CRANIUM

DTIA's in de praktijk

Lisa De Smet
Principal Data Protection Consultant & Business Manager
CRANIUM

Koen Verbeke
Principal Data Protection Consultant & Solutions Manager
CRANIUM

Transfers toegelicht

- AVG Hoofdstuk V - Doorgiften van persoonsgegevens aan derde landen of internationale organisaties
  - Doorgifte mag het in de AVG gewaarborgde beschermingsniveau van natuurlijke personen niet ondermijnen
  - Geldt ook verdere doorgiften vanuit het derde land aan een ander derde land (of internationale organisatie)

➡ Definitie van doorgifte ontbreekt in AVG

- EDPB Richtsnoeren over wisselwerking Art. 3 en Hoofdstuk V AVG:

  Drie cumulatieve criteria:

  1. Verantwoordelijke of verwerker is onderworpen aan AVG voor gegeven verwerking;
  2. Deze verantwoordelijke of verwerker (exporteur) maakt persoonsgegevens openbaar door overdracht of stelt ze op een andere manier ter beschikking aan een andere (gezamenlijke) verantwoordelijke of verwerker (importeur);
  3. De importeur bevindt zich in een derde land of is een internationale organisatie.

Schrems II

HvJ-EU arrest C-311/18 van 16 juli 2020:
Data Protection Commissioner tegen Facebook Ireland Ltd en Maximillian Schrems

- EU-US Privacy Shield ongeldig verklaard
- Bevestiging van geldigheid standaard-contractbepalingen
- Verplichte controle op doeltreffendheid passende waarborgen doorgifte-instrumenten (Art. 46 AVG)
  - Afbreuk door wetgeving of rechtspraktijk in derde land
  - Mogelijkheid tot aanvullende maatregelen

↳ Case-by-case analyse door exporteur
= DTIA

Bron: De Standaard

Trans-Atlantic Data Privacy Framework

- Principeovereenkomst op 25 maart 2022
- Nog geen tastbaar resultaat (ondanks belofte oplossing eind 2022)
- Nieuwe deal wellicht andermaal naar HvJ-EU (cfr. Safe Harbor en Privacy Shield)
- Goedgekeurd raamwerk kan jaren duren

➡ toont noodzaak van DTIA's aan

Bron: Euractive

Handhaving

noyb's 101 modelklachten over gegevens-overdracht tussen de EU en de VS

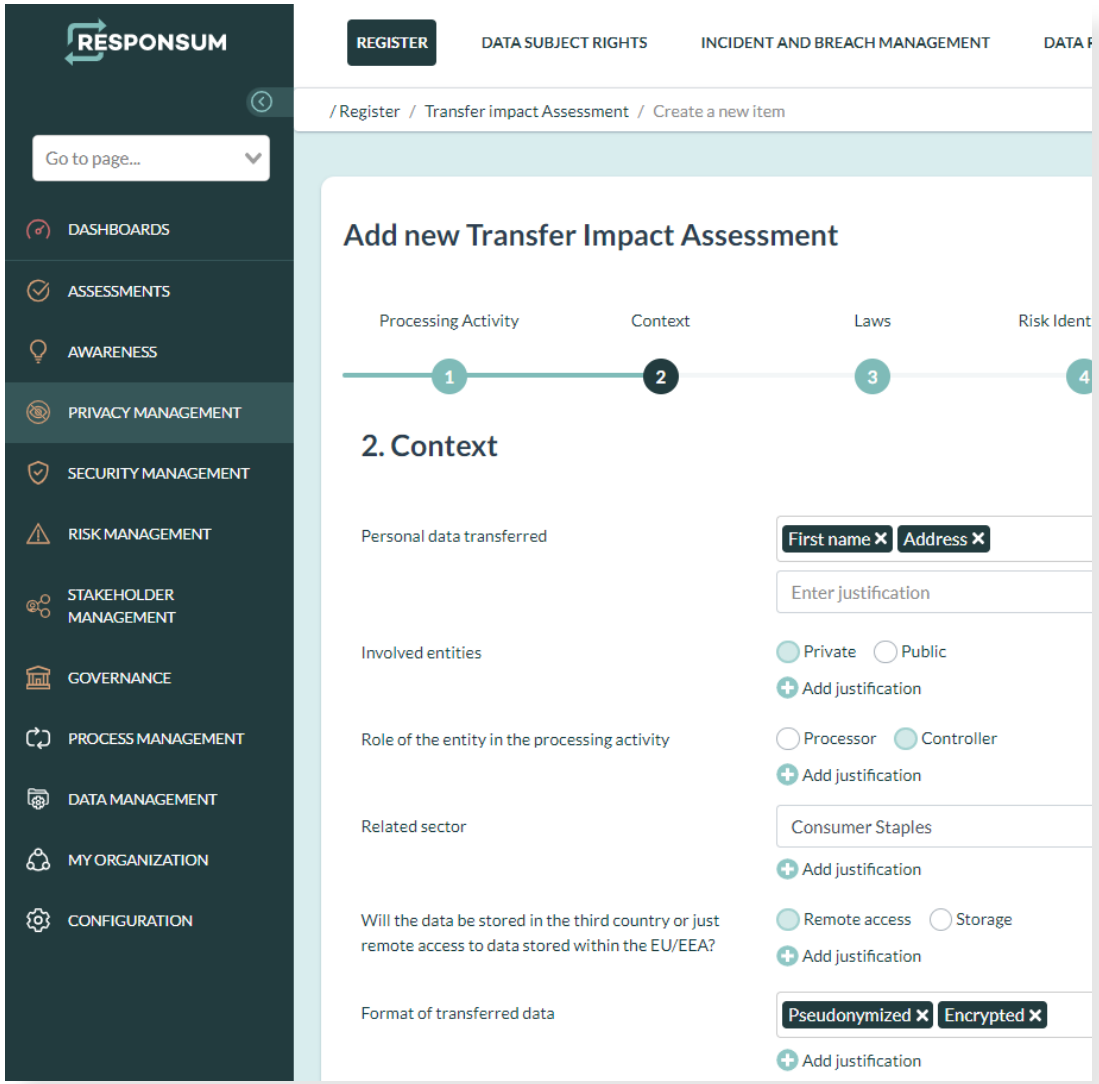
- Oostenrijkse *Datenschutzbehörde*
- Deense *Datatilsynet*
- Franse *CNIL*
- Italiaanse *Garante Privacy*

