CRIVITS & PERSYN

ADVOCATEN

General Data Protection Regulation

CRIVITS & PERSYN
ADVOCATEN

GDPR, ook voor u (en ons)

26 april 2018 - Kortrijk

Bram Baert en Astrid Lescouhier


WHY DO YOU GET THAT LOOK WHENEVER WE TALK ABOUT GDPR COMPLIANCE?
TOM FISH BURNE
© marketoonist.com

CRIVITS & PERSYN
ADVOCATEN

Plan van de avond

1. **Introductie tot de GDPR**
   - ¬ Juridisch kader
   - ¬ Waarom de Verordening?
   - ¬ Toepassingsgebied van de Verordening?
   - ¬ Begrippenkader
2. **Wat houdt de GDPR in**?
   - ¬ Basisbeginselen en overkoepelende principes
   - ¬ Rechtsgrond
   - ¬ Verplichtingen van de verantwoordelijke
   - ¬ Rechten van de betrokkene
3. **Hoe de GDPR implementeren?**
   - ¬ Praktische vertaling en stappenplan

1. Introductie tot de GDPR

- ***G**eneral **D**ata **P**rotection **R**egulation*
  - Algemene Verordening Gegevensbescherming (AVG)
  - In werking getreden op 25 mei 2016
  - Van toepassing vanaf **25 mei 2018**
    - Vervangt de Richtlijn van 1995

1.1. Juridisch kader

- Gegevensbescherming ➔ privacy

- Huidig juridisch kader
  - Wet Verwerking van Persoonsgegevens 1992
  - Richtlijn van 1995 omgezet in 1998

- Aanpassing nationale regelgeving verwacht

1.2. Waarom de Verordening?

- **Harmonisering** van het privacyrecht in de EU
  - Wegnemen belemmering interne markt
  - Kostenbesparing (cf. het “one-stop-shopprincipe”)
  - Maar ruimte voor nationale wetgeving blijft
    - O.m. arbeidsrechtelijk (wet/cao)
    - Ook sancties

1.2. Waarom de Verordening?

- **Actualisering** van de wetgeving (RL)
  - Aanpassen aan de “nieuwe” digitale realiteit
- De Europese burger meer **controle** geven over zijn gegevens

MAAR: “*Een nieuwe wind, geen orkaan*”

1.3. Toepassingsgebied

- **Geautomatiseerde verwerking** van persoonsgegevens
  - Verwerking van persoonsgegevens in een **bestand** opgenomen of daarvoor bestemd
    - Digitale bestanden
    - Maar ook papieren bestanden (personeelsregister, fichebak)
  - Voorbeelden: registratie van aanwezigheden, e-monitoring, database sollicitanten, camerabewaking, track & trace, fotoboek intranet,…

1.3. Toepassingsgebied

- Geautomatiseerde verwerking van **Persoonsgegevens**
  - Alle **informatie** over een geïdentificeerde of identificeerbare natuurlijke persoon;
    - Identificeerbaar a.d.h.v. een identificator
    - Voorbeelden:
      - NAW-gegevens, telefoonnummer, e-mailadres, rijksregisternummer, vingerafdruk, foto, locatiegegevens…
    - Bijzondere categorie: gevoelige gegevens
      - Gegevens m.b.t. ras, etniciteit, afkomst, religieuze of politieke overtuiging…, gezondheid, strafrechtelijke veroordelingen
      - Verwerking van gevoelige gegevens *in principe* verboden

1.3. Toepassingsgebied

- Geautomatiseerde verwerking van **Persoonsgegevens**
  - Gegevens m.b.t. **natuurlijke personen**
    - Voorbeelden: werknemers, sollicitanten, freelancers, onderaannemers, cliënteel, leveranciers (telkens indien natuurlijke personen), …
    - NIET gegevens m.b.t. rechtspersonen
      - bv. info@paycover.be
    - NIET anonieme gegevens
      - LET OP: anonieme lijst loongegevens met functieomschrijving personeel = identificeerbaar

1.3. Toepassingsgebied

- Geautomatiseerde verwerking door:
  - Ondernemingen (groot en klein)
    - Verwerkingsverantwoordelijken en verwerkers
    - gevestigd in de EU
    - gevestigd buiten de EU, maar met:
      - diensten binnen de EU
      - monitoring van inwoners van de EU

1.3. Toepassingsgebied

Uitzonderingen

- ¬ Verwerking in het kader van persoonlijke of huishoudelijke activiteiten
- ¬ Verwerking voor journalistieke, literaire of artistieke doeleinden

