5 JAAR GDPR (AVG)

Retrospectief en perspectief

Timelex | Geert Somers & Bernd Fiten & Jolien Clemens

NCOI M&D Seminars

TIMELEX

1

Agenda

Welke onderwerpen behandelen we vandaag?

Q&A na elke deel
(niet op het einde)

- 1. PRAKTIJKERVARING NA 5 JAAR OP VLAK VAN: (90 min)
  - Preventie
  - Risicomanagement
  - Probleemoplossing
- 2. IMPACT VAN NIEUWE EUROPESE DATA REGELGEVING OP GDPR? (45 min)
  - Cybersecurity (NIS2)
  - AI Act
  - Data Act
- 3. COMPLIANCE AANTONEN IN HET LICHT VAN ACCOUNTABILITY (60 min)
- 4. OMGAAN MET INTERNATIONALISERING VAN GEGEVENSBESCHERMING (20 min)
- 5. GDPR LANDSCHAP BINNEN 5 JAAR (20 min)

2

slido

Join at slido.com
#8391438

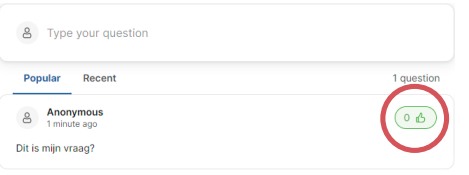
ⓘ Start presenting to display the joining instructions on this slide.

3

DISCUSSIE

Join at slido.com
#8391438

Vragen met de meeste duimpjes worden behandeld (in functie van tijd)



NCOI M&D Seminars

4

1

PRAKTIJKERVARING NA 5 JAAR

Wat leert ons de praktijk van de voorbije 5 jaar op het vlak van preventie, risicomanagement en probleemoplossing?

NCOI M&D Seminars

5

DEEL 1 – Praktijkervaring na 5 jaar

1. **Preventieplichten uit de AVG**
2. **Risicobeheer (risk assessments): LIA, DPIA, DTIA**
3. **Wat als het mis gaat?**
4. **Evolutie op het vlak van handhaving en boetes**
5. **Cyberverzekering?**

NCOI M&D Seminars

6

1.1

Preventieplichten uit de AVG

7

Preventieplichten uit de AVG (privacy by default)

- Audits/maturity audits (huiswerk)
- Training/awareness raising
- Veiligheidsmaatregelen (TOMs)
- Juridische maatregelen (contracten, policies, processen)
- Goede governance (privacy verantwoordelijken en DPO indien nodig)
- Algemene preparedness:
  - voor beheer van incidenten (data breach notification, forensics/data retrieval, schadebeperkingsplicht)
  - voor het beantwoorden van verzoeken van betrokkenen (standaard documenten) - RightSo
  - voor het implementeren van privacy by design (latere aanpassingen vaak kostelijk)

8

1.2

Risicobeoordelingen

LIA, DPIA, DTIA

9

Risicobeoordelingen

- Risico's identificeren/in kaart brengen en minimaliseren
- Rekening houden met aard gegevens, doel van de verwerking, impact op betrokkenen, ...
- Belangrijkste vormen van risk assessments onder de GDPR
  - Legitimate interest assessment
  - Data protection impact assessment
  - Transfer impact assessments

10

Legitimate interest assessment (LIA)

- Legitiem belang: vaak goede wettelijke basis (onafhankelijke rechtsgrondslag, iedereen kan er zich vrij op beroepen)
- Legitiem betekent niet dat het in een wet moet staan, wel dat belangenafweging er niet toe leidt dat er een legitiem belang is.
- Belang kan een belang zijn van de voor de verwerking verantwoordelijke of van een derde, zelfs van de samenleving als geheel
- Sowieso niet legitiem wanneer strijdig met de wet.
- Belangenafweging = accountability (zorgvuldige oefening, niemand heeft absolute rechten)
  - rekening houden met de GDPR basisbeginselen van noodzaak, evenredigheid, minimalisering, beperkte bewaring, redelijke verwachtingen van de betrokkene, etc.
  - afwegen tegen de rechten, vrijheden en belangen van de betrokkenen en ervoor zorgen dat deze niet zwaarder wegen dan het eigen belang

11

Data protection impact assessment (DPIA)

- Trigger: Nieuwe (of gewijzigde) verwerking met waarschijnlijk hoge risico's voor rechten en vrijheden
- Vermoeden: nieuwe technologieën = hoge risico's
- Factoren voor risicobeoordeling: aard, omvang, context en doeleinden van de verwerking
- Altijd verplicht bij: systematische en uitgebreide evaluatie van persoonlijke aspecten; grootschalige verwerking van speciale categorieën; systematisch toezicht op openbare ruimte op grote schaal
- Inhoud DPIA:
  - systematische beschrijving van verwerking en doeleinden
  - beoordeling van noodzaak en evenredigheid
  - risicobeoordeling: overwogen maatregelen om het risico aan te pakken

12

DPIA – Beschrijvend gedeelte

- Wat gaat u doen? => beschrijf uw activiteit in algemene termen
- Wie is erbij betrokken => breng belanghebbenden in kaart, maar ook rollen en relaties
- Waarom wilt u het doen? => breng doeleinden in kaart
- Welke soorten persoonsgegevens heeft u nodig? => breng gegevenselementen, bewaartermijnen, toegangsrechten en ontvangers in kaart
- Hoe gaat u persoonsgegevens verwerken? => focus op systemen voor verzameling, gebruik, opslag, overdracht en vernietiging, zowel infrastructuur- als applicatielaag en bijbehorende bedrijfsprocessen (!)

13

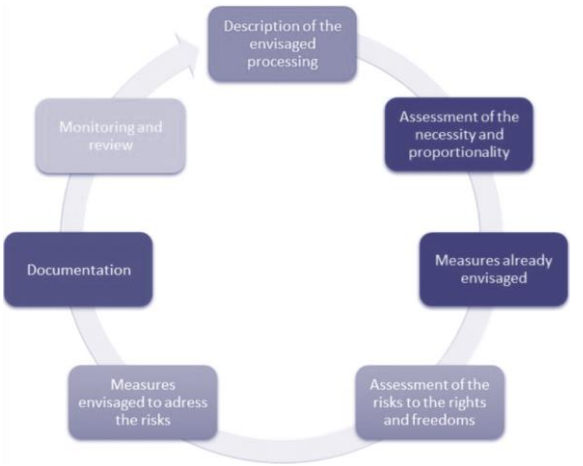
DPIA – Analytisch gedeelte

- Hoe voldoet u aan de fundamentele beginselen inzake gegevensbescherming?
- Hoe gaat u de nodige mogelijkheden inbouwen om de rechten van de betrokkene te waarborgen?
- Welke technische beveiligingsmaatregelen heeft u genomen?
- Welke organisatorische beveiligingsmaatregelen heeft u genomen?
- Welke risico's heeft u geïdentificeerd?
- Hoe worden de risico's beperkt?
- Welke risico's blijven bestaan?

14

DPIA – Soorten DPIA's

- Simpele DPIA
- Technische DPIA
- Uitgebreide DPIA



Data transfer impact assessment (DTIA)

- Wanneer is er een transfer?
  - Gegevens verzenden buiten EER (bv. via e-mail of hosting)
  - Entiteit buiten EER toegang verschaffen tot gegevens binnen EER (bv. IT onderhoud)
- Adequate maatregelen:"**tweestappenbenadering**"
  - Voorafgaand aan de doorgifte: is aan alle andere relevante GDPR-bepalingen voldaan (noodzakelijkheid, wettelijke basis, transparantie, ...)
  - Bij doorgifte: passende beschermingsmaatregelen (SCCs)
- Schrems II
  - Hoe zit het met de regelgeving in het land van bestemming? Wordt er geen afbreuk gedaan aan de bescherming die je via de SCC's wil creëren?
  - Welke maatregelen nemen om toch adequate bescherming te bieden? Of desgevallend geen gegevens naar dat land sturen.

1.3

Wat als het mis gaat?

Notificatieplichten bij datalekken en complexe verzoeken van data subjecten

17

Hoe gaat het meestal mis?

- Meestal: klacht(en)
  - Blijkt uit de beslissingen van de Geschillenkamer
  - Maar ook: seponering
- Niet (tijdig) beantwoorden van verzoeken
- Eigen onderzoek door GBA (bv. temperatuurmeting op luchthaven)
- Datalekken (en deze al dan niet melden)
  - Vroeger: meldplicht telecomsector
  - AVG: meldplicht voor alle sectoren (GDPR)
  - Zal een melding leiden tot een inspectie?
  - Er zijn veel meer meldingen van datalekken dan klachten/verzoeken
- Nood aan prioriteiten

18

Het is misgegaan: damage control!

- Accountability (documentatie op orde om aan te tonen dat je best efforts voor compliance hebt toegepast)
- Data breach procedure
- Verwerkingsregister klaar hebben om te delen met autoriteiten
- Boetes: samenwerken met autoriteiten (boetes beperken of vermijden)
- Schade: algemene schadebeperkingsplicht

19

1.4

Evolutie op vlak van handhaving en boetes – update 2022

20

Refresher: GBA – set-up

Algemeen secretariaat
- Ondersteunende (HR) en uitvoerende taken (bv. DPIA)
- Goedkeuren (of weigeren) van gedragscodes, criteria voor certificering, modelcontractbepalingen, BCRs, enz.

Eerstelijnsdienst (ELD)
- Ontvangen klachten, bemiddeling, informatie, enz.
- Verstrekt informatie over uitoefening van rechten
- Onderzoekt ontvankelijkheid

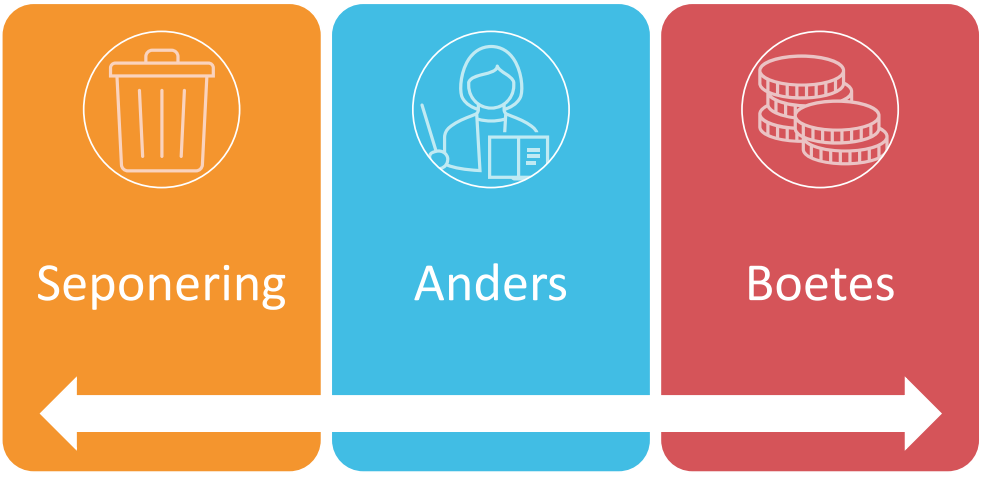
Kenniscentrum
- Adviezen en aanbevelingen
- Bv. richtlijnen over direct marketing

Inspectiedienst
- Onderzoeksorgaan
- Drie manieren om onderzoek te starten
  - Door inspectiedienst zelf (ernstige aanwijzingen) directiecomité, geschillenkamer
- Onderzoeksbevoegdheden (verhoren, ter plaatse gaan…)

Geschillenkamer (GK)
- Inspectiedienst kan overmaken aan geschillenkamer
- Geschillenorgaan (bestuurlijke overheid: geen rechtscollege)
- Intern beroep tegen voorlopige maatregelen, inbeslagneming of verzegeling door de inspectiedienst

21

Selectie van handhavingsacties door de GBA – Mogelijkheden?



