Algemene Verordening Gegevensbescherming (AVG)

Op 25 mei 2018 treedt de Algemene Verordening Gegevensbescherming (AVG) in werking. Deze vervangt de Wet bescherming persoonsgegevens. Met de komst van deze wet worden de regels rond de bescherming van persoonsgegevens flink aangescherpt. Wat moeten tandartspraktijken regelen om aan de nieuwe wettelijke eisen te voldoen? Lees over de 6 belangrijkste zaken, volg een webinar of kom naar de praktische workshops.

Alles weten over de AVG? **Bekijk het webinar <https://www.onlineseminar.nl/knmt/>** waarin jurist Roxanne Kroes en projectleider ICT Martin Rozeboom u informeren over de nieuwe privacywetgeving en wat u moet regelen in de mondzorgpraktijk.

In het eerste kwartaal van 2018 kunt u ook deelnemen aan **speciale, praktische AVG-workshops <https://www.knmt.nl/avgworkshop>** waarin u uw privacy-beleid kunt vormgeven.

1. Informatieplicht aan patiënten over de gegevensverwerking(-en)

Wat?

De AVG eist dat u nog transparanter bent over de persoonsgegevens die door u worden verwerkt. In duidelijke, eenvoudige taal moet u aan de patiënt uitleggen wat u precies met diens persoonsgegevens doet en hoe lang u bijvoorbeeld deze gegevens bewaard. Ook moet u de patiënt wijzen op de rechten die hij heeft, zoals het recht om het dossier in te zien of om gegevens te laten aanpassen. Bovendien moet de patiënt er door u op worden gewezen dat de mogelijkheid bestaat om een klacht in te dienen bij de Autoriteit Persoonsgegevens.

Hoe?

Dit kunt u onder andere doen door een privacy statement op uw website te plaatsen. Heeft u een **KNMT-Praktijkwebsite <https://www.knmt.nl/producten/knmt-praktijkwebsite-direct>** van Pharmeon? Dan wordt dit voor u geregeld. Maak anders gebruik van **het model-privacy- en cookiestatement <https://www.knmt.nl/system/files/model_privacy-_en_cookieverklaring_1.0.docx>** (docx) van de KNMT. Lukt openen niet? Sla het document dan eerst op op uw computer.

2. Treffen van passende beveiligingsmaatregelen

Wat?

U dient als verwerkingsverantwoordelijke passende technische en organisatorische beveiligingsmaatregelen te treffen om de persoonsgegevens goed te beveiligen. Het aansluiten bij goedgekeurde certificeringsmechanismen (denk hierbij aan de NEN-normen) kan worden gebruikt als element om hiermee aan te tonen dat u aan deze verplichting heeft voldaan.

Hoe?

Doorloop de 'technische maatregelen' uit **de checklist Privacy & informatiebeveiliging <https://www.knmt.nl/system/files/22408_checklist_privacy_en_informatiebeveiliging-def.pdf>** (pdf) van de KNMT.

3. Het vaststellen en naleven van een privacybeleid

Wat?

Onderdeel van de passende organisatorische beveiligingsmaatregelen is dat u een passend privacybeleid opstelt en in uw praktijk implementeert. Het is belangrijk om binnen uw praktijk vast te stellen wie welke rol heeft in het kader van de gegevensverwerking(-en). Uiteraard dient u ook uw medewerkers hiervan goed op de hoogte te brengen, zodat zij kunnen bijdragen aan een juiste toepassing van het privacybeleid.

Hoe?

Maak gebruik van het **model-privacybeleid <https://www.knmt.nl/system/files/model-intern_privacybeleid_1.0.docx>** (docx, versie 1.0) en **de toelichting op het model <https://www.knmt.nl/system/files/model-intern_privacybeleid_1.0_toelichting.docx>** (docx) van de KNMT. Lukt openen niet? Sla het document dan eerst op uw computer.

Met het model kunt u zelf uw privacybeleid opstellen of in januari en februari 2018 **deelnemen aan een praktische AVG-workshop <https://www.knmt.nl/avgworkshop>** om het privacybeleid op te stellen en te implementeren.

4. Verplichting om een verwerkingsregister bij te houden

Wat?

