Praktisch werken met privacy

(onder de AVG)

18 januari 2018

mr. Marjoleine van Leerdam

Inleiding

- **Facebook** weet bij wie je gisteren op bezoek ging
- **Apple** hield bij hoe lang je er bleef
- **Samsung** hoorde wat je er zei
- **Google** wist al dat je het van plan was

“Privacy niet belangrijk vinden omdat je niets te verbergen hebt, is hetzelfde als niet geven om vrijheid van meningsuiting omdat je niets te zeggen hebt” (Edward Snowden)

Inleiding

- AVG = Algemene verordening gegevensbescherming:
  één Europese wet
- 25 mei 2018
- Meer verplichtingen: informatie- en verantwoordingsplicht
  (‘accountability’)
- Meer / nieuwe rechten voor betrokkenen: recht op ‘vergetelheid’-
  recht op dataportabiliteit
- Hoge boetes: maximaal 20 miljoen euro of
  4% van de wereldwijde jaaromzet

Programma

Deel I: *Theorie*

1. Reikwijdte en begrippenkader AVG
2. Beginselen van verwerking persoonsgegevens
3. De basisregel: doel + grondslag

Pauze (21.00-21.10)

Deel II: *Praktijk*

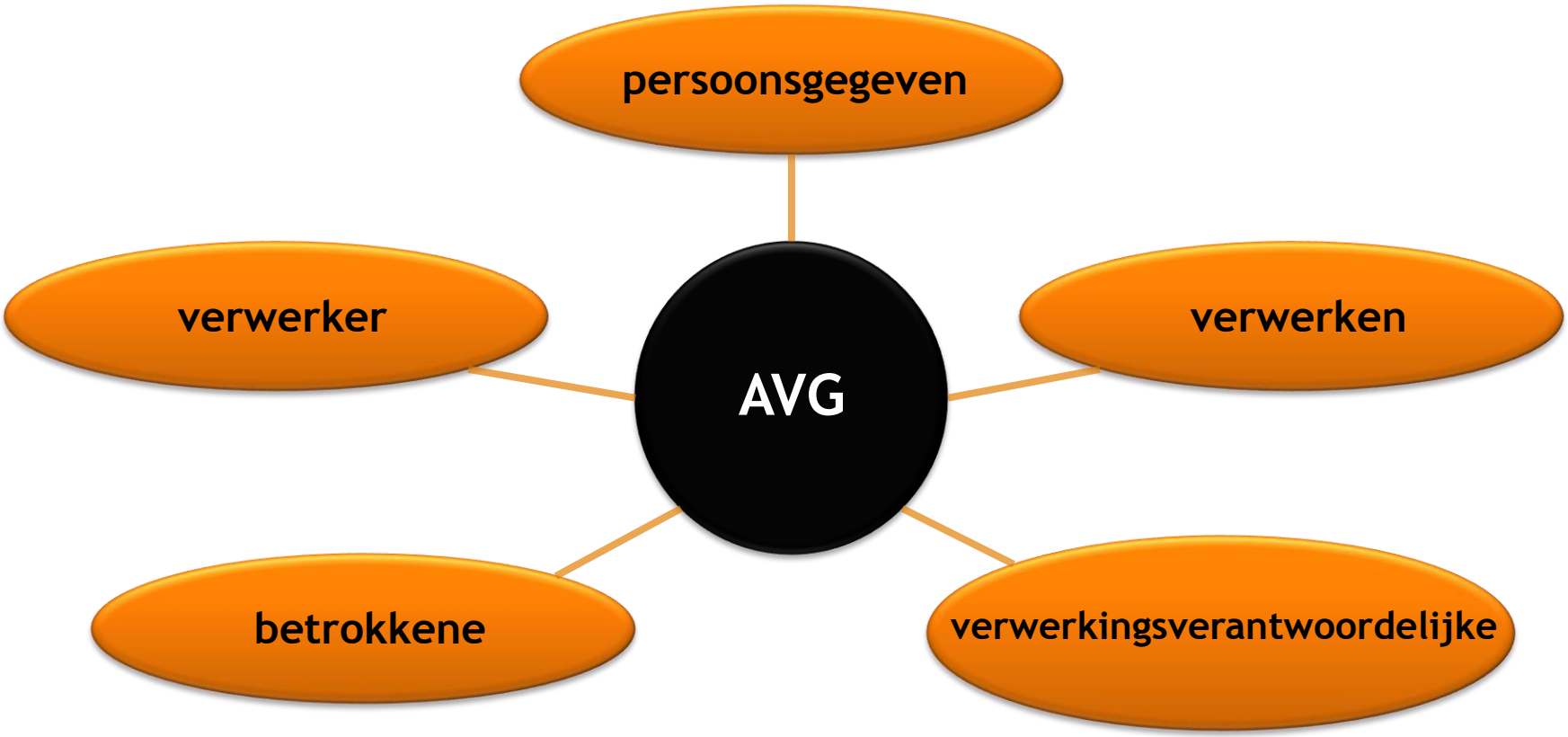
4. Wat betekent dit voor u?

