# Dataprivacy & de bedrijfsjurist - heeft u de controle?

Joris Hutter
Privacy Management Partners

Wolters Kluwer

# Grip op datalekken


Wolters Kluwer

# Wat is een datalek

Inbreuk op de beveiliging

- Schending van vertrouwelijkheid
- Schending van beschikbaarheid
- Schending van integriteit

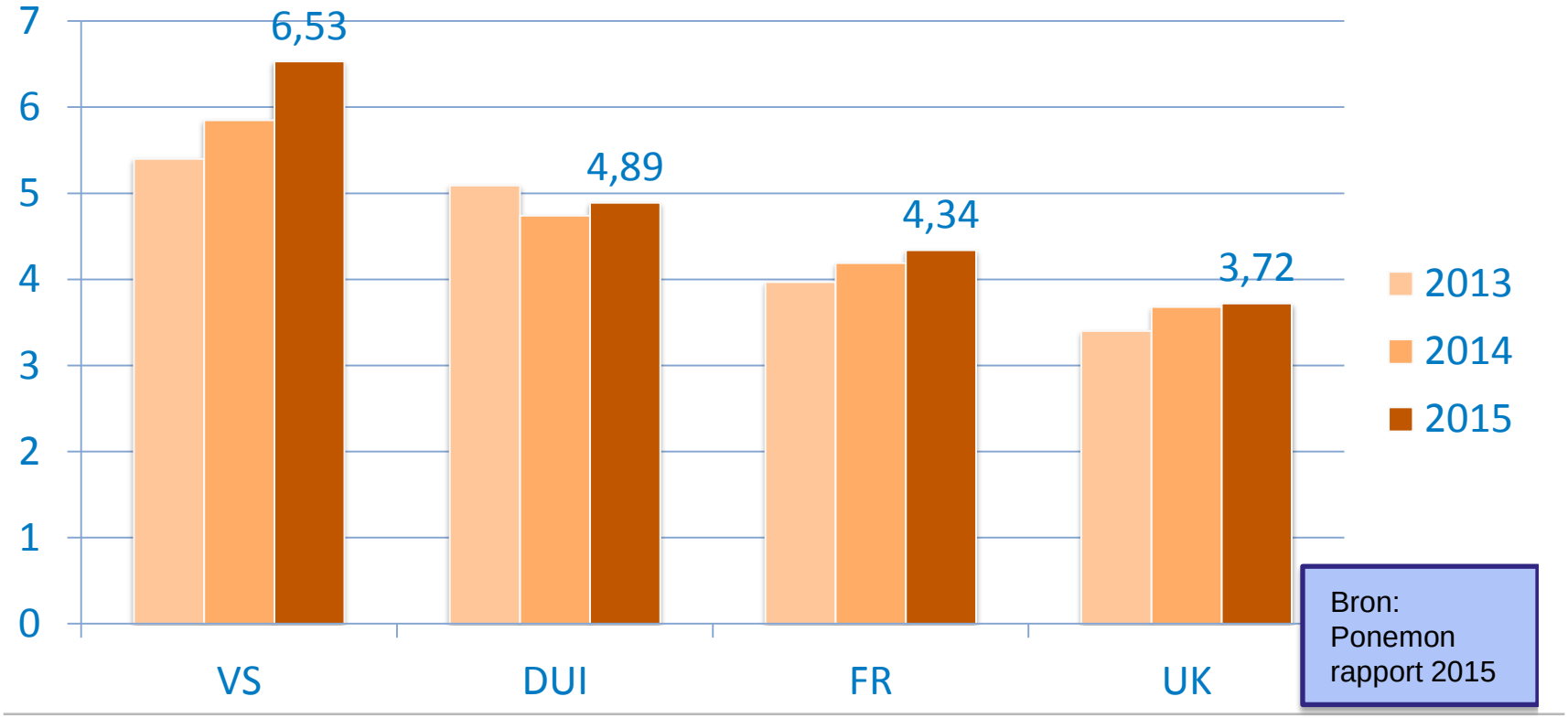
Bij

- Digitale informatie
- Dossiers die uit een bestand komen of in een bestand gezet kunnen worden

Indien het persoonsgegevens betreft

# Datalekken zijn kostbaar

- Gemiddelde kosten van een datalek
  - € 3,35 miljoen (2015)




Wolters Kluwer

# Kosten per betrokkene

Gemiddelde kosten per betrokkene zijn € 200

- Kosten afhankelijk van branche (bron Ponemon 2015)

Wat is de potentiële schade in uw organisatie?