1.4. Begrippenkader

Betrokkene

- ¬ Natuurlijke persoon van wie persoonsgegevens worden verwerkt
- ¬ Bijzondere bescherming voor minderjarigen, kwetsbare groepen,…

Verwerking

- "een **bewerking** of een geheel van bewerkingen **met betrekking tot persoonsgegevens** of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens"

➔ ZEER RUIM

Verwerkingsverantwoordelijke

- "een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het **doel** van en de **middelen** voor de verwerking van persoonsgegevens vaststelt"
- Bepaalt het doel en de middelen

Verwerker

- "een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat **ten behoeve van** de verwerkingsverantwoordelijke **persoonsgegevens verwerkt**."
- Doet de eigenlijke verwerking
- Voorbeelden: sociaal secretariaat, cloud service provider (opslag gegevens), bewakingsfirma, boekhouder, accountant,…

2. Wat houdt de GDPR in?

- Zes basisbeginselen of overkoepelende principes "*inzake de verwerking van persoonsgegevens*"

- Niet nieuw, wel aangepast + meer rechten voor de betrokkenen

- Andere benadering:
  - Risico-gebaseerde benadering
  - Verantwoordingsplicht of "*accountability*" – "*a posteriori – controle*"

2.1. Basisbeginselen en principes

- Welke beginselen?
  I. Rechtmatigheid, behoorlijkheid en transparantie
  II. Doelbinding
  III. Minimale gegevensverwerking
  IV. Juistheid
  V. Opslagbeperking
  VI. Integriteit en vertrouwelijkheid

I. Rechtmatige, behoorlijke en transparante verwerking

- Rechtmatigheid: elke gegevensverwerking vereist een rechtmatige grondslag (zie verder)
  - Artikel 6 AGV

- Behoorlijke en transparante verwerking: betrokkene heeft kennis van de verwerking en kent zijn/haar rechten
  - Bij de verkrijging van de persoonsgegevens of binnen een redelijke termijn na verkrijging via derde
  - Schriftelijk of met andere middelen (elektronisch)
  - *Privacy notice* of verklaring

Transparante verwerking

II. Doelbinding of -beperking

- Persoonsgegevens worden voor *welbepaalde*, *uitdrukkelijk omschreven* en *gerechtvaardigde* doelen verzameld

- Geen verwerking op *een met de doeleinden onverenigbare wijze*
  - evaluatie van verenigbaarheid door verwerkingsverantwoordelijke
  - Voorbeeld: gegevens van een sollicitant gebruiken wanneer die werknemer wordt

- Uitzondering: juridische basis voor de verwerking of toestemming

III. Minimale verwerking

- De gegevens moeten *toereikend* zijn, *ter zake dienend* en *beperkt tot wat noodzakelijk is* voor de doelen waarvoor ze worden verwerkt

- Enkel pertinente gegevens

Minimale verwerking

IV. Juistheid

- Gegevens moeten *juist* en *nauwkeurig* zijn
- Gegevens moeten *geactualiseerd* (kunnen) worden
- Alle nodige maatregelen worden genomen om onjuiste gegevens te verwijderen of verbeteren
  - Tip: contractuele meldingsplicht voorzien

V. Opslagbeperking

- De gegevens worden in een vorm bewaard die mogelijk maakt de betrokkenen *niet langer te identificeren dan* voor de doeleinden waarvoor de gegevens worden verwerkt *noodzakelijk is*

- Hoe lang is “niet langer dan nodig”?
  - Verplichte bewaartermijnen
  - Verjaringstermijnen
  - Garanties en aansprakelijkheid

VI. Integriteit en vertrouwelijkheid

- Basisprincipe

- Waarborgen van passende beveiliging door het nemen van passende technische en organisatorische maatregelen
  - ISO 9001; 27001
  - Gedragscode

- Bescherming tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies/vernietiging

Accountability

- De verantwoordingsverantwoordelijke is verantwoordelijk voor de *naleving* van de basisprincipes en kan deze *aantonen*
  - Formalisering
  - Documentering
- Vervangt huidig aangiftesysteem

2.2. Concretisering: de rechtsgrond

I. Toestemming

- *Best practice* of *last resort*?