22

Selectie van handhavingsacties door de GBA – Mogelijkheden?

23

Selectie van handhavingsacties door de GBA – Sepot

- **Sepotbeleid** van de Geschillenkamer

- **Waarom**? 2 mogelijkheden:
  - Technisch sepot (onderzoek/behandeling = onmogelijk)
  - Sepot om opportuniteitsredenen

- **Wanneer**? 2 momenten:
  - Na doorverwijzing door ELD
  - Na procedure ten gronde

- Ook beroep bij het Marktenhof mogelijk (maar…)

24

Selectie van handhavingsacties door de GBA – Sepot

Technisch sepot

- Onvoldoende bewijs
- Kennelijk ongegrond
- AVG niet van toepassing
- Feiten voor 25 mei 2018 of > 5 jaar oud
- Geen belang
- Klacht ingetrokken

Sepot om opportuniteitsredenen

- Op basis van strategisch plan
- Kan wijzigen
- 2 prioriteitscriteria:
  - Impact: heeft de verwerking een grote maatschappelijke en/of persoonlijke impact?
  - Efficiëntie: is de tussenkomt van de GK relevant?

25

Selectie van handhavingsacties door de GBA – Sepot

- In 2022 nam de Geschillenkamer **21 sepotbeslissingen**
- **Vb. sepotbeslissing oneigenlijk gebruik e-mailadressen**
  - Geen inbreuk op AVG gepleegd
- **Vb. sepotbeslissing – privacyverklaring en DPO**
  - Technisch sepot: geen belang klager
- **Vb. Sepotbeslissing – klacht gegevensverwerking in fiscaal onderzoek door belastingdienst**
  - Opportuniteit Sepot: geen prioriteit om tussen te komen in een lopende administratieve procedure

26

Selectie van handhavingsacties door de GBA – Mogelijkheden?

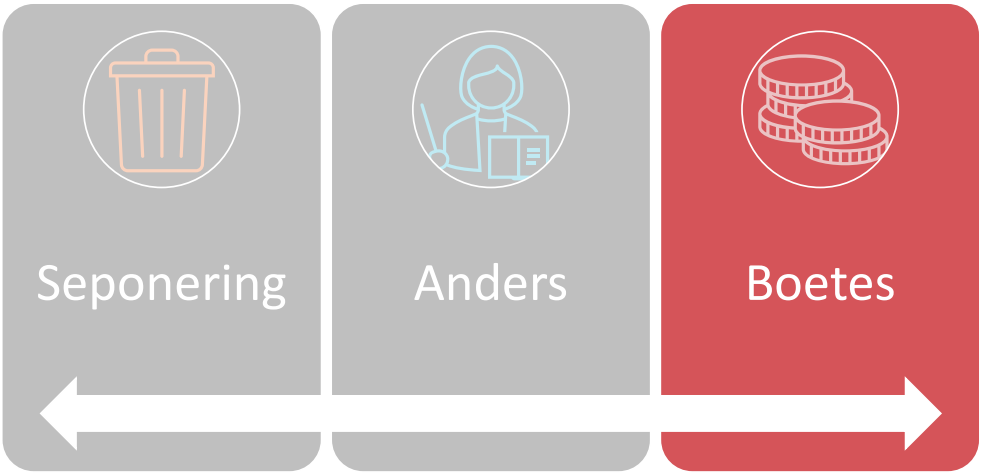
27

Wat zijn de belangrijkste andere mogelijkheden voor de GBA?

- Buitenvervolgingstelling (4 beslissingen in 2022)
- Opschorting van de uitspraak (0 beslissingen in 2022)
- Waarschuwing en berisping (41! beslissingen in 2022)
- Bevel om verwerking in overeenstemming met de AVG te brengen (16 beslissingen in 2022)

28

Selectie van handhavingsacties door de GBA – Mogelijkheden?



29

Selectie handhavingsacties door de GBA – Belangrijkste boetebeslissingen in 2022

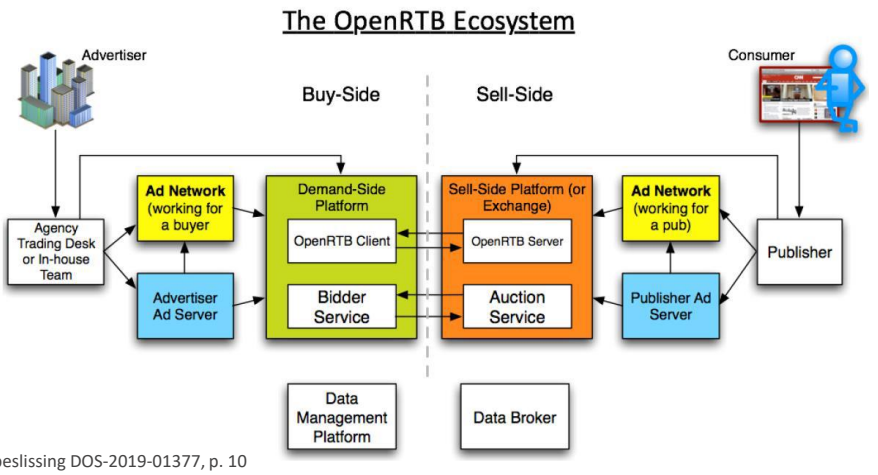
Organisatie	Land	Boete	Inbreuk
IAB Europe (TCF)	BE	€ 250.000	Gebrek aan rechtsgrond verwerking TC string, gebrek aan transparantie, gebrek aan technische en organisatorische maatregelen, nalaten register van verwerkingsactiviteiten bij te houden, DPO aan te stellen en een DPIA uit te voeren.
Cookiebeslissingen	BE	€ 50.000 (Roularta & Groupe Rossel)	Cookies werden geplaatst zonder geldige toestemming & gebrek aan transparante informatie.
Luchthaven Brussels Airport Zaventem en Brussels South Charleroi	BE	€ 200.000 (Brussels Airport Zaventem) € 100.000 (Brussels South Charleroi)	Geen geldige rechtsgrond om gezondheidsgegevens van reizigers te verwerken.

30

Selectie handhavingsacties door de GBA – IAB Europe beslissing

- **IAB Europe beslissing**
- Transparency and Consent Framework (TCF): mechanisme dat het beheer van gebruikersvoorkeuren voor online gepersonaliseerde advertenties vergemakkelijkt
- Open Real Time Bidding: ogenblikkelijke, geautomatiseerde en online veiling van gebruikersprofielen voor het verkopen en aankopen van advertentieruimte op het internet
- TCF is ontwikkeld door IAB Europe

Selectie handhavingsacties door de GBA – IAB Europe beslissing



Bron: beslissing DOS-2019-01377, p. 10

Selectie handhavingsacties door de GBA – IAB Europe beslissing

- **TCF is een reactie op een aantal risico's van het RTB ecosysteem**:
  - Profilering en automatische besluitvorming
  - Grootschalige verwerking en onzichtbare verwerking van persoonsgegevens
  - Innovatieve technologische of organisatorische oplossingen
  - Matching of samenvoeging van datasets
  - Analyse en voorspelling van gedrag, locatie of verplaatsingen van personen
- **TCF: accountability en transparantie**
- **TCF: beleidslijnen, technische specificaties, voorwaarden en afspraken gecreëerd, beheerd en bestuurd door IAB Europe**
  - Informeren van websitebezoekers over de gerechtvaardigde belangen van de adtech vendors
  - Geldige toestemming van de gebruikers

Selectie handhavingsacties door de GBA – IAB Europe beslissing

- **Toestemming van websitebezoekers**? Consent Management Platforms (CMPs)
- CMP genereert **een TC string**: een tekenreeks van letters, cijfers en andere tekens → capteert de voorkeuren van een gebruiker
  - Vb. BOSSotLOSSotLAPABAENBc-AAAAgR7
- **Vendors ontcijferen de TC string** om zo te bepalen of ze over een rechtsgrondslag beschikken om de persoonsgegevens van de gebruikers te kunnen verwerken

Selectie handhavingsacties door de GBA – IAB Europe beslissing

- **Beslissing Geschillenkamer**
  - TC String: de voorkeuren van de gebruikers in een TC String vormen persoonsgegevens;
  - IAB Europe is een gezamenlijke verwerkingsverantwoordelijke binnen het TCF aangezien zij een belangrijke invloed heeft op de keuze van de doeleinden en de middelen;
  - Er bestaat geen gerechtvaardigd belang voor de verwerking van de persoonlijke voorkeuren van gebruikers in de TCF string;
  - Er bestaat geen geldige rechtsgrondslag voor de verdere verwerking van persoonsgegevens door de adtech-spelers;
  - De informatie die onder het TCF wordt aangeboden aan betrokkenen voldoet niet aan de transparantieverplichtingen;
  - IAB Europe voldoet niet aan haar beveiligingsverplichting;
  - IAB Europe moest een DPIA uitvoeren;
  - IAB Europe moest een DPO aanstellen;

35

Selectie handhavingsacties door de GBA – IAB Europe beslissing

- IAB Europe tekende beroep aan tegen de beslissing bij het Marktenhof
- Het Marktenhof stelt een aantal **prejudiciële vragen** aan het Hof van Justitie:
  - Kwalificatie van IAB Europe als gezamenlijke verwerkingsverantwoordelijke
  - De vraag of de TC String een persoonsgegeven is
- **To be continued…**

36

Selectie handhavingsacties door de GBA – Temperatuurcontrolebeslissing

- De luchthavens (Brussels Airport & Brussels Charleroi) gebruikten **thermische camera's** om te controleren welke personen een temperatuur van meer dan 38°C hadden;
- De warmtecamerabeelden zijn uitgerust met een software die een alarmsignaal geven wanneer een temperatuur van 38°C of hoger wordt vastgesteld.
- In Zaventem: vragenlijst over symptomen in verband met het coronavirus (werd uitgevoerd door Ambuce Rescue Team);

37

Selectie handhavingsacties door de GBA – Temperatuurcontrolebeslissing

- **Wettelijke grondslag (artikel 6.1 c AVG)**: Artikel 4 van het ministerieel besluit van 30 juni 2020 houdende dringende maatregelen om de verspreiding van het coronavirus te beperken.
- **Protocol "Commerciële Luchtvaart Passagiers"** van de Belgische FOD Mobiliteit en Vervoer
- **Uitzondering in Artikel 9.2 i) AVG:** algemeen belang op het gebied van volksgezondheid.

38

Selectie handhavingsacties door de GBA – Temperatuurcontrolebeslissing

- Het protocol is **geen afdoende wettelijke bepaling** waarop de verwerking kan worden gebaseerd in de zin van artikel 6.1 c en 9.2 i AVG
  - Het protocol heeft een niet-bindend karakter wat betreft de temperatuurmetingen;
  - Het protocol bevat niet op een eenduidige en heldere wijze de precieze doelstelling van de verwerking;
  - De essentiële elementen van de verwerking worden niet vastgelegd;
- Inbreuken wat betreft **de informatieverstrekking aan de reizigers** en de **kwaliteit van de DPIA** die werd uitgevoerd

Thematiek Cookies – Prioriteit voor 2022

- In 2022 kreeg de GBA expliciet de bevoegdheid om toezicht te houden op cookies
- De GBA startte een onderzoek via de Inspectiedienst naar het gebruik van cookies op de populairste Belgische Perssites → 20 mediawebsites werden onder de loep genomen
- Proactief onderzoek
- Hieruit kwamen 2 beslissingen ten gronde en 8 schikkingsbeslissingen

Thematiek Cookies – Eerste GBA Beslissing

- **Boete voor Jubel.be (12/2019) – 15.000 EUR**
- Eerste cookieboete
- Privacy en cookie policy en banner ongeldig, bv.:
  - Cookies konden niet worden geweigerd (m.a.w. een cookiewall),
  - het privacybeleid werd in de verkeerde taal weergegeven en
  - de beheerder vertrouwde op een legitiem belang als rechtsgrond voor het plaatsen van niet-essentiële statistische cookies in plaats van toestemming
- GBA bevoegd naast BIPT (WEC). BIPT is specifiek bevoegd voor toestemming voor cookies

Cookies en tracking – Wat?

