Wet Meldplicht Datalekken

Jeroen Terstegge

PRIVACY MANAGEMENT PARTNERS

Introduction

- **Jeroen Terstegge, CIPP E/US**
  - ✓ Partner, Privacy Management Partners
  - ✓ Voorzitter Privacy Commissie , VNO-NCW / MKB Nederland
  - ✓ Bestuurslid, Vereniging Privacy Recht
  - ✓ Lid High Level Expert Groep *Big Data & Privacy*, Ministerie EZ
- **Voormalige functies**
  - ✓ Corporate Privacy Officer, Royal Philips Electronics
  - ✓ Hoofdredacteur, *Privacy & Compliance*
  - ✓ Voorzitter Privacy & Security Working Group, DigitalEurope
  - ✓ Voorzitter Expert Group Privacy & New Technologies, ECP.nl
- **Awards**
  - ✓ IAPP Privacy Innovation Award 2006 voor BCRs

Playstation hack

- **Feiten datalek**
  - ✓ 77 miljoen accounts
  - ✓ 3 dagen
  - ✓ Creditcard data
    - 12.000 expired accounts
- **Gevolgen**
  - ✓ Outage: 23 dagen
  - ✓ 5,5% koersdaling in 1 dag
  - ✓ SOE: 53 dagen gratis spelen (30 + 23)
    - Hulu: 30 dagen gratis kijken
  - ✓ $ 15M settlement in VS

Home depot malware

- **Feiten datalek**
  - ✓ Malware
  - ✓ 53 miljoen creditcard data en e-mailadressen
  - ✓ Negeren vulnerability warnings
- **Gevolgen**
  - ✓ Kosten nu: $ 230 miljoen
  - ✓ Kan oplopen tot: “billions”, maar verzekering dekt tot $ 100 miljoen
  - ✓ 44 rechtszaken

October 02, 2015

Home Depot breach costs expected to reach billions

Share this article:

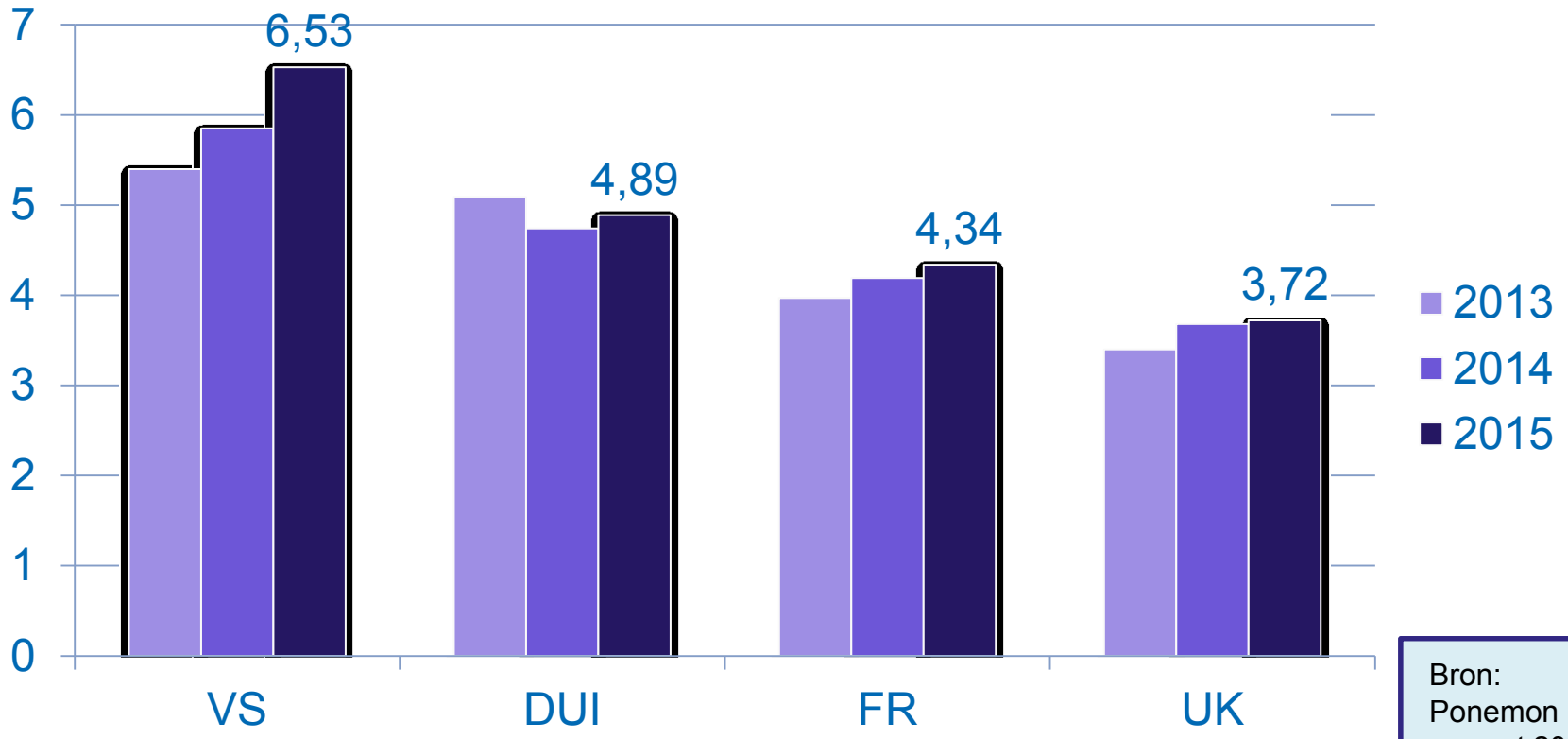
Owing to a slew of lawsuits filed by banks and credit unions, the expected cost to Home Depot for a cyber intrusion may reach into the billions, according to Insurance Business America (IBA).