- Toestemming van de betrokken moet steeds:
  - Vrij zijn
    - Arbeidsrelatie?
  - Geïnformeerd gegeven
  - Specifiek
  - Ondubbelzinnig

- Voorbeeld:

- Toestemming is altijd intrekbaar
  - Andere rechtsgrond?

- Uitzonderlijk versterkte toestemming vereist

CRIVITS & PERSYN
ADVOCATEN

DOWNLOAD DE GDPR WHITEPAPER

E-mail *

Voornaam *

Naam *

Bedrijf *

Functie *

Marketeer

Toestemming

☑ De groep bpost en andere - al dan niet commerciële - openbare organisaties mogen (na overdracht, eventueel via leveranciers van gegevens) de gegevens die ik hen overmaak gebruiken om me producten en diensten voor te stellen die aansluiten bij mijn profiel en mijn interesses.

Uw e-mailadres zal enkel worden gebruikt door bpost (Muntcentrum, 1000 Brussel), verantwoordelijke voor de verwerking, om u deze whitepaper te sturen. Uw e-mailadres zal niet buiten onze systemen worden bewaard. Wenst u hierover meer te lezen?

II. Uitvoering van de overeenkomst

- De verwerking is noodzakelijk voor de uitvoering van de overeenkomst met betrokkene

- Enkel persoonsgegevens die strikt noodzakelijk zijn

- Voorbeelden:
  - Kredietkaartgegevens bij online bestelling
  - Invordering schuld t.a.v. klant
  - Personeelsadministratie, loonverwerking,…

III. Wettelijke verplichting

- De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting

- Enkel persoonsgegevens die strikt noodzakelijk zijn

- Voorbeelden:
  - DIMONA-melding
  - BTW-listing, fiscale fiches
  - Witwaswetgeving

IV. Gerechtvaardigd belang

- Verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verantwoordelijke of een derde
- Belangenafweging
- Mag geen afbreuk doen aan de rechten en de vrijheden van personen
    - Recht op bescherming persoonlijke levenssfeer
- Voorbeeld: direct-marketing binnen een bestaande klantenrelatie, voorkomen van fraude,…

CRIVITS & PERSYN
ADVOCATEN

Oefening: transportopdracht

Transportonderneming maakt deel uit van een internationale groep en voert hoofdzakelijk internationale vervoersopdrachten uit. Welke rechtsgrond is van toepassing voor de verwerking in functie van…?

Rechtsgrond?	Verwerking in functie van
	Levering van goederen aan een klant
	Opmaken verplichte douane documenten
	Centrale administratie van de groep
	Mailing aan prospecten m.o.o. reclame

2.3. Verplichtingen verantwoordelijke

I. Informatieverplichting

- Cfr. transparantiebeginsel
- Uitgebreide informatieverplichting
- Bestaand: coördinaten verantwoordelijke, doel van verwerking, categorie ontvanger en gegevens, recht op toegang en verbetering
- Nu uitgebreid met:
  - Rechtsgrond, opslagtermijn, uitwisseling
  - Nieuwe rechten
  - Eventueel coördinaten DPO, geautomatiseerde besluiten

- TO DO:
  - Opmaken of aanpassen van **privacy notice**
  - Eventueel gelaagde structuur
  - Voorbereiden templates met oog op:
    - Informatie aan sollicitanten
    - Informatie aan nieuwe werknemers
    - Informatie aan werknemers die al in dienst zijn