Lancering door EDPB van gecoördineerde handhaving op cloudgebruik door publieke sector

- in België: focus op ICT-dienstverleners voor overheid en overheidsinstanties die grote hoeveelheden gezondheidgegevens verwerken

Bron: noyb

CRANIUM



Bron: RESPONSUM

Methodologie

- Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermings-niveau van Persoonsgegevens in de Unie te waarborgen
- Risicogebaseerd - Rosenthal methode (afgewezen door verschillende autoriteiten)
- Tools en checklists

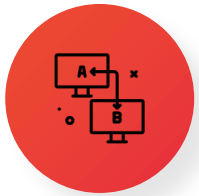
Nadruk op documentatie op grond van het beginsel van verantwoordingsplicht!

CRANIUM

Methodologie

1. In kaart brengen van doorgiften

Wees op de hoogte van wat u doorgeeft.



2. Bepalen van doorgifte-instrumenten

Een adequaatheidsbesluit, standard-contractbepalingen dan wel afwijkingsbepalingen.

3. Beoordelen wetgeving en praktijk

Elementen van het derde land die afbreuk doen aan doeltreffendheid passende waarborgen van doorgifte-instrumenten.

4. Nemen van aanvullende maatregelen

Nodig om doorgegeven gegevens in grote lijnen op beschermingsniveau te brengen van EU-norm.

5. Formele procedurele stappen

Vereist voor de toepassing van een aanvullende maatregel.

6. Regelmatig herevalueren

Doorlopend en in voorkomend geval samen met gegevensimporteur.

