In het kort

De Algemene Verordening Gegevensbescherming (AVG) is een nieuwe Europese verordening die de regelgeving rondom gegevensbescherming in de EU uniformeert. In de AVG staan belangrijke en nieuwe vereisten voor het beheren van persoonsgegevens en hoe deze worden gebruikt, verzameld, bewaard en gedeeld. De regels zijn van toepassing op alle gegevensverantwoordelijken en gegevensverwerkers in de EU. Bovendien heeft de AVG een extraterritoriale werking.

De Europese Commissie (EC) handhaaft de AVG vanaf 25 mei 2018. In Nederland gebeurt dit door de Autoriteit Persoonsgegevens. Vanaf dat moment is dus alle bestaande regelgeving in de EU gecentraliseerd en aangepast aan het digitale tijdperk. Het zal de wijze waarop zorginstellingen persoonsgegevens verwerken aanzienlijk beïnvloeden.

Zorginstellingen voorbereiden op de Algemene Verordening Gegevensbescherming (AVG) De gegevens van patiënten veilig en toegankelijk

Digitalisering in de zorgverlening neemt toe

Patiëntgegevens worden steeds vaker digitaal opgeslagen op moderne medische apparatuur, in elektronische patiënten dossiers en digitaal uitgewisseld tussen zorgverleners. Speciale apps en portalen stellen zorgorganisaties en patiënten in staat gegevens uit te wisselen gedurende het zorgproces. De inzet van nieuwe technologieën volgen elkaar steeds sneller op. Deze dragen significant bij aan de vernieuwing in de zorg. Dat maakt een effectiever en efficiënter behandeltraject mogelijk. Tegelijkertijd moet de zorgverlener ook rekening houden met de bescherming van de privacy van de patiënt.

Zo moet de zorgverlener onder meer:

- Gegevens opslaan in een beveiligde omgeving, zoals het Elektronisch Patiënten Dossier.
- Binnen 72 uur datalekken melden.
- Alleen gegevens delen met een andere zorgverleners voorzover dat noodzakelijk is voor de behandeling van de patiënt.
- Alleen gegevens uitwisselen met andere zorgverleners via de beveiligde uitwisselingsportalen.
- Een functionaris voor de gegevensbescherming aanstellen.
- Een register van verwerkingsactiviteiten bijhouden.
- Privacy impact assessments uitvoeren.

Data analyse voor (wetenschappelijk) onderzoek een bron van waardevolle gegevens

De toegenomen digitalisering en de inzet van nieuwe technologieën dragen ook significant bij aan wetenschappelijk onderzoek in de zorg. Door de inzet van slimme technologieën en sensoren worden personen real-time gemonitord en dat levert een enorme hoeveelheid waardevolle data op. Het analyseren van deze gegevens voor (wetenschappelijk) onderzoek biedt nieuwe inzichten en verhoogd de kwaliteit van ons zorgstelsel en de behandeling van de patiënt. Omdat de medische gegevens van personen door de AVG als bijzondere persoonsgegevens betiteld zijn, moeten deze gegevens vertrouwelijk worden behandeld. Zo mag de onderzoeker:

- Onderzoeksgegevens alleen gebruiken voor onderzoeksdoeleinden op basis van toestemming.
- Gegevens van de personen zoveel mogelijk opslaan in een beveiligde omgeving.
- Onderzoeksgegevens alleen – gepseudonimiseerd – uitwisselen via beveiligde uitwisselingsportalen om de kans op datalekken te minimaliseren.