II. Documentatieplicht

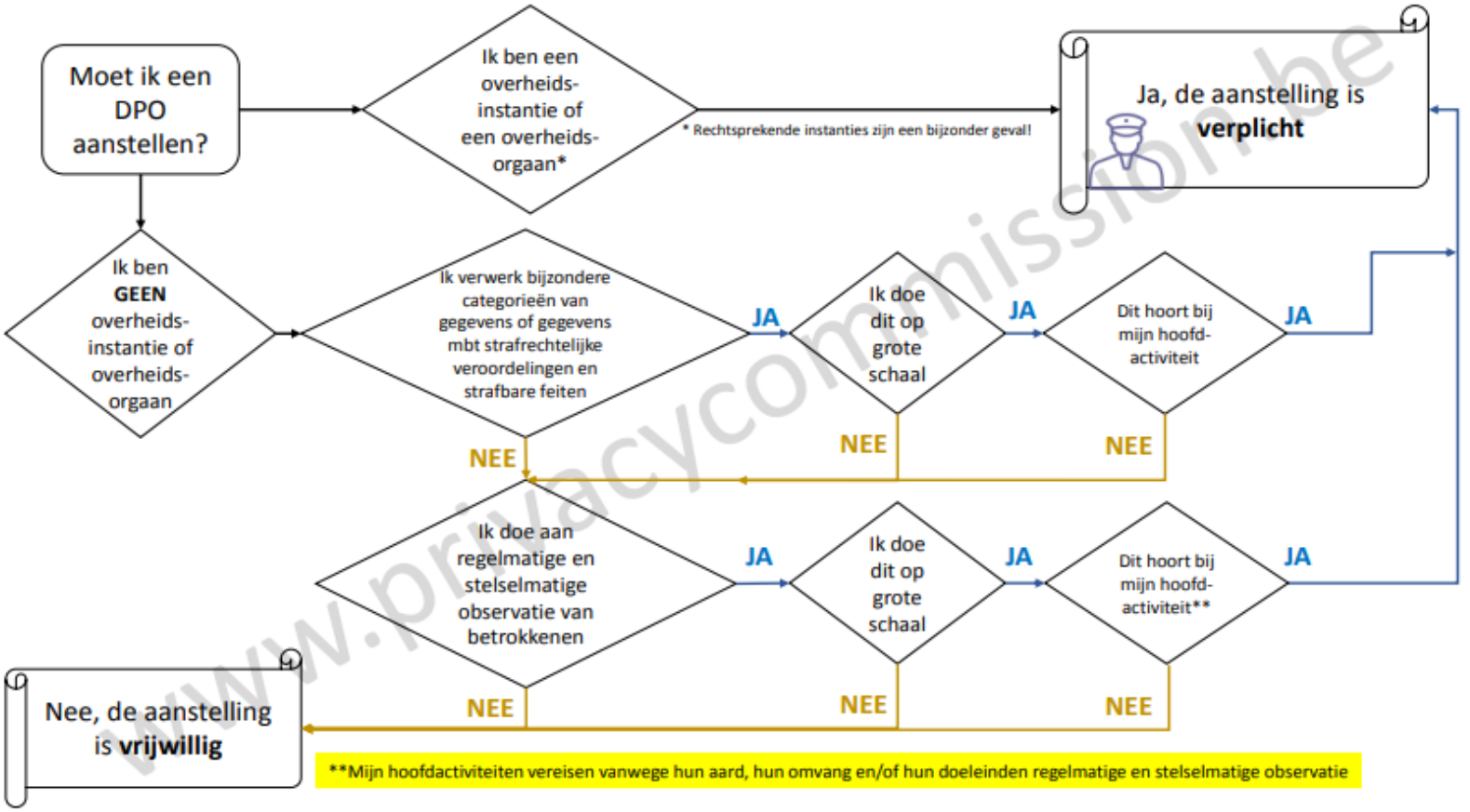
- Vervangt aangifteplicht

- Wat? **Register van verwerkingsactiviteiten**
  - Alle informatie m.b.t. de verwerking
  - Verplichte vermeldingen
  - Schriftelijk (ook digitaal)
  - Dynamisch
  - Te controleren door Gegevensbeschermingsautoriteit

- TO DO:
  - Opmaken register voor verwerkingsactiviteiten
  - Up-to-date houden van register – duidt een verantwoordelijke aan

III. Functionaris voor gegevensbescherming

- Ook wel **D**ata **P**rotection **O**fficer (DPO)
- Deskundige op gebied van wetgeving en de praktijk - contactpersoon
- Verplicht in bepaalde gevallen:
  - Grootschalige verwerking van gevoelige gegevens
  - Verwerkingen die regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen
  - Overheidsinstanties

