Infoavond GDPR

08 MAART 2018

ADVOCAAT
NICOLAS VANSPEYBROUCK

Indeling van de infoavond

- Inleiding
- GDPR en juridische aspecten (Mr. Nicolas Vanspeybrouck)
- Pauze
- IT-oplossingen inzake GDPR (Ronald Casteleyn, Faromedia bvba)

Wat is de GDPR ?

General Data Protection Regulation
Algemene Verordening Gegevensbescherming

- EU Verordening ⇔ Europese Richtlijn
- De bescherming van natuurlijke personen
- Verwerking van persoonsgegevens
- Vrije verkeer van deze gegevens

Stelling: De GDPR-verordening is niet van toepassing op mijn KMO.

Dit zou alleen maar kunnen, voor zover er geen persoonsgegevens verwerkt worden.

Wat verstaat de GDPR onder persoonsgegevens ?

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identicator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Voorbeelden van persoonsgegevens

De evidente:

- Voornaam
- Naam
- Geslacht
- Geboortedatum
- Geboorteplaats
- Adres

Voorbeelden van persoonsgegevens

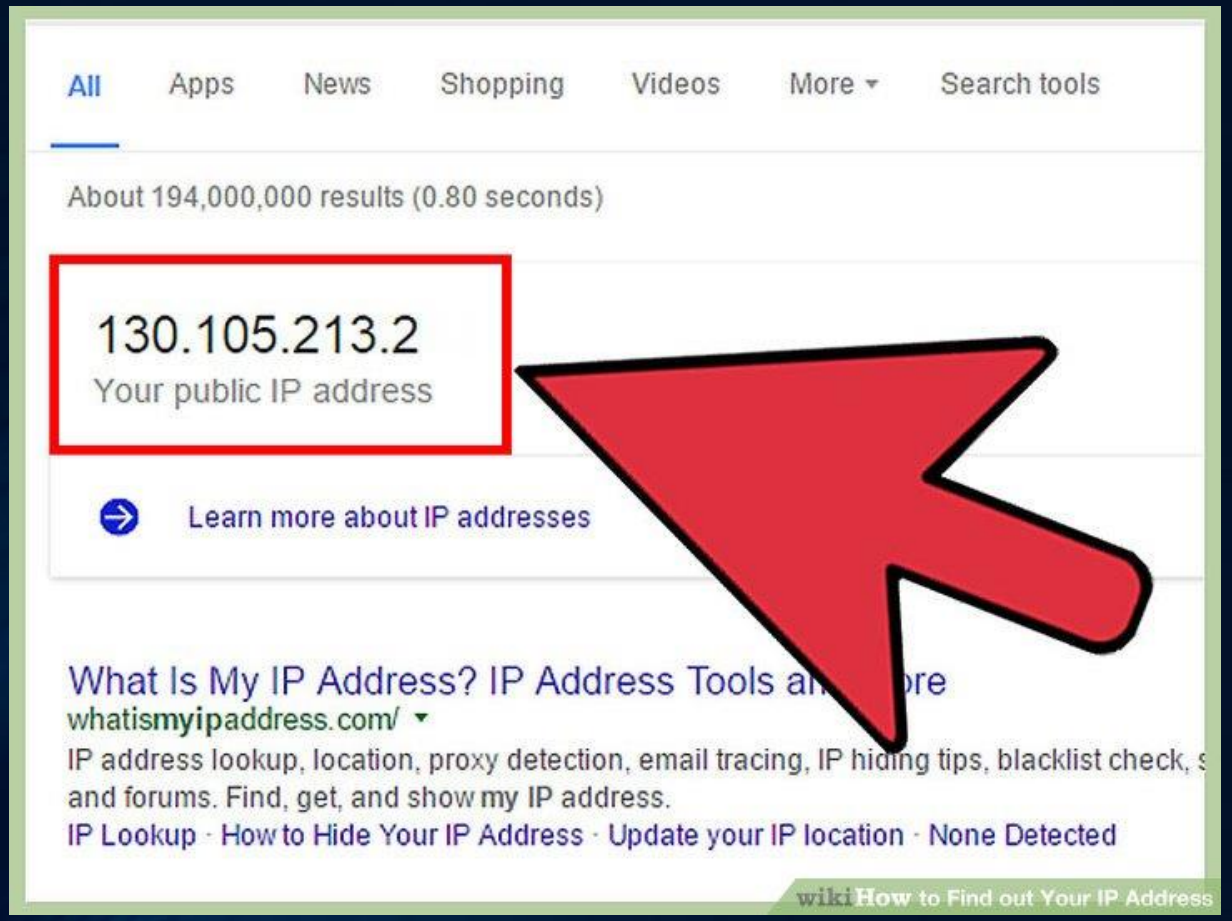
Minder evidente:

