



**CRANIUM**

# Oei, een datalek...

## Wat nu?

**Bavo Van den Heuvel**

Chief Knowledge Officer & Founder of  
CRANIUM

Alle foto's en tekst copyright door Bavo Van den Heuvel voor CRANIUM tenzij anders vermeld



# Agenda

1. Wat is een datalek?
2. Het toepassingsgebied
3. De risicoanalyse
4. Beleid en procedures
5. Stappenplan
6. Post Mortem: leren van je incidenten



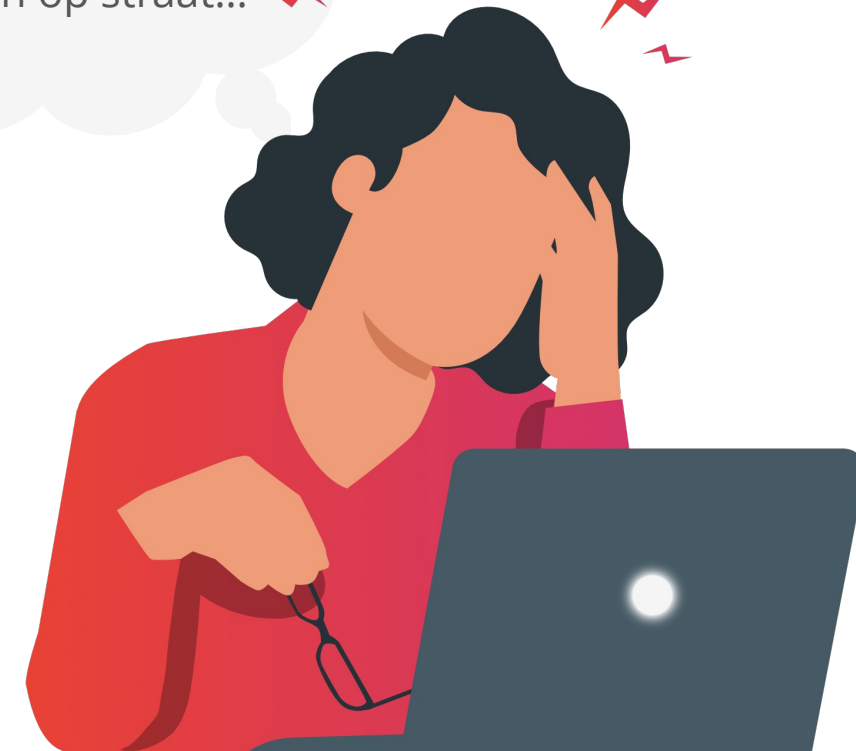
# 1. Definitie: Wat is een datalek?

= een inbreuk in verband met persoonsgegevens:  
een **inbreuk op de beveiliging** die **per ongeluk of op onrechtmatige wijze** leidt tot

- de **vernietiging**,
- het **verlies**,
- de **wijziging**
- of de **ongeoorloofde verstrekking** van
- of de **ongeoorloofde toegang** tot **doorgezonden, opgeslagen** of anderszins **verwerkte** gegevens;

= meer dan:

Oei, onze  
persoonsgegevens  
liggen op straat...



# 1. Definitie: Wat is een datalek?

## Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679

<b>I. MELDING VAN INBREUKEN IN VERBAND MET PERSOONSGEGEVENS KRACHTENS DE AVG</b> .....	<b>6</b>
A. BASISBESCHOUWINGEN INZAKE VEILIGHEID.....	6
B. WAT IS EEN INBREUK IN VERBAND MET PERSOONSGEGEVENS? .....	7
1. Definitie .....	7
2. Soorten inbreuken in verband met persoonsgegevens .....	8
3. De mogelijke gevolgen van een inbreuk in verband met persoonsgegevens.....	10
<b>II. ARTIKEL 33 - MELDING AAN DE TOEZICHTHOUDENDE AUTORITEIT</b> .....	<b>11</b>
A. WANNEER MELDEN .....	11
1. Vereisten van artikel 33.....	11
2. Wanneer heeft een verwerkingsverantwoordelijke er "kennis" van gekregen? .....	11
3. Gezamenlijke verwerkingsverantwoordelijken.....	15
4. Verplichtingen van de verwerker .....	15
B. VERSTREKKING VAN INFORMATIE AAN DE TOEZICHTHOUDENDE AUTORITEIT .....	16
1. Te verstrekken informatie .....	16
2. Melding in stappen.....	17
3. Melding met vertraging.....	18
C. GRENDOVERSCHRIJDENDE INBREUKEN EN INBREUKEN BIJ VESTIGINGEN BUITEN DE EU .....	19
1. Grensoverschrijdende inbreuken.....	19
2. Inbreuken bij vestigingen buiten de EU.....	20
D. VOORWAARDEN WAARONDER GEEN MELDING VEREIST IS .....	21
<b>III. ARTIKEL 34 – MEDEDELING AAN DE BETROKKENE</b> .....	<b>22</b>
A. PERSONEN IN KENNIS STELLEN.....	22
B. TE VERSTREKKEN INFORMATIE.....	23
C. CONTACT OPNEMEN MET PERSONEN .....	24
D. VOORWAARDEN WAARONDER GEEN MEDEDELING VEREIST IS .....	25
<b>IV. BEOORDELING VAN HET RISICO EN HOOG RISICO</b> .....	<b>26</b>
A. RISICO ALS AANLEIDING VOOR MELDINGEN/MEDEDELINGEN .....	26
B. FACTOREN WAARMEE REKENING MOET WORDEN GEHOUDEN BIJ DE BEOORDELING VAN RISICO'S.....	27
<b>V. VERANTWOORDINGSPLICHT EN REGISTRATIE</b> .....	<b>30</b>
A. INBREUKEN DOCUMENTEREN .....	30
B. ROL VAN DE FUNCTIONARIS VOOR GEGEVENSBESCHERMING.....	32
<b>VI. KENNISGEVINGSVERPLICHTINGEN OP GROND VAN ANDERE RECHTSINSTRUMENTEN</b> .....	<b>32</b>
<b>VII. BIJLAGE</b> .....	<b>35</b>
A. STROOMSCHEMA MET KENNISGEVINGSVERPLICHTINGEN .....	35
B. VOORBEELDEN VAN INBREUKEN IN VERBAND MET PERSOONSGEGEVENS EN AAN WIE DE INBREUKEN MOETEN WORDEN GEMELD/MEEGEDEELD .....	36