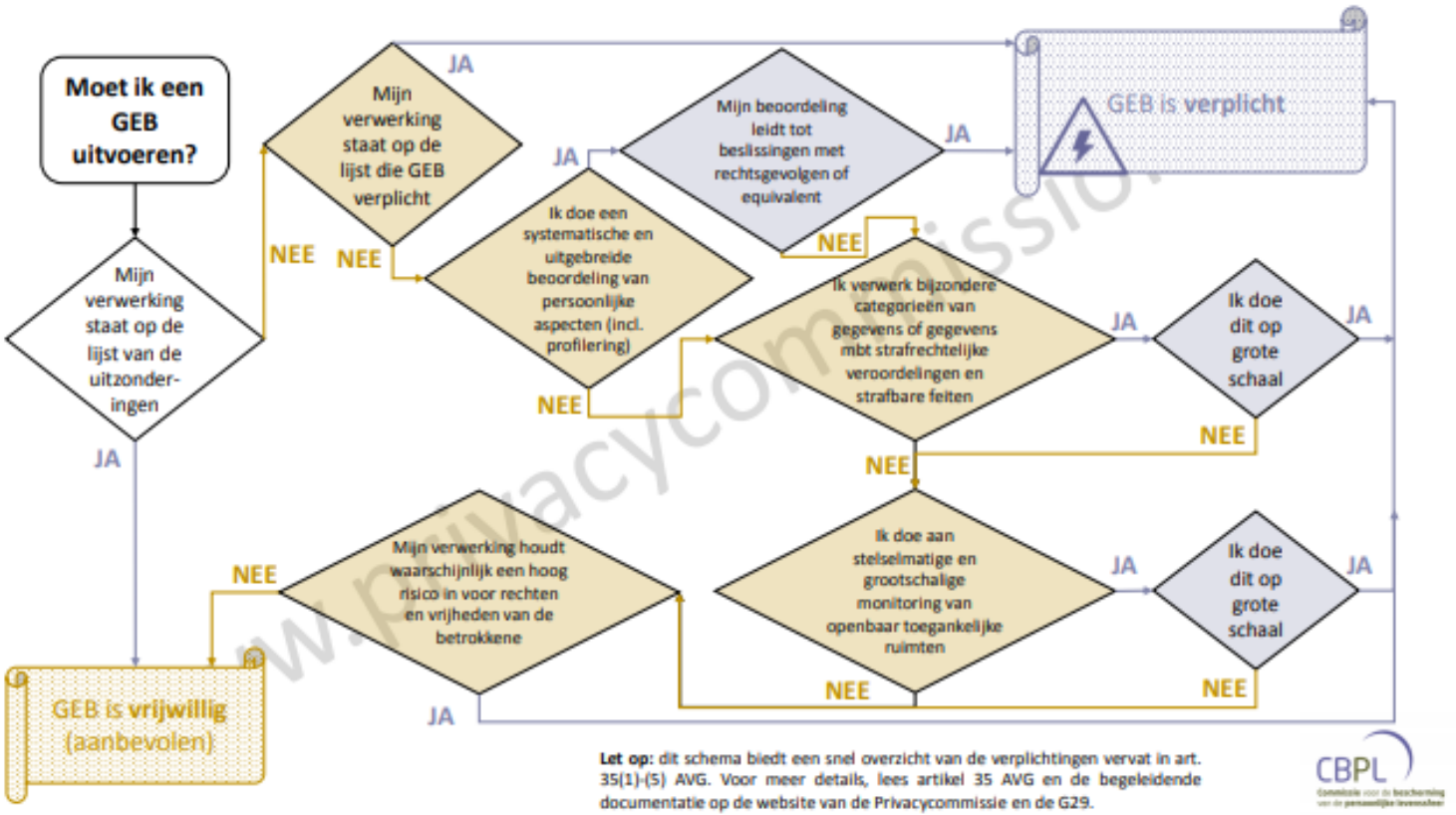

Moet ik een DPO aanstellen?
Ik ben een overheids-instantie of een overheids-orgaan*
* Rechtsprekende instanties zijn een bijzonder geval!
Ja, de aanstelling is verplicht
Ik ben GEEN overheids-instantie of overheids-orgaan
Ik verwerk bijzondere categorieën van gegevens of gegevens mbt strafrechtelijke veroordelingen en strafbare feiten
JA
Ik doe dit op grote schaal
JA
Dit hoort bij mijn hoofd-activiteit
JA
NEE
NEE
NEE
Ik doe aan regelmatige en stelselmatige observatie van betrokkenen
JA
Ik doe dit op grote schaal
JA
Dit hoort bij mijn hoofd-activiteit**
JA
NEE
NEE
NEE
Nee, de aanstelling is vrijwillig
**Mijn hoofdactiviteiten vereisen vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie
www.privacycommission.be

IV. Beveiligingsmaatregelen

- Cfr. basisprincipes van integriteit en vertrouwelijkheid
- Elke verwerkingsverantwoordelijke en verwerker voorziet passende technische en organisatorische maatregelen
- Gegevensbeschermingseffectbeoordeling (DPIA)

Gevoelige gegevens	Kwetsbare betrokkenen
Grootschalige verwerking	Innovatieve oplossingen
Matchen/combineren van datasets	Systematische monitoring
Verwerking kan leiden tot uitsluiting van rechten	Automatische besluitvorming
	Profiling