Voorbeelden van persoonsgegevens:

Minder evidente:

Voorbeelden van persoonsgegevens:

Minder evidente:

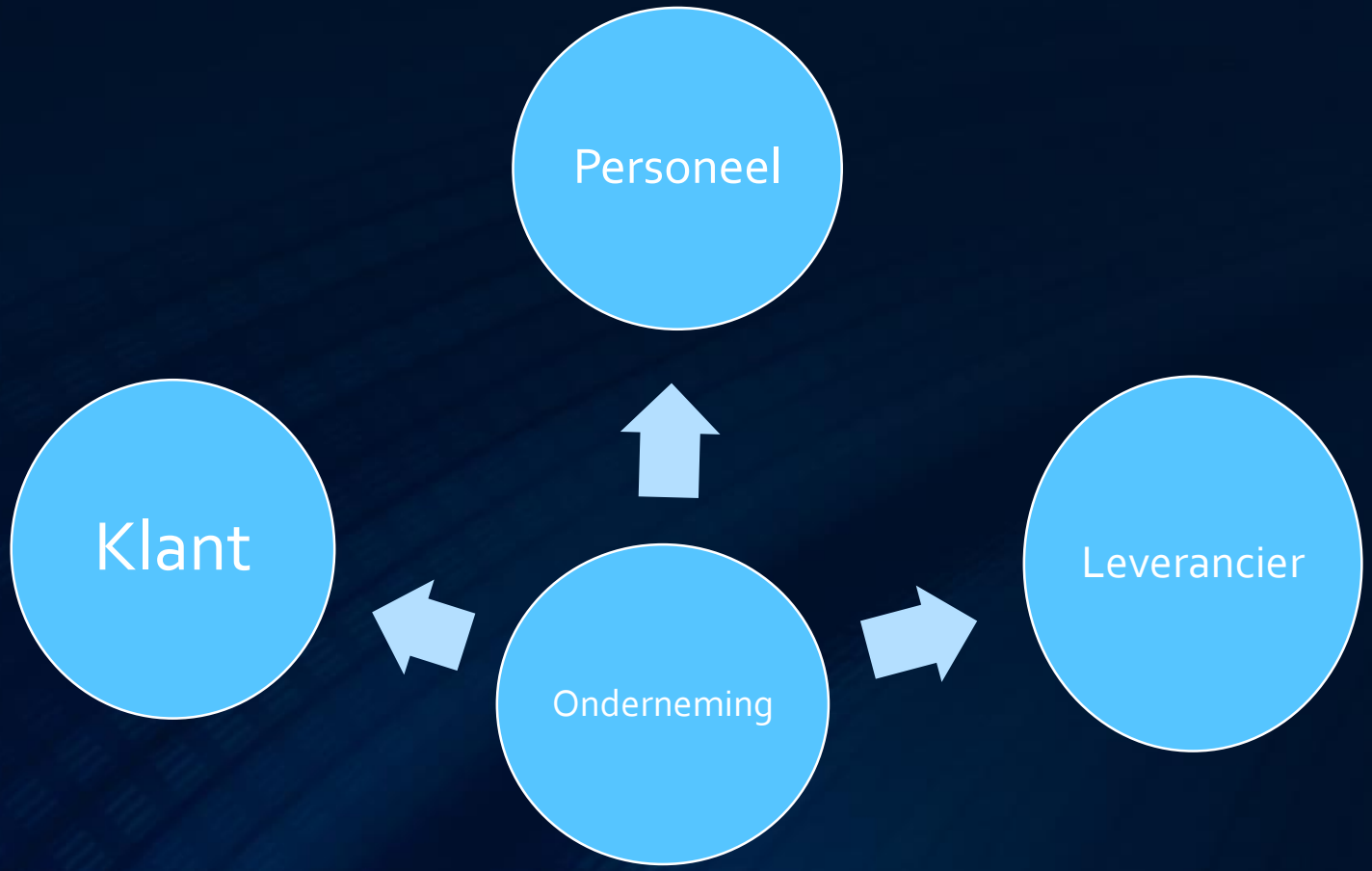


Vraag: zijn dit ook persoonsgegevens ?

