RECHT-VAARDIG ADVIES
JURIDISCH & COMPLIANCE ADVISEUR

DE AVG IN EEN NOTENDOP

Maike van Zutphen
Legal, Compliance & Privacy Officer


ON YOUR MARK
GET READY
25 mei 2018
GDPR

Algemeen

- **Algemene verordening gegevensbescherming**
- Europese wet die geldt voor iedereen in de EU (GDPR = AVG)
- De AVG neemt de plaats in van de Wet bescherming persoonsgegevens (Wbp)
- Betrekking op persoonsgegevens
- **Doel: 25 mei 2018** uiterlijk compliant!
- **Ready…….set……..PRIVACY!**

AVG samengevat – wat moeten we doen?

Aantonen

Zorg dat compliance kan worden aangetoond, ook over 10 jaar

Wees transparant

Implementeren

Implementeer Privacy by Design

Implementeer Privacy by Default

Documenteren

Houd intern register verwerkingen bij

Houd incidentenregister bij

Samenwerken

Werk samen met toezichthouders (AP)

Raadpleeg AP in high-risk cases

Beveiligen

Beveilig data en IT systemen

Gebruik encryptie

Test beveiliging

Informeren

Gebruik privacy statements

Wijs betrokkene op zijn rechten

Informeer betrokkene en AP over datalekken

Doen

Check verwerkersovereenkomsten (DPA)

Doe Privacy Impact Assessments (PIA)

Trainen medewerkers

Monitor compliance

Professionals

Benoem Data Protection Officer

Zorg voor een datalekkenteam

Wat staat er in de overeenkomst?

Algemene Voorwaarden
t.b.v. VvE Beheerders

- Artikel 2.5: "*De VvE verleent – voorzover noodzakelijk voor een juiste uitvoering van de door haar opgedragen werkzaamheden – de Beheerder toestemming om bij de* ***uitvoering van de haar werkzaamheden*** *de persoonsgegevens van de leden te verwerken met in acht neming van de Wet*"

Wat zijn persoonsgegevens?

- Persoonsgegevens zijn:

  "alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon verstaan. De informatie dient direct of indirect (door middel van herleiding) te kunnen leiden tot identificatie van een natuurlijk persoon"

- Voor de hand liggende persoonsgegevens zijn iemands naam, adres, woonplaats, BSN-nummer en (e-mail)adres. Minder voor de hand liggende persoonsgegevens zijn kentekengegevens en IP-adressen.

VERWERK IK PERSOONSGEGEVENS?

Verwerken = verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken,...

+

Persoonsgegevens = alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (naam, volgnummer, locatie, ...). Deze persoon noemen we de **betrokkene**

Ik verwerk persoonsgegevens, dus ik moet **voldoen** aan de Privacywetgeving (*)

Ik ben **verwerkingsverantwoordelijke** ('controller'): ik zeg hoe en waarom de persoonsgegevens worden verwerkt

Ik ben **verwerker** ('processor'): ik treed op ten behoeve van de verwerkingsverantwoordelijke

Wanneer mag ik persoonsgegevens verwerken?

De verwerking moet rechtmatig zijn.

Dit zijn de **rechtvaardigheidsgrondslagen** uit de AVG

Uitleg grondslagen

- Uitdrukkelijke en expliciete ondubbelzinnige **toestemming** van de klant. Dit moet je kunnen aantonen (en net zo makkelijk opt-out).
- Vitale belangen “dringende medische noodzaak”
- In de uitvoering van een wettelijke verplichting noodzakelijk (bijv. hennep)
- Om uitvoering te geven aan de **overeenkomst** (bijv. VVE beheer)
- Algemeen belang t.b.v. publiekrechtelijke taak of gezag
- Gerechtvaardigd belang (belangen afweging Verantwoordelijke – Betrokkene)

Gerechtvaardigd belang direct marketing

- *Direct marketing* kan een gerechtvaardigd belang zijn….maar **let op**: maak altijd een belangenafweging tussen het belang van de VVE beheerder en haar leden. En de richtlijnen op het gebied van soft-op-in.

