je kan doen en waar je rekening mee kan houden.

September 2020
Update april 2024
Amsterdam

Inhoudsopgave

1. De wet AVG, AVG regels en definities
2. Verwerkingsovereenkomsten en privacy verklaring (op de website)
3. Veilig Incident Melden (VIM procedure)
4. Wat is een datalek?
5. Privacy in de fysieke ruimte, aan de telefoon en achter de computer
6. (On) veilig e-mailen

1. De wet AVG

- AVG staat voor Algemene Verordening Gegevensbescherming.
- Het is een uniform beleid in de EU met strengere handhavingsmogelijkheden (o.a. hogere boetes en meer bevoegdheden).
- Doel van de AVG: het beschermen van privacy van ‘betrokkenen’ (individuen) m.b.t. het *verwerken* van hun *persoonsgegevens.*
- **Als zorgaanbieder ben je verplicht om aan de AVG te voldoen.**

AVG regels

- Alleen medische gegevens verwerken wanneer er een grondslag is.
- De rechten van de betrokkenen staan centraal. De huisarts/zorgverlener is slechts de hoeder van het patiëntendossier.

Grondslagen centraal

Op basis hiervan mag je persoonsgegevens verzamelen:

- Gebruik alleen gegevens die nodig zijn
- Bewaar gegevens niet langer dan nodig

De bescherming van de betrokkene staat altijd centraal!

Rechten van de betrokkene

Mensen moeten controle kunnen uitoefenen

Rechten van de betrokkenen

Wettelijke definities

Wat zijn persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een **naam**, een **identificatienummer**, **locatiegegevens**, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, **fysiologische**, genetische, **psychische**, economische, culturele of sociale identiteit van die natuurlijke persoon.

Wat zijn bijzondere persoonsgegevens: verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over **gezondheid**, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.

Wat zijn verwerkingen: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het **verzamelen**, **vastleggen**, ordenen, structureren, opslaan, bijwerken of **wijzigen**, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of **vernietigen** van gegevens.

2. Verwerkingsovereenkomst

Wat is een verwerkingsovereenkomst?

- De afspraak met een leverancier over hoe de leverancier om moet gaan met de persoonsgegevens die hij in opdracht van jou verwerkt.
- Bijvoorbeeld: VIPLive, EZDA, LSP/Whitebox, Zorgdomein, SecureMail, Hosting e-mail verkeer, HIS, ANH, ASP, etc.
- Gebruik de voorbeeldlijst van de ROHA
- Bedenk voor je eigen praktijk: is jullie lijst van contracten en verwerkings-overeenkomsten compleet? Zijn alle overeenkomsten getekend?

Privacy verklaring op de website

- Een privacy verklaring is eigenlijk een ‘moetje’ van de AVG, waarmee je als praktijk aan je cliënten uitlegt hoe je omgaat met de verzamelde persoonsgegevens.
- Gebruik het voorbeeld van de LHV , pas het aan voor je eigen praktijk en zet het op je website.

3. Veilig Incident Melden

- Vanaf 1 juli 2016 is het verplicht om een VIM-procedure te hebben in je praktijk.
- Informatieveiligheidsincidenten zijn alle zaken die tot een inbreuk hebben geleid van beschikbaarheid, integriteit of vertrouwelijkheid van informatie of zaken die daar bijna toe hebben geleid, of kunnen leiden
- Incidenten worden geregistreerd samen met de betrokken zorgverlener, collega's en andere deskundigen, en worden onderzocht.
- Als het nodig is, worden zo snel mogelijk maatregelen getroffen ter waarborging van de kwaliteit van de zorg
- Meldingen worden periodiek geanalyseerd. De betrokkenen worden ingelicht over uitkomsten en conclusies van de analyse.
- Vervolgens worden eventuele (structurele) verbetermaatregelen doorgevoerd.

4. Wat is een datalek?

- Verlies of diefstal of onrechtmatige verwerking van tot de persoon herleidbare gegevens.
- Wanneer niet uit te sluiten is dat data verloren zijn gegaan of onrechtmatig worden verwerkt.
- Vergelijkbaar met de VIM melding; ook datalekken moeten als zodanig worden geregistreerd.
- Meld een datalek altijd zo spoedig mogelijk (binnen 24 uur) bij de security officer of de functionaris gegevensbescherming van de ROHA, ook bij twijfel!
- De security officer of de functionaris gegevensbescherming adviseren je over de eventuele vervolgstappen (conform het ROHA-protocol meldplicht datalekken) en zorgen voor de registratie in het Datalek Register. Wanneer noodzakelijk doen ze melding bij de Autoriteit Persoonsgegevens.

5. Privacy in de fysieke ruimte

- Let op briefjes, recepten, dossiers, aantekeningen etc.;
- Zorg voor een Clean Room en Clean Desk beleid;
- Kasten met sloten en deuren met sloten in ruimtes met privacygevoelige informatie;
- Kijk met een privacy-blik door de praktijk en spreek elkaar aan wanneer je iets ziet of niet vertrouwd.

Privacy aan de telefoon

Denk eens na over de volgende situaties:

- Wat doe je aan de balie met privacygevoelige gesprekken?
- De arts krijgt een telefoontje tijdens spreekuur, wat dan?
- De arts houdt telefonisch spreekuur en de deur staat open...
- En ook adolescenten en hun rechten; wat mag een moeder/vader vragen over een 12-16 jarige?
- Wat mag je de buurvrouw vertellen aan de telefoon?

Privacy achter de computer

- Afspraken rondom laptop, mobiel/tablet en persoonsgegevens (wachtwoorden, opslag, etc.) Waar bewaar je bijvoorbeeld je wachtwoorden?
- Vergrendel je computer altijd wanneer je even wegloopt;
- Zorg voor een schoon bureaublad op de computer;
- Gooi oude e-mails weg en de prullenmand van zowel je e-mail als je computer regelmatig leeg;
- Inloggen en wachtwoorden > zorg altijd voor tweefactorauthentificatie (2FA);
- Onveilig WIFI gebruik > ga nooit met je werklaptop of telefoon op openbare WIFI-netwerken (hackers kunnen via een openbaar WIFI-netwerk gemakkelijker je computer of telefoon binnenkomen);
- Waarnemers en tijdelijke krachten > zorg dat ook zij met persoonlijke accounts op netwerken en in de applicaties kunnen.

6. (On) veilig e-mailen

- Bijzondere persoonsgegevens mogen **niet** verstuurd worden over de gewone e-mail;
- Toegang tot de mailserver gebeurt altijd met tweefactorauthenticatie;
- Gebruik voor je e-mail alleen sterke wachtwoorden, geen zwakke en gemakkelijk te kraken wachtwoorden zoals 'Welkom123';
- Gebruik je e-mail niet als opslag van privacygevoelige informatie;
- Gebruik Zorgmail, VipLive, Secure Mail en het patiëntenportaal om veilig te mailen.