ALGEMENE VERORDENING GEGEVENSBESCHERMING

ORDRE DES MEDECINS
CONSEIL NATIONAL

ORDE DER ARTSEN
NATIONALE RAAD

1. SITUERING

1.1. WETTELIJK KADER IN BELGIË

Belgische Privacywet

- Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens

Richtlijn Bescherming Persoonsgegevens

- Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens

!

Algemene Verordening Gegevensbescherming – Toepassing : 25 mei 2018

- Verordening 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 gegevens en tot intrekking van de Richtlijn 95/46/EG

1.2. DOEL VAN DE NIEUWE REGELGEVING

- Aanpassen van het juridisch kader aan de digitale revolutie
- Het verschil in nationale wetgevingen harmoniseren
- Het creëren van een grotere bewustwording voor bedrijven / organisaties om met privacygegevens om te gaan
- Meer individuele rechten voor de betrokkene
- Meer verplichtingen voor bedrijven / organisaties
- Meer sancties en controle
  - Administratieve geldboeten tot 20.000.000 EUR of 4% van de totale omzet
  - Reputatieschade

2. DEFINITIES

2.1. PERSOONSGEGEVENS

Persoonsgegevens (art. 4)

- Iedere informatie over een geïdentificeerd of identificeerbaar natuurlijk persoon
- Direct of indirect
- Bijvoorbeeld: naam, foto, telefoonnummer, e-mailadres, nummerplaat, …

Gevoelige gegevens (art. 9)

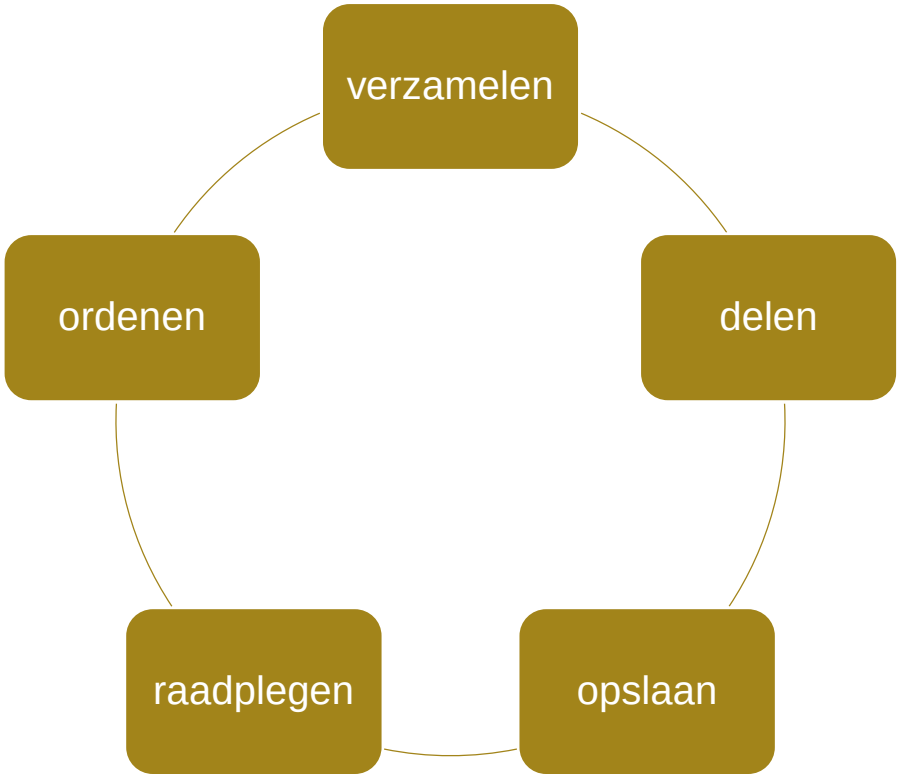
- Persoonsgegevens waaruit ras en etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lid maatschap bij een vakbond blijken, verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over de gezondheid of iemands seksueel gedrag.
- Bijvoorbeeld: medisch dossier, juridisch dossier, politieke voorkeur, lidmaatschap vakbond, …
- Ruimte voor de lidstaten om de regels te specifiëren

Bijzondere gevallen

- Overleden personen – GDPR niet van toepassing
- Anonieme gegevens – GDPR niet van toepassing

2.2. DE VERWERKING VAN PERSOONSGEGEVENS

Een verwerking is een (geheel van) bewerking(en) met betrekking tot (een geheel van) persoonsgegevens, 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.