- Wat met gebruik van een nieuwe technologie?
  - Intelligente transportsystemen
  - Volgsystemen op basis van GPS
- Aanbeveling nr. 01/2018 van 28/02/2018 CBPL
- TO DO:
  - In kaart brengen beveiligingsmaatregelen en evaluatie
  - Intern beleid en vorming


Moet ik een GEB uitvoeren?
Mijn verwerking staat op de lijst van de uitzonder-ingen
JA
NEE
Mijn verwerking staat op de lijst die GEB verplicht
JA
NEE
Mijn beoordeling leidt tot beslissingen met rechtsgevolgen of equivalent
JA
GEB is verplicht
Ik doe een systematische en uitgebreide beoordeling van persoonlijke aspecten (incl. profilering)
JA
NEE
Ik verwerk bijzondere categorieën van gegevens of gegevens mbt strafrechtelijke veroordelingen en strafbare feiten
JA
Ik doe dit op grote schaal
JA
NEE
Ik doe aan stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten
JA
Ik doe dit op grote schaal
JA
NEE
Mijn verwerking houdt waarschijnlijk een hoog risico in voor rechten en vrijheden van de betrokkene
NEE
JA
GEB is vrijwillig (aanbevolen)
Let op: dit schema biedt een snel overzicht van de verplichtingen vervat in art. 35(1)-(5) AVG. Voor meer details, lees artikel 35 AVG en de begeleidende documentatie op de website van de Privacycommissie en de G29.
CBPL
www.privacycommissie.be

V. Due diligence

- Is verwerker GDPR compliant?
- Schriftelijke **verwerkersovereenkomst** verplicht
- TO DO:
  - “Doorlichting” verwerkers en bestaande overeenkomsten
  - Overeenkomsten aanpassen of verwerkersovereenkomsten opstellen

VI. Melding inbreuken

- Datalek verplicht te documenteren (intern logboek)
- Datalek melden aan toezichthoudende autoriteit indien *risico voor rechten en vrijheden betrokkene*
- Principe: binnen 72 uur na kennisname
- Soms ook meldingsplicht aan betrokkenen

- TO DO:
  - Modeldocumenten melding voorzien
  - Intern beleid en vorming

2.4. Rechten van de betrokkene

- Recht van inzage en kopie
- Recht op rectificatie
- Recht op vergetelheid
- Recht op overdraagbaarheid van gegevens
- Recht van bezwaar en *profiling*

- Bestaande rechten:
  - Inzage en kopie
  - Rectificatie (cfr. juistheid)
  - Gegevensuitwissing
  - Bezwaar tegen onrechtmatige of incorrecte verwerking
  - Bezwaar tegen geautomatiseerde besluitvorming

- Nieuwe rechten:
  - Beperking van de verwerking
  - Overdraagbaarheid (“meeneembaarheid”)

- Praktisch:
  - T.a.v. verwerkingsverantwoordelijke
  - Binnen één maand gevolg geven
    - Uitzonderlijk te verlengen indien complex verzoek
  - Kosteloos tenzij ongegrond of buitensporig

- TO DO:
  - Informatie aan betrokkenen
  - Intern beleid en vorming

3. Praktisch – hoe “GDPR Proof” worden?

Stap 1 – Duid een verantwoordelijke aan

- Indien geen gegevensbeschermingsfunctionaris verplicht
- Eén persoon of een team
- Staat in voor de voorbereiding en implementatie van de GDPR
- Betrek ook interne of externe IT consultant
  - Multidisciplinaire aanpak

Stap 2 – Inventarisatie of “audit”

- Data flows en risico’s in kaart brengen:
  - Van wie houdt u persoonsgegevens bij?
    - Klanten, leveranciers, personeel, sollicitanten, prospecten, …
    - **Categorie van betrokkene**
  - Welke persoonsgegevens houdt u bij?
    - Identiteitsgegevens, facturatiegegevens, lokalisatie-gegevens, foto,…
    - **Categorie van persoonsgegevens**
    - **Extra aandacht voor gevoelige gegevens**
  - Waar komen deze gegevens vandaan?
    - Via betrokkene zelf, via derden, publieke databank,…
    - **Authentieke bron**

- Waar en hoe worden de gegevens bewaard?
  - Server, cloud in eigen beheer, cloud via een provider, op papier,…
- Hoe lang worden de gegevens bewaard?
  - **Bewaartermijnen**
- Wie heeft toegang tot de gegevens?
- Treedt u op als verwerkingsverantwoordelijke of als verwerker?
- Worden de gegevens gedeeld met andere ondernemingen buiten de EU?