De 10 belangrijkste veranderingen met de komst van de AVG

1. **Betere kwaliteitstoestemming vereist**
   Zorginstellingen moeten aan striktere kwaliteitsvereisten voor het geldig verkrijgen van toestemming voldoen wanneer zij gebruikmaken van de toestemmingsgrondslag voor het verwerken van persoonsgegevens.
2. **Recht om vergeten te worden**
   Personen hebben het recht persoonsgegevens te laten wissen als deze niet langer vereist zijn voor het oorspronkelijke doel en er geen wettelijke verplichting bestaat deze gegevens te bewaren.
3. **Recht op overdraagbaarheid van gegevens**
   Personen hebben het recht om te verlangen dat de eigen persoonsgegevens in een algemeen toegankelijk format worden overgedragen aan een andere organisatie.
4. **Recht van bezwaar**
   Personen hebben het recht om bezwaar te maken tegen het feit dat hun gegevens worden gebruikt, tenzij de verantwoordelijke hier klemmende en legitieme redenen voor heeft, zoals het uitvoeren van een wettelijke taak.
5. **Profileren wordt moeilijker**
   Organisaties hebben over het algemeen niet het recht om uitsluitend op basis van geautomatiseerde verwerking besluiten te nemen over burgers, tenzij zij een juridische basis hebben om dit te doen (over het algemeen op basis van een wettelijke taak).
6. **Privacy by design en by default**
   Organisaties dienen de verwerking van persoonsgegevens zoveel mogelijk te beperken en privacy van betrokkenen maximaal te beschermen. Organisaties moeten hier automatisch rekening mee houden bij het ontwerpen en aanbieden van nieuwe diensten.
7. **Melden van datalekken**
   Organisaties hebben slechts 72 uur de tijd om een datalek te melden aan de toezichthouders en in sommige gevallen ook aan de betrokken individuen.
8. **Privacy Impact Assessment**
   Er moet een Privacy Impact Assessment worden uitgevoerd als nieuwe technologieën worden gebruikt en als de verwerking van persoonsgegevens waarschijnlijk zal leiden tot een groot privacy risico voor de betrokkenen.
9. **Functionaris voor gegevensbescherming**
   Uit de AVG volgt dat voor zorginstellingen de verplichting bestaat om een functionaris voor gegevensbescherming aan te stellen.
10. **Verhoogde boetes en sancties**
    In geval van ernstigste schendingen van de AVG kunnen hoge boetes worden opgelegd. Er gelden maximale boetes van € 20.000.000 of (als dit hoger is) 4% van de wereldwijde bruto jaaromzet.

pwc

Zorginstellingen dienen een vertrouwelijke digitale omgeving te hebben

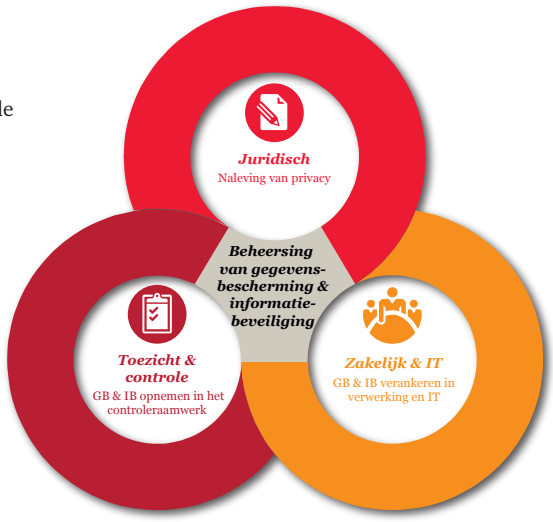
Omdat de medische gegevens van patiënten bijzondere persoonsgegevens zijn, moet de patiënt erop kunnen vertrouwen dat de zorginstelling, naast de zorg voor de patiënt, ook de privacy van de patiënt voorop stelt. De zorginstelling moet daarom minimaal zorgen dat:

- er inzicht is in de gegevens die men van patiënten verwerkt en met welke zorgverleners deze gegevens worden uitgewisseld.
- inzichtelijk is op welke wettelijke grondslag gegevens worden verzameld.
- toestemming van de patiënt voor het verzamelen van (wetenschappelijke) gegevens is geregistreerd.
- systemen, portalen en dossiers waarin medische gegevens worden opgeslagen voldoende zijn beveiligd zodat de kans op een datalek wordt geminimaliseerd.
- er voor de uitwisseling van medische gegevens met patiënten, zorgverleners en onderzoekers beveiligde portalen zijn ingericht. Er mag bijvoorbeeld geen gebruik worden gemaakt van email.
- zorgverleners bewust zijn van de noodzaak om gegevens vertrouwelijk te behandelen.
- er afspraken zijn gemaakt met derde partijen over de uitwisseling of de verwerking van medische gegevens voor zorgverlening of (wetenschappelijk) onderzoek.
- ook aan de kant van de bedrijfsvoering (HR systemen, Leveranciers, toegangssystemen voor personeel et cetera) de privacy is gewaarborgd.

Hoe kan PwC u helpen om de AVG na te leven?

PwC kan zorginstellingen begeleiden door het verschaffen en het aan elkaar verbinden van de vereiste technische, organisatorische en juridische vaardigheden. Wij bieden een standaard aanpak met bewezen methodes voor het beoordelen van de mate waarin organisaties klaar zijn voor de AVG en voor het vaststellen van noodzakelijke maatregelen die moeten worden getroffen voorzien van een prioriteitenstelling. Verder kunnen wij u helpen de benodigde maatregelen te implementeren in uw organisatie en deze duurzaam te borgen in uw processen en ICT. Wij kijken hier minimaal naar de volgende 13 aandachtsgebieden:

1. Strategie, governance & verantwoordelijkheden
2. Reglementen & Richtlijnen
3. Data Management
4. Uitwisselingen van persoonsgegevens
5. Grondslagen & informed consent
6. Transparantie
7. Processen & controles
8. Gegevensopslag & beveiliging
9. Training & awareness
10. Cultuur en gedrag
11. Gebruik maken van bewerkers
12. Bewaartermijnen
13. Rechten van betrokkenen



De aanpak van PwC

Wij gebruiken een gefaseerde aanpak. Hierdoor kunnen wij samen met u bepalen met welke stap of stappen wij u het beste kunnen helpen en op welk moment u het beste kunt instappen.

Stap 1 – Voorbereiden

Project mobilisatie

- Identificeren van belanghebbenden en projectdeelnemers;
- Kick-off organiseren;
- Beheer opzetten;
- Een eerste overzicht verkrijgen van de mate waarin de organisatie klaar is voor de AVG.

Stap 2 – Beoordelen

R.A.T.

- De Readiness Assessment Tool gebruiken om de huidige naleving te beoordelen.

Workshop

- Een workshop organiseren om de visie en ambities van het programma vast te stellen;
- Begrijpen wat de essentiële verankerde risico's zijn.

Stap 3 – Meten

GAP analyse

- Een Gap-analyse uitvoeren om te bekijken wat er gedaan moet worden om de gewenste mate van compliance te bereiken.

Stap 4 – Plannen

Roadmap

- Een roadmap ontwikkelen op basis van geprioriteerde risico's.

Stap 5 – Uitvoeren

Implementatie

- Strategie, governance & verantwoordelijkheden
- Reglementen & richtlijnen
- Data management
- Uitwisselingen van persoonsgegevens
- Grondslagen & informed consent
- Transparantie
- Processen & controles
- Gegevensopslag & beveiliging
- Training & awareness
- Cultuur en gedrag
- Gebruik maken van bewerkers
- Bewaartermijnen
- Rechten van betrokkenen

Contactgegevens

Remco van Mosel
PwC | Privacy & security
+31 (0)6 10 92 57 31
remco.van.mosel@pwc.com

Yvette van Gemerden
PwC | Privacy
+31 (0)6 52 00 59 24
yvette.van.gemerden@pwc.com

Sandra Mochèl
PwC | Privacy
+31 (0)6 53 35 36 41
sandra.mochel@pwc.com