   - invoeren AVG-conform privacybeleid (privacy goed regelen!)

Reikwijdte van de AVG

AVG is van toepassing op:

- de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens van betrokkenen alsmede
- de verwerking van persoonsgegevens die in een bestand zijn opgenomen


persoonsgegeven
verwerker
AVG
verwerken
betrokkene
verwerkingsverantwoordelijke

Kernbegrippen AVG

1. Persoonsgegeven:

- Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon
  - Geïdentificeerd (direct):
    - Specifieke kenmerken: naam, adres, geboortedatum
    - Singling out
  - Identificeerbaar (indirect):
    - te herleiden tot een persoon (BSN-nummer, stem, lichaamslengte, vingerafdruk, IP-adres)
    - de mogelijkheid om (zonder onevenredige inspanning) de identificatie tot stand te brengen door redelijk toegeruste verwerkingsverantwoordelijke
  - Natuurlijke persoon: van geboorte tot overlijden

Kernbegrippen AVG

1. Persoonsgegeven:

- Bijzondere persoonsgegevens
  - Ras
  - Etniciteit
  - Politieke opvattingen
  - Religie/levensovertuiging
  - Lidmaatschap vakbond
  - Genetische gegevens
  - Biometrische gegevens
  - Gezondheidsgegevens
  - Seksueel gedrag/gerichtheid

- verwerking verboden, tenzij …
  - vaak: toestemming

Kernbegrippen AVG

2. Verwerking:

elke bewerking of geheel van bewerkingen m.b.t. persoonsgegevens al dan niet uitgevoerd via geautomatiseerde procedés, zoals:

- verzamelen
- vastleggen
- ordenen
- structureren
- opslaan
- bijwerken/wijzigen
- opvragen
- raadplegen
- gebruiken
- verstrekken d.m.v. doorzending
- vernietigen van gegevens
- verspreiden/ter beschikking stellen
- wissen
- etc. etc.

Kernbegrippen AVG

3. Verwerkingsverantwoordelijke:

stelt doel en middelen van verwerking vast → vb. vereniging, werkgever, verhuurder

4. Betrokkene:

degene wiens gegevens worden verwerkt → vb. verenigingslid, werknemer, huurder

5. Verwerker:

verwerkt buiten dienstverband ('in opdracht') persoonsgegevens t.b.v. verantwoordelijke → vb. sportlink, ICT-dienstverlener

wille donker

advocaten

Beginselen van verwerking persoonsgegevens

Verwerking van persoonsgegevens moet zijn:

- rechtmatig, behoorlijk en transparant
- voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden
- mogen niet verder worden verwerkt (doelbinding)
- toereikend, ter zake dienend en beperkt tot wat noodzakelijk is
- juist zijn en worden geactualiseerd indien nodig
- worden bewaard in een vorm die de opslag beperkt tot wat nodig is
- beveiligd worden door het nemen van passende technische en organisatorische maatregelen
- VERANTWOORDINGSPLICHT: omgekeerde bewijslast

Basisregel

Voor elke verwerking heb je altijd nodig:

DOEL + GRONDSLAG

anders geen rechtmatige verwerking

Basisregel

Doel (art. 5 AVG)

Zelf conform beginselen vaststellen:

- inschrijving nieuw lid
- aangaan overeenkomst met vrijwilliger/medewerker
- het toezicht en de beveiliging op personen en gebouwen
- het berekenen en vastleggen van inkomsten en uitgaven en het doen van betalingen
- het behandelen van geschillen

Basisregel

Grondslag (art. 6 AVG)

AVG geeft limitatieve opsomming:

- toestemming betrokkene (maar: kan worden ingetrokken!)
- noodzaak sluiten/uitvoeren overeenkomst (lidmaatschapsovereenkomst, vrijwilligersovereenkomst)
- noodzaak naleving wettelijke verplichtingen (fiscaal)
- noodzaak vitaal belang
- noodzaak uitoefening taak van algemeen belang
- noodzaak gerechtvaardigd belang

wille donker

advocaten

Pauze

Wat betekent dit voor u?

Inventarisatie:

- Verwerkingen **in kaart brengen**

- **aantonen** dat de verwerking van persoonsgegevens plaatsvindt conform **de beginselen van de AVG** (artikel 5 AVG)
  - doel + grondslag

- **Privacy Impact Assessments (PIA's)** op gegevensverwerkingen met een hoog risico en maatregelen doorvoeren in manier van werken

Wat betekent dit voor u?

Vastleggen:

- een **register van verwerkingsactiviteiten** bijhouden
  - van meldplicht naar documentatieplicht
  - register bevat metadata over persoonsgegevens (bewaartermijn, doel, ontvangers, vindplaats, etc.)

- een **verwerkersovereenkomst** afsluiten
  - bestaande bewerkersovereenkomsten aanpassen
  - standaard bij aangaan overeenkomsten

Inzoomen: verwerkersovereenkomst

- borging: verwerker in staat om AVG na te komen
- deskundigheid, betrouwbaarheid en middelen
- hoofdelijke aansprakelijkheid verantwoordelijke én verwerker
- inhoud: algemene omschrijving, schriftelijke instructies, geheimhouding, beveiliging, sub-bewerkers, rechten betrokkenen, gegevens verwijderen, audits

Wat betekent dit voor u?

