GDPR en wat nu?

Marlies Eggermont

oktober 2018

VBOV

marlieseggermont@hotmail.com

I. Wat?

General Data Protection Regulation (GDPR)

- **Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG**
- **= Algemene Verordening Gegevensbescherming (AVG)**

II. Waarom?

- de bescherming van natuurlijke personen i.v.m. de **verwerking** van **persoonsgegevens**
- **Vrij verkeer** van persoonsgegevens

II. Waarom?

- Uniforme privacyregeling
- Rechtstreeks van toepassing in alle EU-landen
- Van kracht vanaf 25 mei 2018

Waarom?

Schriftelijke waarschuwing

Boete
10 milj of 2% jaaromzet

- Gebrek aan bescherming vanaf ontwerp en als standaard
- Niet melden van datalek aan GBA of betrokkene
- Gebrek aan register

Boete
20 milj of 4% jaaromzet

- Niet naleving van basisbeginselen
- Schending toestemmingsvereisten
- Schending doorgifte persoonsgegevens buiten EU

III. Gegevensbeschermingsautoriteit

GBA
Gegevensbeschermingsautoriteit

VAN CBPL NAAR GBA

Sinds 25 mei 2018 heeft de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL) haar plaats afgestaan aan de nieuwe Gegevens-beschermingsautoriteit. Wij nodigen jullie dus uit om de website van de Gegevensbeschermingsautoriteit te bezoeken:

www.gegevensbeschermingsautoriteit.be

III. Gegevensbeschermingsautoriteit

- Nieuwe wetgeving: https://www.gegevensbeschermingsautoriteit.be/wetgeving-en-normen
  - Wet gegevensbeschermingsautoriteit 3/12/2017
  - = de Toezichthoudende autoriteit voor de verwerking van persoonsgegevens
  - Wet 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (art. 222 ev. strafsancties), Wet privacy en KB worden opgeheven; nog uitvoeringsbesluiten

IV. Terminologie

verwerken

- **een bewerking** of **geheel van** bewerkingen **m.b.t. (geheel van) persoonsgegevens, al dan niet** uitgevoerd via **geautomatiseerde procédés**

bestand

- **Een gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria** centraal of decentraal **toegankelijk zijn**

persoons-gegevens

- **Alle informatie m.b.t. geïdentificeerd of** direct/indirect **identificeerbaar** (a.d.h.v. identificatienummer) natuurlijk **persoon**

IV. Terminologie

- Principes:
  - Rechtmatige basis verwerking (bv. wet, legitiem doel, toestemming)
  - Gerechtvaardigde doeleinden (geen re-use, tenzij toestemming of uitz. (bv. research))
  - Minimaal (enkel wat nodig is)
  - Juistheid
  - Opslagbeperking (patiëntendossier voor individuele zorgverlener: 20 jaar)
  - Technische maatregelen tegen verlies, vernietiging, beschadiging

IV. Terminologie

- **Verwerkingsverantwoordelijke**: zorgverlener bepaalt doel/middelen
- Verwerker: derde bv. softwarefirma, verwerkt ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens, zonder gezag
- Bewerker: persoon gemachtigd om gegevens te verwerken, onder gezag verwerkingsverantwoordelijke
- Gevoelige gegevens: politiek, seksueel, gezondheid, genetisch
- Verwerking is verboden, maar uitz.
  - Toestemming
  - Wet. Verplichting sociaal recht
  - Medische diagnose, gezondheidszorg

IV. Terminologie

- **Anonieme geg.**: alle gegevens die niet (meer) met een geïdentificeerd of identificeerbaar persoon in verband kunnen worden gebracht en die dus geen persoonsgegevens (meer) zijn (geen GDPR)
- **Gepseudonimiseerde geg.**: persoonsgegevens die op zodanige wijze verwerkt worden dat ze niet meer aan een specifieke natuurlijke persoon kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld

V. Rechten van de patiënt

- Informatie over verwerking (formulier)
- Inzage
  - Cfr. Patiëntenrechtenwet
  - Ook elektronisch
  - Geen info over derden
- Rectificatie
- Gegevenswissing/vergetelheid (beperkt, gezien bewaarplicht)
- Gegevensoverdracht (nieuwe zorgverlener, overheid, RIZIV, verzekering)

VI. GDPR in de praktijk

- Situatie 1: Je bent bij een patiënte thuis en je krijgt telefoon van een andere patiënte die je meteen om advies vraagt, het is dringend. Wat doe je?
  - A. Ik praat voluit, mijn andere patiënte moet dringend worden geholpen
  - B. Ik neem nooit mijn telefoon op als ik bij een patiënte ben
  - C. Ik praat voluit, maar zonder me eerst af

