



UZ
LEUVEN



GDPR = General Data Protection Regulation (of AVG = Algemene Verordening Gegevensbescherming)

JJD (met dank aan Christine Mathieu)
29.11.2017

UZ
Leuven

Herestraat 49
B - 3000 Leuven

www.uzleuven.be
tel. +32 16 33 22 11

UNIVERSITY HOSPITALS LEUVEN



Organization Accredited
by Joint Commission International



- **Wat?** Verordening 2016/679
- **Van kracht:** 25 mei 2018 (zonder overgangsmaatregelen – vervangt de Richtlijn 95/46/EC)
- **Rechtstreekse werking** in Belgisch recht maar toch nog nood aan nieuwe wetgeving, bvb:
 - Wet over Gegevensbeschermingsautoriteit (“DPA”) (ontwerp ingediend in augustus)
 - Regeling waarvoor Verordening bijkomende bescherming mogelijk maakt of nationale wetgeving nodig maakt (zoals voor “research exemption”)
- **Strengere boetes** bij inbreuk

- **Ruim toepassingsgebied:**

- Persoonsgegevens: alle informatie over geïdentificeerde of identificeerbare natuurlijke persoon, via identificatoren zoals naam, nummer, adres, *maar ook* alles wat kenmerkend is voor fysieke, fysiologische, genetische of psychische identiteit.
- Verwerking: 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 persoonsgegevens.*

- **Nieuwigheden:**
 - Register voor verwerkingsactiviteiten
 - Data Protection Officer = DPO (“Functionaris voor Gegevensbescherming”)
 - Data Protection Impact Assessment = DPIA (“Gegevensbeschermingseffectenbeoordeling”)
 - Hervorming Data Protection Authority = DPA (bvb. onderzoeksbevoegdheden zoals toegang tot alle documenten / audit)
 - Meldplicht bij datalekken
 - Bijzondere bescherming persoonsgegevens van kinderen

- **Lawfulness, fairness and transparency:** steeds een *rechtmatige basis* voor verwerking (ofwel toestemming, ofwel legitiem doel zoals diagnose en therapie, ofwel uitvoering van een wettelijke/contractuele verplichting, ofwel nodig voor algemeen belang of vitale belangen van betrokkene)
- **Purpose limitation:** verwerking gebeurt voor *omschreven en gerechtvaardigde doelen*, geen secundaire verwerking tenzij toestemming of binnen uitzonderingsregeling voor wetenschappelijk onderzoek
- **Data minimisation:** verwerking beperken tot *wat nodig is*
- **Accuracy:** juist en geactualiseerd
- **Storage limitation:** niet langer bewaard dan nodig voor doeleinde
- **Integrity en confidentiality:** passende technische en organisatorische maatregelen tegen verlies, vernietiging, beschadiging
- **Accountability:** verwerkingsverantwoordelijke (“controller”) moet *naleving van beginselen kunnen aantonen*

- **Bijzonder regime** voor gevoelige gegevens zoals politieke overtuiging, sexuele voorkeur, gezondheid, genetische gegevens
- **Ruime definitie “gegevens met betrekking tot gezondheid”** (miv gegevens over verleende gezondheidsdiensten waaruit informatie over gezondheid kan worden afgeleid)
- **Principe:** verwerking van gevoelige gegevens is verboden
- **Uitzonderingen** (art 9.2): toestemming van de betrokkene (schriftelijk, begrijpelijk, duidelijk en specifiek, vrij – quid “broad consent”? Zie afweging 33 vd GDPR), wettelijke verplichtingen ikv sociaal recht, redenen van substantieel algemeen belang, nodig voor wetenschappelijk onderzoek (“research exemption” (zie art 89): nog wettelijke regeling nodig), ...