Wat is het **technisch**:

Kort gezegd: u zoekt naar nieuwe schoenen op Zalando en krijgt nadien op Facebook reclame over de schoenen die u heeft bekeken…

Soorten: origine, doel, bewaartermijn

Niet enkel cookies!

Wat is het **juridisch**:

Voorheen: art. 129 WEC

Nu: art. 10/2 Kaderwet

Cookies en tracking – Art. 10/2 Kaderwet

Lid 1: toestemming voor cookies (→ "cookies"?)

- In toepassing van artikel 125, § 1, 1°, van de wet van 13 juni 2005 betreffende de elektronische communicatie en onverminderd de toepassing van de Verordening en deze wet is de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of een gebruiker slechts toegestaan op voorwaarde dat:
  - 1° de betrokken abonnee of gebruiker, overeenkomstig de voorwaarden bepaald in de Verordening en in deze wet, duidelijke en precieze informatie krijgt over de doeleinden van de verwerking en zijn rechten op basis van de Verordening en van deze wet;
  - 2° de abonnee of eindgebruiker zijn toestemming heeft gegeven na ingelicht te zijn overeenkomstig de bepaling onder 1°.

Lid 2: geen toestemming voor "noodzakelijke" cookies

- Het eerste lid is niet van toepassing voor de technische opslag van informatie of de toegang tot informatie opgeslagen in de eindapparatuur van een abonnee of een eindgebruiker met als uitsluitend doel de verzending van een communicatie via een elektronische-communicatienetwerk uit te voeren of een uitdrukkelijk door de abonnee of eindgebruiker gevraagde dienst te leveren wanneer dit hiervoor strikt noodzakelijk is.

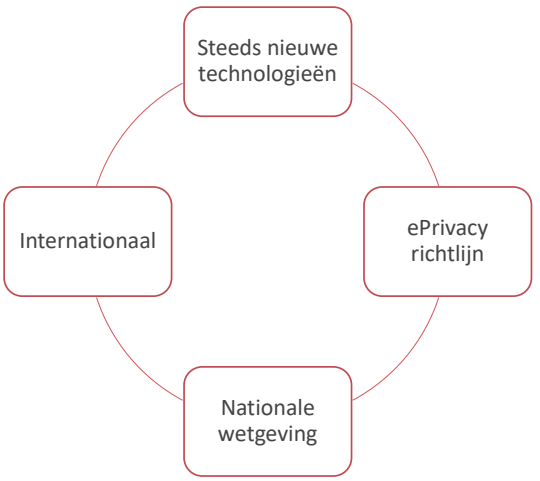
43

Cookies en tracking – Art. 10/2 Kaderwet - Analyse

- Voor cookies en trackers:
  - **informeren** en **toestemming** vragen
  - Tenzij: voor de technische opslag van informatie of de toegang tot informatie opgeslagen in de eindapparatuur van een abonnee of een eindgebruiker met als uitsluitend doel:
    - de verzending van een communicatie via een elektronische-communicatienetwerk uit te voeren of
    - een uitdrukkelijk door de abonnee of eindgebruiker gevraagde dienst te leveren wanneer dit hiervoor strikt noodzakelijk is.
    - *Bv.: load balancing, authenticatie, winkelmandje, taalkeuze, opslaan cookievoorkeuren, tracken van beperkt toegelaten gratis gebruik van betalende website, enz.*
      - *Wat met cookies zoals Google Analytics? (cf. infra)*
- Toepassing naast/bovenop AVG
- Toestemming kunnen intrekken (eenvoudig en gratis)

44

Cookies en tracking – Wat maakt het complex?



45

Cookies en tracking – Hoe een nieuwe technologie beoordelen?

1. hoe werkt de technologie?

2. valt dit onder art. 10/2 Kaderwet?

zo ja: toestemming verplicht

zo neen: toestemming niet verplicht (maar meestal wel nodig onder AVG)

46

Cookiebeslissingen 2022 – Roularta beslissing

- **Roularta Beslissing – Knack.be en Levif.be**
- De GBA is bevoegd om te oordelen over de rechtsgeldigheid van een gegeven toestemming voor het plaatsen van cookies.
- Niet strikt noodzakelijke cookies werden geplaatst zonder een geldige toestemming van de gebruiker
- Statistische cookies zijn niet strikt noodzakelijk en vereisten een geldige toestemming (←→ CNIL, AP)
- Vooraf aangevinkte vakjes voor partners/vendors zijn **geen geldige toestemming** (zie Planet49 arrest)

47

Cookiebeslissingen 2022 – Roularta beslissing

- Gebrek aan duidelijke en transparante informatie (! Belang van het individueel documenteren van de cookies):
  - Doeleinden
  - Bewaartermijn
  - Derde ontvangers
- Intrekken van de toestemming is niet even eenvoudig als het geven van de toestemming

48

Cookiebeslissingen 2022 – Groupe Rossel

- Verschillende **niet-strikt noodzakelijke cookies** werden geplaatst **zonder voorafgaande toestemming** van de gebruiker
- **Statistische cookies zijn niet strikt noodzakelijk en vereisten een geldige toestemming** (←→ CNIL en AP)
- Cookiebeleid was **onvolledig en ontoegankelijk**
- **Further browsing praktijk**: verder surfen door de gebruiker werd gezien als een geldige toestemming → geen duidelijke, voldoende specifieke en actieve handeling
- **Vooraf aangevinkte toestemmingsvakjes** (Planet49 arrest)

49

Cookies en tracking – Richtsnoeren GBA (update 2022)

Cookie banner en cookie policy in de juiste taal	Juridisch correcte inhoud en gebruik consistente terminologie	Minimum verplichte vermeldingen (bv. grondslag, doeleinden, bewaartermijn) → per geplaatst cookie	Geldige toestemming voor niet-noodzakelijke cookies (ook statistische / Google Analytics)
Granulaire toestemming (bv. per soort cookie en ook voor partners)	Geen vooraf aangevinkte vakjes (Planet49-arrest)	Voorzie een weigeringsknop (goede praktijk) + toestemming intrekken mogelijk voorzien op website	Implementatie (geen cookies laden zonder toestemming, cookies moeten verwijderd worden wanneer gebruiker toestemming intrekt, etc.)
	Further Browsing is geen actieve toestemming en is dus niet toegestaan	Gebruik een Europese dienstverlener	

50

Cookies en tracking – CNIL (FR)

- specifieke pagina om cookie-keuzes te beheren en de mogelijkheid toestemming in te trekken.
- verschillende cookies te gebruiken voor elk afzonderlijk doel
- toestemming voor elk doel afzonderlijk
- globale toestemming is alleen mogelijk als alle noodzakelijke informatie vooraf aan de betrokkene is verstrekt.
- namen van de gebruikte trackers moeten expliciet zijn en, indien mogelijk, gestandaardiseerd, ongeacht de actor die ze uitvoert.
- positieve actie is vereist voor toestemming om geldig te zijn. Further browsing is geen geldige toestemming.
- Als er op meer dan één site cookies en andere trackers worden gebruikt, moet de gebruiker op elk van deze sites toestemming geven.
- bewijs van keuze te bewaren gedurende zes maanden
- afwijzingsoptie moet net zo zichtbaar zijn
- niet nodig om de gebruiker toestemming te vragen indien nodig zijn voor de goede werking van de site en de levering van de dienst.

51

Cookies en tracking – Initiatieven op EU-niveau

- Verschillende klachten door NOYB omtrent **cookiebanners** voor Europese Autoriteiten
- EDPB heeft een taskforce opgericht om de behandeling van deze klachten te kunnen coördineren
- Eerste rapport gepubliceerd op 17 januari 2023

52

Cookies en tracking – Initiatieven op EU-niveau

- **Resultaat onderzoek van de cookiebanner Task Force**:
  - Geen weigeringsknop in de cookiebanner (first layer)
  - Vooraf aangevinkte vakjes in cookiebanner (second layer)
  - Een link ipv een knop voor cookies te weigeren
  - De link voor te weigeren heeft een minder opvallende kleur (case-by-case analyse nodig)
  - Gerechtvaardigd belang is niet de geschikte rechtsgrond voor het plaatsen van cookies
  - Cookies worden vaak foutief gekwalificeerd als strikt noodzakelijke cookies
  - Geen weigeringsknop beschikbaar

Cookies en tracking – Initiatieven op EU-niveau

- **Cookiebanner – voorbeeld van een goede praktijk**:

Handhaving op EU-niveau – Trends & Cijfers – Boetes

Bedrijf	Land	Boete	Jaar
1. Meta	Ierland	1,3 billion	2023
2. Amazon	Luxemburg	781 million	2021
3. Instagram	Ierland	427 million	2022
4. Facebook	Ierland	265 million	2022
5. WhatsApp	Ierland	225 million	2021
6. Google LLC	CNIL	99 million	2021
7. Google Ireland	CNIL	60 million	2021
8. Facebook	CNIL	60 million	2021
9. Google	CNIL	50 million	2019
10. H&M	Duitsland	35 million	2020

55

Handhaving op EU-niveau – Trends & Cijfers – Boetes

Organisatie	Land	Boete	Jaar
British Airways	VK	204,6 milj. EUR → 23 milj. EUR ↓	2019
Marriott International	VK	110,4 milj EUR → 21 milj. EUR ↓	2019
Austrian Post	AT	18 miljoen EUR → 0 EUR ↓	2019
Deutsche Wohnen	DE	14,5 miljoen EUR → 0 EUR ↓	2019
1&1 Telecom	DE	9,5 miljoen EUR → 900.000 EUR ↓	2019
Google	SE	75 miljoen EUR → 52 miljoen EUR ↓	2020

56

Handhaving op EU niveau – Trends & Cijfers – Sectoren

- Media, Telecom en Televisie (245 boetes – totaal bedrag € 2,910,010,691)
- Industrie en Handel (383 boetes – totaal bedrag € 863,202,141)
- Transport en Energie (83 boetes – totaal bedrag: € 65,601,614)
- Werkgevers (113 boetes – totaal bedrag: € 48,432,177)
- Financiële, verzekeringen en consulting sector (173 boetes – totaal bedrag: € 38,800,658)
- Publieke sector en onderwijs (188 boetes – totaal bedrag: € 24,268,363)
- Horeca sector (56 boetes – totaal bedrag: € 22,446,648)

Bron: Yahya Jarraya, https://www.linkedin.com/search/results/all/?fetchDeterministicClustersOnly=true&heroEntityKey=urn%3Ali%3Afsd_profile%3AACoAAAGoakEBSzJpMJRPVwo4jLsOuY3dJluQAZs&keywords=yahya%20jarraya&origin=RICH_QUERY_SUGGESTION&position=0&searchId=5618a3d6-ba3d-4ee5-b0de-a84bce397494&sid=O-I

57

Handhaving op EU-niveau – Trends & Cijfers – Thema's

Data transfers	AI & nieuwe technologie	Data breaches en beveiliging	Rechten
Google Analytics beslissingen (CNIL, Nederlandse AP, Oostenrijkse Autoriteit, Italiaanse DPA, Spaanse DPA)	Clearview AI beslissingen (CNIL, Oostenrijkse DPA, Italiaanse DPA)	Geen melding of te laat melden van een data breach (Poolse DPA, Nederlandse AP, etc.)	Tekortkoming transparantieverplichtingen
Mailchimp beslissing (Duitse DPA)	Gezichtsherkenningstechnologie Politie (Zweedse DPA & Finse DPA)	Onvoldoende TOMs (Nederlandse AP, Poolse DPA, Zweedse DPA, etc.)	Te laat antwoorden of niet antwoorden (Finse DPA, GBA, AP, etc.)
Facebook Pixel (Oostenrijkse Autoriteit)			Recht op toegang (Italiaanse DPA, GBA, Hof van Justitie, etc.)

