GDPR (Avg) en ISO 27001

Beer Franken, Piasau

Beer Franken

- Loondienst
  VUmc (7 jaar), VWS (9 jaar), ZonMw (7 jaar), AMC (8 jaar)

- Zelfstandige (6 jaar)
  Wolters Kluwer, Quintiles IMS, Baker McKenzie, Z-CERT

- Privacy
  Wbp, Avg, Wgbo etc.

- Informatiebeveiliging
  ISO 27001/27002, NEN 7510 etc.

Privacy is niet nieuw

1890 Warren & Brandeis (The right to privacy)

1948 Universele verklaring van de rechten voor de mens

1953 Europees Verdrag voor de rechten van de mens

1980 OECD Privacy richtlijn

1983 NL Grondwet: bescherming persoonlijke levenssfeer

1995 EU Privacy richtlijn

2000 NL Wet bescherming persoonsgegevens (Wbp)

2004 EU Handvest voor de grondrechten

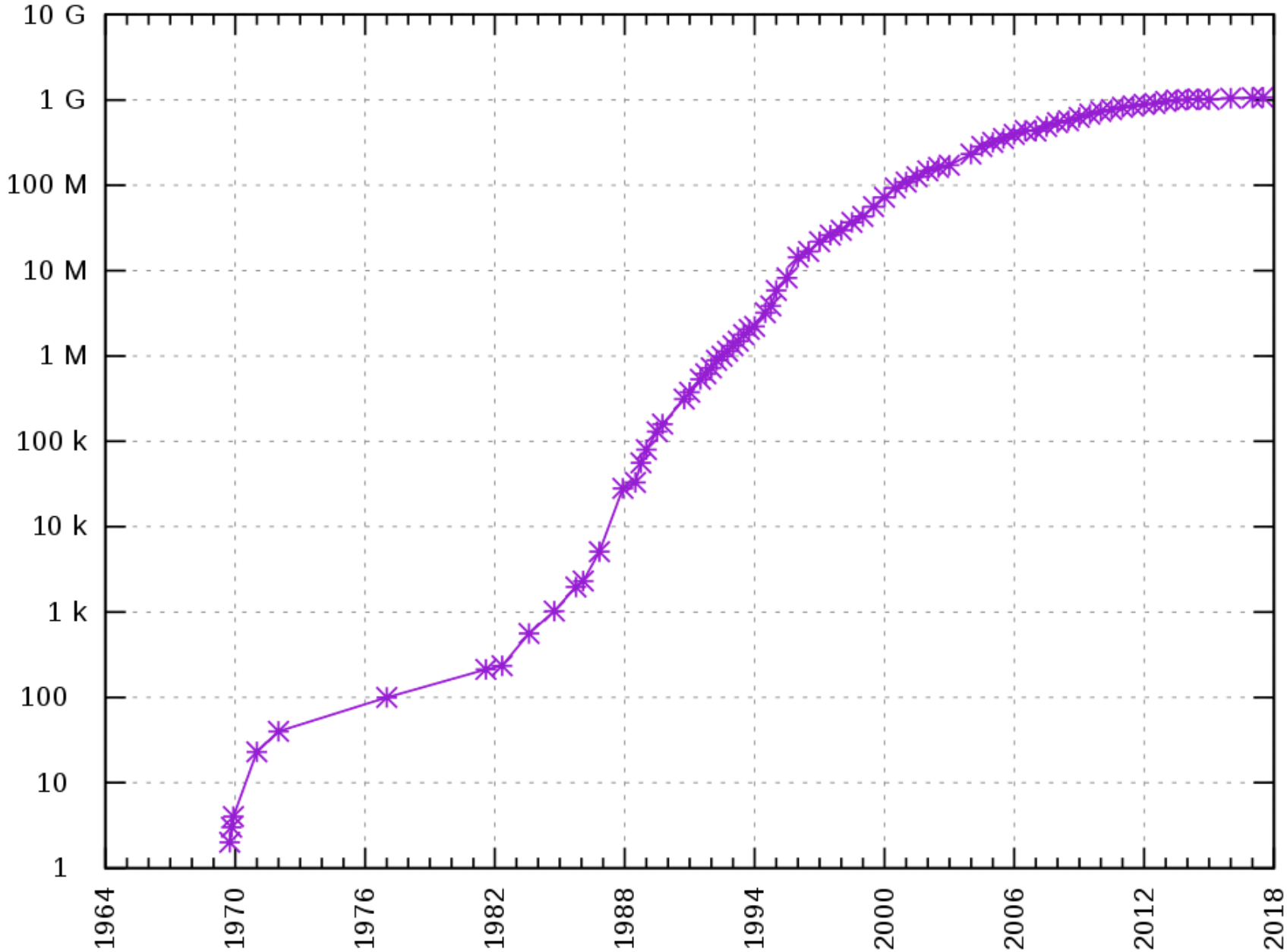
2018 EU (& NL) Algemene verordening gegevensbescherming

Informatiebeveiliging is ook niet nieuw

- jaren 80 Shell Infosec policy manual
- 1995 BS 7799
- 2000 ISO 17799
- 2005/7 ISO 27001 & 27002
- 2013 reviews van ISO 27001 en 27002

aanvullingen uit uiteenlopende sectoren (zorg al sinds 2004)