- info@aanzeehotel.be
- voorzitter@ganzeweide.be
- bert@rommelaerenv.be
- sylvie.micholt@amistadlaw.be

Dus zelfs in een loutere B2B context kan er ook sprake zijn van persoonsgegevens!

Waar kunnen er persoonsgegevens aangetroffen worden?



Let op! Bepaalde gegevens zijn gevoeliger dan andere.

- Bijzondere categorieën van gegevens:
  - Persoonsgegevens waaruit de raciale of etnische afkomst, politieke opvattingen, godsdienstige of levensbeschouwelijke overtuiging of **lidmaatschap van een vakbond**, en **gegevens i.v.m. de gezondheid** of gegevens met betrekking tot het seksleven of seksuele geaardheid van een natuurlijk persoon.

- Strafrechtelijke gegevens
- Nationaal identificatienummer
- Genetische gegevens
- Biometrische gegevens (vingerafdruk/irisscan/handpalm)

Principe: VERBODEN, tenzij specifieke rechtsgrond.

Verplichtingen binnen de GDPR

Stelling:

- Mijn onderneming voldoet aan de GDPR door het opstellen van een aantal documenten.
- Mijn KMO heeft een externe firma aangesteld die dit zal regelen en voor de rest moet ik mij daar niets aantrekken.

Verplichtingen binnen de GDPR

De GDPR-verordening vergt van ons een mentaliteitswijziging.

We moeten voortaan stilstaan over de manier hoe we omgaan met de verwerking van persoonsgegevens én hoe we deze beschermen tegen verlies.

Privacy by default/ Privacy by design
Verantwoordingsplicht ➡ omkering van bewijslast

Verplichtingen binnen de GDPR

Basisbeginselen inzake persoonsgegevens:

- Rechtmatigheid
- Doelbinding
- Relevant
- Juistheid
- Opslagbeperking
- Vertrouwelijkheid

Verplichtingen binnen de GDPR

Rechten van natuurlijke personen:

- Transparantie en informatie
- Recht op inzage
- Recht op rectificatie
- Recht op bezwaar
- Recht op vergetelheid

Verplichtingen binnen de GDPR

Stelling: Indien iemand vraagt om vergeten te worden, ben ik verplicht om dit na te leven.

Dit is **niet absoluut**: bv verzoek tot wissing uit strafregister

Kan geweigerd worden wegens bepaalde wettelijke verplichtingen

- Vrijheid van meningsuiting en informatie
- Bijhouden facturen/boekhouding
- Bewaring van dossiers (art. 2276 & 2276bis B.W.)

Verplichtingen binnen de GDPR

Kan uw onderneming het technisch aan om iemand te wissen?

- Software
- Back-up
- Hard copy

Opgelet: De GDPR beperkt zich niet tot de louter elektronische bestanden, maar strekt zich uit tot alle mediums waar er persoonsgegevens op staan.

Verplichtingen binnen de GDPR

Stelling: Ik verhuis mijn zetel buiten de EU en moet niet meer voldoen aan de GDPR.

Niet correct!

Vanaf het moment dat uw onderneming diensten of producten aanbiedt aan de Europese markt (28 EU-lidstaten + Noorwegen, IJsland en Liechtenstein), moet deze voldoen aan de GDPR.

Bv: Amerikaanse webshop met prijzen in Euro.

Verplichtingen binnen de GDPR

Stelling: Voortaan moet ik bij iedere verwerking van persoonsgegevens de toestemming van de betrokkene vragen.

Niet correct! Toestemming is maar één van de zes rechtvaardigingsgronden.

Er zijn nog:

- Uitvoering van de overeenkomst
- Wettelijke verplichting
- Vitaal belang
- Algemeen belang
- Gerechtvaardigd belang

Verplichtingen binnen de GDPR

Het gebruik van toestemming als rechtvaardigingsgrond moet zelfs zoveel als mogelijk vermeden worden omdat het op elk moment kan worden ingetrokken.

Voorbeeld: werknemer

Er bestaat zelfs betwisting binnen rechtspraak en –leer of een arbeider een toestemming op een vrije manier kan geven.