58

Handhaving op EU-niveau – Problemen

- NOYB publiceert artikel over problematiek bij Europese autoriteiten (https://noyb.eu/en/5-years-gdpr-national-authorities-let-down-european-legislator).

Conflict tussen nationale wetgeving & GDPR

Systematische vertragingen in beslissingen

Gebrek aan procedures en beslissingen

59

Handhaving op EU-niveau – Conclusie

Wat kunnen we concluderen op Europees niveau?

- Hoogste boete worden geregeld verpulverd (746 milj. EUR ->)
- Hoge boete? Combinatie van inbreuken (of zeer ernstige inbeuken)
- België zit niet in de top 10 (hoogste boete in België: 600.000 EUR)
- Top 5 boetes zijn allemaal recent (boetes lijken ook te stijgen)
- Boetepraktijk verschilt per land
  - Soms weinig boetes maar hogere boetes
  - Soms meer boetes maar lagere boetes

60

1.5

Cyberverzekering

Wat is het nut en wat is verzekerbaar?

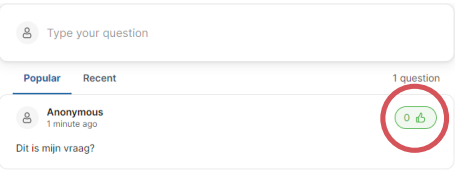
Cyberverzekering

- Algemene verzekeringen dekken in principe geen cyberincidenten
- Verzekerbaarheid GDPR boetes betwistbaar
- Burgerrechtelijke schade wel verzekerbaar
- Mogelijke dekking tegen
  - Verlies van gegevens (kwaadwillige handelingen, computerdiefstal of menselijke fouten)
  - Reputatieschade
  - Data breach response verplichtingen (forensics onderzoek bij cyberincidenten, inschakelen van andere deskundigen, dichten van lekken, meldingen van datalekken aan de bevoegde autoriteit binnen het tijdsbestek van 72 uren)

DISCUSSIE

Join at slido.com
#8391438

Vragen met de meeste duimpjes worden behandeld (in functie van tijd)



63

2

IMPACT VAN NIEUWE EUROPESE DATA REGELGEVING OP GDPR

Wat is de impact van de nieuwe Europese data regelgeving op de GDPR?

64

DEEL 2 – Impact nieuwe regelgeving

1. **Cybersecurity (NIS2)**
2. **AI Act**
3. **Data Act**

*De bedoeling is om te **focussen op de interactie of raakpunten tussen deze instrumenten en de AVG**, **niet** om in detail in te gaan op het toepassingsgebied of verplichtingen onder deze instrumenten*

65

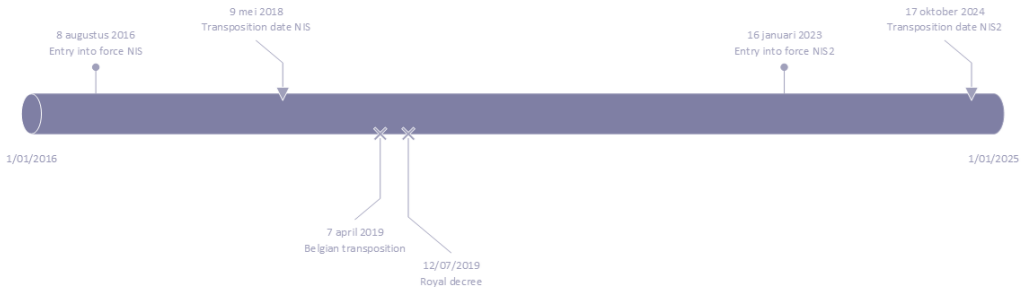
2.1

Cybersecurity (NIS2)

66

Cybersecurity (NIS2) – Inleiding

- Richtlijn inzake cybersecurity (opvolger van NIS1)
- Bedoeling zou zijn om nog dit jaar om te zetten (?)
- Onderworpen entiteiten zijn ofwel “**essential**” of “**important**” (maar complex systeem > zie volgende slide)



67

Sector	Subsector	Jurisdiction	Critical entities (CER)	Large **at least 250 employees OR** with an annual turnover of **at least 50 million euros** (or an annual balance sheet total of at least 43 million euros)	Medium entities: **at least 50 employees OR** with an annual turnover (or balance sheet total) of **at least 10 million euros**	Small & Micro
Annex I: Sectors of high criticality						
1. **Energy**	Electricity; district Heating &cooling; Gas; Hydrogen; oil;	The Member State(s) where it is established	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as** essential **or** important **by national authorities** due to sole service, significant impact, essential to society
2. **Transport**	Air (commercial carriers; airports; traffic); Rail (infra and undertakings); Water (transport companies; ports; traffic services); Road (ITS & charging stations)					
	Special case: Public Transport: **only** if identified as CER					
3. **Banking**	Credit institutions (**attention: DORA lex specialis**)					
4. **Financial Market Infrastructure**	Trading venues, central counterparties (**attention: DORA lex specialis**)					
5. **Health**	Healthcare providers; EU reference laboratories; R&D of medicinal products; manufacturing basic pharma products and preparations; manufacturing of medical devices critical during public health emergency					
	Special case: entities holding a distribution authorization for medicinal products: **only** if identified as CER					
6. **Drinking Water**						
7. Waste Water	(only if it is an essential part of their general activity)					
8. **Digital Infrastructure**	Qualified trust service providers			Essential		
	DNS service providers (excluding root name servers)	**One stop**: Only the MS where they have their main establishment				
	TLD name registries	Member State in which they **provide their services**		Essential		Important, except if identified as essential based on National risk assessment
	Providers of public electronic communications networks	The Member State(s) where it is established				
	Non-qualified trust service providers		Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as** essential **or** important
	Internet Exchange Point providers					
	Cloud computing service providers	**One stop**: Only the MS where they have their main establishment				
	Data centre service providers					
	Content delivery network providers					
8a. ICT-service management (B2B)	Managed Service Providers, Managed Security Service Providers					
9. Public Administration entities	Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security). Of regional governments: risk based. (Optional for Member States: of local governments)	MS that established them		Essential		
10. Space	Operators of ground-based infrastructure (by MS)	The Member State(s) where it is established		Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as** essential **or** important
Annex II: other critical sectors						
1. Postal and courier services		The Member State(s) where it is established	Essential	Important, except if identified as essential by Member State		Not in Scope, **except if identified as** essential **or** important **by national authorities** due to sole service, significant impact, essential to society
2. Waste Management	(only if principal economic activity)					
3. Chemicals	Manufacture, production, distribution					
4. Food	Production, processing and distribution					
5. Manufacturing	(in vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)					
6. Digital providers	online marketplaces, search engines, social networking	**One stop**: Only the MS where they have their main establishment				
7. Research	Research organisations (**excluding education institutions**) (Optional for Member States: education institutions)	The Member State(s) where it is established				
Entities providing domain name registration services		**One stop**: Only the MS where they have their main establishment	*All sizes, but only subject to Article 3(3) and Article 28*			

68

Cybersecurity (NIS2) – Raakpunten tussen NIS2 en AVG

- Enkele voorbeelden van raakpunten met de AVG:
  - 1. Territoriaal toepassingsgebied
  - 2. Verplichtingen
  - 3. Rechtsgrond
  - 4. Samenwerking tussen autoriteiten
  - 5. Dubbele bestraffing?

69

Cybersecurity (NIS2) – 1. Territoriaal toepassingsgebied

- **In principe**: land waar onderworpen entiteit is gevestigd

- Enkele **uitzonderingen**, bv.:
  - DNS service providers, TLD name registries, domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online marketplaces, providers of online search engines and social networking services platforms
    - Systeem van "**main establishment**" geïnspireerd op (niet één op één hetzelfde) de AVG.
    - Maar met een **registratieverplichting** (voor 17/01/2025) bij ENISA (art. 27)
    - Main establishment onder NIS2 kan **verschillen** van main establishment onder AVG (waar trouwens geen registratieverplichting geldt)

70

Cybersecurity (NIS2) – 2. Verplichtingen

- **NIS2:** zeer specifieke verplichtingen op vlak van
  - Governance
  - Cybersecurity risk-management measures
  - Systems & facilities (bv.: mapping van systemen)
  - Incident handling
  - Business continuity management
  - Monitoring, auditing, training, testing
  - Reporting

  → Technical, **operational** and organizational measures ("TOOMs")
- **AVG:** beperkt tot art. 32 AVG ("TOMs") → Veel minder specifiek
  - Maar niet uitgesloten dat NIS2 maatregelen ook "passend" zijn onder AVG

71

Cybersecurity (NIS2) – 3. Rechtsgrond

- Overweging 121 NIS2: de verwerking van persoonsgegevens in het kader van cybersecurity maatregelen kan op grond van rechtsgrond (c) of (f).
  - "Measures related to the prevention, detection, identification, containment, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated vulnerability disclosure, the voluntary exchange of information about those incidents, and cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools could require the processing of certain categories of personal data, such as IP addresses, uniform resources locators (URLs), domain names, email addresses and, where they reveal personal data, time stamps."
  - "The processing of personal data, to the extent necessary and proportionate for the purpose of ensuring security of network and information systems by essential and important entities, could be considered to be lawful on the basis that such processing complies with a **legal obligation** to which the controller is subject, in accordance with the requirements of Article 6(1), point (c), and Article 6(3) of Regulation (EU) 2016/679."
    - Afhankelijk van de Belgische omzetting, maar waarschijnlijk bedoeld voor reporting verplichtingen
  - "Processing of personal data could also be necessary for **legitimate interests** pursued by essential and important entities, as well as providers of security technologies and services acting on behalf of those entities, pursuant to Article 6(1), point (f), of Regulation (EU) 2016/679, including where such processing is necessary for cybersecurity information-sharing arrangements or the voluntary notification of relevant information in accordance with this Directive."

72

Cybersecurity (NIS2) – 4. Samenwerking tussen autoriteiten

- Art. 31.3 NIS2: plicht tot samenwerking
  - *"The competent authorities shall work in close cooperation with supervisory authorities under Regulation (EU) 2016/679 when addressing incidents resulting in personal data breaches, without prejudice to the competence and tasks of the supervisory authorities under that Regulation."*

- "Competent authorities"
  = Autoriteit onder NIS2 (BE: Centre for Cyber Security Belgium – CCB)
- "Supervisory authorities under Regulation (EU) 2016/679"
  = Autoriteit onder AVG (BE: GBA)

- Samenwerkingsplicht voor wat het waard is in de praktijk… (vgl. GBA/VTC)

73

Cybersecurity (NIS2) – 4. Samenwerking tussen autoriteiten

- Art. 35.1 NIS2: informeren van toezichthoudende autoriteit onder AVG
  - *"Where the competent authorities become aware in the course of supervision or enforcement that the infringement by an essential or important entity of the obligations laid down in Articles 21 and 23 of this Directive can entail a personal data breach, as defined in Article 4, point (12), of Regulation (EU) 2016/679 which is to be notified pursuant to Article 33 of that Regulation, they shall, without undue delay, inform the supervisory authorities as referred to in Article 55 or 56 of that Regulation"*

- Art. 35.3 NIS2: grensoverschrijdende gevallen
  - *"Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority, the competent authority shall inform the supervisory authority established in its own Member State of the potential data breach referred to in paragraph 1."*

74

Cybersecurity (NIS2) – 5. Dubbele bestraffing?

