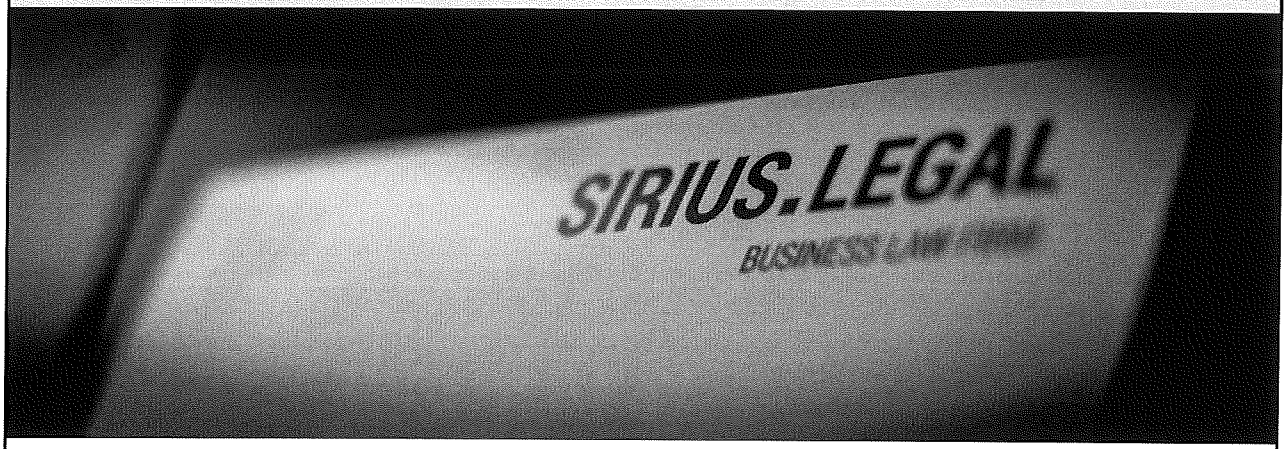
Sirius Legal

GDPR workshop

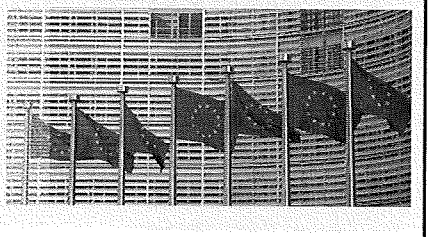
Logeren in Vlaanderen



SIRIUS.LEGAL
BUSINESS LAW FIRM

Inhoud van vandaag…

- Context nieuwe Verordening en wettelijk kader
- Op die is de GDPR van toepassing?
- Basisprincipes GDPR
- Wat moet er nu concreet gebeuren?
- Potentiële risico's bij niet-naleving
- Als u iets moet onthouden vandaag…
- Vragen



SIRIUS.LEGAL
BUSINESS LAW FIRM

We leven in een digitale wereld…

Basis van alles wat online gebeurd is data

Collect all you can now – figure out what to do with it later
Profiling
Maximale tracking
Location based
Trigger based
Internet of things

Data is in veel gevallen een betaalmiddel geworden online…
(cfr. Proposal Directive 2015/0287)

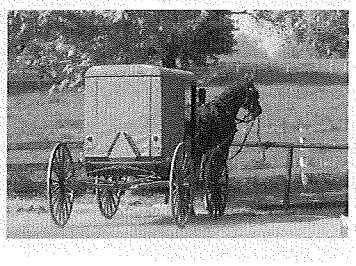
SIRIUS.LEGAL
BUSINESS LAW FIRM

Huidig wetgevend kader

De Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (Op basis van Richtlijn 95/46/EG - Boek XII WER)

Andere tijden…

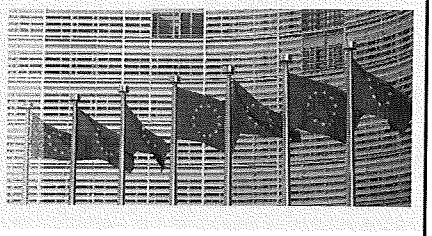
- Geen online marketing
- Geen "profiling"
- Geen "cookies"
- Geen "tracking"
- Geen "location based marketing"
- Geen "trigger based marketing"
- Geen e-commerce
- Geen social media
- Minder dan 1% van de EU-bevolking gebruikte internet in 1995…



