mHealth en de AVG

Mobile Healthcare | 8 november 2018

Sofie van der Meulen

AUTORITEIT
PERSOONSGEGEVENS

Agenda

- mHealth en privacy: wanneer mogen er medische persoonsgegevens verwerkt worden?
- Hoe ziet het toezicht van de Autoriteit Persoonsgegevens eruit?

Andere toezichthouders vandaag:

- **Inspectie Gezondheidszorg en Jeugd**
- E-health in mijn zorginstelling. Waar kijkt de inspectie naar?
- **Zorginstituut Nederland**
- E-health: altijd een vernieuwing, soms een verbetering
- **Nederlandse Zorgautoriteit**
- Bekostiging en regels mogen e-health niet in de weg staan!

Juridisch kader privacy in de zorg

Privacywetgeving

- AVG
- Uitvoeringswet AVG

Zorgspecifieke wet- en regelgeving

- Zorgverzekeringswet
- Wet op de geneeskundige behandelingsovereenkomst
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
- Besluit elektronische gegevensverwerking door zorgaanbieders

Gegevens over gezondheid

Dit zijn alle persoonsgegevens over de gezondheid van een betrokkene.

Deze gegevens geven informatie over de lichamelijke of geestelijke gezondheidstoestand van de betrokkene in het verleden, het heden en de toekomst.

Voorbeelden:

- Informatie over ziekte, handicap, ziekterisico
- Medische voorgeschiedenis
- Patiëntennummers

Wanneer mogen er medische persoonsgegevens verwerkt worden?

Uitgangspunt: verboden, tenzij…

- Grondslag, bijvoorbeeld geneeskundige behandelovereenkomst
- Uitzondering op het verbod, zoals:
    - noodzakelijk voor goede behandeling of verzorging van de betrokkene
    - noodzakelijk voor beheer van zorginstelling, b.v. financiële administratie
    - een uitzonderingsgrond in de wet.

! Als zorgverleners medische gegevens verwerken vallen deze onder het medisch beroepsgeheim.

Doorbreking medisch beroepsgeheim

- Door het verlenen van toestemming door de patiënt
- Op basis van een wettelijk voorschrift
- In geval van een conflict van plichten

Zie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/gebruik-van-medische-gegevens#mag-mijn-zorgverlener-mijn-medische-gegevens-aan-anderen-doorgeven-4423

Voorwaarden verwerking

- Alleen noodzakelijke gegevens (‘dataminimalisatie’)
- Doelbinding
- Juiste (actuele) gegevens
- Informatieplicht aan de patiënt
- Verwerking gebaseerd op toestemming (moet kunnen worden aangetoond en voldoen aan eisen voor toestemming)
- Specifiek voor zorg: bewaartermijn van 15 jaar (WGBO)

! Let op rollen: verwerkingsverantwoordelijke of verwerker?

> *‘Een verwerker is een natuurlijke persoon of rechtspersoon die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt’*

Bijvoorbeeld: cloud aanbieder voor opslag gegevens en aanbieder HIS

Beveiliging

- Organisatorische en technische maatregelen (autorisaties)
- Richtsnoeren beveiliging
- NEN 7510 / NEN 7512 / NEN 7513
- ICT-beveiligingsrichtlijnen voor mobiele apps (NCSC, 2017)
- Beleids- en beheersingsrichtlijnen voor de ontwikkeling van veilige software (NCSC, 2018)

Wat betekent dit voor de tricorder?

Data protection impact assessment

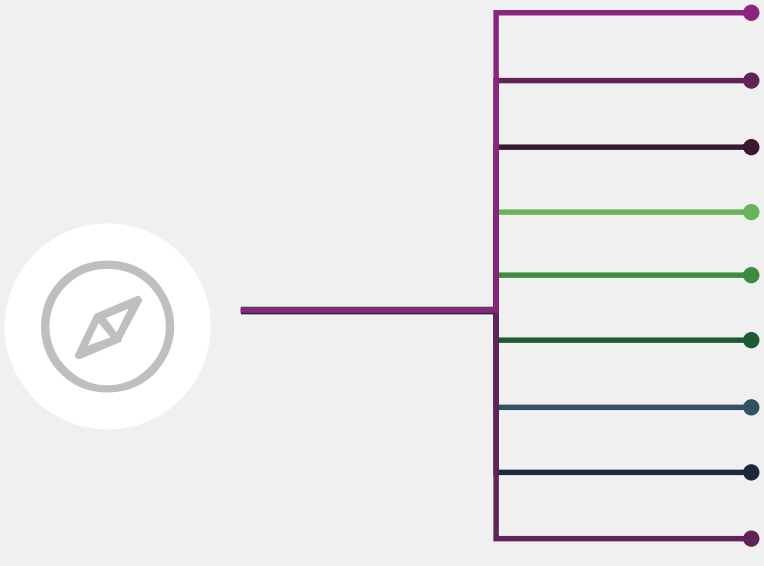
Verplicht bij verwerkingen die hoog privacyrisico opleveren

Systematisch en uitvoerig persoonlijke aspecten evalueren

Grote schaal bijzondere persoonsgegevens

Grote schaal systematisch mensen volgen in publiek toegankelijk gebied

Wanneer een DPIA uitvoeren



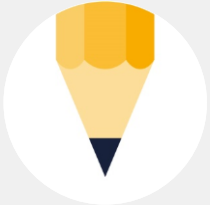
- Beoordelen van mensen op basis van persoonskenmerken
- Geautomatiseerde beslissingen
- Stelselmatige en grootschalige monitoring
- Gevoelige gegevens
- Grootschalige gegevensverwerkingen
- Gekoppelde databases
- Gegevens over kwetsbare personen
- Gebruik van nieuwe technologieën
- Blokkering van een recht, dienst of contract