- **Informatie** over verwerking
- Recht van **inzage**
- Recht op **rectificatie**
- Recht op **gegevenswissing** (“right to be forgotten”)
- Recht op **beperking van de verwerking**
- Recht op **gegevensoverdracht** (“data portability”)
- Recht van **verzet** (tegen bvb direct marketing) en **om niet te worden onderworpen aan geautomatiseerde besluitvorming** (bvb profiling) (“right to object and automated individual decision-making”)

- Aanwijzing van een **verantwoordelijke voor de verwerking** (“controller”)
- Afsluiten van **overeenkomsten met verwerkers** (“processors”)
- **Register** van verwerkingsactiviteiten (art. 30):
 - Overzicht van alle verwerkte categorieën van gegevens
 - Gegevensstromen (wie kan wat zien)
 - Beschrijving van de beveiligingsmaatregelen
- **Aanstelling DPO**
- **DPIA**
- **Melding van inbreuken** (aan DPA (binnen 72u) en betrokkenen)

Gedragscode voor de sector (art 40)

« Verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen, kunnen gedragscodes opstellen, of die codes wijzigen of uitbreiden, teneinde de toepassing van deze verordening nader toe te lichten »

- > Wordt ter goedkeuring voorgelegd aan DPA
- > Kan eigen toezichtsystemen voor de sector omvatten

Momenteel initiatief van Zorgnet-Icuro

BERED
JE
VOOR
IN
13
STAPPEN

ALGEMENE VERORDENING GEGEVENSBESCHERMING

1. BEWUSTMAKING 

Informeer sleutelfiguren en beleidsmakers over de aankomende veranderingen. Zij moeten inzien welke gevolgen de AVG zal teweegbrengen voor het bedrijf of de organisatie.

2. DATAREGISTER 

Breng in kaart welke persoonsgegevens je bijhoudt, waar deze vandaan komen en met wie je deze hebt gedeeld. Registreer je verwerkingen. Mogelijks dien je hiervoor een informatie-audit te organiseren.

3. COMMUNICATIE 

Evalueer je bestaande privacyverklaring en plan noodzakelijke wijzigingen hieraan in het licht van de AVG.

4. RECHTEN VAN DE BETROKKENE 

Ga na of de huidige procedures in je bedrijf of organisatie alle rechten voorzien waarop de betrokkene zich kan beroepen, inclusief hoe persoonsgegevens kunnen worden verwijderd of hoe gegevens elektronisch zullen worden meegedeeld.

5. VERZOEK TOT TOEGANG 

Update je bestaande toegangsprocedures en bedenk hoe je verzoeken tot toegang voortaan zal behandelen onder de nieuwe termijnen in de AVG.

6. WETTELIJKE GRONDSLAG VOOR HET VERWERKEN VAN PERSOONSGEGEVENS 

Documenteer de verschillende types van gegevensverwerkingen die je uitvoert en identificeer de wettelijke grondslag voor elk van hen.

7. TOESTEMMING 

Evalueer de wijze waarop je toestemming vraagt, verkrijgt en registreert, en wijzig waar nodig.

8. KINDEREN 

Ontwikkel systemen die de leeftijd van de betrokkene nagaan en die de ouder(s) of voogd(en) om toestemming vragen voor de gegevensverwerking van minderjarige kinderen.

9. DATALEKKEN 

Voorzie adequate procedures om persoonlijke datalekken op te sporen, te rapporteren en te onderzoeken.

10. GEGEVENSBESCHERMING DOOR ONTWERP EN GEGEVENSBESCHERMINGSEFFECTBEOORDELING 

Maak je vertrouwd met de begrippen "gegevensbescherming door ontwerp" en "gegevensbeschermingseffectbeoordeling" en ga na hoe je deze concepten in de werking van jouw bedrijf of organisatie kan implementeren.

11. FUNCTIONARIS VOOR GEGEVENSBESCHERMING 

Duid, indien nodig, een functionaris voor gegevensbescherming aan, of iemand die de verantwoordelijkheid draagt voor het naleven van de databeschermingsregels. Beoordeel welke plaats deze inneemt binnen de structuur en het beleid van jouw bedrijf of organisatie.

12. INTERNATIONAAL 

Bepaal onder welke toezichhoudende autoriteit je valt indien jouw bedrijf of organisatie internationaal actief is.

13. BESTAANDE CONTRACTEN 

Beoordeel je bestaande contracten, hoofdzakelijk met verwerkers en onderaannemers, en breng tijdig de noodzakelijke veranderingen aan.