SIRIUS.LEGAL
BUSINESS LAW FIRM

Nieuwe privacywetgeving komt eraan…

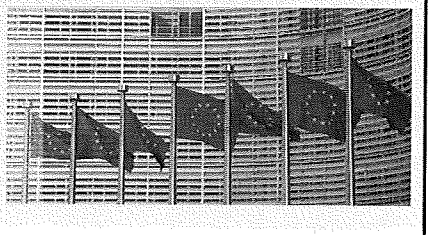
- General Data Protection Regulation 2016/679 (GDPR/AVGB) <-> Richtlijn
- 1 verordening voor 28 LS
- Inwerkingtreding op 25 mei 2018 (zonder overgangsperiode !)
- Nieuwe regels zijn VEEL strenger dan de bestaande wetgeving en hebben een impact op IEDEREEN



SIRIUS.LEGAL
BUSINESS LAW FIRM

Nieuwe privacywetgeving komt eraan…

- Oude principes verder uitgediept
- Nieuwe rechten en verplichtingen
- Verantwoording van verantwoordelijken
- Hogere sancties (!)
- Drempelverlaging voor betrokkenen
- Hervorming Privacycommissies

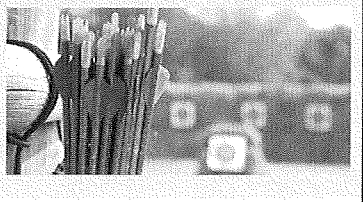


SIRIUS.LEGAL
BUSINESS LAW FIRM

Op wie is de GDPR van toepassing?

- IEDEREEN die persoonsgegevens verwerkt
- Persoonsgegevens= alle info die toelaat om een persoon te identificeren, direct of indirect, nu of in de toekomst, alleen of met de hulp van derde partijen

Vb. naam, voornaam, geboortedatum, persoonlijke voorkeuren, "likes", allergieën,…



- Wat zijn géén persoonsgegevens ? anonieme data, tellingen, statistieken, vennootschappen, overledenen,…

SIRIUS.LEGAL
BUSINESS LAW FIRM

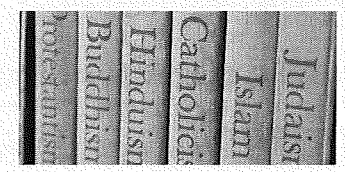
Op wie is de GDPR van toepassing?

Opgelet: er zijn een aantal bijzondere categorieën persoonsgegevens

ras, etnie, religie, seksuele oriëntatie, politieke voorkeuren, lidmaatschap vakbonden, medische, genetische en biometrische gegevens

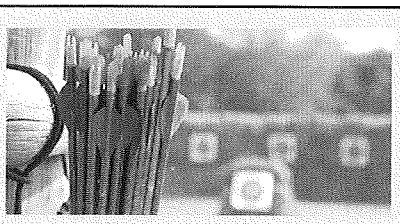
Uitzonderlijk verwerking toegestaan, onder meer indien:
- toestemming, of
- sociale rechten, rechtsvorderingen, of
- betrokken verenigingen, stichtingen en organisaties.

Extra maatregelen vereist!



SIRIUS.LEGAL
BUSINESS LAW FIRM

Op wie is de GDPR van toepassing?



⇒ **Waar zitten persoonsgegevens in uw onderneming?**

Klantendatabase, boekhouding, kast met fysieke dossiers?, mailbox, mailchimp-account, Dropbox, Google Drive, harde schijf van pc?,…

SIRIUS.LEGAL
BUSINESS LAW FIRM

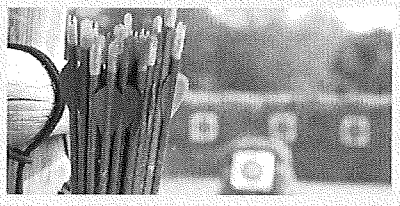
Op wie of wanneer is de GDPR van toepassing?