## 2. Het toepassingsgebied

- **Informatiebeveiligingsincident:** "een ongewenste en/of onverwachte gebeurtenis die afwijkt van het verwachte of overeengekomen kwaliteitsniveau zoals gedefinieerd in het beleid, en die een significante of potentiële impact heeft op de informatiebeveiliging met betrekking tot de criteria van CIA en veerkracht van de verwerkingssystemen en de gegevens die ze verwerken".
- Informatiebeveiligingsincidenten met een impact op de verwerking van persoonsgegevens = **inbreuk op persoonsgegevens**.
- = is breder dan enkel IT-systemen! Datalekken kunnen zich ook voordoen in "papierverwerking", "fysieke beveiliging"...



# 3. De risicoanalyse.

**Hoog risico:** de betrokkene wordt alleen op de hoogte gebracht van inbreuk als deze waarschijnlijk een hoog risico voor de rechten en vrijheden inhoudt.

**Normaal risico:** meldplicht bij de bevoegde toezichthoudende autoriteit is vereist wanneer inbreuk waarschijnlijk leidt tot risico voor de rechten en vrijheden van de betrokkene.

**Laag risico:** alle andere gevallen.



# 3. De risicoanalyse.



Documenteer en inventariseer alle inbreuken op persoonsgegevens:

- Elementen van melding
- datum
- tijd
- motivatie van beoordeelde risiconiveau

# 3. De risicoanalyse.

Waar rekening mee houden tijdens je risico analyse?

- **Soort** inbreuk
- **Aard, gevoeligheid** en **omvang** van de persoonsgegevens
- **Gemak** waarmee personen kunnen worden geïdentificeerd
- **Ernst van gevolgen** voor personen
- Bijzondere kenmerken van de **persoon**
- Bijzondere kenmerken van de **verwerkingsverantwoordelijke**
- Het **aantal getroffen personen**



**Algemene regel: in geval van twijfel moet de verwerkingsverantwoordelijke het zekere voor het onzekere nemen en de inbreuk melden.**

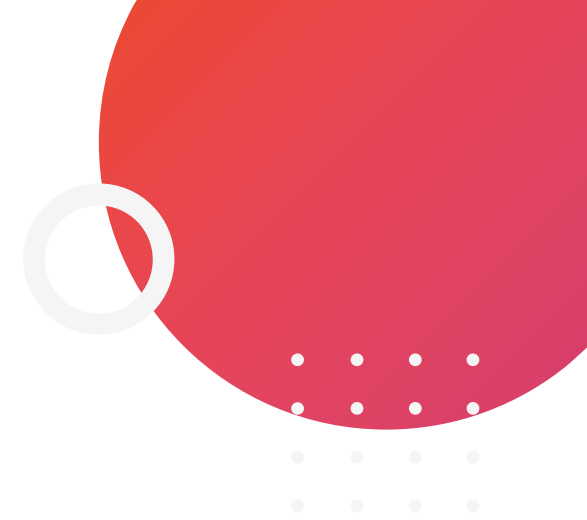
# 4. Beleid en procedure.

## Een uitdaging

= risico voor de betrokkenen inschatten op het moment dat je het incident opmerkt.

≠ alleen het incident indammen, maar ook het risico dat uit het incident kan vloeien beoordelen.

Quiztime: Beperkt Encryptie ieder risico?



# 5. Stappenplan.



# 5. Stappenplan

## Wanneer autoriteit inlichten?

- Elke inbreuk moet gemeld worden bij de toezichthoudende **autoriteit**, tenzij het datalek waarschijnlijk niet zal leiden tot een risico voor de rechten van de vrijheden van natuurlijke personen.
- Wanneer de inbreuk waarschijnlijk een hoog risico inhoudt, dan moeten **de betrokkenen op de hoogte gebracht worden**.



