14:00 – 15u15

LEZING

Meester in cyberveiligheid

Een juridische blik

26/04/24

/OVBCONGRES
DE MAGIE V/H RECHT
ELISABETH CENTER
ANTWERPEN

Antoon Dierick specialiseert zich voornamelijk in de juridische aspecten van de informatiemaatschappij.

Hij werkte als advocaat tot 2017. Daarna werkte hij drie jaar als Chief Legal Officer in een internationaal IT-bedrijf.

Sinds 1 januari 2020 is hij opnieuw actief als vennoot bij MDP Advocaten.

Hij adviseert cliënten omtrent een brede waaier aan IT- en data-gerelateerde zaken, (online) consumenten- en ondernemingsrecht.

1. Poging tot definitie

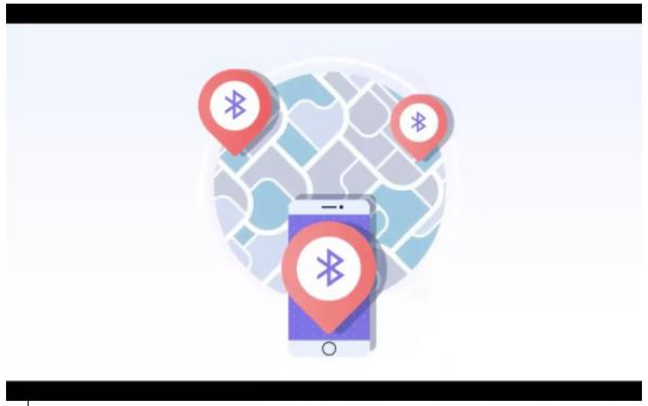
- Cyberveiligheid verwijst naar het **beschermen** van computersystemen, netwerken, en gegevens **tegen ongeautoriseerde toegang, aanvallen of schade**.

- Voorbeelden:
  - Voorkomen van datalekken
  - Voorkomen van diefstal van persoonlijke of gevoelige informatie
  - Tegengaan van cybercriminaliteit zoals phishing, malware, en ransomware

- Belang voor advocatenkantoren

Contact tracing

Datalek gevonden in een van de mogelijke corona-apps



Screenshot uit het promofilmpje van Covid-19 Alert, een verzameling ontwikkelaars die een app maakten om de verspreiding van het coronavirus tegen te gaan. Beeld

Beste klant,

60% van de cyberaanvallen op bedrijven is in België **gericht op KMO's**. Met tal van risico's: diefstal van je accountgegevens, geld, bedrijfsdata, blokkering van je bedrijf, enzovoort. En dat kan veel kosten! Bij een **ransomware-aanval** betalen bedrijven gemiddeld €10.000, en het "record" ligt op **€496.000**.

Fraude & veiligheid

Meer CEO-fraude in tijden van corona

Belgische bedrijven bij de slachtoffers van 'grootste hack in tien jaar'

Microsoft zegt ook Belgische klanten te hebben die het slachtoffer werden van de grootschalige hack van SolarWinds, een ontwikkelaar van software om netwerken en servers te beheren. De Amerikaanse nationale veiligheidsadviseur Robert O'Brien keerde vanuit Europa

26/04/24

DE MAGIE V/H RECHT
ELISABETH CENTER
ANTWERPEN

2. Wettelijke bepalingen

- Algemene vaststelling:
  - geen algemeen kader inzake informatieveiligheid
  - wel diverse specifieke wettelijke bepalingen

2. Wettelijke bepalingen

- Strafrechtelijk gesanctioneerde gedragingen inzake informatie:
  - Art. 309 Sw: Hij die geheimen van de fabriek waarin hij werkzaam geweest is of nog is, kwaadwillig of bedrieglijk aan anderen meedeelt, wordt gestraft met gevangenisstraf van drie maanden tot drie jaar en met geldboete van vijftig euro tot tweeduizend euro. (medewerkers)
  - Art. 458 Sw: Geneesheren, heelkundigen, officieren van gezondheid, apothekers, vroedvrouwen en alle andere personen die uit hoofde van hun staat of beroep kennis dragen van geheimen die hun zijn toevertrouwd, en deze bekendmaken buiten het geval dat zij geroepen worden om in recht of voor een parlementaire onderzoekscommissie getuigenis af te leggen en buiten het geval dat de wet, het decreet of de ordonnantie hen verplicht of toelaat die geheimen bekend te maken, worden gestraft met gevangenisstraf van een jaar tot drie jaar en een geldboete van honderd euro tot duizend euro of met een van die straffen alleen. (beroepsgeheim)