The retailer recently stated it has already spent $232 million as a result of the breach last September, when hackers used a vendor's stolen logon credentials to penetrate its computer network and insert malware that siphoned off payment-card data and email addresses of 56 million customers.

Owing to a slew of lawsuits filed by banks and credit unions, the

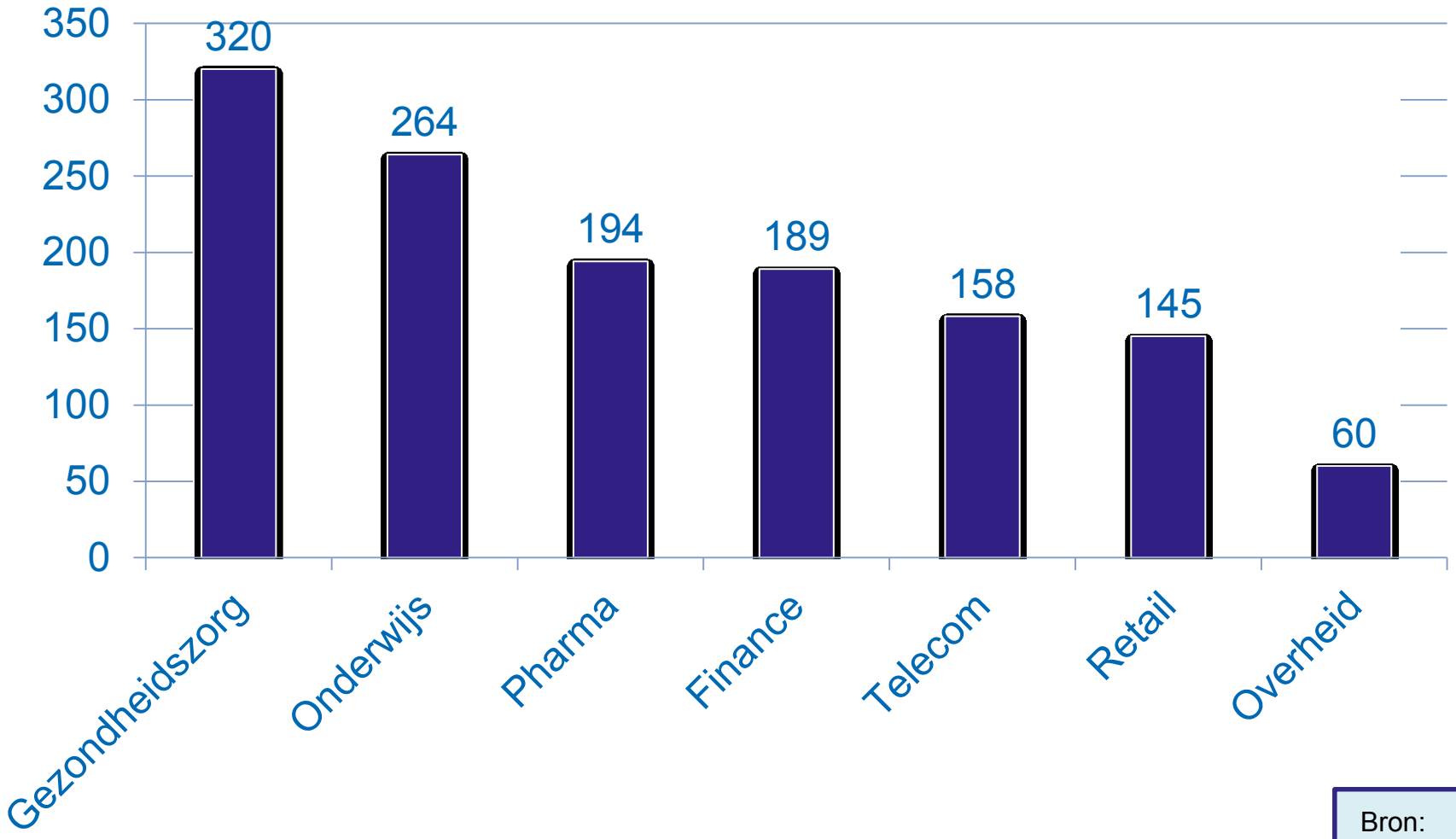
Datalekken zijn kostbaar

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



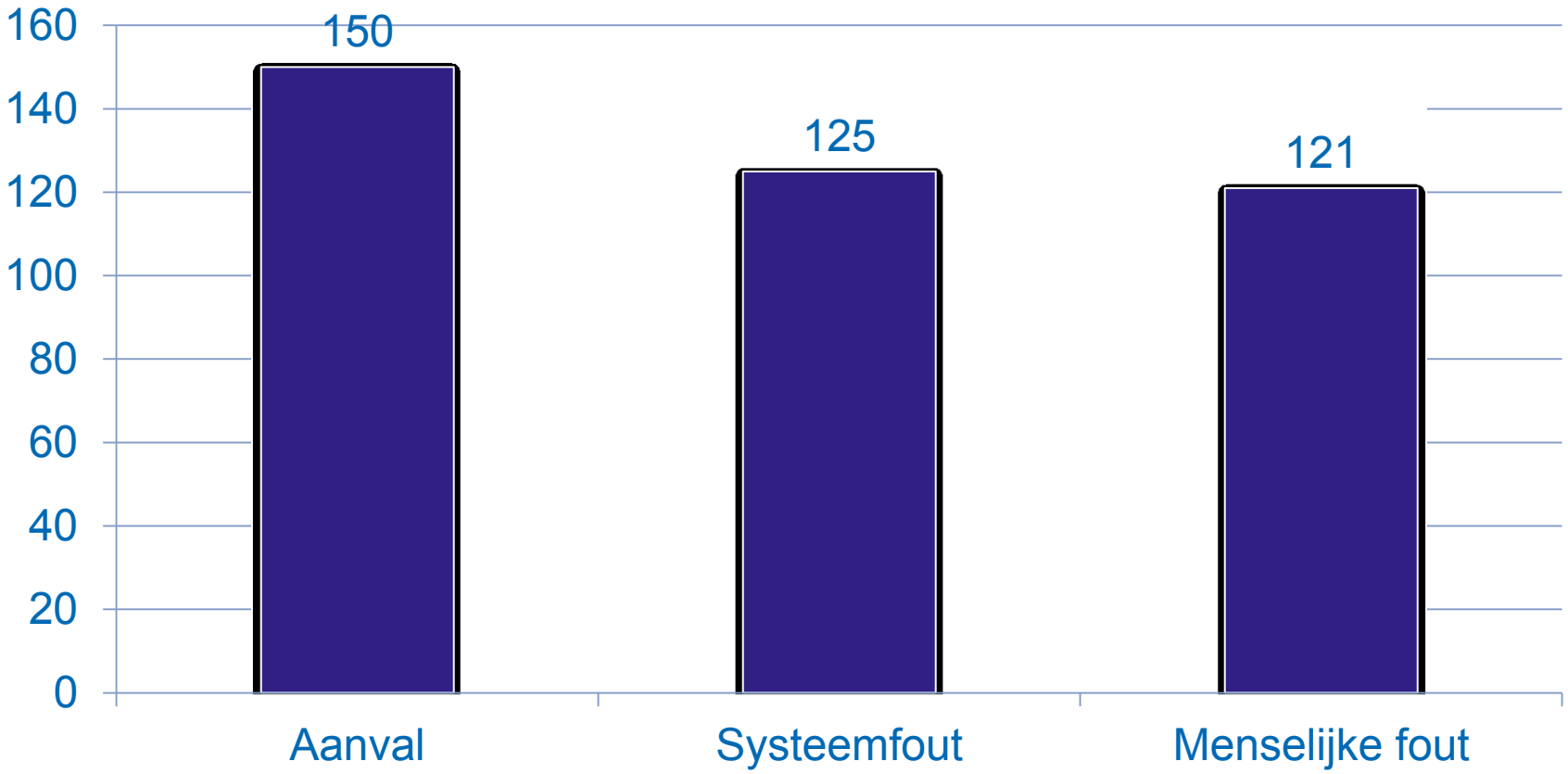
Bron: Ponemon rapport 2015

Kosten per betrokkene
- per sector



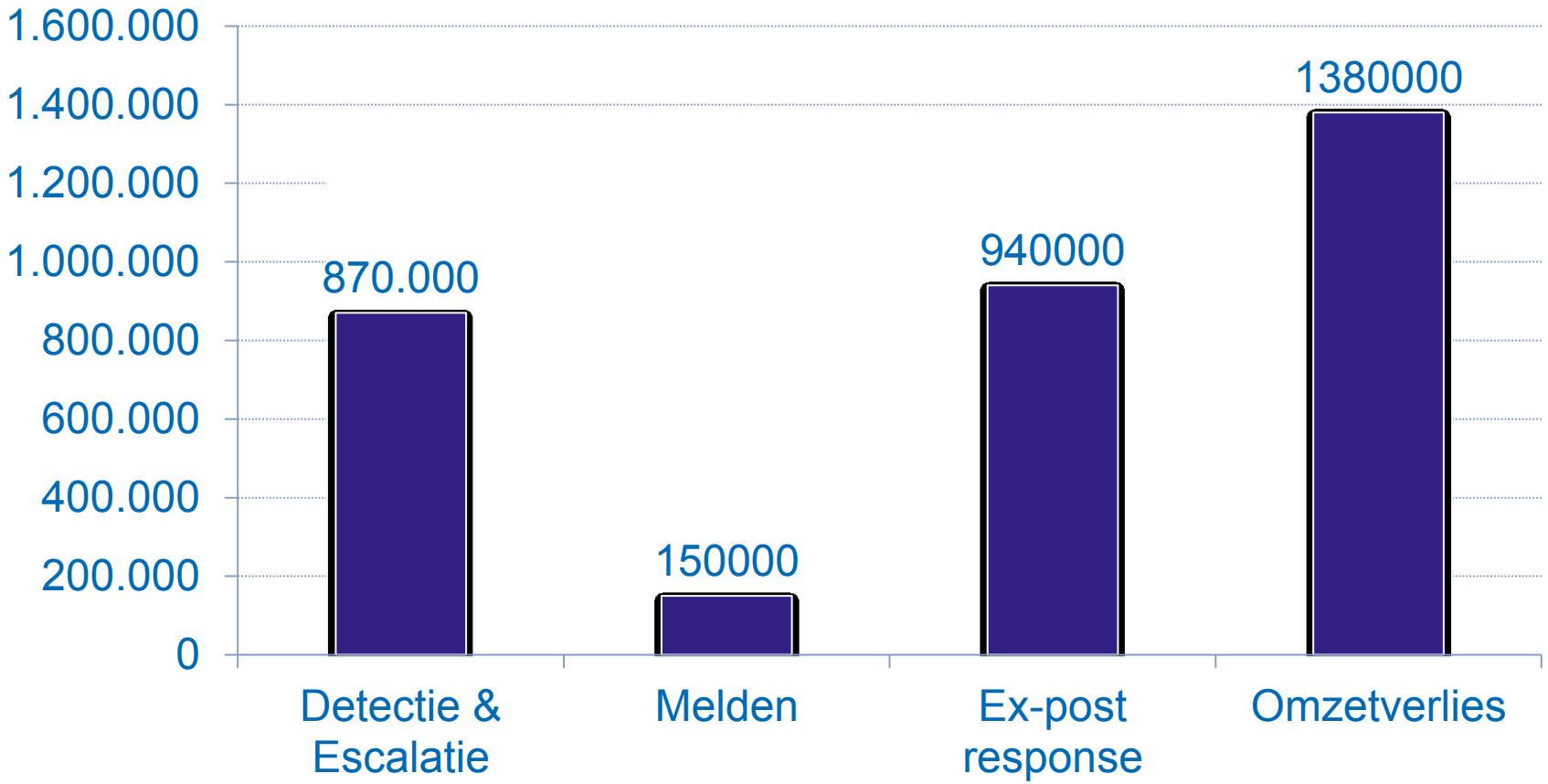
Bron:
Ponemon
rapport 2015

Kosten per betrokkene
- per type datalek



Bron:
Ponemon
rapport 2015