- Art. 35.2 NIS: geen dubbele administratieve geldboete (maar wel andere maatregelen)
  - *"Where the supervisory authorities as referred to in Article 55 or 56 of Regulation (EU) 2016/679 impose an administrative fine pursuant to Article 58(2), point (i), of that Regulation, the competent authorities shall not impose an **administrative fine** pursuant to Article 34 of this Directive for an infringement referred to in paragraph 1 of this Article arising from the same conduct as that which was the subject of the administrative fine under Article 58(2), point (i), of Regulation (EU) 2016/679. The competent authorities may, however, impose the **enforcement measures** provided for in Article 32(4), points (a) to (h), Article 32(5) and Article 33(4), points (a) to (g), of this Directive."*

75

Cybersecurity (NIS2) – Bedenkingen

- Enkele bedenkingen bij art. 35 NIS:
  - Wie legt als eerste aan administratieve geldboete op?
    - Autoriteit onder AVG? Autoriteit onder NIS2 kan geen boete opleggen voor zelfde inbreuk
    - Autoriteit onder NIS2? AVG heeft geen gelijkaardige bepaling als de NIS2… (non bis in idem?)
  - Grensoverschrijdende gevallen zullen leiden tot vertragingen (want uit verschillende zaken blijkt dat toezichthoudende autoriteiten onder de AVG niet altijd bijzonder goed samenwerken).

76

2.2

AI Act

77

Overzicht

- Wat is AI?
- Waarom is het relevant in het kader van AVG?
- Wat is de relatie tussen de AVG en de AI Act?
- Stavaza AI Act

78

Wat is AI?

- Artificial Intelligence (AI) – Kunstmatige Intelligentie
- Definitie? Geen eensgezindheid over een definitie.
  - Containerbegrip voor een groot aantal subdomeinen (EESC)
  - AI zijn intelligente systemen die zelfstandig taken kunnen uitvoeren in complexe omgevingen en eigen prestaties kunnen verbeteren door te leren van ervaringen (Nationale AI-cursus NL)
- Juridische definitie → AI Act (zie verder)
- Media, onderwijs, wetenschap, industrie,… praten anders over AI

79

Wat is AI?

- Ver van mijn bed?
- Neen, denk aan:
  - Aanbevelingen door Netflix, YouTube, enz.
  - Spamfilter voor e-mails
  - Automatische piloot
  - Vertalingen door Google Translate, DeepL, enz.
  - Beoordelen van longfoto's

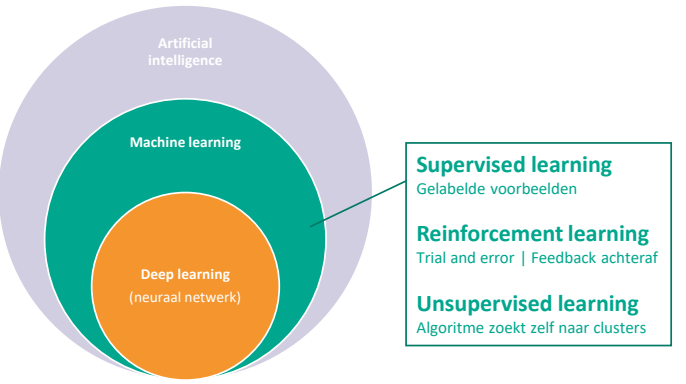
80

AI = General Purpose Technology (GPT)

- Niet te verwarren met “Generative Pre-trained Transformer” (ChatGPT)
- GPT kan samenlevingen ontwrichten door hun impact op bestaande economische en sociale structuren
  - Zoals het internet en elektriciteit
- AI is **geen technologie op zich**, maar een uitkomst (of doel) van verschillende technologieën
- Drie overkoepelende technologieën:
  - Whole brain emulation (WBE) of “mind upload”
  - Brain-computer interfaces (BCI)
  - Machine learning (ML)
    - Machines leiden zelf regels af uit data (⇔ programmeren door de mens) → **Onze focus**

81

Dé AI-technologie bestaat niet

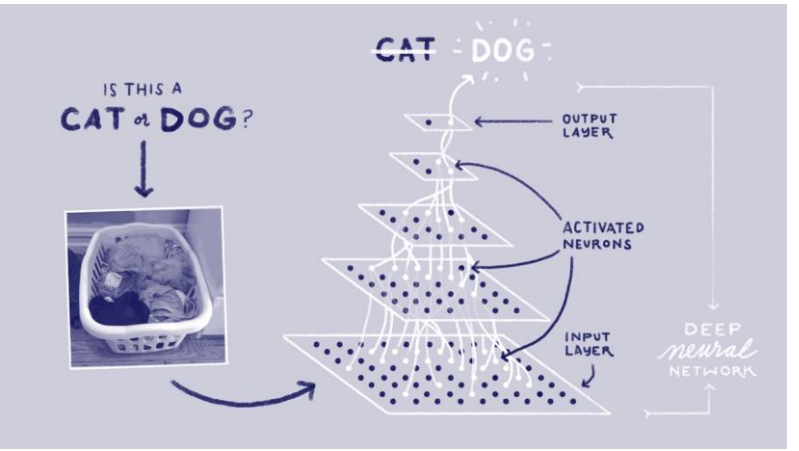


Drie ingrediënten zijn wel noodzakelijk:

Data, algoritme** en **rekenkracht

82

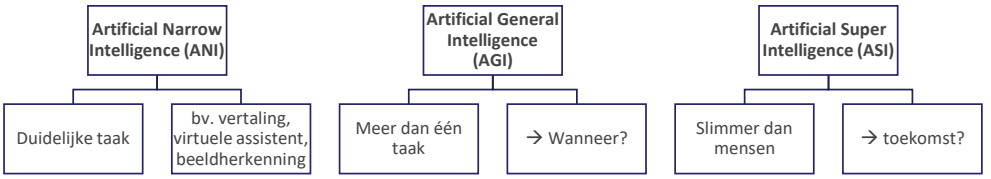
Hoe werkt deep learning?



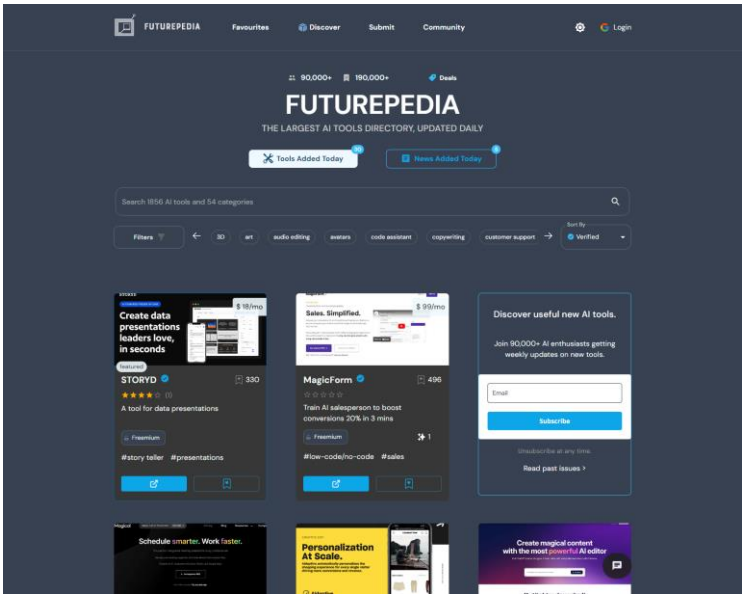
Toepassingen van AI

- Toepassingen soms voorgesteld als aparte technologie:
  - **Natural language processing (NLP):** menselijke taal begrijpen
    - Bv.: chatbots
  - **Speech processing:** spraaksignalen herkennen en verwerken
    - Bv.: virtuele assistenten
  - **Computer vision:** informatie uit beelden halen, herkennen en interpreteren
    - Bv.: longfoto's
  - **Affective computing:** emoties opsporen en herkennen
    - Bv.: marketing
  - ...
- Eigenlijk een onderdeel van machine learning

Wel eensgezindheid over de indeling van AI



85



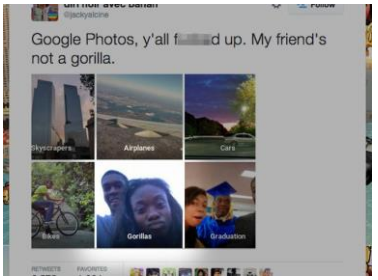
Overzicht:
https://www.futurepedia.io/

86

Wanneer AI “ai ai ai” wordt

1

2



3

4

Advocaat in nauwe schoentjes vanwege ‘precedenten’ gehallucineerd door ChatGPT

Schaamrood bij het Amerikaanse advocatenkantoor Levidow, Levidow & Oberman: een rechter stuurde hen hun papieren terug met de mededeling dat ze ‘precedenten’ hadden aangehaald die helemaal verzonnen waren. De schuldige? ChatGPT.

87

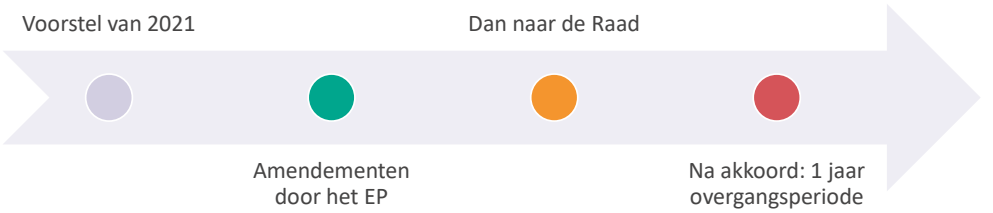
Relatie tussen AI Act en AVG

AI Act
- Uitgangspunt: **PRODUCTREGULERING**
- AI = een product dat kwalitatief moet zijn
- Conformiteitsbeoordeling
- Niets over de verwerking van persoonsgegevens (behalve i.h.k.v. regulatory sandboxes)

AVG
- Uitgangspunt: **GRONDRECHTEN**
- AI = een manier om persoonsgegevens te verwerken
- DPIA

88

Stavaza AI Act



89

AI Act: belangrijkste bepalingen en verplichtingen

- Categorieën o.b.v. **risico**
  - Onacceptabel risico → verboden
  - Hoog risico → verplichtingen, waaronder…
    - Conformiteitsbeoordeling (self assessment of door een externe derde)
    - Monitoring
    - Meldplichten
    - Transparantieverplichtingen
- Oprichting toezichthoudende autoriteit
- Boetes potentieel hoger dan AVG (30 miljoen of 6%)

- → Maar tekst kan (en zal) nog veranderen

90

AI Act: belangrijkste bepalingen en verplichtingen

- Overw. 41: de AI Act vormt geen rechtsgrond onder de AVG
  - *"The fact that an AI system is classified as high risk under this Regulation should not be interpreted as indicating that the use of the system is necessarily lawful under other acts of Union law or under national law compatible with Union law, such as on the protection of personal data, on the use of polygraphs and similar tools or other systems to detect the emotional state of natural persons. Any such use should continue to occur solely in accordance with the applicable requirements resulting from the Charter and from the applicable acts of secondary Union law and national law."*
  - *"This Regulation should not be understood as providing for the legal ground for processing of personal data, including special categories of personal data, where relevant."*
- Overw. 72: behalve in het kader van het algemeen belang in een regulatory sandbox
  - *"This Regulation should provide the legal basis for the use of personal data collected for other purposes for developing certain AI systems in the public interest within the AI regulatory sandbox, in line with Article 6(4) of Regulation (EU) 2016/679, and Article 6 of Regulation (EU) 2018/1725, and without prejudice to Article 4(2) of Directive (EU) 2016/680"*

AI Act: belangrijkste bepalingen en verplichtingen

- Artikel 10.5 AI Act: gevoelige persoonsgegevens verwerken voor bias monitoring
  - *"To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued."*
- Artikel 54.1 AI Act: gebruik van persoonsgegevens in regulatory sandboxes
  - *"In the AI regulatory sandbox personal data lawfully collected for other purposes shall be processed for the purposes of developing and testing certain innovative AI systems in the sandbox under the following conditions: […]*
    - *(d) any personal data to be processed in the context of the sandbox are in a functionally separate, isolated and protected data processing environment under the control of the participants and only authorised persons have access to that data,*
    - *(e) any personal data processed are not be transmitted, transferred or otherwise accessed by other parties*
    - *(g) any personal data processed in the context of the sandbox are deleted once the participation in the sandbox has terminated or the personal data has reached the end of its retention period"*

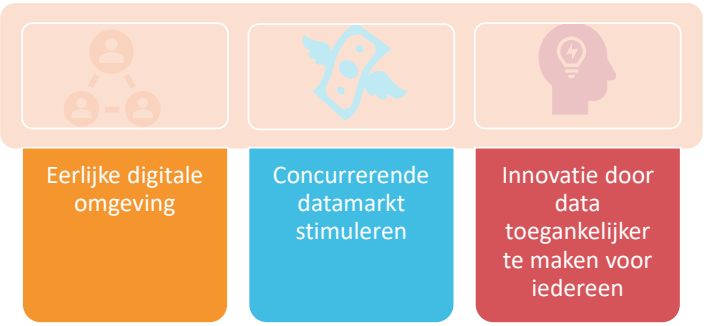
2.3

Data Act

93

Data Act – Over wat hebben we het?