67. Een verwerking van persoonsgegevens is immers slechts rechtmatig indien daartoe een rechtsgrond bestaat. De Geschillenkamer kan niet anders dan vaststellen dat er geen enkele rechtsgrond zoals bepaald in artikel 6.1. AVG de doorzending van de e-mail door verweerder 2 aan zijn raadsman rechtvaardigt.

plaatsvinden, dewelke zijn gedekt door het beroepsgeheim. De Geschillenkamer erkent uiteraard het principe dat een cliënt aan zijn advocaat vertrouwelijke mededelingen moet kunnen doen, maar dit kan, in de mate dat het persoonsgegevens betreft, enkel op voorwaarde dat die persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig is (artikel 5.1 a) AVG en artikel 6.1. AVG). Nu blijkt echter in voorliggend geval dat de doorzending aan de raadsman van verweerder 2 plaatsvond met miskenning van het rechtmatigheidsbeginsel bij gebrek aan ook maar enige rechtsgrond zoals bepaald in artikel 6.1. AVG.

2. Wettelijke bepalingen

- Strafrechtelijk gesanctioneerde gedragingen inzake informatie:
  - Titel IXbis. Misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en van de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen (artikels 550bis-550ter)
  - Diverse bepalingen, bijvoorbeeld
    - art. 193 Sw: "*Valsheid in geschriften, **in informatica** of in telegrammen, met bedrieglijk opzet of met het oogmerk om te schaden, wordt gestraft overeenkomstig de volgende artikelen.*"
    - Art. 210bis Sw: aanpassen van elektronische gegevens met impact op de juridische draagwijdte (valsheid in informatica)
    - Art. 504quater Sw (informaticabedrog)
  - Sancties voorzien in WER

2. Wettelijke bepalingen

- **Wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid**
  - Omzetting NIS-richtlijn 2016/1148 (*die wordt ingetrokken*)
  - Aanbieders van essentiële diensten
  - De aanbieder van essentiële diensten neemt passende en evenredige technische en organisatorische maatregelen om de risico's voor de beveiliging van netwerk- en informatiesystemen waarvan zijn essentiële diensten afhankelijk zijn, te beheersen.
  - Regels specifiek voor digitaledienstverleners

2. Wettelijke bepalingen

- **Wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid**
  - NIS 2: Richtlijn 2022/2555
  - Ruimer toepassingsgebied (essentiële en belangrijke entiteiten)
  - Meer gedetailleerde verplichtingen
  - Sancties tot 10mio/2% (essentiële entiteit) of 7mio/1,4% (belangrijke entiteit)
  - Omzetting tegen 17 oktober 2024

2. Wettelijke bepalingen

- **Boek XI WER - Titel 8/1. Bedrijfsgeheimen**
  - Omzetting richtlijn 2016/943 van 8 juni 2016 betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan.
  - Verbod op onrechtmatige verkrijging (art. XI.332/4 §1 en §3)
  - Bepalingen over onrechtmatig gebruik (art. XI.332/4 §§2-4)
  - Praktijk

2. Wettelijke bepalingen

- **Verordening 2016/679 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (AVG)**
  - Verantwoordelijkheid van de verwerkingsverantwoordelijke (art. 24 AVG)
  - Gegevensbescherming door ontwerp en door standaardinstellingen (art. 25 AVG)
  - Verwerkersovereenkomst (art. 28 AVG)
  - Register van de verwerkingsactiviteiten (art. 30 AVG)
  - Beveiliging van de verwerking (art. 32 AVG)
  - Melding datalekken (art. 33 en 34 AVG)
  - Functionaris voor gegevensbescherming (art. 37 e.v. AVG)
  - Sanctieregeling

3. Proactieve aanpak

- **Maatregelen van technische / operationele aard**
  - Up to date houden van systemen
  - Controle op het gebruik van programma's en toestellen
  - Access management
  - Back-up van data
  - Antivirus: virusscans, firewall, wachtwoorden, enz.
  - Detectie
  - Bewijsgaring
  - Policies zoals BC en DR plannen
  - …

kunnen ingrijpen.

De Orde van Vlaamse Balies doet hieronder **enkele aanbevelingen** voor het beveiligingsbeleid en de minimale maatregelen voor verwerkingen door advocaten. Die aanbevelingen moeten worden aangepast en geëvalueerd in het licht van nieuwe richtlijnen en beslissingspraktijken van de toezichthoudende overheden, de Europese toezichthouder of de (inter)nationale rechtbanken.