Stap 3 – Wettelijke grondslag

- Waarom houdt u persoonsgegevens bij?
  - Wat is de verwerkingsactiviteiten
  - Zeer veel categorieën mogelijk: personeelsbeheer, klantenbeheer, leveranciersbeheer, debiteurenbeheer, dossierbeheer, marketing en reclame,…
- Welke grondslag?
  - Toestemming
  - Uitvoering van overeenkomst
  - Wettelijke verplichting
  - Gerechtvaardigd belang

Stap 4 – Passende beveiliging

- Ga na of u veilig (ver)werkt
- Welke beveiligingsmaatregelen worden toegepast?
  - Fysieke beveiliging van gegevens en omgeving
    - Toegangscontrole, toegangsbeveiliging,…
  - Communicatie- en opslagbeveiliging
    - Wachtwoord, antivirus, firewall, back-up,…
  - Vorming personeel
    - Awareness, interne procedures,…
  - Leidraad: ISO normen, gedragscodes,…
- Versterking nodig van beveiligingsmaatregelen?

Stap 5 – Register verwerkingsactiviteiten

- Vul op basis van de gegevens uit stap 2 en 3 het register van verwerkingsactiviteiten aan

- Model register ter beschikking gesteld op website van de Privacy Commissie
  - Tip: minder complex model volstaat, zolang basisdoel behouden (volledig overzicht van verwerkingsactiviteiten)
  - Tip: werk met een gelaagde structuur

CRIVITS & PERSYN
ADVOCATEN

Verwerkings-activiteit	Doel verwerking	Categorie betrokkene	Categorie gegevens	Rechtsgrond	Termijn	Verwerker	Bron
Beheer personeel	Loons-administratie	Werknemers	Identiteits-gegevens	Uitvoering vd. overeenkomst	Wet. termijn	Sociaal secr. Boekhouder	Betrokkene
		//	Financiële gegevens	//	//	//	//
	DIMONA-aangifte	Werknemers	Identiteits-gegevens	Wettelijke verplichting	Wet. termijn	Sociaal secr.	Betrokkene
	…						
Beheer klanten	Klanten-administratie	Klanten	Identiteits-gegevens	Uitvoering vd. overeenkomst	Verjarings - termijn	n.v.t.	Betrokkene
			Financiële gegevens	//	//	Incasso	//
	Mailen van e-nieuwsbrief	Klanten	Identiteits-gegevens	Toestemming	n.v.t.	IT leverancier	Betrokkene
	Direct marketing	Klanten	Identiteits-gegevens	Gerechtvaard. belang	Verjarings - termijn	n.v.t.	Betrokkene
…							

Stap 6 – Privacybeleid

- Stel een privacybeleid op (“intern beleid”)
  - Cfr. documentatieplicht
  - Welke maatregelen worden toegepast?
  - Hoe wordt het personeel ingelicht, gevormd?
  - Welke IT-regels zijn er?
- Stel een privacy notice op (“extern beleid”)
  - Cfr. informatieplicht
  - Mee te delen aan betrokkene
  - Ook voor werknemers, sollicitanten,…

Stap 7 – verwerkersovereenkomsten

- Werkt u samen met verwerkers?
  - Doorgaans wel van toepassing
  - Sociaal secretariaat, accountant of boekhouder, interne of externe preventiedienst,…
- Maak een verwerkersovereenkomst op en laat deze ondertekenen
  - Al diverse modellen in omloop
  - Voor 25 mei!