Kosten per type
- per datalek



- NB. Geschatte administratieve lasten en nalevingskosten volgens MvT:
  - ✓ € 1.517.655 voor het hele bedrijfsleven per jaar

Bron: Ponemon rapport 2015

Wat regelt de nieuwe wet?

- **Art. 34a WBP: Meldplicht datalekken**
  - ✓ Bij AP
  - ✓ Bij betrokkenen
- **Art. 14: Bewerkersovereenkomsten**
  - ✓ Datalek bij bewerker
- **Art. 66 WBP: Boetebevoegdheid AP**
  - ✓ Max 820.000 euro
  - ✓ Max 10% jaaromzet rechtspersoon
- **Van kracht**
  - ✓ 1 januari 2016

Wat is een datalek ?

- **Art. 34a WBP**
  - ✓ “Een inbreuk op de beveiliging als bedoeld in artikel 13 WBP”
- **Artikel 13 WBP**
  - ✓ Passende technische en organisatorische maatregelen
  - ✓ Tegen verlies of enige vorm van onrechtmatige verwerking

Wat is een datalek ?

Wat is een datalek ?

- **EU Privacy Verordening (2018)**
  - ✓ Art. 4(9): ‘Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Wie moet melden ?

- **Art. 34a WBP: De verantwoordelijke**
  - ✓ Bij het AP
  - ✓ Bij de betrokkene
  - ✓ De verantwoordelijke is de (rechts)persoon die alleen of samen met anderen het doel en de middelen van de verwerking bepaalt.
- **Art. 14 WBP: De bewerker**
  - ✓ Bij de verantwoordelijke
  - ✓ De bewerker is de (rechts)persoon die in opdracht van de verantwoordelijke namens hem persoonsgegevens verwerkt

Wanneer moet worden gemeld ?

- **Bij het CBP**
  - ✓ **Inbreuk op de beveiliging als bedoeld in art. 13 WBP**
    - Ook melden als er geen of onvoldoende maatregelen zijn getroffen
    - Ook melden als residual risk wordt uitgebuit
  - ✓ **Ernstige nadelige gevolgen voor de bescherming gegevens**
    - Bagatelzaken hoeven dus niet gemeld te worden
    - Aard en omvang van de inbreuk
    - Aard van de gelekte persoonsgegevens
  - ✓ **Heeft / Aanzienlijke kans op**
    - Aard van de inbreuk
    - Omvang en aard van de verwerking

Wanneer moet worden gemeld?

- **Ernstige datalekken**
  - ✓ Datalekken betreffende
    - Bijzondere gegevens
    - Financiële data
    - Data die kan worden gebruikt voor discriminatie
    - Data die kan worden misbruikt voor ID-diefstal
    - User names / passwords
    - DNA
    - Data die onder een beroeps-/wettelijke geheimhoudingsplicht vallen

Wanneer moet worden gemeld ?

