AVG & NEN 7510:2017

Theo Hooghiemstra

7 december 2017

PBLQ

verbinders in de informatiesamenleving

Agenda

I. **Waarom?**

Slide van vanochtend

II **Hoe?**

Normatief kader AVG in een notendop, linkjes met NEN 7510: 2017

III **Jullie vragen**?

I. Waarom AVG + NEN 7510:2017 = Informatiebeveiliging zorggegevens?

verbinders in de informatiesamenleving

Noodzaak:

- AVG informatiebeveiliging verplicht: ‘Passende maatregelen’.
- NEN 7510:2017 verplicht: ‘Besluit elektronische gegevensverwerking door zorgaanbieders’
- AP en IGZ: NEN 7510: 2017 dé norm voor informatiebeveiligingsaudits in de zorg

AVG =

- Dataprotectie-wetgeving in de praktijk, sociale media + harmonisatie + handhaving + sectoroverstijgend.
- **Accountability**, nieuwe rechten, FG vaak verplicht, data protection by design, PIA, certificering,..

***NEN 7510: 2017* =**

- **Kans** voor informatiebeveiliging in en buiten de Nederlandse zorg
- **Kans** voor gezondheidsgegevens buiten de zorg! O.a. persoonlijke gezondheidsomgevingen & wearables.
- **Kans** voor goede invulling certificeringsplicht AVG

II. Wbp/AVG in een notendop

PBLQ
verbinders in de informatiesamenleving

- Wbp: transparantie, doelbinding, beveiliging, dataminimalisatie en rechten betrokkenen (inzage, correctie), meldplicht datalekken (art. 34a Wbp).
- AVG = Wbp met als belangrijkste aanvullingen:
  1) **Accountability**
  2) **Extra rechten voor betrokkenen**
  3) **Functionaris Gegevensbescherming vaak verplicht**
  4) ***Data protection-by-design***;
  5) **Gegevensbeschermingseffectbeoordeling** (PIA);
  6) **Strengere eisen** voor **verwerkers** (in de Wbp waren dat bewerkers);
  7) **Certificering**
- Kortom: als reeds op orde met de Wbp, dan zijn de aanvullingen ten opzichte van AVG te overzien. Als nog niet op orde met de Wbp, dan extra veel werk te doen.

Ad 1) Accountability

PBLQ
verbinders in de informatiesamenleving

- Documenteren: met bewijs kunnen aantonen dat AVG wordt nageleefd, inclusief plicht tot informatiebeveiliging! Bijhouden verwerken soorten persoonsgegevens, voor welk doel en met welke grondslag (toestemming, overeenkomst, wet, publieke taak, vitaal of algemeen belang).

- Hoever is jouw organisatie met het in kaart brengen van gegevensverwerkingen volgens de AVG-voorwaarden?

Ad 2) Extra rechten: Kansen, knelpunten & dilemma's?

PBLQ
verbinders in de informatiesamenleving

- **Recht op vergetelheid**. Wbp kent correctie en verwijderrecht. Zorg: vernietigingsrecht. Breder recht dan Wbp in AVG. Sociale media: Google >150 mensen. Dilemma: Reëel?
- **Toestemming:** Toestemming geven net zo makkelijk maken als intrekken. In begrijpelijke taal, actief en aantoonbaar naar vragen. Kans: vertrouwen. Dilemma: garantie?
- **Elektronische inzage**: Knelpunt: authenticatie voldoende? In de zorg 3 jaar uitstel. *NEN 7510: 2017:* twee factor-authenticatie, bijvoorbeeld bij patientportalen (uitspraak AP)
- **Dataportabiliteit.** Door betrokkene verstrekte gegevens. Bijv. via toestemming of overeenkomst. Gaat om gestructureerde, machine leesbare gegevensoverdracht voor overdraagbaarheid. Verbinden met ontwikkelingen regie op gegevens door personen / ketens (kans: PGO, PGB. Risico: In verkeerde handen). Meenemen in contracten met leveranciers en bij inkoop en aanbestedingen. Knelpunt: Tijd, waarborgen PGO's.

Ad 3) Functionaris Gegevensbescherming

verbinders in de informatiesamenleving

Overheden en organisaties die hoofdzakelijk belast zijn met **grootschalige verwerking van gezondheidsgegevens** moeten (gezamenlijk) een FG aanstellen.

Algemene kerntaak: ziet toe op **naleving van de AVG**

Positie van de FG in de organisatie

- *(…) "**naar behoren en tijdig betrokken** bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens"*
- ***Onafhankelijk***

Wanneer? Zo snel mogelijk!

- Staat centraal in nieuwe juridische kader voor gegevensbescherming binnen organisaties
- Hoeksteen voor verantwoording
- Maakt naleving makkelijker
- Fungeert als tussenpersoon tussen de verschillende belanghebbenden.

Ad 4) *Data protection-by-Design:* meer dan techniek!