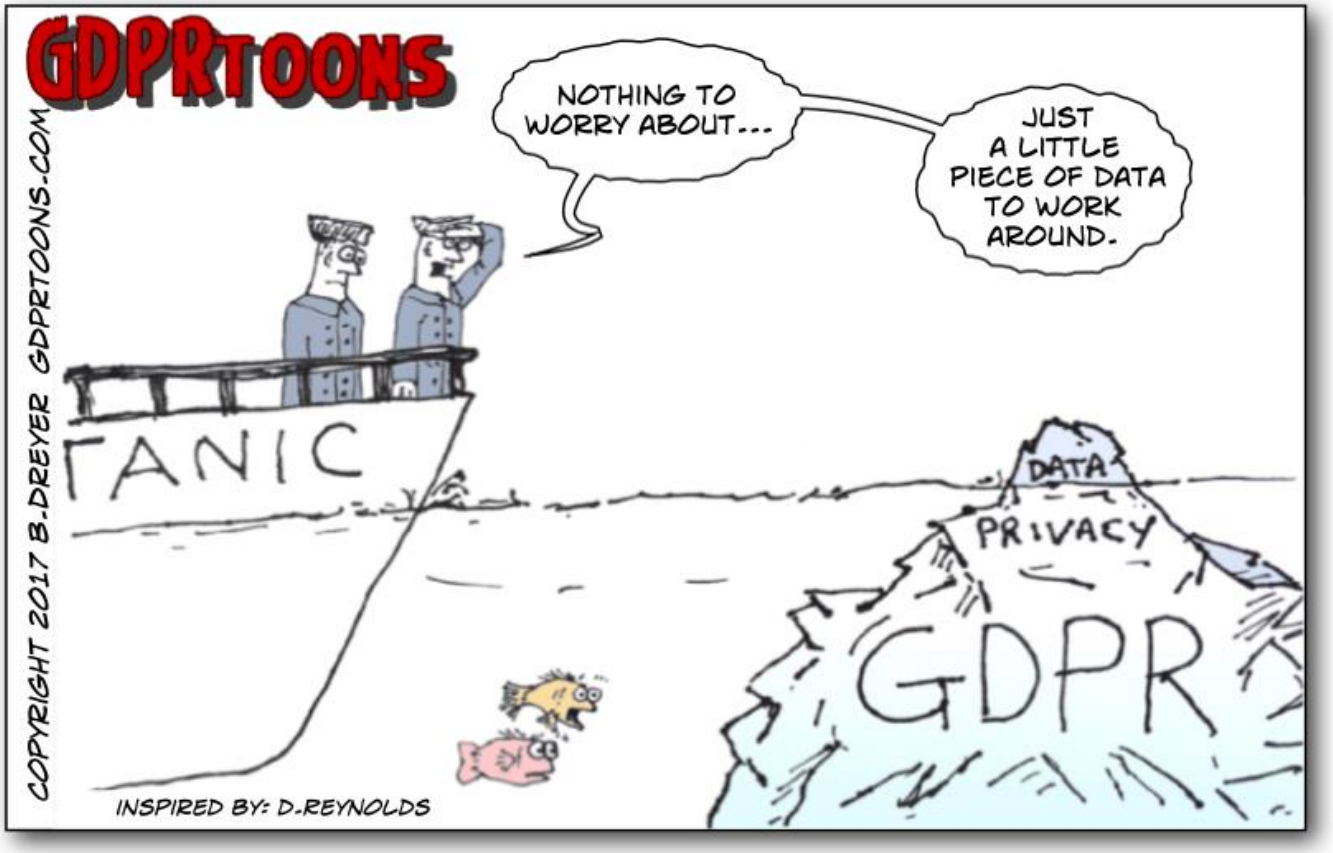
Stap 8 – Voorbereiding op datalek

- Voorzie een interne procedure in geval van datalek
  - cfr. meldingsplicht
  - Detectie
  - Wanneer melden
  - Wie is verantwoordelijk
- Houd een intern logboek bij
- Voorzie een template om een datalek te melden

Tot slot…

- … Verplichtingen zijn geen maat voor niets
- Vermijd aansprakelijkheid
- Vermijd administratieve sanctie(s)
  - Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit (GBA)
  - Naast adviesbevoegdheid nu ook controle – en sanctiebevoegdheid:
    - Berisping, waarschuwing, schorsing van verwerking
    - Administratieve geldboete

Vragen?


GDPRTOONS
NOTHING TO WORRY ABOUT...
JUST A LITTLE PIECE OF DATA TO WORK AROUND.
TANIC
DATA
PRIVACY
GDPR
COPYRIGHT 2017 B.DREYER GDPRTOONS.COM
INSPIRED BY: D.REYNOLDS

CRIVITS & PERSYN
ADVOCATEN

Bedankt!

- Vragen of opmerkingen?
  - advocaten@crivits-persyn.be

- Links:
  - Wegwijs in de AVG voor KMO's

    https://www.privacycommission.be/sites/privacycommission/files/documents/KMO_NL.pdf
  - Article 29 Working Party

    http://ec.europa.eu/newsroom/article29/news-overview.cfm