- Klant moet altijd het recht hebben om bezwaar hier tegen te maken (opt-out)

- Aan de beheerder de taak om aan te tonen dat het belang van de beheerder zwaarder weegt dan het belang van het desbetreffende lid

Overzicht verwerkingen

Verplicht om alle verwerkingen in kaart te brengen. Welke persoonsgegevens worden er verwerkt, onder welke ***grondslagen***, met welk doel, hoe lang ze worden bewaard en met wie worden ze gedeeld?

Voorbeeld verwerkingen binnen de VVE:

- Het afhandelen van betaling/incasso
- Informeren over wijziging van diensten en producten
- Verzenden van nieuwsbrief en/of nieuwsberichten
- Cameratoezicht (gerechtvaardigd belang)
- Kentekenregistratie parkeren (gerechtvaardigd belang)
- Etc.

Bewaartermijn
Persoonsgegevens mogen niet meer langer worden bewaard dan noodzakelijk
Bepaal voor alle verwerkingen de bewaartermijn en ga daarna over tot wissen.
Let op; unstructered data (mailbox, persoonlijke files e.d.)

Overzicht verwerkingen

Delen van persoonsgegevens*:* De vraag is dus, wat deel je en met wie deel je dat? Welke informatie bevat privacy (niet zomaar opvraagbaar) en welke informatie kan je vrij delen met leden en derden

Tip: Laat je leden geheimhoudingsovereenkomst tekenen als zij omgaan met privacy informatie van leden.

Verplicht register? Een register moet in elk geval worden bijgehouden wanneer een organisatie meer dan 250 pers in dienst heeft **OF**

- risicovolle verwerkingen (zoals het opstellen van klantprofielen, of het verwerken van grote hoeveelheden gegevens)
- wanneer structureel persoonsgegevens verwerkt worden
- of bij het verwerken van gevoelige gegevens.

Lijkt voor een VVE beheerder niet snel het geval te zijn

Rechten van betrokkene

- Onder de AVG krijgen leden meer en **verbeterde** privacy rechten. Sommige rechten bestaan al, sommige rechten zijn nieuw.

Rechten van betrokkene

- Onder de AVG krijgen leden meer en **verbeterde** privacy rechten. Sommige rechten bestaan al, sommige rechten zijn nieuw.

Recht op informatie (privacy statement)

- **Leden uitgebreid infomeren over (forse uitbreiding)**
  Contactgevens, verwerkingsdoeleinden en rechtsgrond, gerechtvaardigd belang bij verwerking, de ontvanger(s), doorgifte aan derde landen. Termijn opslag persoonsgegevens, rechten van betrokkene, of verstrekking verplicht is er wat de gevolgen zijn van niet verstrekking en de doeleinden bij verdere verwerking.

- **Tijdstip:** Bij verkrijgen van de persoonsgegevens.

- Data niet rechtstreeks verkregen van de leden? Ook informatie over de categorieën van persoonsgegevens en de bron, binnen een maand na eerste contact (tenzij onmogelijk, onevenredig of wettelijk verbod)

- **Tip:** bewaren kopie privacy statement in dossier

Recht om
in te zien

Recht om
te wijzigen

Recht om vergeten
te worden

Recht om gegevens
over te dragen

- Werk met een inzageprotocol en verzoekformulier
- Check **altijd** identiteit van de verzoeker
- Verstrek alleen kopie persoonsgegevens verzoeker, geen overige data (let op: *fishing expeditions)*
- Verwijder alle persoonsgegevens van derden (denk hierbij aan interne notities, personeelsgegevens)
- Bewaar een kopie van het verzoek en de reactie.

Bewerkers?

- Geeft u persoonsgegevens door aan een verwerker? Bijv. aan een leverancier?
- **Tip**: Geef alleen persoonsgegevens die **strikt** noodzakelijk zijn om de dienst uit te kunnen voeren. Bijv. schilderwerkzaamheden. Geef alleen adres, telefoonnummer en/of e-mailadres. Beperk het verstrekken van persoonsgegevens. Welke persoonsgegevens zijn echt noodzakelijk?
- Identificeer alle verwerkers in de keten en sluit een contract. Ook als er incidenteel persoonsgegevens worden gedeeld! Is de bewerker een dochteronderneming? Dan ook!
- Als verantwoordelijke **aansprakelijk** voor gedragingen verwerker.
- Standaard contractbepalingen zijn mogelijk, beschikbaar in de markt. Maak goede afspraken en evalueer deze. Leg afspraken contractueel vast.