Rechten van betrokkenen

Transparante informatie
voor de uitoefening van rechten

Informatie bij
verzameling

Recht van inzage



Recht om te wijzigen

Recht op verwijdering

Recht op beperking
van de verwerking

Kennisgevingsplicht
rectificatie, verwijdering,
beperking

Dataportabiliteit

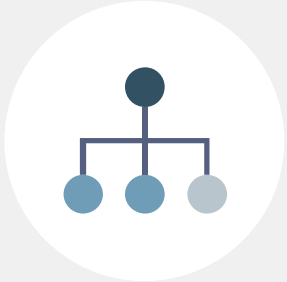
Wat doet de Autoriteit Persoonsgegevens

Toezicht en handhaving

Wetgevingsadvisering

Taken

Voorlichting algemeen publiek



Voorlichting organisaties

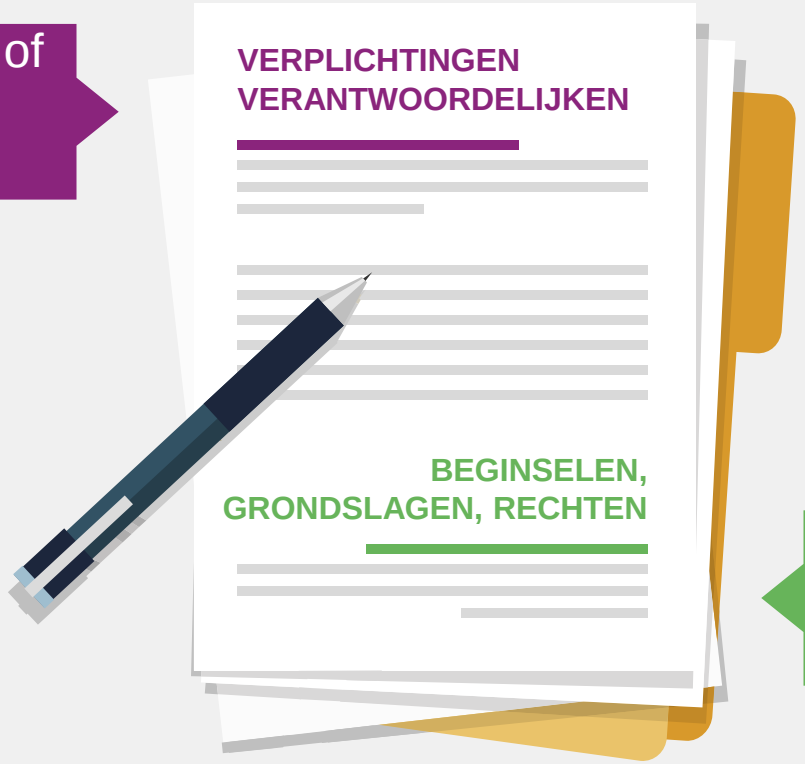
Toezicht en handhaving

Internationale samenwerking

Steviger boetebevoegdheden

Boetebevoegdheid

Max **€10 miljoen** of **2%** wereldwijde jaaromzet



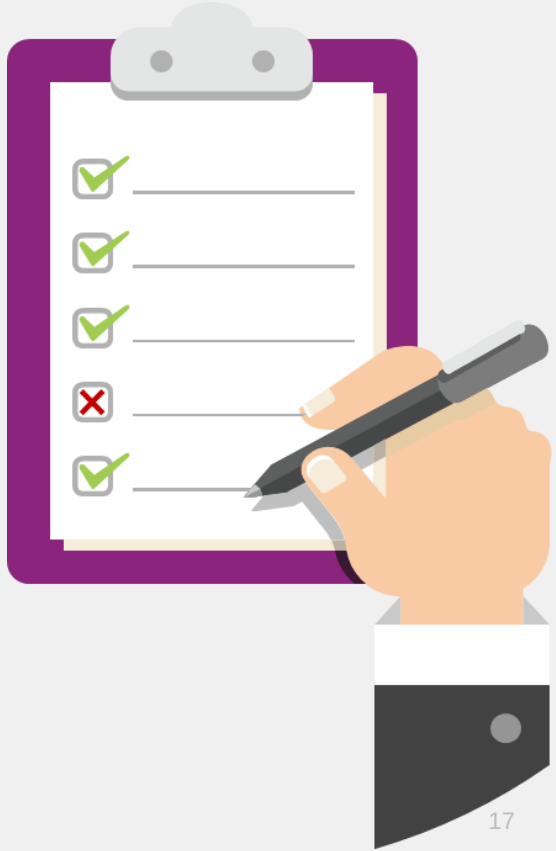
Max **€20 miljoen** of **4%** wereldwijde jaaromzet

Hoogte van boetes

- de aard, de ernst en de duur van de inbreuk
- aard, omvang of het doel van de verwerking in kwestie
- welke categorieën van persoonsgegevens (medische?)
- opzet of nalatigheid
- maatregelen om de schade te beperken
- *first offender* of structurele/herhaaldelijke overtreding
- hoe heeft de AP kennis gekregen van de inbreuk
- samenwerking met de AP om de inbreuk te verhelpen

EU: Code of Conduct on mobile health apps

- https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps
- http://www.osborneclarke.com/insights/mhealth-apps-the-code-of-conduct-on-privacy-explained/



AUTORITEIT PERSOONSGEGEVENS