Vorming gegevensdeling ELZ Dender

Jens Lemarcq - DPO

Agenda

- ✓ Wie ben ik?
- ✓ GDPR
  - ✓ Pauze
- ✓ Doorgifte van persoonsgegevens
- ✓ Interessante uitspraken GBA
- ✓ Vragen?
  - ✓ Phishing

Even voorstellen

- Jens Lemarcq
  - DPO
    - eGov
    - lokale besturen
    - Sociale huisvestingsmaatschappijen
    - Provinciale centra
  - Verleden in lokaal bestuur

Wat doet een DPO?

- Informeren, controleren, adviseren en sensibiliseren
- Toezien op de naleving van voorschriften en wetgeving
- Documentatie aanleggen i.v.m. informatieveiligheid en bescherming van persoonsgegevens
- Opstellen beleidsdocumenten en procedures
- Rapporteren vastgestelde inbreuken & zwakheden
- Opmaken informatieveiligheidsplan
- Contactpunt voor de toezichthoudende autoriteiten

Agenda

- ✓ Wie ben ik?
- ✓ GDPR
  - ✓ Pauze
- ✓ Doorgifte van persoonsgegevens
- ✓ Interessante uitspraken GBA
- ✓ Vragen?
  - ✓ Phishing

lets te verbergen?
vs.
Privacy?

Waarom informatieveiligheid

Persoonsgegevens

- **Alle** informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene)
  - **direct** of **indirect** te identificeren, met name aan de hand van een **identificator**:
    - Naam
    - Identificatienummer
    - Locatiegegevens
    - Online identificator
    - Elementen kenmerkend voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit

Principes waarop de AVG bouwt

1. Transparantie
2. Doelbinding
3. Gegevensminimalisatie
4. Juistheid
5. Vertrouwelijkheid
6. Verantwoording

Principe 1: Transparantie

GDPR geeft aan de cliënt vrijwel absoluut recht op volledige transparantie

- Uitgebreide schriftelijke informatie aan cliënt, zowel wanneer gegevens bij de betrokkene als wanneer gegevens bij een derde (bv. authentieke bron, buren, familieleden, etc.) worden bekomen (artikel 13-14 GDPR)

  → Aanpak in de praktijk: privacyverklaring en clausules op formulieren

- Quasi absoluut recht op inzage in eigen gegevens en recht op mededeling van een kopie (uitzonderingen enkel mogelijk via wettelijke bepalingen)

Principe 2: Doelbinding

Persoonsgegevens mogen enkel worden verwerkt voor welbepaalde, gerechtvaardigde doeleinden

- Doelbinding betekent ook: nooit de ingewonnen informatie voor iets anders gebruiken indien dat niet verenigbaar is met het oorspronkelijke doel

Principe 3: Gegevensminimalisatie

Enkel relevante gegevens verwerken die noodzakelijk zijn om het doel te bereiken

- Hoe minder gegevens, hoe beter
- need to know vs. nice to know
- Gegevens die niet meer nodig zijn: opkuisen (principe van opslagbeperking), maar met aandacht voor wettelijke bewaartermijnen en eventuele archiefverplichtingen

Principe 4: Juistheid

De gegevens moeten juist zijn en geactualiseerd indien nodig

- “Alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren”

- Cliënt heeft het recht om onjuiste gegevens te laten corrigeren of onvolledige gegevens te laten aanvullen (recht op rectificatie)

Principe 5: Vertrouwelijkheid

Nemen van technische en organisatorische maatregelen zodat een passende beveiliging gewaarborgd is

- Bescherming van persoonsgegevens “tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging”

- Technische maatregelen: bv. anti-malware, antivirus, back-ups, wachtwoorden, …
- Organisatorische maatregelen: bv. toegang beperken tot bepaalde profielen, kasten op slot, sensibilisering, …
- Maatregelen moeten geëvalueerd en indien nodig geactualiseerd worden
- Verhouding tussen verwerkingsverantwoordelijke en verwerker vastleggen in verwerkerscontracten

Datalek

- USB-stick verloren met persoonsgegevens
- verkeerd verzonden e-mail met persoonsgegevens
- dossier verloren
- open kasten of dossiers op bureau bij afwezigheid
- Stroompanne
- Op cafe babbeltje doen over je cliënt
- Informatie met derde delen over de cliënt zonder akkoord

Wat te doen?

- Belet verdere schade
- Zo snel mogelijk melden aan
    - verantwoordelijke
    - DPO
- Verzamel info
- Datalek-check door FG
    - 72u voor melding bij toezichthoudende instantie

Principe 6: Verantwoording

De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van de GDPR en moet deze kunnen aantonen

- Accountability-principe
- Is in feite een omkering van bewijslast
- Rol van de toezichthoudende overheid (Vlaamse Toezichtcommissie): controleren
- Rol van de onafhankelijke “functionaris voor gegevensbescherming” (de DPO): bijstaan en adviseren

Rechtmatigheid verwerking

- 6 grondslagen (5 voor publieke sector) om te mogen verwerken:
  - Toestemming
  - Uitvoering van overeenkomst
  - Wettelijke verplichting
  - Vitale belangen
  - Algemeen belang
  - Gerechtvaardigde belangen van de verantwoordelijke of van een derde
    - belangenafweging: als belangen betrokkenen doorwegen geen grondslag
    - (geen grondslag voor publieke sector)

Toestemming

Expliciete toestemming nodig

- Geïnformeerd
- Ondubbelzinnig
- Vrij
- Specifiek

Geen vooraf aangevinkte vakjes
‘Opt-out’ even eenvoudig als de ‘opt-in’

Beroepsgeheim

- Van toepassing?
  - beroepsgeheim in wetgeving
  - de maatschappelijke erkenning van de noodzakelijke vertrouwensfunctie blijkt uit een geheel aan wettelijke elementen (impliciet)
  - de maatschappelijke erkenning van de noodzakelijke vertrouwensfunctie blijkt uit de traditie of de gewoonte.