Beveiliging van persoonsgegevens

- Passende technische en organisatorische maatregelen
  Doel: een passend beveiligingsbeleid waarborgen

- Tips
  - Analyseer je risico's (bankrekening extra gevoelig)
  - Beveilig alle data en IT systemen
  - Ken de stand van de techniek + gebruiken in de markt
  - Check richtsnoeren beveiliging AP
  - Test geïmplementeerde beveiliging jaarlijks
  - Zorg voor beschikbaarheid data in geval falen beveiliging
  - *Principle of least privilege*: Als je het niet hoeft in te zien heb je ook geen rechten om het in te zien (IAM)

Meldplicht datalekken en incidenten

- De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan de registratie

- Praktische tips
  - Ken je dataflows
  - Denk aan het beveiligd versturen van persoonsgegevens (Zivver of Wetransfer zakelijk)
  - Inventariseer je risico's
  - Bepaal noodzakelijke beveiligingsniveau
  - Maak afspraken met Verwerkers over datalekken
  - Check de beleidsregel datalekken

Meldplicht datalekken en incidenten

Speerpunten AVG (Resumé)

- **Data-inventory**. Maak inzichtelijk hoe en welke persoonsgegevens uw organisatie verwerkt. Het moet duidelijk zijn welke persoonsgegevens worden gebruikt, met welk doel, onder welke rechtsgrond, waar ze worden opgeslagen en wie er toegang hebben tot die gegevens.

- Is de rechtsgrond **toestemming?** Evalueer de manier waarop u mensen toestemming vraagt, krijgt en registreert. De AVG stelt strengere eisen aan de toestemming die mensen moeten geven voor het verwerken van gegevens.

- De tijd van klakkeloos persoonsgegevens verzamelen en gebruiken is voorbij! Je hebt een **rechtsgrond** nodig. *Een VVE-vergadering*. Natuurlijk heb je naam- en telefoonnummer nodig. Wil je een geboortedatum zodat je informatie kan geven aan een leverancier om een gericht commercieel aanbod te doen? Dan moet je daar toestemming voor vragen.

- Bedenk je een nieuw product of dienst? Dan moet je direct rekening gaan houden met de privacy en toetst altijd de rechtsgrond. Verwerk alleen persoonsgegevens die noodzakelijk zijn voor het doel.

- Maak duidelijk in een **privacy-statement** hoe je omgaat met persoonsgegevens, welke persoonsgegeven er worden verwerkt, voor welk doel, om welke reden en aan wie deze worden doorgegeven. Zorg dat dit helder, kort en overzichtelijk is.