- "Verwerking" van persoonsgegevens

  = *"elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens"*

- Zeer ruime definitie!

- Uitzonderingen:
  - persoonlijke, huishoudelijke doeleinden
  - Journalistieke, artistieke en literaire doeleinden
  - wetenschap, historiek en statistiek



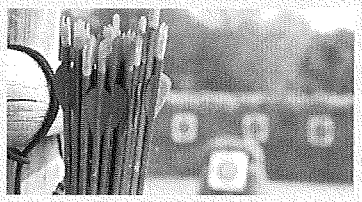
SIRIUS.LEGAL
BUSINESS LAW FIRM

Op wie of wanneer is de GDPR van toepassing?

"**verwerker**" en "**verantwoordelijke voor de verwerking**"

Verwerker: voert verwerking uit IN OPDRACHT VAN verantwoordelijke voor de verwerking

Verantwoordelijke voor de verwerking: bepaalt het DOEL en de MIDDELEN voor de verwerking



⇒ Soms verenigd in dezelfde persoon/onderneming
⇒ Bepaalt verantwoordelijkheden onder GDPR

SIRIUS.LEGAL
BUSINESS LAW FIRM

Basisprincipes GDPR

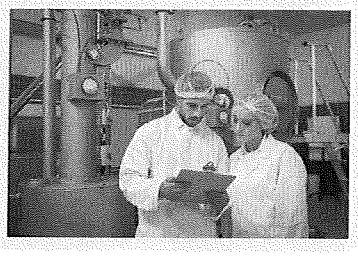
- Verantwoording
- Transparantie
- Data Protection by design / by default
- Doelbinding
- Data minimisation (noodzakelijkheid-evenredig)
- Accuraatheid
- Beperkte bewaartijd
- Data beveiliging

SIRIUS.LEGAL
BUSINESS LAW FIRM

Wat moet er concreet gebeuren?

1. **Ga na wie onderaannemers zijn die persoonsgegevens verwerken** ***(lees: toegang hebben tot…")*** **+ contractcheck**

- Wie?
- Waarom? Verplichting om enkel samen te werken met onderaannemers die garantie kunnen geven op vlak van beveiliging + geschreven ovk
- Hoe? Oplijsten onderaannemers + nazicht/voorzien contract

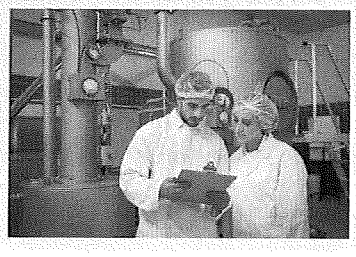


SIRIUS.LEGAL
BUSINESS LAW FIRM

Wat moet er concreet gebeuren?

2. Opmaak verwerkingsregister

- Wie?
- Waarom? In kaart brengen datastromen + nazicht rechtsgronden en basisprincipes verwerking
- Hoe? Oplijsten in excell



SIRIUS.LEGAL
BUSINESS LAW FIRM

Wat moet er concreet gebeuren?

2. Opmaak verwerkingsregister

- Hoe? Oplijsten in excell

Op basis van volgende vragen:

Wat? (Welke PG, type persoonsgegevens, rechtsgrond)
Waarom? (Reden van de verwerking, wie is verantwoordelijke voor de verwerking?)
Wiens PG en van wie? (Wie is de betrokkene, PG verkregen van betrokkene zelf of via derde)
Wanneer/hoe lang/van wie? (wanneer verzameld, wanneer geüpdated, hoe lang bewaard)
Waar? (Waar verwerkt, waar bewaard, beveiliging, doorgite buiten EU)

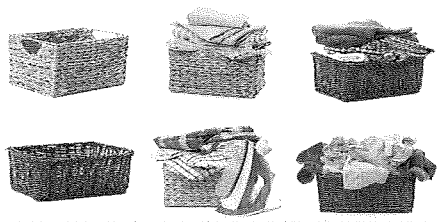
SIRIUS.LEGAL
BUSINESS LAW FIRM

Wat moet er concreet gebeuren?