2.3. DE VERWERKER - DE VERWERKINGSVERANTWOORDELIJKE

- Betrokkene – de geïdentificeerde of identificeerbare natuurlijke persoon wiens persoonsgegevens verwerkt worden.

- Verwerkingsverantwoordelijke – stelt het doel van en de middelen voor de verwerking van persoonsgegevens vast, neemt maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de verordening wordt uitgevoerd. De maatregelen worden geëvalueerd en zo nodig geactualiseerd.

- Verwerker – verwerkt persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke.

Voorbeeld ter verduidelijking: U bestelt een product online bij een webshop. De webshop doet op haar beurt beroep op een transportbedrijf om het product te leveren. In casu bent u de betrokkene wiens gegevens worden verwerkt, is de webshop de verwerkingsverantwoordelijke en fungeert het transportbedrijf als verwerker.

3. ALGEMENE BEGINSELEN VAN DE GDPR

3.1. KENMERKEN

- Rechtmatigheid, behoorlijkheid en transparantie - de persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is.

- Doelbinding – de persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld en mogen enkel op een met die doeleinden verenigbare manier worden verwerkt.

- Minimale gegevensverwerking – de persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor ze worden verwerkt.

- Juistheid – de persoonsgegevens moeten juist en geactualiseerd zijn. Onjuiste gegevens moeten worden gewist of aangepast.

- Opslagbeperking – de persoonsgegevens mogen niet langer dan nodig worden bewaard. Ook mogen er niet meer persoonsgegevens dan noodzakelijk worden bewaard.

- Integriteit en vertrouwelijkheid – de nodige (technische en organisatorische) maatregelen worden genomen om een beveiligde verwerking van de persoonsgegevens te garanderen.

3.2. RECHTEN VAN DE BETROKKENE

- Informatieverstrekking – de betrokkene moet voorafgaand aan de verwerking van de gegevens op transparante wijze in kennis worden gesteld van allerhande in de verordening informatie.

- Inzage – de betrokkene heeft recht op inzage en afschrift van de verwerkte persoonsgegevens (o.a. het patiëntendossier). De regels van de Wet Patiëntenrechten blijven gelden.

- Opvragen logingegevens – de betrokkene heeft het recht in kennis te worden gesteld van personen die het dossier hebben geraadpleegd. (nominatief benoemen – functie meedelen)

- Rectificatie – de betrokkene heeft het recht om verkeerde informatie te laten verbeteren (vb. het adres van de patiënt. Quid medische gegevens?)

- Gegevenswissing *"right to be forgotten"* – de betrokkene heeft het recht om vergeten te worden. Dit geldt echter niet onverkort voor medische dossiers. Hier blijft de bewaartermijn van toepassing.

- Beperking van de verwerking – de betrokkene heeft het recht om in wel bepaalde gevallen een beperking van de verwerking te verkrijgen.

- Bezwaar – de betrokkene heeft het recht om bezwaar te maken tegen de verwerking van persoonsgegevens. De wetgever heeft hiermee voornamelijk direct marketingpraktijken beoogd.

- Geautomatiseerde besluitvorming – de betrokkene heeft het recht bezwaar in te dienen tegen een besluit dat voortvloeit uit geautomatiseerde besluitvorming.

- Overdraagbaarheid – dit is een verbeterde vorm van toegang waarbij de betrokkene het recht heeft de persoonsgegevens die op hem van toepassing zijn in een gestructureerde, gangbare en elektronische vorm te verkrijgen.