- Voorstel van de Europese Commissie voor een verordening betreffende geharmoniseerde regels inzake eerlijke toegang tot en eerlijk gebruik van data – 23 februari 2022 (“European strategy for data”)
- **Doelstellingen:**



94

Data Act – Wat zijn de belangrijkste nieuwe regels?

- Toegang tot data gegenereerd door IoT producten of gerelateerde diensten
- Oneerlijke bedingen in B2B relaties
- Overstappen naar andere dataverwerkingsdiensten
- Verplichting om data beschikbaar te stellen aan overheid op grond van uitzonderlijke noodzaak
- Beveiliging van niet-persoonsgebonden gegevens binnen de EU
- Nieuwe eisen voor interoperabiliteit

95

Data Act – Praktijkvoorbeeld

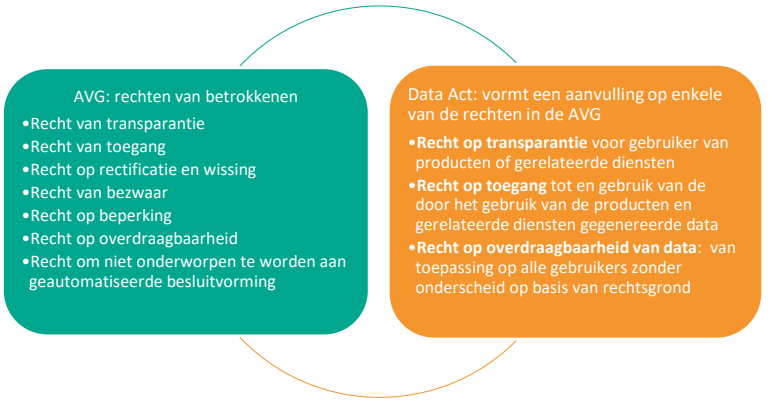
- "Data van Tesla-klokkenluider vermeldt duizende storingsgevallen Autopilot" (https://tweakers.net/nieuws/210124/data-van-tesla-klokkenluider-vermeldt-duizenden-storingsgevallen-autopilot.html)
- Reactie Tesla: "de volledige rapporten zijn alleen voor intern gebruik en terugkoppeling aan de getroffen klant mag alleen verbaal"
- **Data Act**: verplichting om gegenereerde data toegankelijk te maken voor de gebruiker (Artikel 3 en 4) & recht om data te delen met derden (Artikel 5)

96

Relatie tussen AVG en Data Act – Scope

97

Relatie tussen AVG en Data Act – Rechten



98

Relatie tussen AVG en Data Act – Data Transfers

AVG: Data transfers van persoonsgegevens

- Zie eerdere bespreking
- Doorgiftemechanisme
- Afwijkingen en uitzonderingen

Data Act: data transfers van niet-persoonsgebonden gegevens op basis van een besluit, rechterlijke uitspraak en elke beslissing van een administratieve autoriteit van een derde land

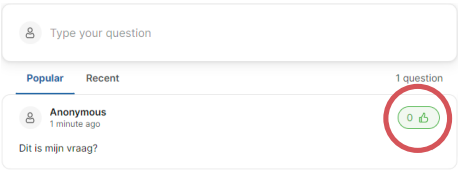
- Moet gebaseerd zijn op een international overeenkomst vb. Verdrag inzake wederzijdse rechtsbijstand
- Geen internationale overeenkomst: naleving strikte voorwaarden

99

DISCUSSIE

Join at slido.com
#8391438

Vragen met de meeste duimpjes worden behandeld (in functie van tijd)



100

3

COMPLIANCE AANTONEN IN HET LICHT VAN ACCOUNTABILITY

Hoe kunnen organisaties hun compliance best aantonen in het licht van hun accountability verplichtingen?

NCOI M&D Seminars

101

DEEL 3 – Compliance aantonen i.h.k.v. accountability

1. **Register van verwerkingsactiviteiten**
2. **Policies en procedures**
3. **Contracten (nadruk op verwerkingsovereenkomst)**
4. **De DPO (FG)**
5. **Certificatie**

NCOI M&D Seminars

102

3.1

Register van verwerkingsactiviteiten

103

Inleiding

Allerhande benamingen	• Register van verwerkingsactiviteiten • Record of processing activities (RPA of RoPA) • Inventory, data register, mapping,…
Wat is het?	• Belangrijk accountability verplichting (art. 30 AVG) – Niet te verwarren met het beeldverwerkingsregister! • Zeer beperkte uitzonderingen • (bv. < 250 werknemers, maar wel als de gegevensverwerking "gewoonlijk" is, zoals personeelsbeheer) • Vergelijk het met boekhouding
Waarom?	• Intern gebruik • Extern gebruik • Boete van de "lichtste" categorie (10 milj. EUR of 2%)
Praktijk	• Zeer veel organisaties hebben nog geen (volledig) register! • Wat zijn de typische uitdagingen (en hoe op te lossen)?

104

Typische uitdagingen i.h.k.v. het register

- Wie is verantwoordelijk?
- Welke vorm en taal?
- Welke verplichte of aanvullende inhoud?
- Waarvoor willen we het gebruiken?

105

1. Wie is verantwoordelijk?

- **Als organisatie:**
  - Verwerkingsverantwoordelijke of verwerker gevestigd in de EER
  - Of vertegenwoordiger indien niet gevestigd in EER maar AVG wel van toepassing

- **Binnen de organisatie:**
  - Stel een verantwoordelijke aan
  - Neem het op in de taakbeschrijving
  - Bedenk een werkbaar systeem voor updaten

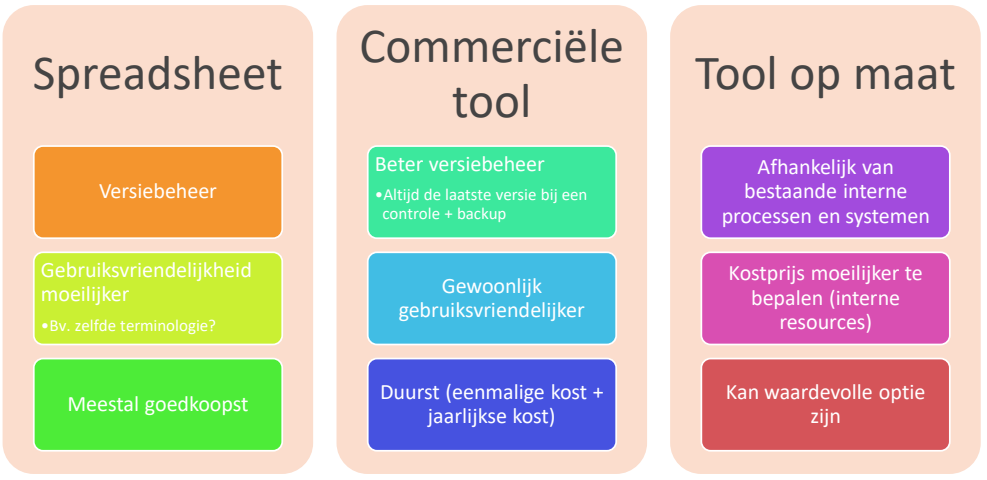
106

2. Welke vorm en taal?

- Geen *verplicht* **standaardmodel**
  - Maar wel templates beschikbaar (bv. GBA – maar niet ingevuld)
  - Vrij te kiezen, maar wel schriftelijk
- **Taal?**
  - Vrij te kiezen, maar GBA kan vertaling in landstalen vorderen
  - Wat met Engels?
- Verschillende **opties:**
  - Spreadsheet (bv. Excel)
  - Commerciële tool
  - Tool op maat (bv. in SharePoint)

107

2. Welke vorm en taal?



108

3. Welke verplichte of aanvullende inhoud?

109

4. Waarvoor willen we het gebruiken?

- **Wat is de aanpak?**
  - Minimaal: louter voldoen aan de wet (vermijden van boete)?
  - Extra: beter overzicht krijgen over persoonsgegevens in de organisatie? Bv.
    - Welke entiteiten betrokken bij welke verwerkingen?
    - Handige statistieken trekken
    - Handig bij beantwoorden van verzoeken, onderzoek van datalekken, enz.
  - Anders: bekomen van een certificaat?
- **Aanpak bepaalt o.a.:**
  - Al dan niet en welke aanvullende inhoud
  - Hoe granulair / gedetailleerd
    - Bv.: categoriën van ontvangers of namen van ontvangers?
- **Let wel:** enkel verplicht het “minimale” te verstrekken bij een controle

110

Onderzoek door de AP – 5 concrete aanbevelingen

- Benoem **hoe lang** en met **welk doel** je persoonsgegevens wil bewaren.
  - Onder de Europese privacywetgeving is het niet toegestaan persoonsgegevens langer te bewaren dan noodzakelijk is voor het doel waarmee ze verzameld zijn. Ook moeten organisaties kunnen motiveren waarom ze deze gegevens verzamelen.
- Neem de **contactgegevens** van de verwerkingsverantwoordelijke op in het register.
- Zorg voor een **overzichtelijk bestand** van alle verwerkingen van persoonsgegevens waarin gebruikers eenvoudig kunnen navigeren.
- Geef duidelijk aan **op welke locatie of in welk bestand** persoonsgegevens bewaard worden en neem deze locaties of bestanden op in het register.
  - Deze informatie is relevant als mensen een verzoek om inzage of verwijdering indienen.
- Maak duidelijk **welk doel bij welke verwerking** hoort.
  - Alleen een opsomming van de verwerkingen per afdeling in combinatie met een opsomming van de diverse doeleinden van de verwerkingen is niet voldoende.

Voorbeelden uit het register van de AP

- Hierna voorbeelden van twee typische verwerkingscategorieën:
  - Personeels- en loonadministratie
  - Werving en selectie

(let wel, internationale doorgifte en beveiligingsmaatregelen ontbreken in deze voorbeelden!)