Is dit risico geadresseerd?

# Waar liggen de kosten

Waar liggen de kosten (Ponemon rapport 2015):

- Detectie en escalatie: 26%
- Melden: 5%
- Ex-post response: 28%
- Omzetverlies: 41%

# Wat verwacht wetgeving

- Sinds 1 januari 2016
  - Meldpicht in WBP
  - Boetebevoegheid in relatie tot datalekken
    - Falen van melden (120.000 – 500.000 euro)
    - Falen van beveiliging (120.000 – 500.000 euro)
    - Falen van management (350.000 – 820.000 euro)

- Bij van kracht worden van Algemene Verordening Gegevensverwerking
  - Ook meldplicht
  - Ook boetes
  - Zwaarder accent op accountability en ‘in control’
  - Documentatieplicht (privacyboekhouding op orde)

# Aan wie melden

Vanuit regelgeving:

1. Melden aan autoriteit (Autoriteit Persoonsgegevens)
2. Melden aan betrokkene
3. Bewerker meldt aan verantwoordelijke

Maar ook communicatie met:

- Bestuur, aandeelhouders
- Medewerkers
- Branche, ketenpartners, klanten
- Media

# Oorzaken en type maatregelen

1. Menselijk falen => bewustwording / training
2. Organisatorisch/technisch falen => procedures & technische middelen
3. Bewust menselijk handelen => integriteit, zwaardere security maatregelen

# Wat zijn nu typische missers

1. Security patches niet op orde
2. Phishing
3. Testen of analytics met productiegegevens
4. Thuiswerken, met mobiele apparaten werken, met onbekende apps werken
5. E-mail
6. Tijdelijke samenwerkingsgroepen en autorisatie
7. …

# Drie samenhangende aanpakken

1. Voorkomen en bemoeilijken van datalek
2. Ontdekken van datalek
3. Bestrijden, melden en herstellen (datalekresponse)

# Datalekresponse

- Ontstaan van datalek
- Ontdekken
- In actie komen en bestrijden
- Bepalen impact en bepalen aanpak op melding en herstel
- Melden
- Herstel
- Evalueer

# Snelheid van actie vereist in warme fase

# Rol van jurist in datalekresponse

- Ontstaan van datalek
- Ontdekken
- In actie komen en bestrijden
- Bepalen impact en bepalen aanpak op melding en herstel
- Melden
- Herstel
- Evalueer

→

- Leveren van nazorg naar benadeelden
- Beperken van (reputatie)schade, klantbehoud, in business blijven
- Beperken boetes en aansprakelijkheid, verhalen van schade op veroorzaker
- Leveren van documentatie op beveiliging, response en omgang met privacy

# Wat betekent dit voor u als jurist

1. Datalek is een businessrisico
2. Datalek is/wordt een aansprakelijkheidsrisico
3. Aantoonbare documentatie vereist:
   - Governance
   - Data & risico's in beeld
   - Op afspraken met ketenpartners
   - Op voorkomen van datalek
   - Op bestrijden van datalek, melden en beperken van schade voor derde partijen
4. Sturen op controls (framework):
   - Datalekresponse
   - Datalekrisicomanagement
   - Privacy

# Vragen…?

**Joris Hutter**

*Privacy Management Partners*

*Utrecht*

E: joris.hutter@pmpartners.nl

T: 085 – 401 3866

**wolterskluwer.nl/gripopdatalekken**