Beter hier is: uitvoering van de overeenkomst of wettelijke verplichting

Voornaamste verplichte documenten

- Klanten:
  - Privacy-policy
  - Update algemene voorwaarden

- Website:
  - Privacy-policy (contactformulier)
  - Cookie-policy
    - Facebook of LinkedIn plugin
    - Google Analytics: tracking IP
    - Google Adwords (Product Shopping ad)
    - Heatmaps (Hotjar)

Voornaamste verplichte documenten

- Leveranciers:
  - Voldoet mijn leverancier aan de GDPR (verantwoordelijk)?
  - Verwerkingsovereenkomst
  - Schadebeperkingsclausules?
- Personeel:
  - Update van de arbeidsovereenkomst
- Bijhouden van een verwerkingsregister

Stelling: De GDPR-verordening is weer zo'n wetgeving die binnen een paar maanden in onbruik zal geraakt zijn.

Fout. De GDPR-verordening is de meest gelobbyde wetgeving in de geschiedenis van de EU, met meer dan 3,000 amendementen en vier jaar onderhandelingen.

→ De EU hecht hier zeer veel belang aan.

Heb ik een DPO nodig?

Data Protection Officer

- Houdt toezicht op de naleving
- Verleent bijstand en advies
- Vergemakkelijkt het proces om GDPR compliant te worden

Is niet voor elk bedrijf verplicht, maar meestal wel aan te raden.

Heb ik een DPO nodig?

Verplicht voor:

- Openbare overheden
- Ondernemingen die hoofdzakelijk belast zijn met:
    - regelmatige en op grote schaal, stelselmatige observatie van natuurlijke personen

    Of

    - verwerking van bijzondere categorieën van gegevens of strafrechtelijke feiten

Heb ik een DPO nodig?

De GDPR blijft vaag over deze voorwaarden.
Spreekt zich enkel uit over uitersten.

Heeft zeker **wel** een DPO nodig:
- Ziekenhuis
- Verzekeringsfirma of bank
- Sociaal bureau

Heeft zeker **geen** DPO nodig:
- Individuele arts
- Individuele advocaat

Wachten op rechtspraak

Heb ik een DPO nodig?

Het aanstellen van een interne DPO is niet altijd een evidentie.

- Mag geen instructies krijgen i.v.m. zijn taken als DPO
- Moet autonoom kunnen beslissen
- Mag niet ontslagen worden omwille van de uitvoering van zijn taken
- Legt enkel verantwoording af ten aanzien van de directie

Heb ik een DPO nodig?

Mogen **niet** aangesteld worden als interne DPO

- Directieposten
- Sales-verantwoordelijke
- Marketing-verantwoordelijke
- IT-verantwoordelijke
- HR-verantwoordelijke

Waarom is er nu zoveel te doen omtrent de GDPR?

Toegegeven, de meeste rechten die de GDPR – AVG met zich meebrengt, zijn niet nieuw en waren vroeger al geïmplementeerd via wetgeving of rechtspraak.

- De Belgische Privacywet van 08.12.1992 (*B.S.* 18.03.1993)
- De Europese Privacyrichtlijn van 24.10.1995 (95/46/EG)
- De Europese e-Privacyrichtlijn van 12.07.2002 (2002/58/EG)
- De Telecommunicatiewet van 13.06.2005 (*B.S.* 20.06.2005)
- Het Wetboek Economisch Recht
- De Belgische Camerawet van 21.03.2007
- Arbeidswetgeving en privacygerelateerde Cao's (cao nr. 38, 39, 68, 81 en 89)

Waarom is er nu zoveel te doen omtrent de GDPR?

De handhaving van deze rechten, was echter problematisch aangezien er **geen sancties** aan verbonden waren.

De GDPR – AVG brengt daar verandering in met een gans scala aan sancties en maatregelen:

- Zware sancties die oplopen tot **20.000.000 € of 4% van de wereldwijde omzet**
- Omkering bewijslast
- Mogelijkheid tot het instellen van collectieve vorderingen
- Krachtdadige toezichthoudende overheidsinstanties per lidstaat
- Accountability – Verantwoordingsplicht

Moet ik wakker liggen van de sancties?

Neen

- Er zal eerst gekeken worden naar de grote spelers
- Maar, dit wil niet zeggen dat men mag blijven stilzitten

Ja

- Bij klachten zal men toch controleren en desnoods bestraffen

Vragen ?

ADVOCAAT
NICOLAS VANSPEYBROUCK