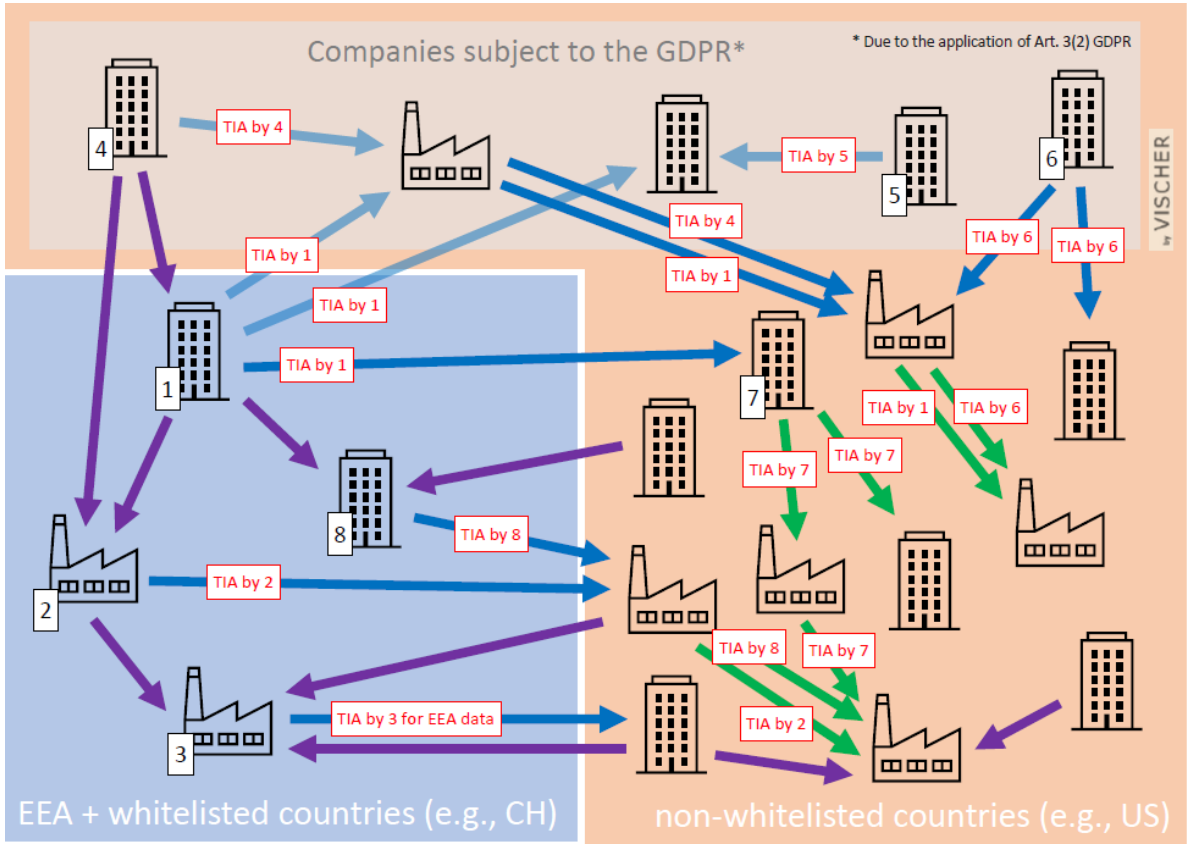
CRANIUM

1. In kaart brengen van doorgiften

- Welke persoonsgegevens en met welk doel:
  - gegevensminimalisatie (passend, relevant en beperkt tot het noodzakelijke)
- Ook toegang op afstand en/of opslag in een cloud buiten de EER
- Ook voor verdere doorgiften (aan subverwerkers)

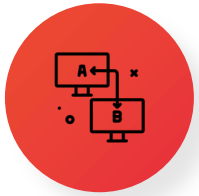
Bronnen:

- Register van de verwerkingsactiviteiten
- Website
- Contract
- Vragenlijst



Bron: Rosenthal

CRANIUM



2. Bepalen van doorgifte-instrumenten

- Adequaatheidsbesluiten (Art. 45 AVG)
  - Volgende stappen optioneel
  - Voorkomt niet dat een burger klacht indient

- Doorgifte-instrumenten (Art. 46 AVG)
  - Standaardbepalingen inzake gegevensbescherming
  - Bindende bedrijfsvoorschriften
  - Gedragscodes
  - Certificeringsmechanismen
  - Ad-hoc contractuele bepalingen

  Doorgegeven persoonsgegevens moeten in het algemeen in grote lijnen overeenkomstig worden beschermd (“essentially equivalent”)

- Afwijkingen (Art. 49 AVG)
  - Uitzonderlijk van aard

CRANIUM

3. Beoordelen wetgeving en praktijk

Essentie van de DTIA: Bevat wetgeving en/of geldende praktijken elementen die afbreuk doen aan doeltreffendheid passende waarborgen van doorgifte-instrument? (documenteren!)

Of: toegang tot gegevens mogelijk door overheidsinstanties van het derde land?

(gezien contractuele karakter niet bindend voor overheidsinstanties van derde landen)

1. In eerste instantie richten op relevante wetgeving
2. Onderzoek naar praktijken overheidsinstanties

Indien geen bescherming: doorgifte opschorten of (eventueel) aanvullende maatregelen nemen (Stap 4)

Beoordeling beperkt tot hetgeen relevant is voor de bescherming van de specifieke gegevens:
doel, soorten entiteiten, sector, categorieën, indeling van gegevens, verdere doorgiften

Gebruik ervaring van importeur alleen als aanvullende bron!