# 5. Stappenplan

Wat melden bij de autoriteit of betrokkene?

- **Aard** van de inbreuk in verband met persoonsgegevens;
- **Contactgegevens** waar meer informatie kan worden verkregen;
- **Beschrijving** van de waarschijnlijke **gevolgen** van de inbreuk in verband met persoonsgegevens;
- **Beschrijving** van de **maatregelen** die je hebt genomen of zal nemen in verband met de persoonsgegevens (rekening houdend met passende maatregelen om negatieve gevolgen in te perken)



# 5. Stappenplan

Hoe een datalek ontdekken?

IT incident

IT helpdesk

De pers ☹️

Callcenter

DLP Systeem

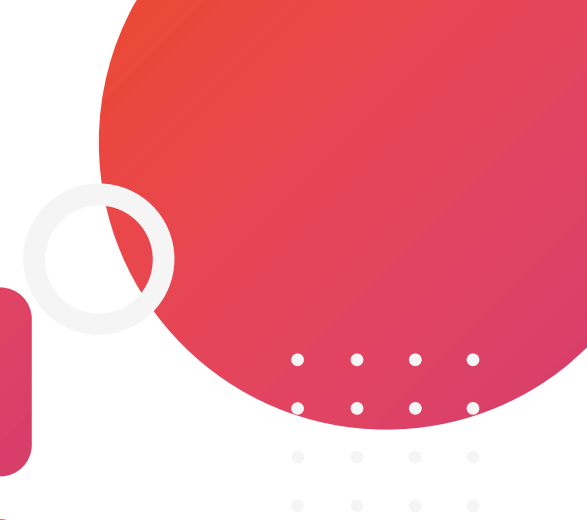
Monitoring van processen

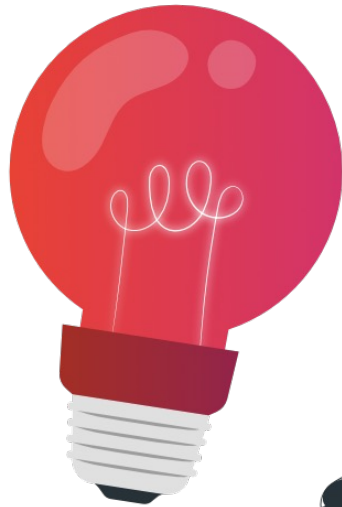
Via verwerkingsverantwoordelijke

Facility helpdesk

Eigen medewerkers

...





## 6. Post Mortem

Leren van je incidenten.



1.

Beleid,  
procedures en  
standaarden  
updaten en  
bijwerken

2.

Technische en  
organisatorische  
maatregelen  
(TOMs) toevoegen  
en bijwerken

3.

Starten met  
specifieke en  
doelbewuste  
awareness sessies

4.

DPIAs, DPbDesign  
en DPbDefault  
methodes  
bijwerken

5.

Verwerkingsregister  
bijwerken

6.

Remediëringsplan  
aanpassen

# Thank you.

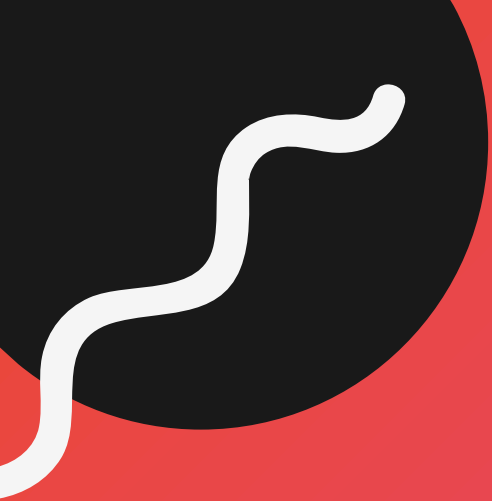


**Bavo Van den Heuvel**

Chief Knowledge Officer &  
Founder

[bavo@cranium.eu](mailto:bavo@cranium.eu)

**CRANIUM**



---

# Let's stay in touch!



## Website.

[www.cranium.eu](http://www.cranium.eu)



## Socials.



[@cranium-eu](https://www.linkedin.com/company/cranium-eu)



[@cranium\\_eu](https://www.instagram.com/cranium_eu)



[@craniumeu](https://www.facebook.com/craniumeu)



## Contact us.

# Bronnen / referenties

---

Article 29 Working Party, Opinion 03/2014 on “Personal Data Breach Notification (2014).

---

Article 29 Working Party, Guidelines on Personal Data Breach Notification Under Regulation 2016/679 (2018).

---

EDPB, Guidelines 1/2021 on Examples regarding Data Breach Notification (2021).

---

DPC (Ireland), Guidance for Individuals who Accidentally Receive Personal data (2020).

---

Methodiek voor beoordeling van de ernst van inbreuken op persoonsgegevens:  
<https://www.enisa.europa.eu/publications/dbn-severity>

---

WP248\_01: <https://ec.europa.eu/newsroom/article29/items/611236>

---

WP250\_01: <https://ec.europa.eu/newsroom/article29/items/612052/en>