NEN-7510 een praktisch hulpmiddel voor implementatie van de AVG / GDPR

Theo de Breed

Agenda

- AVG voorbereiding in 10 stappen (Bron: AP)
- Praktische invulling door gebruik van NEN7510:2017
- Vragen?

AVG voorbereiding in 10 stappen

Om u op weg te helpen, heeft de Autoriteit Persoonsgegevens (AP) de 10 belangrijkste stappen (pdf) voor u op een rijtje gezet. Dat zijn:

1. Bewustwording
2. Rechten van betrokkenen
3. Overzicht verwerkingen
4. Data protection impact assessment (DPIA)
5. Privacy by design & privacy by default
6. Functionaris voor de gegevensbescherming
7. Meldplicht datalekken
8. Bewerkersovereenkomsten
9. Leidende toezichthouder
10. Toestemming

1. Bewustwording

A.18.1.1 Vaststellen van toepasselijke wetgeving en contractuele eisen, A.18.1.4 Privacy en bescherming van persoonsgegevens alsmede de gerelateerde implementatierichtlijnen uit deel 2 helpen u om duidelijkheid te verkrijgen over de wettelijke, regelgevende en contractuele eisen en bewust te worden aan welke eisen moet worden voldaan.

- Algemene Verordening Gegevensbescherming
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
- Wet Geneeskundige Behandel Overeenkomst
- Etc.

(art. 5)

2. Rechten van betrokkenen

A.12.1.1 Gedocumenteerde bedieningsprocedures en de implementatierichtlijn in 12.1.1 van deel 2 helpen u met het documenteren van procedures en het beschikbaar stellen aan alle gebruikers (waaronder de betrokkenen).

- Transparant
- Duidelijk
- Begrijpelijk
- Jip en Janneke taal

(art. 12-22)

3. Overzicht verwerkingen

A.8 Beheer van bedrijfsmiddelen en de implementatie richtlijnen in hoofdstuk 8 van deel 2 helpen u in kaart te brengen:

- Over welke persoonsgegevens u beschikt in uw organisatie;
- Waar deze persoonsgegevens zijn opgeslagen;
- Hoe lang deze persoonsgegevens bewaard dienen te blijven;
- En wie toegang heeft tot deze persoonsgegevens.

Stuk voor stuk vereisten vanuit de AVG!

(art. 30)

4. Data Impact Protection Assessment

A.8.2.1 Classificatie van informatie en de implementatie richtlijn in paragraaf 8.2.1 uit deel 2 alsmede paragraaf 6.1 uit deel 1 helpen u bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.

- Welke mate van beschikbaarheid?
- Welke mate van integriteit?
- Welke mate van vertrouwelijkheid?
- Welke mate van controleerbaarheid?
- Welke dreigingen?
- Welke maatregelen?

(art. 35)

5. Privacy by design

A.14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen en de implementatie richtlijnen in hoofdstuk 14 van deel 2 helpen u te waarborgen dat informatiebeveiliging integraal deel uitmaakt van de levenscyclus van informatiesystemen. Bijv. op het gebied van:

- Identificatie
- Authenticatie
- Autorisatie
- Audit

(art. 25)

6. Functionaris Gegevensbescherming

A.6.1.1 Rollen en verantwoordelijkheden bij Informatiebeveiliging en de implementatierichtlijn 6.1.1 uit deel 2 van de norm helpen u bij het vaststellen van een beheerkader om de implementatie en uitvoering van de Informatiebeveiliging binnen de Organisatie te initiëren en te beheersen. Taken:

- Ondersteunen bij het opstellen van een PIA
- Opstellen en bijhouden register van verwerkingsactiviteiten
- Ondersteunen en/of opstellen van verwerkersovereenkomsten
- Adviseren over technologie en beveiliging omtrent gegevensverwerking
- Verantwoordelijk voor de coördinatie en beheer van datalekken

(art. 37)

7. Meldplicht datalekken

A.16.1 Beheer van informatiebeveiligingsincidenten en verbeteringen en de implementatie richtlijn in paragraaf 16.1 van deel 2 helpen u een consistente en doeltreffende aanpak te bewerkstelligen van het beheer van beveiligingsincidenten met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.

- Communicatie naar AP binnen de 72 uur;
- Communicatie naar betrokkenen;
- In geval van verwerker, communicatie naar de verwerkingsverantwoordelijke

(art. 33)

8. Verwerkersovereenkomst

A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten en de implementatierichtlijn in 15.1.2 van deel 2 helpen u om te waarborgen dat er geen misverstand bestaat tussen de u en uw leverancier ten aanzien van de verplichtingen van beide partijen om te voldoen aan relevante informatiebeveiligingseisen. Bijvoorbeeld door het opnemen van:

- Omschrijving van de informatie die moet worden verschaft of toegankelijk moet worden en methoden om de informatie te verschaffen of toegankelijk te maken;
- Classificatie van de informatie in overeenstemming met het classificatieschema van de organisatie
- Wettelijke en regelgevende eisen, met inbegrip van gegevensbescherming, rechten van intellectuele eigendom en auteursrecht, en een beschrijving van hoe wordt gewaarborgd dat eraan wordt voldaan;
- Verplichting van elke contractuele partij om een overeengekomen aantal beheersmaatregelen te implementeren, waaronder toegangsbeveiliging, prestatiebeoordeling, monitoren, rapporteren en auditen;

(art. 28)

9. Leidende toezichthouder

A.18.1.4 Privacy en bescherming van persoonsgegevens en de implementatierichtlijn 18.1.4 uit deel 2 van de norm helpen u, indien uw gegevens verwerking impact heeft in meerdere lidstaten, om de leidende toezichthouder te bepalen.

(art. 51)

10. Toestemming

A.18.1.4 Privacy en bescherming van persoonsgegevens en de implementatierichtlijn 18.1.4 uit deel 2 van de norm helpen u om de geïnformeerde toestemming van cliënten te beheren. Waar mogelijk moet geïnformeerde toestemming van cliënten worden verkregen voordat persoonlijke gezondheidsinformatie per email, fax of telefonisch wordt gecommuniceerd of anderszins bekend wordt gemaakt aan partijen buiten de zorginstelling.

- Controleerbaar aantoonbaar verkregen
- Op basis van duidelijke informatie
- Uit vrije wil verstrekt
- Kan worden ingetrokken

(art. 6)

Vragen?