Member of BOW TIE SECURITY

DJ ACADEMY SERIES DATA PROTECTION

Complexe verplichtingen pragmatisch vertaald

dj TALKS

Inleiding

1. GDPR, de fundamenten uitgelicht voor de ondernemer (14/7)
2. **GDPR, complexe verplichtingen pragmatisch vertaald** (28/7)
3. GDPR use case: direct marketing (11/8)
4. GDPR use case: personeelsbeleid (25/8)

Sprekers:

Kris Seyen, Partner

Duygu Öztürk, CIPP/E

Larissa De Keyser, CIPT

OPWARMEN MET EEN QUIZ

Vraag 1

Wat is correct met betrekking tot technische en organisatorische maatregelen (TOM's)?

- ❑ Dit betekent dat een organisatie moet voldoen aan de ISO 27001 normen;
- ❑ Sommige organisaties hoeven geen TOM's te hebben;
- ❑ Heeft enkel betrekking op IT-systemen;
- ❑ TOM's moeten regelmatig worden geëvalueerd.

Vraag 1 - antwoord

Wat is correct met betrekking tot technische en organisatorische maatregelen (TOM)?

- ❑ Dit betekent dat een organisatie moet voldoen aan de ISO 27001 normen;
- ❑ Sommige organisaties hoeven geen TOM's te hebben;
- ❑ Heeft enkel betrekking op IT-systemen;
- ❑ **TOM's moeten regelmatig worden geëvalueerd.**

Vraag 2

Welke thema’s hebben volgens het strategisch plan (2020-2025) van de Gegevensbeschermingsautoriteit prioriteit en zullen dus met voorrang gehandhaafd worden? (2 juiste antwoorden);

- ❑ Direct marketing;
- ❑ Foto’s en films maken en gebruiken;
- ❑ Data Transfer;
- ❑ Combineren van databanken.

Vraag 2 - antwoord

Welke thema's hebben volgens het strategisch plan (2020-2025) van de Gegevensbeschermingsautoriteit prioriteit en zullen dus met voorrang gehandhaafd worden? (2 juiste antwoorden);

- ❑ **Direct marketing**
- ❑ **Foto's en films maken en gebruiken**
- ❑ Data Transfer
- ❑ Combineren van databanken

Praktijkgericht voorbeeld

Kledingwinkel *Zahara* heeft een webshop waar verschillende kledingstukken voor mannen, vrouwen en kinderen worden verkocht.

De webshop verwerkt persoonsgegevens van **bezoekers** van de website, **gebruikers** die een account hebben voor de webshop en **klanten** die een kledingstuk bestellen.

BIJZONDERE CATEGORIEËN VAN PERSOONSGEGEVENS

"Gevoelige gegevens"

“Gevoelige gegevens”

- ras/etnische afkomst
- politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond
- gezondheidsgegevens
- genetische gegevens
- biometrische gegevens ter identificatie
- seksuele voorkeur
- strafrechtelijke antecedenten

Algemene aandachtspunten:

- Verwerking is principieel **verboden**
- Verwerkingsgrond nodig **+ wettelijke uitzonderingssituatie**

“Gevoelige gegevens”

- ras/etnische afkomst
- politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond
- gezondheidsgegevens
- genetische gegevens
- biometrische gegevens ter identificatie
- seksuele voorkeur
- strafrechtelijke antecedenten

Wettelijke uitzonderingsgronden:

- Toestemming;
- Arbeidsrecht/socialezekerheidsrecht / sociale beschermingsrecht;
- Vitale belangen betrokkene;
- Politieke, levensbeschouwelijke, godsdienstige, of vakbondsorganisaties;
- Gegevens ‘kennelijk’ zelf openbaar gemaakt;
- Rechtsvordering;
- Gerechten die hun rechtsbevoegdheid uitoefenen;
- Preventieve of arbeidsgeneeskunde, medische diagnosen, verstrekken van gezondheidszorg;
- Zwaarwegend algemeen belang volgens nationaal echt of EU-recht;
- Algemeen belang voor de volksgezondheid;
- Archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

“Gevoelige gegevens”

- ras/etnische afkomst
- politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond
- gezondheidsgegevens
- genetische gegevens
- biometrische gegevens ter identificatie
- seksuele voorkeur
- strafrechtelijke antecedenten

Bijkomende verplichtingen/waarborgen:

- Opstellen lijst met categorieën van personen (bv. functies in het bedrijf) die toegang krijgen tot gevoelige gegevens;
- Deze categorieën van personen moeten gehouden zijn het vertrouwelijk karakter in acht te houden (bv. NDA of confidentialiteitsclausule);
- Nooit vrijgesteld van verplichting tot houden verwerkingsregister;
- Op ‘grote schaal’?
  - DPO aanstellen;
  - DPIA uitvoeren.