2. Opmaak verwerkingsregister

- Rechtsgronden voor de verwerking?

1. Toestemming
2. Uitvoering of sluiten van overeenkomst
3. Wettelijke verplichting
4. Vitaal belang
5. Openbaar belang
6. Gerechtvaardigd belang



SIRIUS.LEGAL
BUSINESS LAW FIRM

Wat moet er concreet gebeuren?

2. Opmaak verwerkingsregister

- Rechtsgronden voor de verwerking?

⇒ Opletten met verwerking PG minderjarigen (!)

⇒ Vereist expliciete toestemming ouders + *"reasonable efforts"* om dit te controleren

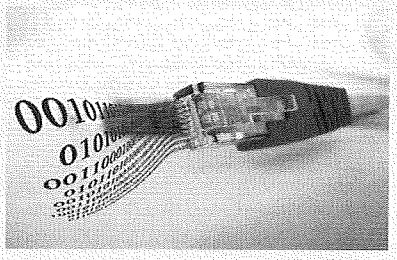
SIRIUS.LEGAL
BUSINESS LAW FIRM

Wat moet er concreet gebeuren?

2. Opmaak verwerkingsregister

- Opletten met doorgifte van persoonsgegevens (!)

✓ Enkel indien noodzakelijk voor doeleinde, verenigbaar met oorspronkelijke verwerking en kennisgeving betrokkene
✓ Binnen EU: vrij verkeer
✓ Buiten EU: "witte lijst", adequaatheid, "binding corporate rules", "model clauses"



SIRIUS.LEGAL
BUSINESS LAW FIRM

Wat moet er concreet gebeuren?

3. Opmaak nulmeting / verslag

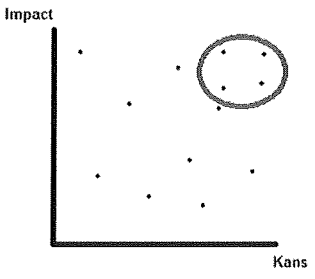
- Wie?
- Waarom? Accountability / verantwoording
- Hoe? Aan de hand van register voor de verwerking
  - ✓ Wie heeft toegang?
  - ✓ Waar worden data opgeslagen en verwerkt?
  - ✓ Hoe worden data toegankelijk gemaakt?
  - ✓ Aan wie worden data doorgegeven?
  - ✓ Is alles technisch en juridisch goed afgedekt?
  - ✓ Wat is de rechtsgrond? Toestemming gegeven + bewijs?

SIRIUS.LEGAL
BUSINESS LAW FIRM

Wat moet er concreet gebeuren?

3. Opmaak nulmeting / verslag

- Hoe? Aan de hand van register voor de verwerking
  - ✓ Wie heeft toegang?
  - ✓ Waar worden data opgeslagen en verwerkt?
  - ✓ Aan wie worden data doorgegeven?
  - ✓ Is alles technisch en juridisch goed afgedekt?
  - ✓ Wat is de rechtsgrond? Toestemming gegeven?
  - ✓ Is website/database beveiligd met paswoord,…?
  - ✓ Welke zijn potentiële risico's?



=> Inschatting risico's
⇒ Actiepunten + plan van aanpak + timing ?
⇒ MAXIMAAL documenteren!

SIRIUS.LEGAL
BUSINESS LAW FIRM

Wat moet er concreet gebeuren?

4. Technische én organisatorische beveiligingsmaatregelen

- Wie?
- Waarom? Databeveiliging, basisprincipe verwerking van persoonsgegevens
- Hoe? Beveiliging a.h.v. paswoorden, kasten/deuren afsluiten, sleutelbeheer, screensaver, firewall,...

SIRIUS.LEGAL
BUSINESS LAW FIRM

Wat moet er concreet gebeuren?