U kunt met uw IT-leverancier of interne IT verantwoordelijke overlopen of, en op welke manier, u beveiligingsmaatregelen kunt implementeren, controleren en aanpassen rekening houdende met uw praktijk.

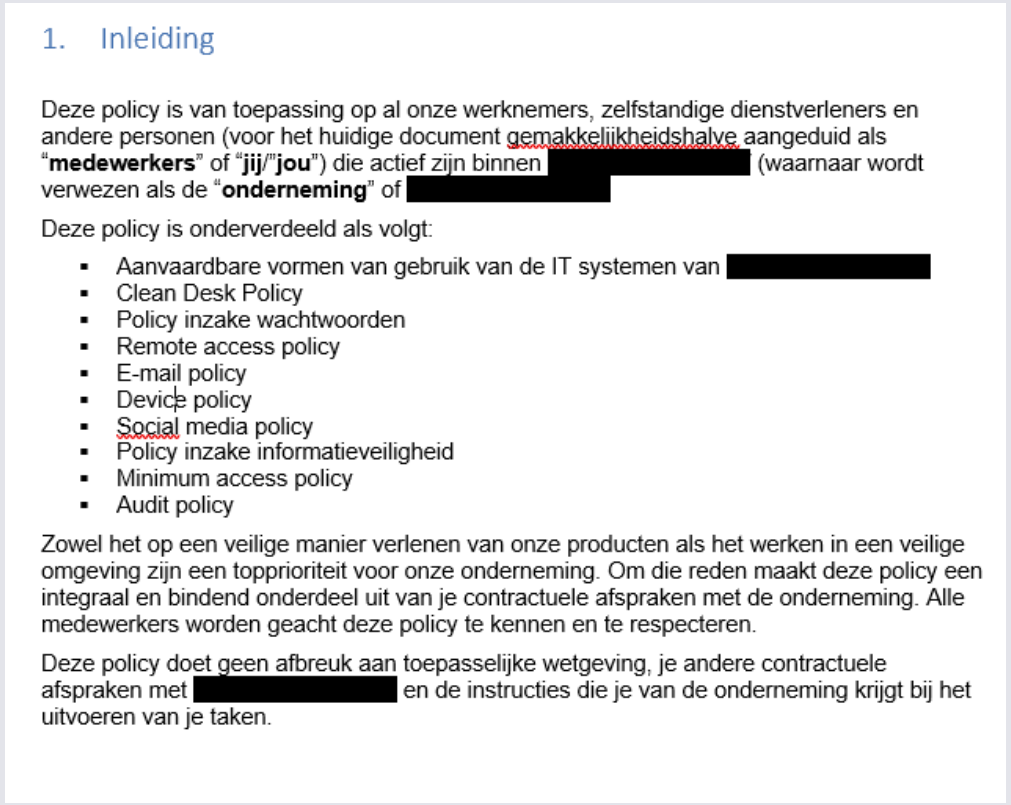
Digitale informatiesystemen

Elk digitaal informatiesysteem dat door u wordt gebruikt om persoonsgegevens te verwerken, moet aan de volgende vereisten voldoen:

1. De systemen maken enkel gebruik van software met een geldige licentie.
2. Indien de software pseudonimisering en/of versleuteling mogelijk maakt, moet u die functionaliteit gebruiken. U volgt de goede prakrijken op voor de regelgeving en richtlijnen rond de aankoop, beveiliging en updates van software en/of clouddiensten, met inbegrip van eventuele toekomstige normen of aanbevelingen die de Orde van Vlaamse Balies of de lokale Ordes publiceren.
3. De systemen worden beschermd door een adequate firewall en anti-virussoftware met ten minste de volgende functionaliteiten: het tegenhouden van virussen, spyware, ransomware en andere malware; het waarschuwen voor onveilige links en bijlagen in e-mail; en het scannen naar oorzaken die de performantie van computers verminderen.
4. De systemen kennen een passende wachtwoordbeveiliging, dat wil zeggen met een voldoende

3. Proactieve aanpak

- **Maatregelen ten aanzien van personeel / medewerkers**
  - Contractuele afspraken (AOK, …)
  - Policies informatieveiligheid
  - Deel aanpak GDPR compliance
  - Awareness
  - Functionaris