Voorbeeld (AP) 1: personeels- en loonadministratie

Taak	Doeleinden	Categorieën persoonsgegevens	Rechtsgrond (art. 6.1)	Verwerkings-verantwoordelijke	Categorieën betrokkenen	Categorieën ontvangers	Bewaartermijn
Personeels- en loonadministratie	Uitvoering geven aan arbeidsovereenkomst	Naam, adres, woonplaats, BSN, bankgegevens, gegevens met betrekking tot arbeidsovereenkomst, functie, CV, kopie identificatiedocument, kopie diploma's, loonbelastingverklaring, formulier salarisbetaling, verlof, ziekteverzuim, vergoedingen, toeslagen, gratificaties, declaraties, inhoudingen, loonbeslag, gegevens omtrent functioneren in de vorm van gespreksverslagen, nevenfuncties, opleiding/training	Uitvoering van overeenkomst (b); wettelijke verplichting (c)	[…]	Huidige en oud-medewerkers (vanwege bewaarplicht)		7 jaar na administratieve afhandeling van het ontslag
Personeels- en loonadministratie	Administratieplicht fiscale wetgeving	Op grond van wet- en regelgeving verplichte gegevens	Idem	[…]	Idem		Idem

Voorbeeld (AP) 2: werving en selectie

Taak	Doeleinden	Categorieën persoonsgegevens	Rechtsgrond (art. 6.1)	Verwerkings-verantwoordelijke	Categorieën betrokkenen	Categorieën ontvangers	Bewaartermijn
Werving en selectie	Werving en selectie van interne en externe kandidaten voor een binnen de AP opengestelde vacature	Naam, adres, woonplaats, titulatuur, geslacht, geboortedatum en -plaats, telefoonnummer, e-mailadres, nationaliteit, gegevens omtrent opleiding, loopbaan en functie waarop is gesolliciteerd	Toestemming (a); Uitvoering van overeenkomst in de pre-contractuele fase (b)	[…]	Interne en externe kandidaten		Bij afwijzen solllicitanten: 1 maand na afwijzing, 1 jaar indien persoonsgegevens met toestemming van de betrokkene na beëindiging van de sollicitatieprocedure worden bewaard. Bij aanstellen nieuwe medewerkers: 7 jaar na administratieve afhandeling van het ontslag (uitdiensttreding)

3.2

Policies en procedures

115

Policies en procedures

- Veelvoorkomende vraag: ***"welke policies en procedures hebben we nodig?"***
  - Maar AVG mag niet herleid worden tot *paper compliance*
  - Policies en procedures zijn pas het sluitstuk van een uitgevoerde audit
- **Verplicht** de AVG bepaalde policies of procedures?
  - Neen, maar wel in het kader van accountability
- **Welke dan?**
  - Afhankelijk van de organisatie
  - Typisch meer policies en procedures nodig in grotere organisaties

116

Wat is meestal het minimum?

Privacybeleid
Informatieveiligheidsbeleid
Privacyverklaring aan personeel
Privacyverklaring aan sollicitanten
Privacyverklaring algemeen (voor andere betrokkenen)
Verplichtingen voor personeel bij verwerkingen
Beleid inzake bewaartermijnen
Verwerkingsregister + beeldverwerkingsregister (indien van toepassing)
Takenpakket privacyverantwoordelijke of DPO (FG)
Procedure voor datalekken
Procedure voor behandeling verzoeken betrokkenen
GDPR training als sluitstuk van de implementatie (de deliverables worden getraind)

117

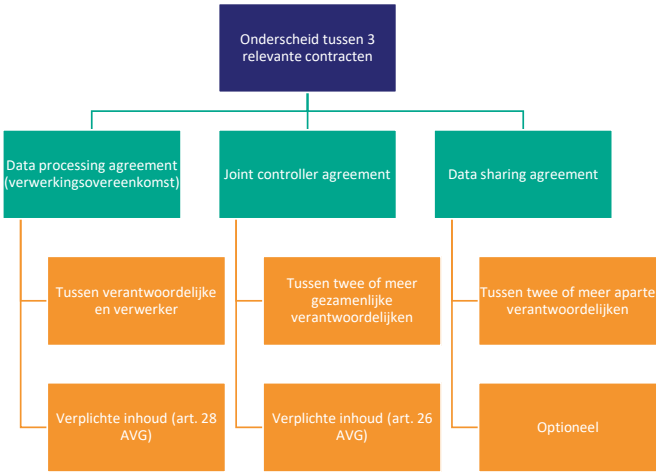
3.3

Contracten

Met focus op de verwerkingsovereenkomst (of data processing agreement)

118

Contracten



119

Verwerkingsovereenkomst – Overzicht

- Vorm
- Inhoud
- Typische clausules
- Voorbeeldclausules

120

Verwerkingsovereenkomst – Vorm?

- **Onderhandelde overeenkomst**
  - Hoofdovereenkomst, bijlage of addendum
  - Indien bijlage:
    - Check hoofdovereenkomst inzake wijzigingen
    - Hoofdovereenkomst kan relevant zijn voor leemtes in de bijlage (bv.: aansprakelijkheid, beëindiging, enz.)
- Meer en meer in **algemene voorwaarden** (van verwerkers)
  - Dat kan, maar opletten voor mogelijke conflicten
  - Tegenstrijdige clausules heffen elkaar op (art. 5.23, derde lid BW)
    - → Opletten voor leemtes

121

Verwerkingsovereenkomst – Inhoud?

- Moet voldoen aan **artikel 28 AVG** (juridisch minimum)
- Voor de rest: **contractvrijheid, maar:**
  - Beperkt door bepalingen inzake onrechtmatige bedingen
    - B2B: art. VI.91/3 WER (lex specialis)
    - Maar overheidsopdrachten en financiële diensten: gemeenrecht van art. 5.52 BW
- Afhankelijk van **positie** (verwerkingsverantwoordelijke of verwerker)

122

Verwerkingsovereenkomst – Inhoud? Artikel 28.3 AVG

- Gedocumenteerde instructies
- Onderwerp van verwerking
  - Algemene beschrijving van de verwerking
- Duur van verwerking (exact of criteria)
- Aard van verwerking (bv.: filmen, opnemen, archiveren, verzamelen, enz.)
- Doel van verwerking
- Type van persoonsgegevens (bv.: videobeelden, contactgegevens, enz.)
- Categorieën van betrokkenen

123

Verwerkingsovereenkomst – Typische clausules

- Algemene bepaling
- Sub-verwerking
- Confidentialiteit
- Compliance
- Informatie en bijstand
- Audit
- Security
- Datalekken
- Internationale doorgifte
- Aansprakelijkheid
- Verwijdering of teruggave
- Opschorting en beëindiging
- Overige bepalingen

124

Verwerkingsovereenkomst – Sub-verwerking

- Juridisch minimum (art. 28.2 AVG)
  - Type van toestemming (algemeen of specifiek)
  - Algemene toestemming
    - Recht van bezwaar
    - Gevolgen

125

Verwerkingsovereenkomst – Sub-verwerking

Tips & tricks

Verantwoordelijke

- Specifieke toestemming te verkiezen
- Indien algemene toestemming:
  - Pro-verantwoordelijke bezwaar
  - Of gebalanceerd
- Third-party beneficiary clausule
- Kopie sub-verwerkersovereenkomst
- Garantie voor sub-verwerkers
- Bestaande sub-verwerkers?

Verwerker

- Vermijd specifieke toestemming
- Algemene toestemming te verkiezen
  - Pro-verwerker bezwaar
  - Of gebalanceerd
- Bepaal deadlines
  - Zodat verantwoordelijke niet kan blokeren

126

Verwerkingsovereenkomst – Sub-verwerking (voorbeelden)

- Pro-verantwoordelijke bezwaar
  - *"If the controller informs the processor of any objection to the proposed addition or replacement, the processor will not provide or disclose the personal data of the controller to the proposed sub-processor, unless with prior, written and explicit consent of the controller."*
  - *(+ right to terminate)*
- Pro-verwerker bezwaar
  - *"If the controller informs the processor within one (1) month after receiving notification from the processor of any objection (on reasonable grounds) to the proposed addition or replacement, the processor will work in good faith with the controller to achieve a commercially reasonable change in the service that avoids the use of the proposed sub-processor, and if such a change cannot be implemented within one (1) month after receipt by the processor of such notification, the controller may, by means of written notification, with immediate effect and without judicial intervention terminate this agreement."*

127

Verwerkingsovereenkomst – Sub-verwerking (voorbeelden)

- Gebalanceerd bezwaar
  - *"[…] the processor will not provide or disclose the personal data of the controller to the proposed sub-processor until reasonable steps have been taken to address concerns of the controller and the controller has been informed in writing with a reasonable explanation of the steps taken."*

128

Verwerkingsovereenkomst – Sub-verwerking (voorbeelden)

- Third-party beneficiary clause (pro-verantwoordelijke)
  - *"The processor agrees with the sub-processor on a third-party beneficiary clause whereby - in the event of the processor's bankruptcy - the controller acts as a third-party beneficiary of the sub-processor agreement and has the right to enforce the agreement against the sub-processor engaged by the processor, for example by enabling the controller to order the sub-processor to delete or return the personal data."*

129

Verwerkingsovereenkomst – Sub-verwerking (voorbeelden)

- Recht op kopie (pro-verantwoordelijke)
  - *"A copy of such sub-processor agreement and of any subsequent amendments will - upon the customer's first request - be submitted to the controller, so that it may assess whether the same or equivalent data protection obligations are imposed on the sub-processor as in this agreement.* ***Provisions on business-related issues not affecting such assessment need not be submitted to the controller."***
  - Kan ook dubbel zijn: neemt de verantwoordelijke hier extra verantwoordelijkheid?
  - Laatste zin: belangrijk om aan te denken als verwerker!

130

Verwerkingsovereenkomst – Sub-verwerking (voorbeelden)

- Garantie voor sub-verwerker (pro-verantwoordelijke)
  - *"The processor **guarantees** that it complies with the conditions referred to in Articles 28.2 and 28.4 GDPR for engaging a sub-processor. The processor will also **guarantee** that its sub-processors comply with all their obligations under the GDPR, as well as other applicable data protection legislation, such as the conditions referred to in the Articles 28.2 and 28.4 GDPR for engaging a sub-processor."*
  - *"The processor warrants that any sub-processor will perform the obligations of this agreement **as if the sub-processor were a party** to this agreement instead of the processor."*

- Is dit niet hetzelfde als art. 28.4 GDPR?
  - *"Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations."*

→ Nee, de verwerker is niet alleen volledig aansprakelijk, maar geeft ook een **garantie**

131

Verwerkingsovereenkomst – Sub-verwerking (voorbeelden)

- Bestaande sub-verwerkers
  - *"The processor may continue to use sub-processors mentioned in Annex 1 which are already engaged by the processor prior to the entry into force of this agreement."*

132

Verwerkingsovereenkomst – Audit

- Juridisch minimum (art. 28.3 (h) AVG)
  - De verwerkingsverantwoordelijke stelt alle informatie ter beschikking die nodig is om de nakoming van de in dit artikel neergelegde verplichtingen aan te tonen en **audits, waaronder inspecties**,
  - door de verwerkingsverantwoordelijke of een door de verwerkingsverantwoordelijke gemachtigde controleur
  - mogelijk maakt en eraan bijdraagt
- Dus de verantwoordelijke heeft sowieso o.b.v. AVG laatste zeg over de auditor

133

Verwerkingsovereenkomst – Audit

Tips & tricks

Verantwoordelijke

- Uitgebreid auditrecht (eender wanneer)
- Kosten minimaliseren en voor de verwerker bij inbreuken
- Auditor aanstellen
- Follow-up maatregelen na de audit