5. Informatieverplichtingen + rechten betrokkene garanderen

- Wie?
- Waarom? Transparantie, info moet worden gegeven vóór verwerking
- Hoe? Opmaak/aanpassing privacy policy

SIRIUS.LEGAL
BUSINESS LAW FIRM

Wat moet er concreet gebeuren?

5. Informatieverplichtingen + rechten betrokkene garanderen

- Hoe? Opmaak/aanpassing privacy policy

Wat: persoonsgegevens
Waarom: doelstellingen
Wie: verantwoordelijke (naam en adres)
verwerkers
Rechten & uitoefening (waar en hoe)
Andere: direct marketing, doorgifte,...

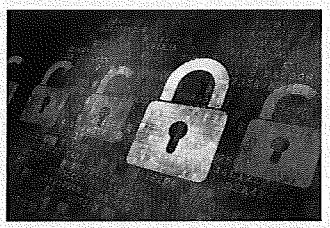
SIRIUS.LEGAL
BUSINESS LAW FIRM

Wat moet er concreet gebeuren?

5. Informatieverplichtingen + rechten betrokkene garanderen

- Hoe? Opmaak/aanpassing privacy policy + garanderen rechten betrokkene

- ✓ Recht op informatie
- ✓ Recht op toegang tot persoonsgegevens: antwoord binnen 45 dagen
- ✓ Recht op verbetering: antwoord binnen 1 maand
- ✓ Recht op verzet: indien 'ernstige en gerechtvaardige redenen';
  steeds en kosteloos i.g.v. direct marketing (o.a. reclame)
- ✓ Recht om vergeten te worden
- ✓ Recht om zich te verzetten tegen profiling + automatische beslissingsname
- ✓ Recht op gegevensoverdraagbaarheid
- ✓ Recht op beperking van de verwerking



SIRIUS.LEGAL
BUSINESS LAW FIRM

Wat moet er concreet gebeuren?

6. Data protection impact assessment

- Wie?
- Waarom? Ook na 25 mei 2018 compliant blijven (!)
- Hoe? Analyse verwerkingsactiviteit op basis van 4 vragen:

✓ Heb ik een rechtsgrond voor de verwerking? (contract, toestemming, wet, gerechtvaardigd belang, publiek belang, vitaal belang)
✓ Heb ik de betrokkene correct geïnformeerd?
✓ Zit de data veilig bij mij?
✓ Is de verwerking die ik wil uitvoeren "proportioneel"? (doelgebonden, dataminimalisatie, niet langer bewaren dan nodig)

SIRIUS.LEGAL
BUSINESS LAW FIRM

Wat moet er concreet gebeuren?

6. Data protection impact assessment

- Wie?
- Waarom? Ook na 25 mei 2018 compliant blijven
- Hoe? Analyse verwerkingsactiviteit op basis van 4 vragen

⇒ Hoog risico? Passende maatregelen / advies Privacy commissie

Bv. nieuwe technologieën, gevoelige data, draadloos en online

SIRIUS.LEGAL
BUSINESS LAW FIRM

Wat moet er concreet gebeuren?

7. Data breach procedure voorzien

- Wie?
- Waarom? Verplichting voor verantwoordelijke voor verwerking om Priv Comm te informeren binnen 72uur
- Hoe? Garanties vragen aan onderaannemers, opstellen van "draaiboek" met verantwoordelijkheden (indien personeel aanwezig)

SIRIUS.LEGAL
BUSINESS LAW FIRM

Wat moet er concreet gebeuren?

8. Onderzoek aanstelling Data Protection Officer

- Wie?
- Waarom? In bepaalde gevallen verplichting om DPO aan te stellen:
  - ✓ Verwerking door overheidsorgaan
  - ✓ Hoofzakelijk belast met verwerking die "systematische en stelselmatige observatie op grote schaal" vereist
  - ✓ "Grootschalige verwerking" van gevoelige gegevens
- Hoe? Onderzoek in verslag/audit opnemen => accountability (!)

SIRIUS.LEGAL
BUSINESS LAW FIRM

Wat moet er concreet gebeuren?