Tandartsen hebben onder de AVG een verantwoordingsplicht. U moet kunnen aantonen dat u zich houdt aan de AVG. Dit doet u onder meer door het instellen van een register waarin u alle gegevensverwerkingen registreert. In dit register moet een aantal verplichte elementen zijn opgenomen, zoals:

- de contactgegevens van de verwerkingsverantwoordelijke (en eventueel van de functionaris gegevensbescherming);
- de categorieën van gegevens die u verwerkt;
- de categorieën van betrokkenen (om wiens gegevens gaat het);\
- de categorieën van ontvangers (aan wie worden gegevens verstrekt);
- de doeleinden waarvoor u gegevens verwerkt;
- welke beveiligingsmaatregelen u heeft getroffen;
- de bewaartermijnen;
- en -indien hiervan sprake is- : informatie over doorgifte van gegevens naar landen buiten de EU.

Hoe?

Maak gebruik van **het model-verwerkingsregister <https://www.knmt.nl/system/files/model_verwerkings_-_en_datalekkenregister_versie_1.0_-20_dec_2017.xlsx>** (xlsx) van de KNMT (lees ook **de toelichting <https://www.knmt.nl/system/files**

/toelichting_model_verwerkings-_en_datalekkenregister.pdf> ; pdf). Er zijn ook leveranciers van tandheelkundige software die registers zullen aanbieden; vraag ernaar bij uw leverancier.

5. Het sluiten van ‘verwerkersovereenkomsten’

Wat?

Als u voor uw gegevensverwerking gebruik maakt van de diensten van derden (bijvoorbeeld een softwareleverancier tandheelkundig informatiesysteem of factoringmaatschappij), kan deze derde als ‘verwerker’ worden aangemerkt en moet u met deze partij een verwerkersovereenkomst afsluiten. In deze overeenkomst worden specifieke afspraken gemaakt over de omgang met de persoonsgegevens.

Hoe?

Zorg dat u met alle derde partijen die als een ‘verwerker’ kunnen worden aangemerkt een verwerkersovereenkomst hebt gesloten. U kunt hiervoor gebruikmaken van de model-verwerkersovereenkomst van de KNMT.

Model-verwerkersovereenkomst <https://www.knmt.nl/system/files /knmt_template_verwerkersovereenkomst_.docx> (docx)

Krijgt u een verwerkersovereenkomsten aangeboden ter ondertekening, bijvoorbeeld van factoringbedrijven of leveranciers van praktijksoftware? Benut onze checklist, zodat u weet waar u op kunt letten.

Checklist verwerkersovereenkomst <https://www.knmt.nl/system/files /checklist_verwerkersovereenkomst.pdf> (pdf)

6. Alle datalekken moeten worden geregistreerd

Wat?

De meldplicht voor datalekken geldt al langer. De huidige privacywetgeving schrijft voor dat u datalekken alleen hoeft bij te houden als u deze ook moet melden aan de Autoriteit persoonsgegevens. Onder de AVG bent u echter verplicht om alle datalekken te registreren, dus ook de datalekken die u niet hoeft te melden aan de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens kan deze registratie opvragen om te toetsen of u deze verplichting naleeft.

Hoe?

Maak gebruik van **het model-register datalekken <https://www.knmt.nl/system/files /model_verwerkings_-_en_datalekkenregister_versie_1.0_-20_dec_2017.xlsx>** van de KNMT (xlsx). Lees ook **de toelichting <https://www.knmt.nl/system/files /toelichting_model_verwerkings-_en_datalekkenregister.pdf>** (pdf).

Nog drie verplichtingen - voor sommige praktijken

Naast de bovenstaande 6 belangrijkste verplichtingen kunt u afhankelijk van de situatie met nog meer verplichtingen uit de AVG te maken krijgen.

A. Vooraf rekening houden met privacyaspecten bij ontwerp en

via standaardinstellingen

Wat?

Bij het bepalen van de middelen die u inzet voor de gegevensverwerking dient u al rekening te houden met privacy. Dit geldt bijvoorbeeld voor het softwarepakket dat u gebruikt. Als er een nieuwe toepassing komt, moet vanaf het begin al rekening worden gehouden met het belang van privacy en hoe dat wordt gewaarborgd. Ook in de standaardinstellingen van nieuwe diensten moet rekening worden gehouden met de privacyaspecten. Dit wordt onder de AVG ‘privacy bij design’ en ‘privacy bij default’ genoemd.

Hoe?