3.3. BASIS – VERWERKING PERSOONSGEGEVENS

- Toestemming van de betrokkene
  - de toestemming moet op vrijwillige basis worden gegeven, moet geïnformeerd zijn, moet specifiek en ondubbelzinnig zijn
  - de verwerkingsverantwoordelijke moet de toestemming aantonen
  - de betrokkene heeft het recht zijn toestemming ten allen tijde in te trekken
- Noodzakelijk voor de uitvoering van een overeenkomst
- Noodzakelijk om te voldoen aan een wettelijke verplichting
- Noodzakelijk om de vitale belangen van de betrokkene te beschermen
- Noodzakelijk voor een vervulling van een taak van algemeen belang
- Noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke

3.4. SPECIFIEK – VERWERKING GEZONDHEIDSGEGEVENS

In principe

Verbod van verwerking van gezondheidsgegevens

Relevante rechtsgronden die de verwerking rechtvaardigen

- Er is een uitdrukkelijke toestemming van de patiënt.
- De verwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon indien de betrokkene fysiek of juridisch niet in staat is toestemming te geven.
- De verwerking is noodzakelijk voor de doeleinden van preventieve of arbeidsgeneeskunde.
- De verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid.

4. GDPR – CONFORM MAKEN

4.1. BEWUSTWORDING

- De sleutelfiguren van de organisatie dienen op de hoogte te worden gesteld van de nieuwe regelgeving. Zij zijn het beste geplaatst om in te schatten:
  - welke gevolgen de GDPR heeft voor de organisatie;
  - waar mogelijks de probleempunten liggen binnen de organisatie.

- Alle personeelsleden – in het bijzonder diegene die persoonsgegevens verwerken – dienen bewust te worden gemaakt hoe zij met persoonsgegevens dienen om te gaan.

4.2. AANDUIDEN VAN EEN “PILOOT”

- Functionaris voor gegevensbescherming – DPO
- Wanneer?
  - de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan (Orde der artsen!);
  - de verwerkingen vereisen vanwege hun aard of hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen;
  - grootschalige verwerking van bijzondere categorieën van gegevens (vb. gezondheidsgegevens.)
    - De individuele arts valt hier niet onder (aanwijzingen van de Privacycommissie)
    - Ziekenhuizen vallen hier uiteraard wel onder
    - Quid groepspraktijken?
- Taken?
  - toezien op de naleving van de verordening;
  - informeren en adviseren van de verwerkingsverantwoordelijke en de verwerker over hun verplichtingen;
  - …
- Kenmerken?
  - objectief;
  - binnen of buiten de entiteit;
  - kennis omtrent privacy;
  - …

4.3. REGISTER VAN VERWERKINGSACTIVITEITEN - BEVEILIGING

- Uitvoeren van een interne audit van de gegevensverwerkingen en de opmaak van een register van verwerkingsactiviteiten:

  - In kaart brengen van de verwerkingsverantwoordelijke, en eventueel deze van de functionaris van de gegevensbescherming;
  - de verwerkingsdoeleinden;
  - de beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
  - de termijnen waarbinnen de persoonsgegevens dienen te worden gewist;
  - de beveiligingsmaatregelen die worden genomen;
  - …

- Beveiliging van de verwerking

  - de verwerker en de verwerkingsverantwoordelijke treffen maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, (vb. door de pseudonimisering en versleuteling van persoonsgegevens, ervoor zorgen dat de beveiligingssystemen betrouwbaar zijn, …)

- Voorzien interne procedures voor gegevensbeheer

  - Informatie, opleiding en sensibilisering van personeelsleden;
  - Regelmatige beoordelingen en updates;
  - Procedures voor de opmaak van rechtmatige gegevensverwerking (beleidsdocumenten, opmaak standaardformulier geïnformeerde toestemming, …);
  - Procedures voor informatieverzoeken en klachten (vb. omgaan met de rechten van de betrokkene);
  - Procedures voor datalekken;
    - Uitgangspunt: voldoende beschermingsmaatregelen
    - Melding aan de toezichthoudende overheid binnen de 72 uur
    - Onverwijlde melding aan de betrokkene bij hoog risico voor schending van diens rechten en vrijheden
    - Bij gevoelige gegevens is er een groter risico
  - …

Vragen?