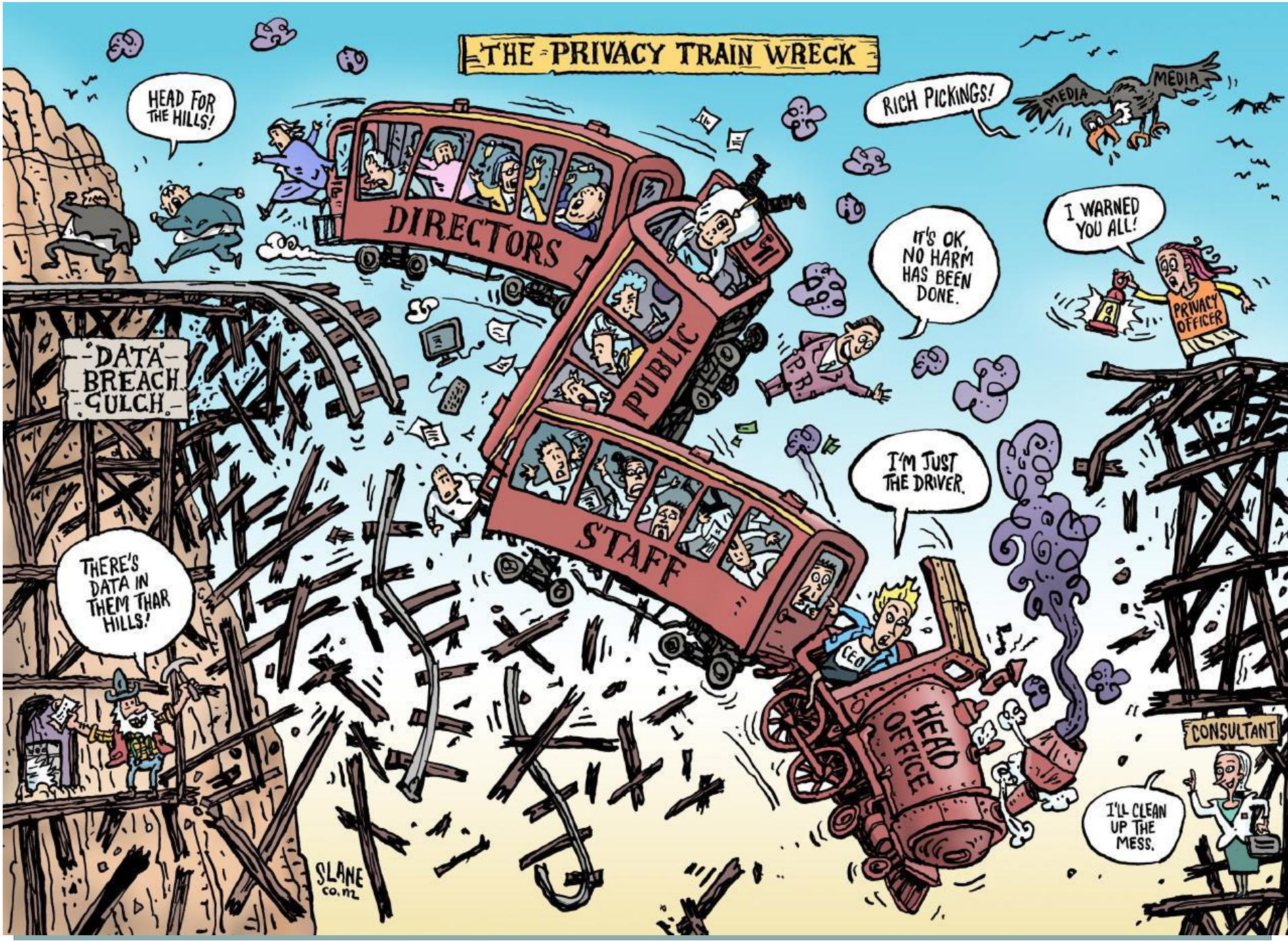
Speerpunten AVG (Resumé)

- Zorg dat elke **medewerker** die werkt met persoonsgegevens de nieuwe privacywetgeving begrijpt en kent.

- Je bent **aansprakelijk** voor alle persoonsgegevens binnen jouw bedrijf. Ook als die door externe partijen worden opgeslagen of toegepast. Sluit daarom bewerkersovereenkomsten!

- Worden er persoonsgegevens verwerkt in systemen? Zorg dat deze systemen technisch worden bekeken qua beveiliging **(data-security**) maar ook zodat het mogelijk is om data aan te passen, te verwijderen, of om desgevraagd inzage te geven. En denk ook alvast na over deze processen.

- Je moet er alles aan doen om persoonsgegevens veilig te bewaren. Toch een ***datalek*** door een verloren USB-stick of laptop, of een hack in het systeem? Dan moet je dat binnen 72 uur melden bij de Autoriteit Persoonsgegevens.


THE PRIVACY TRAIN WRECK
HEAD FOR THE HILLS!
DIRECTORS
PUBLIC
STAFF
RICH PICKINGS!
MEDIA
MEDIA
I WARNED YOU ALL!
PRIVACY OFFICER
IT'S OK, NO HARM HAS BEEN DONE.
I'M JUST THE DRIVER.
CEO
HEAD OFFICE
DATA BREACH GULCH
THERE'S DATA IN THEM THAR HILLS!
CONSULTANT
I'LL CLEAN UP THE MESS.
SLANE co.nz