8. Onderzoek aanstelling Data Protection Officer

- Rol/taken DPO?
  - ✓ Informeren & adviseren ("tijdig betrekken")
  - ✓ Toezien op nalevering Verordening
  - ✓ Advies verstrekken m.b.t. DPIA en audit
  - ✓ Samenwerken met Privacy commissie (vb. i.k.v. data breach, klachten)
  - ✓ Intern/extern? Belang van aansprakelijkheid

SIRIUS.LEGAL
BUSINESS LAW FIRM

Wat moet er concreet gebeuren?

9. Nazicht verzekeringen

Als maatregel voor risicobeheersing

10. "Regulariseren" bestaande database

Onderscheid maken o.b.v.: regelmatige/eenmalige klanten, reageren (of openen) nieuwsbrief, schrijven zich in voor een wedstrijd,...

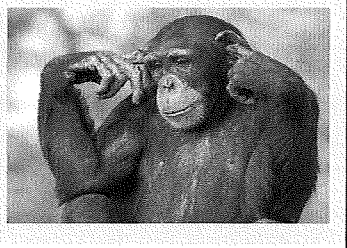
11. Vorming/voorlichting personeel

Als maatregel voor risicobeheersing

SIRIUS.LEGAL
BUSINESS LAW FIRM

Potentiële risico's bij niet naleving

- ✓ Op basis van GDPR: boetes tot 4% van de jaarlijkse wereldwijze omzet of tot 20 mio EUR
- ✓ Op basis van algemene wetgeving: aansprakelijkheid bij fout, schadevergoeding, geen tussenkomst verzekering,...
- ✓ In elk geval: imagoschade, verlies aan klanten/leden,...
- ✓ Potentieel geen dekking verzekering indien wet niet nageleefd



SIRIUS.LEGAL
BUSINESS LAW FIRM

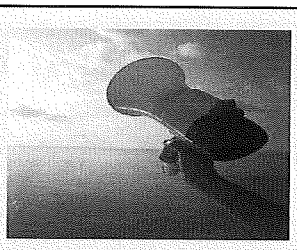
Als u iets moet onthouden vandaag...

⇒ **4 basisvragen** bij verwerking van persoonsgegevens:

1. Heb ik een rechtsgrond voor de verwerking? (contract, toestemming, wet, gerechtvaardigd belang, publiek belang, vitaal belang)
2. Heb ik de betrokkene correct geïnformeerd?
3. Zit de data veilig bij mij?
4. Is de verwerking die ik wil uitvoeren "proportioneel"? (doelgebonden, dataminimalisatie, niet langer bewaren dan nodig)

SIRIUS.LEGAL
BUSINESS LAW FIRM

Vragen



- Mag de politiefiche zomaar doorgemaild en bijgehouden worden?
- Mogen er nog foto's getrokken worden van de gasten die nadien op Facebook verschijnen?
- Bij groepen die logeren worden op voorhand alle gegevens opgevraagd voor de check-in a.d.h.v. een formulier via mail. Hoe mag dit bijgehouden worden?
- Een gast die boekt geeft zijn e-mailadres door bij boeking. Mag die persoon nadien zomaar opgenomen worden in het mailbestand voor nieuwsbrieven?

SIRIUS.LEGAL
BUSINESS LAW FIRM

Vragen

- Wat met de kredietkaartgegevens die je op voorhand opvraagt voor de waarborg?
- Welke vermelding moet er op de website komen bij het contactformulier, inschrijving nieuwsbrief,…?
- Hoe mogen de allergenengegevens van de gasten bijgehouden worden? De uitbater houdt ze nu bij in haar hotelmanagementsysteem.
- …?

SIRIUS.LEGAL
BUSINESS LAW FIRM

Sirius Legal

Media & advertisement law
IP law
Internet & e-commerce
Privacy & cookies
Gambling law
Travel & consumer protection
Commercial & contracts
Corporate - tax - labour - immo

freekje@siriuslegal.be

www.siriuslegal.be

SIRIUS.LEGAL
BUSINESS LAW FIRM