CRANIUM

4. Nemen van aanvullende maatregelen

Aanvullende maatregelen zijn contractueel, organisatorisch of technisch van aard.

Voorbeelden:

- Contractueel: verplichting tot bepaalde technische maatregelen, verplichtingen t.a.v. transparantie, betrokkenen de mogelijkheid bieden hun rechten uit te oefenen
- Technisch: volledige versleuteling, gepseudonimiseerde gegevens, beschermde ontvanger, gesplitste verwerking (“multi-party computation”)
- Organisatorisch: intern beleid, transparantie en verantwoording, gegevensminimalisering, gebruikers beperkte beslissingsrechten voor opslag

5. Formele procedurele stappen

Afhankelijk van doorgifte-instrument:

- Standaardcontractbepalingen
- Bindende bedrijfsvoorschriften
- Ad-hoc contractuele bepalingen

Soms raadpleging nodig van bevoegde toezichthoudende autoriteiten!

6. Regelmatig herevalueren

Beschermingsniveau moet op gezette tijden opnieuw beoordeeld worden.

In de praktijk

- Veelvoorkomend voor tools (Software-as-a-Service) – mogelijk combinaties van DTIA's
  - Broncode repository (Brazilië)
  - Chatbot (Verenigde Staten)
  - Microsoft, Amazon, Google, Meta & Apple (MAGMA)

- Ook voor internationale organisaties
  - Belgische vestiging → Amerikaans moederbedrijf
  - Chinees hoofdkantoor → Belgisch kantoor → Chinees hoofdkantoor → Thailand → Turkije …

- Soms in breder verband om te voldoen aan de verantwoordingsplicht
  - Eenmalige *peer review* tussen internationale collega's (EU-China)
  - Risico's identificeren en mitigeren (afwijkingen Art. 49 AVG)

In de praktijk

Voorbeeld 1: broncode repository

1. In kaart brengen

- Derde landen: VS maar ook Brazilië, India, China, etc. → TIA's vereist
- Doel van de doorgifte: klantenservice (support, feedback, accountbeheer) op SaaS platform dat in EU wordt gebruikt
- Persoonsgegevens: o.a. tijdzone, bugrapporten, contactgegevens (geen speciale categorieën)

Andere criteria: privé-entiteiten (c2p), occasionele toegang, toegang op afstand, encryptie in transit, geen verdere doorgifte

2. Bepalen van doorgifte-instrumenten

Standaardcontractbepalingen (“SCCs”)

In de praktijk

Voorbeeld 1: broncode repository

3. Beoordelen wetgeving en praktijk

- Juridisch kader voor de bescherming van persoonsgegevens
  - Lei Geral de Proteção de Dados ("LGPD") – AVG-geïnspireerd
  - Braziliaans kader voor burgerrechten op internet
  - (meer) onafhankelijke Nationale Gegevensbeschermingsautoriteit (ANPD)
- Toezichtwetgeving (wet 9.296/96):
  - Brede toegang tot opgeslagen persoonlijke gegevens (o.a. abonnementsgegevens zoals NAW-gegevens en oproepgegevens)
  - Brede gegevensbewaring (Anatel-resoluties 426/05 en 614/13, wet 12.850/13, Marco Civil)
  - Enkele waarborgen maar beperkt in de praktijk
- Ervaring van importeur en actoren die binnen dezelfde sector opereren, voor vergelijkbare PA

↳ Standaardcontractbepalingen bieden niet op doeltreffende wijze een in grote lijnen overeenkomend beschermingsniveau (hoewel toegang in de praktijk onwaarschijnlijk lijkt)

CRANIUM

In de praktijk

Voorbeeld 1: broncode repository

4. Nemen van aanvullende maatregelen

- Technisch:
  - verbeterde gegevensminimalisatie en beveiliging
  - verregaande gebruikerscontrole
  - duidelijke definitie van verwijderings- en retentieparameters
  - documentscan met verwijdering van gevoelige informatie voorafgaand aan overdracht
  - voorafgaande hashing van contactgegevens, toepassing van encryptie tijdens doorgifte (met sleutel bij gegevensexporteur)
- Contractueel:
  - striktere contractuele verplichtingen, transparantie toezeggingen en rapporten
- Organisatorisch:
  - verbeterde toegangs- en vertrouwelijkheidsbeleid
  - toepassen van classificatieniveaus