- **Bij betrokkene(n)**
  - ✓ **Inbreuk op de beveiliging als bedoeld in art. 13 WBP**
    - Ook melden als er geen of onvoldoende maatregelen zijn getroffen
    - Ook melden als residual risk wordt uitgebuit
  - ✓ **Ongunstige gevolgen voor de persoonlijke levenssfeer**
    - Geen duidelijk verschil met ‘nadelige’ uit lid 1
  - ✓ **Waarschijnlijk**
    - Lijkt een bredere norm dan “aanzienlijke kans” uit lid 1

Hoe snel moet worden gemeld ?

- **AP**
  - ✓ Onverwijld
    - Binnen 72 uur
    - MvT: “geeft de verantwoordelijke enige gelegenheid om onderzoek te doen naar de inbreuk, te overwegen welke maatregelen hij aanbeveelt en de manier waarop hij communiceert met CBP en betrokkenen”

- **Betrokkene**
  - ✓ Onverwijld

Wat moet worden gemeld ?

- **AP**
  - ✓ Aard van de inbreuk
  - ✓ De instanties waar meer informatie kan worden verkregen over de inbreuk
  - ✓ De aanbevolen maatregelen om de negatieve gevolgen te beperken
  - ✓ Beschrijving van geconstateerde en vermoedelijke gevolgen
  - ✓ Maatregelen die zijn getroffen of worden voorgesteld

Wat moet worden gemeld ?

- **Betrokkene**
  - ✓ Aard van de inbreuk
  - ✓ De instanties waar meer informatie kan worden verkregen over de inbreuk
  - ✓ De aanbevolen maatregelen om de negatieve gevolgen te beperken

Wijze van melden

- **AP**
  - ✓ Via http://datalekken.autoriteitpersoonsgegevens.nl

- **Betrokkene**
  - ✓ Vormvrij
    - "Op zodanige wijze dat een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd"

Uitzondering Meldplicht

- **AP**
  - ✓ Bagatelzaken (= geen ernstige nadelige gevolgen)
  - ✓ Versleutelde gegevens
    - NB. Lid 1 overrulet amendement op lid 6 ??

- **Betrokkene**
  - ✓ Bagatelzaken (= geen ongunstige gevolgen)
  - ✓ Versleutelde gegevens

Boetebevoegdheid AP

- **Bindende aanwijzing (“gele kaart”)**
  - ✓ Concretisering van de vage WBP-norm
  - ✓ Kohnstamm: *“Bindende aanwijzing komt zo dicht bij last onder dwangsom dat ik niet denk dat ik die ooit ga gebruiken”*

- **Zonder bindende aanwijzing (“rode kaart”)**
  - ✓ Opzet / Voorwaardelijk opzet
  - ✓ Ernstige verwijtbare nalatigheid
    - Toelichting Amendement nr. 16: “grof, aanzienlijk onzorgvuldig, onachtzaam dan wel onoordeelkundig handelen”

Boetebevoegdheid AP

- **Boete is maximaal**
  - ✓ 820.000 euro
    - Wordt periodiek aangepast
  - ✓ OF 10% van de (wereldwijde) jaaromzet rechtspersoon “als het boetemaximum geen passende bestraffing biedt”

Categorie I	Categorie II	Categorie III
0 – 200.000 euro	120.000 – 500.000 euro	350.000 – 820.000 euro
	Niet-melden datalek Geen passende beveiliging	

Nabrander

- **Is elke ‘onrechtmatige verwerking’ een datalek?**
  - ✓ Nee, een onrechtmatige verwerking in de zin van een overtreding van de Wbp is geen datalek.

Grip op datalekken

dr. Koen Versmissen CIPP
mr. Sergej Katus CIPM
mr. drs. Jeroen Terstegge CIPP
drs. Joris Hutter CIPM CISM

Wolters Kluwer

PRIVACY MANAGEMENT PARTNERS

Contact

Privacy Management Partners
mr.drs. Jeroen Terstegge CIPP E/US
jeroen.terstegge@pmpartners.nl
www.pmpartners.nl
+31624276833
@PrivaSense