PBLQ
verbinders in de informatiesamenleving

Technisch: Beperk gegevensverwerking (dataminimalisatie)

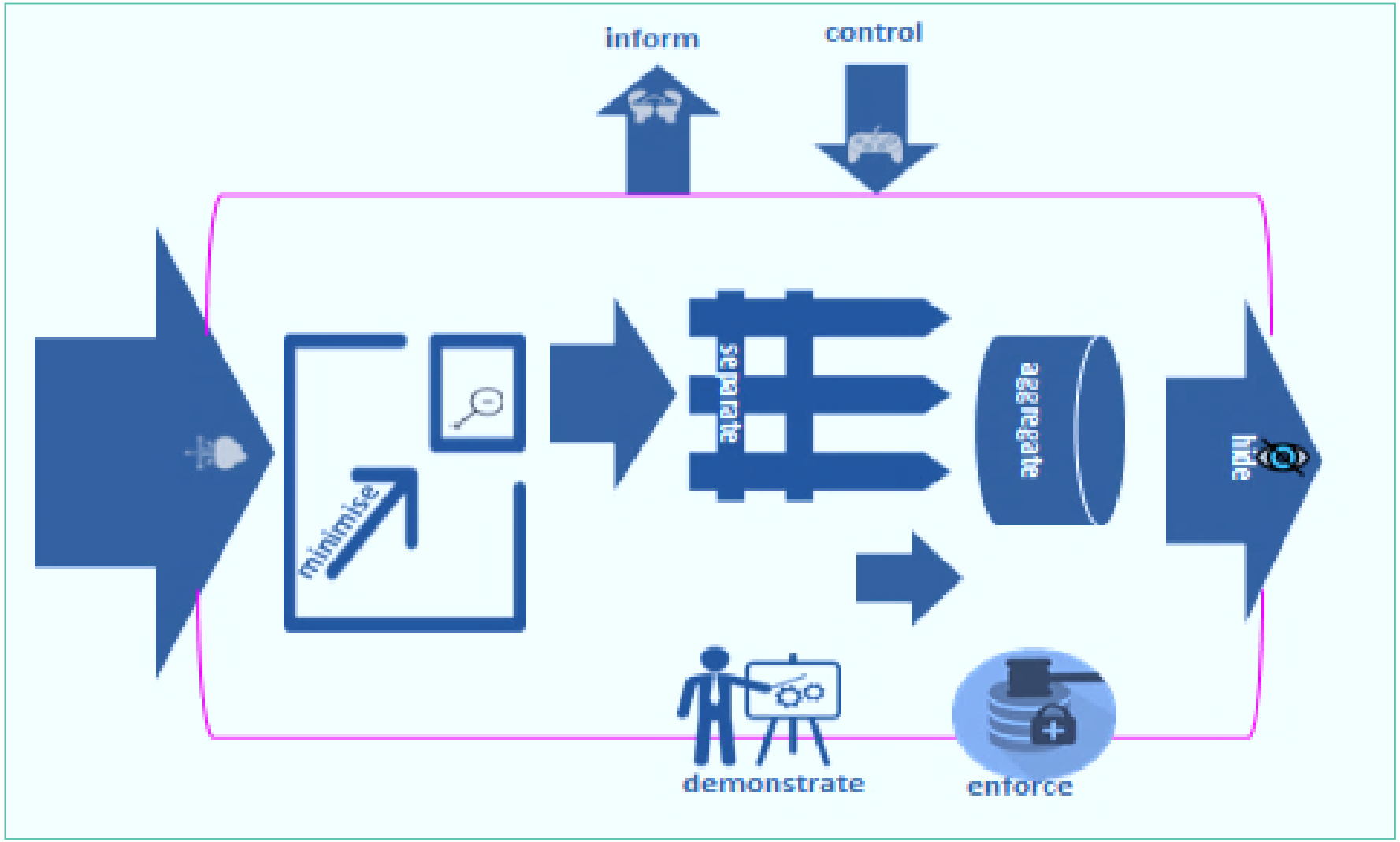
- Bewaar gegevens gescheiden
- Astrabeheer wat relevant is voor het doel
- Bescherm de gegevens die je beheert

Organisatorisch (ook in inkoop- en beleidsprocessen!):

- Informeer begrijpelijk
- Geef controle aan de betrokkene over zijn rechten
- Maak gegevensbeschermings-beleid en laat dit intern naleven
- Toon aan dat dataprotectie, incl. informatiebeveiliging op orde is (accountability).

PBLQ

verbinders in de informatiesamenleving



Ad 5) Gegevenseffectbeoordeling (PIA)

verbinders in de informatiesamenleving

Wanneer **een verwerking een hoog risico inhoudt**, moet de verwerkingsverantwoordelijke een gegevenseffectbeoordeling (PIA) uitvoeren. O.a. bij een grootschalige verwerking van bijzondere gegevens: strafrechtelijke gegevens, gezondheidsgegevens etc.

Hebben jullie hier ervaring mee?

Best practice:
https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia

Ad 6) Strengere eisen voor verwerkers

PBLQ
verbinders in de informatiesamenleving

- Bij Wbp was de bewerker niet verplicht voor een subbewerker toestemming te vragen bij de verantwoordelijke. Bij de AVG is de verwerker (= bewerker onder Wbp) hiertoe wel verplicht.
- Verwerkers moeten een overzicht gaan bijhouden van alle categorieën persoonsgegevens die zij verwerken in opdracht van een verantwoordelijke.
- Verwerkers moeten verwerkingsverantwoordelijke op hoogte stellen datalek.
- Soms moet de verwerker een privacy officer aanstellen: als publieke organisatie, of verwerking van bijzondere gegevens op grote schaal.

Ad 7) Certificering

PBLQ
verbinders in de informatiesamenleving

- Privacycertificering is nieuw. Wordt op grond van artikel 42 AVG belangrijk en de houding van consumenten/gebruikers/patiënten is veranderd.
- Artikel 42 AVG: om transparantie en naleving van de AVG te bevorderen dient het instellen van certificeringsmechanismen en gegevensbeschermingszegels en –merktekens te worden bevorderd, zodat betrokkenen snel producten en diensten hierop kunnen beoordelen.
- De verantwoordelijke zal moeten kunnen aantonen dat persoonsgegevens veilig worden verwerkt, bijvoorbeeld via een privacy-audit.
- NEN 7510: 2017 is goede en specifieke basis voor certificering van informatiebeveiliging in de zorg overeenkomstig de AVG.

Jullie vragen?

PBLQ
verbinders in de informatiesamenleving