Maak uw tandartspraktijk nu al vertrouwd met de uitgangspunten van 'privacy by design' & 'privacy by default' door bij de ontwikkeling of het afnemen van nieuwe diensten of producten al rekening te houden met het waarborgen van de privacy van uw patiënten. Let er dan dus op dat niet meer gegevens worden verzameld dan nodig voor het bepaalde doeleinde en dat deze ook niet langer worden bewaard dan nodig. Indien u hier twijfels over heeft, is het raadzaam om hierover advies in te winnen bij bijvoorbeeld een gespecialiseerd advocaten- of juristenkantoor.

B. Het instellen van een Functionaris Gegevensbescherming

Wat?

Een functionaris gegevensbescherming (FG) kan verplicht zijn als u op grote schaal gevoelige persoonsgegevens (waaronder gezondheidsgegevens) verwerkt of wanneer u personen structureel observeert. In de AVG is echter niet gedefinieerd wat er onder ‘grote schaal’ wordt verstaan. Wel is duidelijk dat een ziekenhuis dat patiëntgegevens verwerkt als onderdeel van de gebruikelijke werkzaamheden in ieder geval een FG moet aanstellen en dat de verwerkingen van bijzondere persoonsgegevens door individuele zorgverleners (‘de éénpitters’) niet als grootschalig worden beschouwd en zij dus geen FG hoeven aan te stellen. Daartussen zit dus een grijs gebied. De komende periode zullen richtsnoeren worden ontwikkeld door de Autoriteit Persoonsgegevens of de gezamenlijke Europese toezichthouders om dit grijze gebied een nadere invulling te geven.

Hoe?

De KNMT voert samen met andere organisaties in de eerstelijns zorg een lobby om de regeldruk voor tandartsen in de hand te houden. Zo willen we bijvoorbeeld niet dat 'gewone' tandartspraktijken een FG hoeven benoemen.

C. Het uitvoeren van een Data Protection Impact Assessment (DPIA)

Wat?

Een DPIA is een onderzoek om de privacyrisico’s in kaart te brengen en deze vervolgens zoveel als mogelijk te beperken. Het uitvoeren van een DPIA is verplicht wanneer er een hoog privacyrisico bestaat voor de betrokkenen. Ook hier speelt het criterium ‘verwerkingen van gevoelige gegevens op grote schaal’ een rol. De AVG biedt geen overzicht van verwerkingen met een hoog privacyrisico en geeft dus niet concreet aan voor welke verwerkingen een DPIA verplicht is. De Autoriteit

persoonsgegevens zal daarom hiervoor op termijn een lijst van verwerkingen opstellen waarvoor een DPIA verplicht is. De Autoriteit persoonsgegevens raadt organisaties echter aan om een DPIA ook vrijwillig uit te voeren, omdat dit de gegevensbescherming ten goede komt en organisaties helpt om aan de verplichtingen uit de AVG te voldoen.

Hoe?

De KNMT houdt de ontwikkelingen op dit gebied in de gaten. Zodra meer duidelijk is over wanneer een DPIA precies verplicht is, informeren we u daarover.

Vragen?

Lees **antwoorden op veel gestelde vragen over de AVG <https://www.knmt.nl/praktijkzaken/privacy-en-informatiebeveiliging/vraag-en-antwoord-avg>**

Heeft deze informatie u geholpen?

Uw waardering:

- **1 </avg?rate=5uwaTTF7wLr9eC3khoTlzMOpDM7M3bqzUAqv2kWwRjw>**
- **2 </avg?rate=75i77ieYi_pr3ZBhgHkMvX7i9UL6k7mN_qoEOImh3K4>**
- **3 </avg?rate=32229ptOxvPpTI3o2cyUqEF9O5tbWdkoORSeXM8IqyM>**
- **4 </avg?rate=L3w5_HwItqyX1CC9vX_kgw97a-waj62a1IYyzbjd-Rg>**
- **5 </avg?rate=ZNWgC1SKs35KpEJOQ7rGUyxNSUDrOXHwO4Ri-1iep88>**

Total votes: 7

Uw toelichting...

Stem

Tags

- **Algemene Verordening Gegevensbescherming (AVG) </tags/algemene-verordening-gegevensbescherming-avg>**
- **informatiebeveiliging </tags/informatiebeveiliging>**
- **privacy </tags/privacy>**

Contact

Orteliuslaan 750, 2e etage

3528 BB Utrecht

nummer voor leden:

030-6076380