1. Inleiding

Deze policy is van toepassing op al onze werknemers, zelfstandige dienstverleners en andere personen (voor het huidige document gemakkelijkheidshalve aangeduid als "**medewerkers**" of "**jij**/"**jou**") die actief zijn binnen [redacted] (waarnaar wordt verwezen als de "**onderneming**" of [redacted]

Deze policy is onderverdeeld als volgt:

- Aanvaardbare vormen van gebruik van de IT systemen van [redacted]
- Clean Desk Policy
- Policy inzake wachtwoorden
- Remote access policy
- E-mail policy
- Device policy
- Social media policy
- Policy inzake informatieveiligheid
- Minimum access policy
- Audit policy

Zowel het op een veilige manier verlenen van onze producten als het werken in een veilige omgeving zijn een topprioriteit voor onze onderneming. Om die reden maakt deze policy een integraal en bindend onderdeel uit van je contractuele afspraken met de onderneming. Alle medewerkers worden geacht deze policy te kennen en te respecteren.

Deze policy doet geen afbreuk aan toepasselijke wetgeving, je andere contractuele afspraken met [redacted] en de instructies die je van de onderneming krijgt bij het uitvoeren van je taken.

3. Proactieve aanpak

- **Contractuele maatregelen**
  - IT-dienstverleningscontracten
  - Leveranciersovereenkomsten
  - Verwerkersovereenkomsten

4.3 Your Security and Backup. You are responsible for properly configuring and using the Service Offerings and otherwise taking appropriate action to secure, protect and backup your accounts and Your Content in a manner that will provide appropriate security and protection, which might include use of encryption to protect Your Content from unauthorized access and routinely archiving Your Content.

Beveiliging van persoonsgegevens binnen de organisatie:

Voeg alle bewijsstukken die u wilt gebruiken voor het staven van uw antwoorden toe aan dit formulier. Verwijs hier ook naar bij het beantwoorden van de vragen hieronder.

1. Beschikt uw organisatie over een risicobeoordelingsproces dat rekening houdt met de informatieveiligheid en de bescherming van persoonsgegevens?	
☐	Ja. Verklaar uw antwoord: ....
☐	Nee. Verklaar uw antwoord: ....

2. Voert uw organisatie met geplande tussenpozen risicobeoordelingen uit?	
☐	Ja. Verklaar uw antwoord: ....
☐	Nee. Verklaar uw antwoord: ....

3. Beschikt uw organisatie over een schriftelijk, door het hoger management goedgekeurd informatieveiligheidsbeleid? Omvat dit de bescherming van persoonsgegevens?	
☐	Ja. Verklaar uw antwoord: ....
☐	Nee. Verklaar uw antwoord: ....

4. Wordt dit beleid en bijhorende procedures regelmatig herzien en geactualiseerd?	
☐	Ja. Verklaar uw antwoord: ....
☐	Nee. Verklaar uw antwoord: ....

5. Zijn alle medewerkers die in contact komen met persoonsgegevens, op de hoogte van hun plichten en verantwoordelijkheden rond informatieveiligheid en in het bijzonder de bescherming van persoonsgegevens en de vertrouwelijkheidsplicht?	
☐	Ja. Verklaar uw antwoord: ....
☐	Nee. Verklaar uw antwoord: ....

6. Als u werkt met derden (bv. uitzendkrachten, consultants, onderaannemingen, diensten- of productleveranciers) worden de informatieveiligheidsvereisten (bv. vertrouwelijkheid, geheimhoudingverklaring) opgenomen in de arbeids- of leveranciersovereenkomsten?	
☐	Ja. Verklaar uw antwoord: ....
☐	Nee. Verklaar uw antwoord: ....

7. Heeft uw organisatie veiligheidsmaatregelen genomen om zowel niet-gemachtigde als onnodige fysieke toegang tot persoonsgegevens te voorkomen?	
☐	Ja. Verklaar uw antwoord: ....
☐	Nee. Verklaar uw antwoord: ....

8. Beschikt uw organisatie over verschillende dragers (b.v. server, PC, externe disk, USB, fileshares) met persoonsgegevens?	
☐	Ja. Verklaar uw antwoord: (zijn deze dragers geïdentificeerd?) ....
☐	Nee. Verklaar uw antwoord: ....

9. Is de toegang tot de informatiesystemen van uw organisatie zodanig beveiligd dat alleen bevoegde personen de persoonsgegevens kunnen raadplegen of bewerken?	
☐	Ja. Verklaar uw antwoord: ....
☐	Nee. Verklaar uw antwoord: ....

Bedankt voor uw aandacht!