Beleid:

- **passende technische en organisatorische maatregelen** nemen
  - informatiebeveiliging (certificaten, vb. ISO 27001/27002)
  - werkprocessen (clean desk, bewaren wachtwoorden, kasten/deuren op slot, vergrendeling scherm)

- voorbereid zijn op een toekomstig **datalek**

Inzoomen: een datalek

- **datalek:** een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking dan wel ongeoorloofde toegang.

To do:

1. Inventariseren: welke verwerkingen kennen hoge risico's? (PIA's, register)
2. Draaiboek vaststellen 'hoe om te gaan met een (mogelijk) datalek?
3. Communicatie afstemmen (melding AP en/of betrokkene);
4. Met verwerkers een meld- en documentatieplicht overeenkomen;
5. Overzicht bijhouden van geconstateerde inbreuken.

Inzoomen: een datalek

- melding datalek binnen 72 uur bij **AP**, tenzij het niet waarschijnlijk is dat de inbreuk een risico is voor de rechten en vrijheden van een natuurlijke persoon

- melding datalek bij **betrokkene** als: inbreuk waarschijnlijk een hoog risico voor rechten en vrijheden inhoudt
  - hoog risico: sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens
  - tenzij:
    - passende maatregelen (vooraf)
    - passende maatregelen (achteraf)
    - onevenredige inspanningen

Voorbeelden

Wel melden AP	Niet melden AP
Verloren laptop/usb/telefoon met onversleutelde, persoonsgegevens	Verkeerd verstuurder brief die ongeopend retour wordt gezonden
Technische storing systeem, hack of virus waardoor onbevoegden toegang hebben tot persoonsgegevens	Zoekraken of hacken van ledenadministratie van een sportvereniging (wel vervelend, niet gevoelig)
Hack waarbij klantgegevens/wachtwoorden zijn ontvreemd	Ziekenhuispersoneel (wel bevoegd) maakt gebruik van wachtwoord van een arts om toegang te krijgen tot medische gegevens. Geen datalek, maar schending voorschriften.
Verlies of diefstal van versleutelde laptop/usb/telefoon met persoonsgegevens, waarvan geen back-up is.	Iemand vergeet een koffer in de trein. Koffer is voorzien van deugdelijk slot en komt via 'gevonden voorwerpen' ongeopend weer terug.
Papieren met persoonsgegevens niet versnipperd weggegooid en door derde uit container is gehaald.	Database is vernietigd door menselijke fout, maar er bestaat een volledige, actuele back-up (geen datalek)
Vanwege fout konden alle gebruikers elkaars accountgegevens zien. Niet vast te stellen of daadwerkelijk toegang was.	
E-mail met daarin persoonsgegevens is aan de verkeerde persoon verstuurd.	
Bij een lek zijn gevoelige gegevens verloren gegaan of verstrekt aan onbevoegden.	

Wat betekent dit voor u?

Beleid:

- **Rechten van betrokkenen** waarborgen:
  - aanspreekpunt verzoeken
  - procedure afhandeling verzoeken
    - binnen een maand (uitstel 2 maanden)
    - belangenafweging
  - administratieve consequenties

Inzoomen: rechten van betrokkenen

- informatie
- inzage + kopie
- correctie
- wissing
- bezwaar
- dataportabiliteit
- beperking verwerking

Wat betekent dit voor u?

Beleid:

- **Functionaris gegevensbescherming (FG):**
  - onafhankelijke functionaris
  - kennis delen, adviseren, toezicht houden, communiceren
- Wanneer **verplicht?**
  - de (semi-)overheid
  - organisaties die als core business:
    - bezig zijn met verwerkingen die vanwege hun aard, omvang of doel regelmatige observatie van betrokkenen vereisen, of
    - op grote schaal bijzondere gegevens verwerken

Wat betekent dit voor u?

Bewustwording:

- **Informatieplicht** (laagdrempelig en in begrijpelijke taal)!
  - privacyverklaring
  - vb. overeenkomst, en privacy statement website

- werken aan **bewustwording**
  - bewustwordingscampagne
  - trainingen (instructie personeel, vrijwilligers)
  - workshops

Resultaat

Compliance op vier niveaus:

1. **Moreel** (maatschappelijke belangen vs. belangen betrokken, ‘moeten we dit wel willen’)

2. **Formeel** (integraal privacybeleid, reglement en protocollen)

3. **Maatschappelijk** (in dialoog kunnen treden met stakeholders)

4. **Toezicht** (uitleggen en aantonen aan de AP, voorkomen boete)

wille donker

advocaten

Dank voor uw aandacht

en graag tot een volgende keer!

Leidse Schouw 2
2408AE Alphen aan den Rijn

T +31(0)172 - 44 24 17
F +31(0)172 - 44 20 28

E info@willedonker.nl
W www.willedonker.nl