VI. GDPR in de praktijk

- Situatie 2: Je bent bij een patiënte thuis en de trotse peter filmt jou en de patiënte terwijl jullie de baby aan het verzorgen zijn. Wat doe je?
  - A. Je glimlacht en legt je haar goed, zodat je mooi op de opname staat, is nu zo gewoon geworden
  - B. Je vertelt de peter meteen dat je niet wenst gefilmd te worden (geen sociale media)
  - C. Je twijfelt, laat de peter begaan en vraagt achteraf om het filmpje privé te houden

VI. GDPR in de praktijk

- Situatie 3: Je hebt een patiënte tijdens de arbeid getransfereerd naar het ziekenhuis. De behandelend gynaecoloog vraagt je per mail om een verslag van de arbeid. Wat doe je?
  - A. Je stuurt je verslag in word-versie/pdf-versie naar de gynaecoloog door
  - B. Je gebruikt voor de communicatie met artsen, collega's, ZH een ehealth-platvorm of een app (www.siilo.com, www.signal.org) of veilige verzendmethode voor mails (www.zivver.eu/nl/, www.tresorit.com)
  - C. Je mailt het door, maar je pseudonimiseert de gegevens (zie voor meer info over encryptie, versleuteling enz…

VI. GDPR in de praktijk

- Situatie 4: Je schaft je een nieuwe PC aan. Waar sla je alle patiëntengegevens op?
  - A. Op mijn C-schijf
  - B. Op een externe Y-schijf
  - C. Op een USB-stick

VI. GDPR in de praktijk

- PC gebruik in het algemeen
  - Wachtwoord (uniek, vaak wisselen, niet doorgeven, opschrijven)
  - Lock systeem (ook voor bepaalde gegevens)
  - Pas op voor phishing, https://www.safeonweb.be/nl/leer-valse-mails-herkennen

VI. GDPR in de praktijk


MEDISCH CONTACT NIEUWS OPINIE KENNIS CARRI

DELEN naar overzicht

Simone Paauw 24 februari 2016 1 minuut leestijd

nieuws

Autoriteit Persoonsgegevens raadt WhatsApp af

1 reactie

WhatsApp voldoet niet aan de norm voor het delen van medische gegevens. Dat stelt de Autoriteit Persoonsgegevens in een reactie op een uitzending van EenVandaag dinsdagavond waarin het gebruik van WhatsApp door artsen aan de kaak wordt gesteld. Volgens EenVandaag is WhatsApp niet meer weg te denken in de medische wereld en zijn artsen laaiend enthousiast over de berichtenapp.

- Situatie 4: Je krijgt regelmatig berichtjes met medische info erin van patiënten (via Whats app en Messenger). Wat doe je?
  - A. Je stuurt wanneer mogelijk een antwoord terug
  - B. Je maakt van in het begin aan de patiënte duidelijk dat je geen medische info kan geven via berichtjes
  - C. Je belt de patiënte op of gaat langs

VII. Verplichtingen zorgverleners

- Aanwijzen verwerkingsverantwoordelijke

- A. Informed consent aan patiënten
- B. Register verwerkingsactiviteiten
- C. Melding van inbreuken aan GBA (report data breach)
- http://www.vroedvrouwen.be/nl/gdpr-general-data-protection-regulation
- NIET (alleen voor instellingen)
  - Aanstelling functionaris voor gegevensbescherming (data protection officer, DPO)
  - Gegevensbeschermingseffectbeoordeling (data protection impact assessment, DPIA)

A. Informed consent

- Standaard formulier aan patiënt aanbieden en van uitleg voorzien
- Privacyreglement in ontwerp

B. Register

- Naam en contactgegevens (gezamenlijke) verwerkingsverantwoordelijke
- Verwerkingsdoeleinden
- Beschrijving van de categorieën van betrokkenen
- Beschrijving van de categorieën van persoonsgegevens
- Bewaartermijn per verwerkingsdoel (bepaald / onbepaald met criteria)
- Beschrijving van categorieën ontvangers

C. Melding datalek

- https://www.gegevensbeschermingsautoriteit.be/melding-gegevenslekken-algemeen
- Melding via eformsapplicatie

TAKE MESSAGE

Your medical record is worth more to hackers than your credit card

Reuters, Sept. 24, 2014