“Gevoelige gegevens”

- ras/etnische afkomst
- politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond
- gezondheidsgegevens
- genetische gegevens
- biometrische gegevens ter identificatie
- seksuele voorkeur
- strafrechtelijke antecedenten

Lokale verschillen tussen de lidstaten!

- Belangrijk om het nationaal recht na te gaan;
- Voorbeeldje uit de gezondheidszorg:
  - de *Wet van 22 augustus 2002 betreffende de rechten van de patiënt*: legt enkele specifieke voorwaarden op met betrekking tot het patiëntendossier.

Praktijkgericht voorbeeld

Indien gebruiker via zijn of haar account een profielfoto kan uploaden

> ***bijzonder persoonsgegeven***

TECHNISCHE & ORGANISATORISCHE MAATREGELEN

De “TOM’s”

Technische en organisatorische maatregelen

(TOM’s)

Algemene aandachtspunten:

- State of the art;
- Afstemmen op de verwerkingsactiviteit (passend);
- Maatregelen moeten worden geëvalueerd.

Praktijkgericht voorbeeld

Voorbeelden TOM's *Zahara:*

- pseudonimisering en versleuteling ('encryptie') van persoonsgegevens;
- Gebruik maken van two-factor identificatie;
- Firewall;
- Antivirussoftware;
- Regelmatig back-up van gegevens;
- Richtlijnen binnen de organisatie over het verwerken van persoonsgegevens;
- Privacy-bewustzijn creëren binnen de organisatie door middel van trainingen.
- Wachtwoordbeleid (d.w.z. vereiste lengte, complexiteit en periodieke resets, herstel van verloren wachtwoord);
- Extra inloggen op het systeem voor bepaalde toepassingen;
- Het automatisch blokkeren van gebruikers na een bepaalde tijd zonder activiteit en vereisen identificatie/wachtwoord om heropend te worden.

DATA PROTECION IMPACT ASSESSMENT

De ‘gegevensbeschermingseffectbeoordeling’ of ‘DPIA’

DPIA

Stap 1:

- **Nagaan of een DPIA verplicht is (of gewenst). Documenteer dit!**

Stap 2:

- **DPIA uitvoeren> *vooraf* privacy risico's in kaart brengen;**

Stap 3:

- **Beslissen welke maatregelen nodig zijn om de risico's te verkleinen en nagaan of een voorafgaande raadpleging nodig is.**

Tool voor de verantwoordingsplicht!

Verplicht bij 3 soorten verwerkingen:

- systematische en uitgebreide beoordeling van de persoonlijke aspecten van personen, inclusief profilering;
- verwerking van gevoelige gegevens op grote schaal;
- stelselmatige en grootschalige monitoring van openbare ruimten.

Restgevallen:

- "Waarschijnlijk een hoog privacyrisico voor betrokkenen".
- Bv. IoT-toepassingen (GBA lijst)

Praktijkgericht voorbeeld

Wanneer zou Zahara een DPIA moeten uitvoeren?

- Nieuw project: Het verzamelen van openbare sociale media gegevens voor het genereren van profielen (profiling).
- Dit project betekent dat:
  - op grote schaal persoonsgegevens zullen worden verwerkt;
  - datasets zullen worden gecombineerd;
  - gevoelige gegevens of gegevens van zeer persoonlijke aard zal verwerken.

→ **DPIA waarschijnlijk vereist**

AANSPRAKELIJKHEID TEGENOVER BETROKKENEN

Aansprakelijkheid onder de GDPR tegenover betrokkenen

‘Aansprakelijkheid’

- Op wie rust de schadevergoedingsverplichting tegenover de betrokkene?

Wat voor schade?

- Materiële en immateriële

Bij wie GDPR schadeclaim indienen?