- 2018 waarschijnlijke start review ISO 27001 en 27002


10 G
1 G
100 M
10 M
1 M
100 k
10 k
1 k
100
10
1
1964
1970
1976
1982
1988
1994
2000
2006
2012
2018

Aanleiding nieuwe EU-regels

- Oude EU-richtlijn uit 1995
- Internet kende nog maar 1 miljoen websites, nu 1 miljard
- Google, Facebook, E-bay, YouTube etc. bestonden niet
- Implementatie in lidstaten uiteenlopend, nu EU-verordening

- Nationale implementatie is niet nodig (Avg = wet)
- EU-wetgeving overtroeft NL-wetgeving

Inhoud/samenstelling Avg

I	Algemene bepalingen
II	Beginselen
III	Rechten van betrokkenen
IV	Plichten van verwerkingsverantwoordelijke en verwerker
V	Doorgifte naar derde landen
VI en VII	Toezichthouders
VIII	Sancties
IX	Nationale afwijkingen → Uitvoeringswet Avg (Uavg)
X en XI	Overig en slotbepalingen

Enkele begrippen

Verwerkingsverantwoordelijke (controller, Wbp: verwerker):
bepaalt doel en middelen van de verwerking

Verwerker (processor, Wbp: bewerker): doet wat de verantwoordelijke zegt dat ie moet doen *en niets meer*

Verwerking bewerking(en), zoals: verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, doorzenden, verspreiden, ter beschikking stellen, aligneren, combineren, afschermen, wissen of vernietigen

Betrokkene natuurlijk persoon, (in)direct identificeerbaar;
niet of *jij* het kunt, maar of *het* kan

Nieuw in Avg

- Accountability
- Gegevenswissing
- Gegevenscorrectie
- Aandacht voor zwakkere partijen
- Beperking van verwerking
- Gegevensoverdraagbaarheid
- Privacy Impact Assessment
- Privacy by Design
- Privacy by Default
- Verplichte FG (als veel + gevoelig)
- Afschrikwekkend hoge boetes
- en meer ...

Beginselen

1 Rechtmatigheid
2 Behoorlijkheid (fairness)
3 Transparantie
4 Doelbinding
5 Minimale gegevensverwerking (dataminimalisatie)
6 Juistheid (accuracy)
7 Opslagbeperking
8 Integriteit
9 Vertrouwelijkheid
10 Verantwoordingsplicht (accountability) → omkering bewijslast

Rechtmatigheid (eerste beginsel)

1. Toestemming van de betrokkene
2. Uitvoering van een overeenkomst
3. Wettelijke verplichting
4. Vitale belangen betrokkenen/anderen
5. Algemeen belang/uitoefening openbaar gezag (wettelijk opgedragen)
6. Gerechtvaardigde belangen verantwoordelijke/derde,
   tenzij grondrechten betrokkene zwaarder wegen, vooral bij kinderen

Rechten van betrokkenen (27002 § 5.1.1)

Beleidsregels ... behoren eisen te behandelen die voortkomen uit ... wet- en regelgeving ...

1 Informatie over gegevensverwerking en persoonsgegevens
beknopt, eenvoudig toegankelijk en begrijpelijk, in duidelijke en eenvoudige taal
2 Toegang tot persoonsgegevens/Recht van inzage
3 Recht op rectificatie* (verbetering, *niet* wijziging)
4 Recht op gegevenswissing* ("recht op vergetelheid")
5 Recht op beperking van de verwerking
6 Recht op overdraagbaarheid van gegevens
7 Recht van bezwaar

* doorgeven aan communicatiepartners uit het verleden

Enkele plichten **v**er**a**ntwoordelijke & **v**er**w**erker

Va+Vw	overzicht van en inzicht in verwerkingsactiviteiten	§ 8.1.1
Va+Vw	implemeteren van technische en organisatorische maatregelen	27002
Va	maatregelen periodiek herzien en verbeteren indien nodig	27001
Va	privacy-by-design	§ 6.1.5, 14.1.1
Va	hoog risico: PIA uitvoeren	
Va	privacy-by-default	§14.1.1
Va	verantwoording: naleving aantonen	
Vw	geen sub-verwerker zonder schriftelijke toestemming Va	§ 15.2.2
Vw	op basis van schriftelijke overeenkomst/wettelijke verplichting	§ 15.1.2
Vw	handelt uitsluitend op basis van schriftelijke opdrachten Va	§ 15.1.2
Vw	personeel moet gebonden worden aan geheimhouding	§ 7.1.2
Va+Vw	aanwijzen FG, indien grootschalig gevoelige persoonsgegevens	
Va+Vw	informatiebeveiliging	27001+27002
Va+Vw	melden datalekken	§ 16.1.5

Verplichte FG (§ 6.1.1)

- Mits grootschalig gevoelige gegevens verwerkt
- Kan een rol of een functie zijn, intern of extern
- Professionele kwaliteiten
- Deskundigheid qua wetgeving (Avg, Uavg, sectoraal etc.)
- Deskundigheid qua inzake gegevensbeschermingspraktijk (incl infosec)
- Vermogen om taken te vervullen:
  - Va/Vw informeren en adviseren
  - Toezien op naleving
  - Adviseren mbt PIA (*niet* PIA uitvoeren) (§ 6.1.2)
  - Contactpunt voor/samenwerken met de AP (§ 6.1.3)

Vragen?

beer.franken@piasau.nl