Verwerker

- Audits per aangetekende brief aangekondigd en dan binnen redelijke termijn (ten vroegste binnen 3 weken)
- Hoe vaak?
- Alleen tijdens kantooruren
- Ontwerp auditrapport voor opmerkingen
- Onafhankelijke auditor gehouden tot confidentialiteit
- Geen onredelijke hindering van activiteit
- Alleen audit indien bestaande rapporten onvoldoende
- Geen kosten bij kleine non-compliance

134

Verwerkingsovereenkomst – Audit (voorbeelden)

- Pro-verantwoordelijke
  - *"The Processor shall at no cost to the Controller:*
    - *Allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller for the purpose of demonstrating compliance by the Processor and the Controller with their respective obligations under Data Protection Laws and this Data Processing Agreement; and*
    - *Provide (and procure) reasonable access for the Controller or such other auditor to:*
      - *The facilities equipment, premises and sites on which Personal Data and/or the records are held, and to any other equipment or facilities used in the provision of the Services (in each case whether or not owned or controlled by the Processor); and*
      - *To the Processor personnel,*
      - *Provided that the Controller gives the Processor reasonable prior notice of such audit and/or inspection*
  - *The Processor shall promptly resolve, at its own cost and expense, all data protection and security issues discovered by the Controller and reported to the Processor that reveal a breach or potential breach by the Processor of its obligations under this Data Processing Agreement.*
  - *If the Processor is in breach of its obligations under this Data Processing Agreement, the Controller may suspend the transfer of Personal Data until the breach is remedied.*
  - *The Controller shall be entitled to share any notification, details, records or information provided by or on behalf of the Processor under this Data Processing Agreement, with the Controller Group, its professional advisors and/or the Supervisory Authority."*

135

Verwerkingsovereenkomst – Audit (voorbeelden)

- Pro-verwerker
  - *"The Controller is entitled to reasonably verify Processor's compliance with this Data Processing Agreement. To this extent, the Controller may, upon request in writing and with prior notice of thirty (30) calendar days at its own expense instruct acknowledged audit professionals to execute such audit:*
    - *a) once every twelve (12) months provided that such additional audit inquiries shall not unreasonably impact in an adverse manner Processor's regular operations and do not prove to be incompatible with the applicable legislation or with the instructions of a competent authority;*
    - *b) where a competent data protection authority requires this under applicable Data Protection Legislation;*
    - *c) following a Personal Data Breach.*
  - *Before the commencement of any such additional audit inquiries, the Controller and Processor shall mutually agree upon the scope, timing and duration of the audit.*
  - *The Controller shall promptly notify Processor with information regarding any non-compliance discovered during the course of additional audit inquiries. The Controller agrees to provide Processor with a draft of the audit report for review. Processor is entitled to propose any amendments and add management comments to this draft before the Controller establishes the final version.*
  - *During such audit, Processor shall provide reasonable cooperation and assistance to the auditors. Processor shall be entitled to invoice the Controller on a time and material basis at the then-current applicable prices for any time expended for any such audit inquiries. Parties shall prior to the audit agree on the costs that Processor is entitled to invoice. The Controller shall not be entitled to claim compensation for any kind of audit expenses incurred by the Controller, unless they are due to insufficient cooperation and assistance by Processor.*
  - *The Processor audit report, any other information to which the Controller or the aforementioned audit professionals have access pursuant to any audit activities, as well as an attestation of the implementation of the technical and organizational measures to protect Personal Data will be considered Processor Confidential Information."*

136

Verwerkingsovereenkomst – Tips & tricks

- Breng eerst als uw dienstverleners **in kaart**
- Deel ze in in categorieën en start met de **kritische dienstverleners**
  - Kritisch =
    - Onmisbaar voor de dagelijkse bedrijfsvoering, of
    - Een incident zou mogelijks een grote impact hebben op uw organisatie
- Controleer of er een **verwerkingsovereenkomst** is
- Controleer de **inhoud** van die verwerkingsovereenkomst
  - Vraag eventueel overzicht van subverwerkers op, of check waar je het kan vinden (kan ook nuttig zijn bij het in kaart brengen van internationale doorgiften, cf. infra)
  - Besteed zeker ook aandacht aan beveiligingsmaatregelen

137

3.4

Rol van de DPO (FG)

138

Rol van de DPO (FG)

- Moet informatie verzamelen om de verwerkingsactiviteiten te identificeren (moet het verwerkingsregister bijhouden)
- Moet de naleving van de verwerkingsactiviteiten analyseren en controleren (moet bij de risicobeoordelingen betrokken worden)
- Moet aan de verwerkingsverantwoordelijke of de verwerker informatie en advies verstrekken en aanbevelingen doen en tegelijk onafhankelijk zijn (zonder instructies kunnen werken en als rechterhand van de directie rechstreeks aan het hoogste management rapporteren)
- Officiële contactpunt tussen de verantwoordelijke organisatie en de bevoegde gegevensbeschermingsautoriteiten
- Moet de rechten van de betrokkenen vrijwaren

139

3.5

Certificatie

140

Certificatie

- Eerste EU certificatiemechanisme Europrivacy in oktober 2022 door de EDPB goedgekeurd.
- Vertaling van de beginselen uit de GDPR in objectieve, meetbare criteria

(// ISO certificatie)

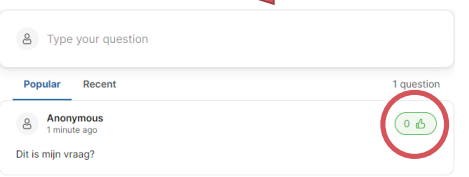
- Vereist de aanwezigheid van een DPO
- Niet van nul beginnen: documenteren wat je gedaan hebt en verbeteren/aanvullen waar nodig => perfect voor aantonen compliance
- Certificaat behalen is vrijwillig
  - Valoriseren van werk dat al werd geleverd (kers op de tart)
  - Kost omvormen tot een asset (profit centre ipv cost centre)
  - Erkenning van geleverde werk door de DPO
  - Trust (extern) en confidence (intern)

141

DISCUSSIE

Join at slido.com
#8391438

Vragen met de meeste duimpjes worden behandeld (in functie van tijd)



142

4

INTERNATIONALISERING VAN GEGEVENSBESCHERMING

Hoe kunnen organisaties best omgaan met de internationalisering van gegevensbescherming?

NCOI M&D Seminars

143

DEEL 4 – Internationalisering

1. **Stand van zaken**
2. **Adequaatheidsbesluit voor de VS?**

NCOI M&D Seminars

144

4.1

Stand van zaken

145

Stand van zaken

- GDPR als golden standard, zowel voor andere regelgevers als voor sommige organisaties
- Naast GDPR, ook nog (nieuw of niet):
  - CCPA (Californië), maar ook COPPA, CalOPPA, HIPAA, enz.
  - PIPEDA (Canada)
  - LGPD (Brazilië)
  - Maar ook: China, Bangladesh, Belarus, Bermuda, Bosnië en Herzegovina, Egypte, India, Japan, Nieuw-Zeeland, Noord-Macedonië, Panama, Zuid-Afrika, Singapore, Zwitserland, Thailand, enz.

146

4.2

Adequaatheidsbesluit VS?

150

Adequaatheidsbesluit VS?

English EN

Search

Home > Press corner > Commission publishes draft adequacy decision for the EU-US

Available languages: English

Press release | 13 December 2022 | Brussels

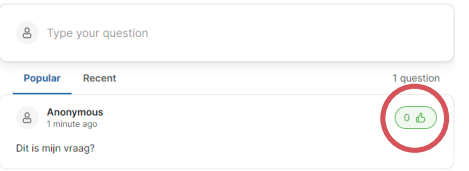
Data protection: Commission starts process to adopt adequacy decision for safe data flows with the US

151

DISCUSSIE

Join at slido.com
#8391438

Vragen met de meeste duimpjes worden behandeld (in functie van tijd)



NCOI M&D Seminars

152

5

GDPR LANDSCHAP BINNEN 5 JAAR

Zullen de snelle ontwikkelingen, bv. op het vlak van A, verzoenbaar kunnen zijn met de GDPR?

NCOI M&D Seminars

153

DEEL 2 – AVG landschap binnen 5 jaar

1 **Procedure Verordening – Geert**

154

5.1

Procedure Verordening

155

Procedure Verordening

- Samenwerking tussen nationale gegevensbeschermingsautoriteiten verloopt niet van een leien dakje
- Veel procedurele verschillen in de verschillende lidstaten
  - Toelaatbaarheid klacht: soms OK via e-mail, soms handtekening op papier nodig, soms enkel voor data subjecten met domicilie in een lidstaat, soms beperkte termijn voor indienen klacht, ...
  - Verloop procedure: sommige autoriteiten bieden geen of onvoldoende inzicht in verloop/timing procedure, sluiten klacht arbitrair af zonder mogelijkheid tot beroep of gaan te snel over tot een minnelijke regeling met de verantwoordelijke organisatie
  - Transparantie: sommige autoriteiten geven geen of beperkte inzage in dossier, vooral aan de klager, of laten enkel toegang ter plaatse toe
  - Taalgebruik: sommige autoriteiten wisselen plots eenzijdig de taal
  - Samenwerking met de EDPB: sommige autoriteiten geven maar zeer beperkt uitvoering aan beslissingen van de EDPB (te veel ruimte voor interpretatie)

156

Procedure Verordening

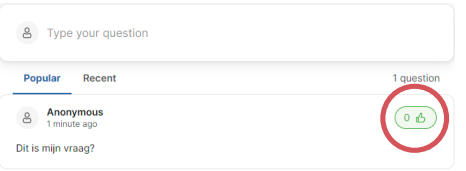
- Lobby voor een aparte verordening
  - van toepassing op procedures uit hoofde van de GDPR
  - wanneer toezichthoudende autoriteiten van meer dan één lidstaat aan de procedure deelnemen, alsmede op daaruit voortvloeiende gerechtelijke procedures.
- Voorbeelden van mogelijke bepalingen
  - het toepasselijke nationale procesrecht mag ingezetenen van andere lidstaten niet hinderen om volledig deel te nemen aan procedures
  - recht op onpartijdige en eerlijke behandeling van de zaak,
  - recht om gehoord te worden alvorens maatregelen worden genomen die nadelig zijn voor de partij (met ingebrip van verwerpen of sluiten van een klacht)
  - recht op toegang tot het dossier
  - recht op een juridisch bindende beslissing van de autoriteit binnen een redelijke termijn met bijvoorbeeld een maximum van 6 maanden.

157

DISCUSSIE

Join at slido.com
#8391438

Vragen met de meeste duimpjes worden behandeld (in functie van tijd)



158

6

Conclusie

Wat te onthouden?

159

Conclusie

Key takeaways

- Handhaving van de AVG liep de voorbije 5 jaar niet altijd over een leien dakje
- Door een stormvloed aan nieuwe EU-wetgeving, staat AVG lang niet meer alleen
- Andere instrumenten nemen bepaalde concepten uit de AVG over
- Controleer uw RoPA, policies en procedures en check of deze nog up-to-date zijn
- Breng eerst uw kritische dienstverleners in kaart en check de verwerkingsovereenkomst
- Overweeg een AVG maturiteitsaudit (zeker als de eerste audit dateert van 2020 of eerder)
- Check uw internationale doorgiften en de genomen maatregelen
- Documenteer uw compliance en risk assessments
- Overweeg certificatie als kers op de taart

160

slido

Wat vond je van het seminarie? (anoniem!)

ⓘ Start presenting to display the poll results on this slide.

161

slido

Geef feedback (anoniem!)

ⓘ Start presenting to display the poll results on this slide.

162

Bedankt

Timelex – Geert Somers & Bernd Fiten & Jolien Clemens

Vragen?

www.timelex.eu / www.linkedin.com/company/timelex

geert.somers@timelex.eu / bernd.fiten@timelex.eu / jolien.clemens@timelex.eu

NCOI M&D Seminars TIMELEX

163