In de praktijk

Voorbeeld 1: broncode repository

5. Resultaat

- Het kader voor gegevensbescherming is gebaseerd op de AVG en biedt bepaalde garanties
- Toezichtwetten zijn van toepassing (in theorie) + beperkte garanties
- Standaardcontractbepalingen bieden onvoldoende bescherming
  - Uitgebreide garanties van de dienstverlener (technisch, contractueel en organisatorisch)
  - Betrouwbare input van importeur en andere actoren binnen dezelfde sector

In dit geval een risicogebaseerde benadering

- Geen speciale categorieën en gevoelige persoonsgegevens uitgesloten
- Waarborgen in combinatie met aanvullende maatregelen worden momenteel voldoende geacht om effectief een wezenlijk gelijkwaardig beschermingsniveau te garanderen.

In de praktijk

Voorbeeld 2: chatbot

1. In kaart brengen

- Derde landen: Verenigde Staten
- Doel van de doorgifte: gericht adverteren d.m.v. simulatie van menselijke interactie (B2B-context)
- Persoonsgegevens: o.a. naam, werkgever/bedrijf, werktitel, werk-e-mail, werktelefoonnummer, IP-adres van een door de werkgever uitgegeven apparaat en geschatte algemene locatie (zoals stad of regio)

Andere criteria: continue doorgifte gedurende overeenkomst, geen significant volume, geen gevoelige informatie of hoog-risico activiteiten

2. Bepalen van doorgifte-instrumenten

Standaardcontractbepalingen (“SCCs”)

In de praktijk

Voorbeeld 2: chatbot

3. Beoordelen wetgeving en praktijk

- Juridisch kader voor de bescherming van persoonsgegevens
  - FISA Amendments Reauthorization Act van 2017
  - Sectie 215 van de Patriot Act
  - PEN Registers en Trap and Trace Statutes
  - Executive Order 12333
  - Stored Communications Act (SCA) (18 U.S.C. §§ 2701-2712)
  - Clarifying Lawful Overseas Use of Data (“CLOUD”) Act
  - National Security Letters (NSL)
- Bevestiging van leverancier nooit een verzoek te hebben ontvangen van de Amerikaanse overheid voor toegang tot de gegevens van een klant op grond van één van bovengenoemde wetten.
- Departement van Handel van de Verenigde Staten: whitepaper met sterke aanwijzingen dat persoonsgegevens waarover chatbot beschikt niet relevant zijn voor autoriteiten.

In de praktijk

Voorbeeld 2: chatbot

4. Nemen van aanvullende maatregelen

- Technisch:
  - systeem wordt getraind in de cloud, on-premises met enkel interconnectie voor facturatie
  - onmiddellijk negeren van overbodige gegevens (weliswaar in de cloud), technisch wel verwerking en doorgifte
- Organisatorisch:
  - vermijden van vrije tekstvelden door gerichte interactie

In de praktijk

MAGMA: Microsoft, Apple, Google, Meta & Amazon

- Persoonsgegevens: metadata (Google Analytics) of direct identificeerbare gegevens (Google Drive)
- Vaak sterk ingebed in organisatie, beperkte marge voor onderhandeling
- Vaak toezeggingen van bedrijven zelf, maar zelden 100% gegarandeerd (procedures, kennisgeving, etc.)
- Analyse: geen nationale privacywetgeving, complex samenspel van nationale, provinciale en lokale wetten en praktijken; daarnaast surveillance wetgeving (toegang door autoriteiten)
- Klachten (vb. *noyb*) en vonnissen die gebruik ontraden

Oplossing:

- Idealiter: gebruik enkel EU based service providers (vb. Matomo, Piwik, Fathom, etc.)
- Indien niet haalbaar (na marktonderzoek geen EU based alternatief):
  - Kies voor zo hoog mogelijke beveiligingsinstellingen
  - Verantwoord geïdentificeerde of resterende risico's
  - Fade-out planning (tijdlijn en mijlpalen)
  - Ondersteuning 24/7 aanpassen aan nood ("follow the sun")
  - Minimale gegevensverwerking

} Documenteer!

CRANIUM

Samengevat

- Wees realistisch
- Voorkomen is beter dan genezen
- Wees op de hoogte van de doorgiften
- Wees kritisch en vraag door
- Evalueer bijkomende beveiliging
- Documenteer
- Doe het niet alleen

Keep calm & call CRANIUM

Q&A

CRANIUM