Beroepsgeheim gedeeld?

- Van toepassing?
  - De bij de informatie-uitwisseling betrokken personen moeten allemaal gebonden zijn aan het beroepsgeheim.
  - binnen dezelfde hulpverleningscontext
  - Met dezelfde finaliteit wat de hulpverlening aan de cliënt betreft

Beroepsgeheim gezamelijk?

- Nieuwer concept
- voorwaarden gelden dezelfde als deze die gelden binnen de context van het gedeelde beroepsgeheim
- MAAR-> noodzakelijkheidscriterium ietwat versoepeld naar een relevantiecriterium
- MAAR -> AVG: informatiedeling steeds beperkt tot hetgeen noodzakelijk is voor het te bereiken doeleinde

Instemming van de cliënt

- Voorwaarden?
  - Voorafgaandelijk
  - Vrij
  - Specifiek
  - Actieve handeling
  - Geïnformeerd
  - INTREKBAAR

Beroepsgeheim

- Soms twijfel over breken (wettelijke basis)
  - Noodtoestand
  - Art 458.bis SWB

Basisprincipes wetgeving persoonsgegevens

⇒gedetailleerd antwoord geven op volgende vragen:

1. Mag het? (= Legaliteitsbeginsel)
2. Waarvoor precies? (= Finaliteitsbeginsel)
3. Is het niet overdreven? (= Proportionaliteitsbeginsel)
4. Is de betrokkene ingelicht? (= Transparantiebeginsel)

Agenda

- ✓ Wie ben ik?
- ✓ GDPR
  - ✓ Pauze
- ✓ Doorgifte van persoonsgegevens
- ✓ Interessante uitspraken GBA
- ✓ Vragen?
  - ✓ Phishing

Doorgifte van gegevens

- Niet zomaar persoonsgegevens doorgeven
- De algemene regel:

  verstrekken van persoonsgegevens alleen als dat verenigbaar is met het doel waarvoor de gegevens zijn verzameld.
- Hangt af van de concrete omstandigheden.
- (Zie de 6 rechtsgronden)

Niet verenigbaar?

- Toestemming
- Wettelijke bepaling

=> Ook ok

Verenigbaar?

- Ieder verband met het doel van verzamelen
- Kader waarin de persoonsgegevens zijn verzameld
- Aard van de gegevens
- Gevolgen van een verstrekking
- Bestaan van passende waarborgende
- verwachtingen van de betrokkene

Hoe regel je doorgifte?

- Zorg voor
  - Verwerkersovereenkomst
  - Samenwerkingsovereenkomst
  - Protocol

Agenda

- ✓ Wie ben ik?
- ✓ GDPR
  - ✓ Pauze
- ✓ Doorgifte van persoonsgegevens
- ✓ Interessante uitspraken GBA
- ✓ Vragen?
  - ✓ Phishing

1) Direct marketing - Roze doos

- Onderneming verdeelt 'Roze Dozen' met stalen, aanbiedingen en infofiches aan aanstaande moeders
- Verdeling via gynaecologen
- Onderneming verkoopt klantgegevens aan deelnemende bedrijven

1) Direct marketing - Roze doos

Beslissing
Overdracht zonder geldige toestemming

- Niet vrij: niet-verlenen van toestemming betekende voor betrokkenen het verlies van voordelen verbonden aan roze doos
- Niet specifiek: toestemming voor ontvangen roze doos werd door Family Service gelijkgesteld met toestemming voor gegevensoverdracht
- Niet transparant: betrokkenen niet op duidelijke én begrijpelijke manier geïnformeerd over verwerking
- Info was des te belangrijker omdat klanten konden denken dat het initiatief van de oh kwam

1) Direct marketing - Roze doos

- Bekom geldige toestemming voor gegevensoverdracht.
  - ik ga akkoord om reclame te ontvangen’
  - ik ga akkoord om reclame te ontvangen van partners van uw bedrijf
  - ik ga akkoord met doorgifte van mijn gegevens aan derden
- Granulair opgebouwd en actief
- Geef transparante info

2) Verstrekking van persoonlijke informatie aan derden zonder toestemming (07/2021)

A. Vennoot stuurde gegevens door van 100% aandeelhouder aan vroegere associé

+

B. Associé stuurde de gegevens naar zijn raadsman die de gegevens stuurde gegevens naar de raadsman van de vennoot

2) Verstrekking van persoonlijke informatie aan derden zonder toestemming (07/2021)

Beslissing:

A. Gegevens waren verzameld voor boekhouding, mochten enkel daarvoor gebruikt worden.
B. Doorzenden op zich is verwerking => associé is verantwoordelijk

2) Verstrekking van persoonlijke informatie aan derden zonder toestemming (07/2021)

A. Zorg voor verenigbaar doel & wees transparant bij doorzenden
B. De informatie die je verkrijgt zonder geldige rechtsgrond mag je niet verder verwerken

contact

Jens Lemarcq
+32 470 21 59 63

Jens.lemarcq@oost-vlaanderen.be

eGov.oost-vlaanderen.be

/company/pivaegov/

@pivaeGov