- Betrokkene kan volledige schadeclaim indienen bij controller óf processor wanneer beide AS
- Regresvordering

Controller

Inspanningsverbintenis

Resultaatsverbintenis

Aansprakelijkheidsregeling:

- Algemeen AS voor alle schade die voortvloeit uit de onrechtmatige verwerking van persoonsgegevens;
- Strenger dan ‘persoonlijk toerekenbare fout’:
  → door controller zelf of door een processor veroorzaakt.

Niet aansprakelijk:

- Bewijs *op geen enkele wijze* verantwoordelijk voor de inbreuk:
  - overmacht;
  - processor heeft buiten of tegen instructies gehandeld.

Processor

Inspanningsverbintenis

Resultaatsverbintenis

Slechts aansprakelijk:

- Niet-naleving van de specifiek tot hem gerichte verplichtingen;

OF

- Buiten of in strijd met de rechtmatige instructies van de controller gehandeld.

Meerdere controller(s)/ processor(s) verantwoordelijk?

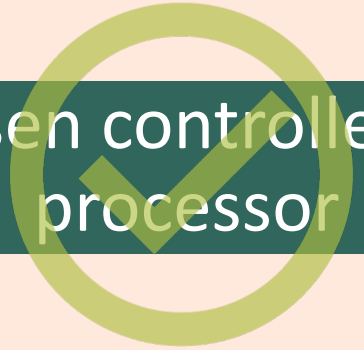
‘Hoofdelijke’ aansprakelijkheid

- Beschermingsmechanisme: effectieve vergoeding voor betrokkene;
- Keuze wie betrokkene aanspreekt voor de vergoeding van de volledige schade;
- Regresvordering (tussen de aansprakelijken).

Contractueel AS beperken?

Tegenover betrokkenen

Tussen controller en processor



Waar kan betrokkene schadevergoeding bekomen?

Gegevensbeschermingsautoriteit (GBA)

Via de gewone bevoegde rechtbanken

Schadeclaim bij *Zahara*

- Er ontstaat een datalek bij *Zahara* waardoor de klantgegevens (inclusief transactiedata) van klanten die de afgelopen maand een aankoop hebben gedaan, terecht is gekomen op het Dark Web;
- Uit onderzoek blijkt dat het datalek is veroorzaakt door de leverancier van *Zahara* (verwerker);
- Verschillende betrokkenen stellen een schadeclaim bij *Zahara* via de rechter;

Zahara moet de schadeclaim van de betrokkenen vergoeden (indien het is toegewezen door de rechter);

De kans op fraude is groot (grote impact voor de privacy van betrokkenen);

Zahara kan regres vorderen bij haar leverancier voor het gedeelte van de schadevergoeding dat overeenkomt met het aandeel in de aansprakelijkheid voor de geleden schade (**let op!**: *raadpleeg de DPA)*

GBA SANCTIES

De GBA

Bevoegdheden:

- Onderzoeken;
- Adviseren;
- Toezicht houden op de naleving van de GDPR.

Administratieve geldboetes

Corrigerende maatregelen

Administratieve boetes

Hoe wordt de hoogte van de boete bepaald?

- Doeltreffend, evenredig en afschrikkend gelet op de concrete omstandigheden;

- Administratieve boete tot **10 miljoen** euro of **2 procent** van omzet (dewelke het hoogste is). Voorbeelden:
  - ➢Geen verwerkingsregister of niet voldoende;
  - ➢TOMS niet in orde;
  - ➢Geen DPO aangesteld;
  - ➢Geen DPIA uitgevoerd;

- Administratieve boete van **20 miljoen** euro of **4 procent** van de omzet (dewelke het hoogste is). Voorbeelden:
  - ➢Algemene beginselen;
  - ➢Geen wettelijke verwerkingsgrond;
  - ➢Toestemming niet geldig;
  - ➢Rechten van betrokkenen niet worden gerespecteerd;
  - ➢Wanneer een corrigerende maatregel van de GBA niet werd nageleefd.

Correctieve maatregelen

Voorbeelden

- Waarschuwing;
- Berisping;
- Bevel om verwerking in overeenstemming te brengen met de GDPR;
- Tijdelijk of definitief verwerkingsbeperking/-verbod opleggen;
- Opschorting van internationale transfer (buiten de EER).

Dankjewel voor je deelname!

Vragen kunnen gemaild worden naar hallo@dejuristen.be .

De antwoorden worden, samen met de replay en de presentatie, aan alle deelnemers ter beschikking gesteld.

deJuristen

SCAN ME

Member of BOW TIE SECURITY

dJ TALKS