Meldplicht Datalekken

Wolter Karssenberg RE, CIPP/E, CIPM
drs. Erik König EMITA

10 december 2015

Agenda

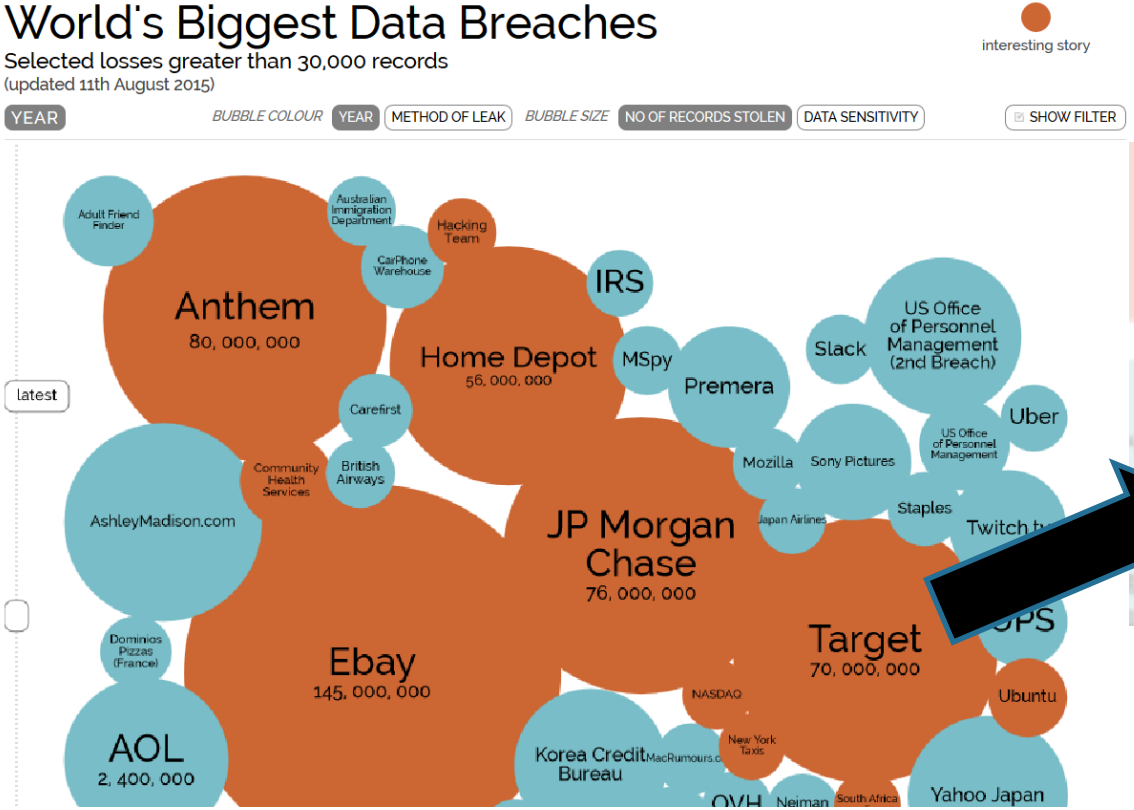
- Datalekken
- Meldplicht
- Beleidsregels
- Beheersen
- So what! We'll just pay the fine!

Agenda

Datalekken

- Meldplicht
- Beleidsregels
- Beheersen
- So what! We'll just pay the fine

Datalekken: world's biggest databreaches



Investigators believe the data was obtained via software installed on machines that customers use to swipe magnetic strips on their cards when paying for merchandise at Target stores. Originally 40m customers. Now 70m!

Click to see the original report

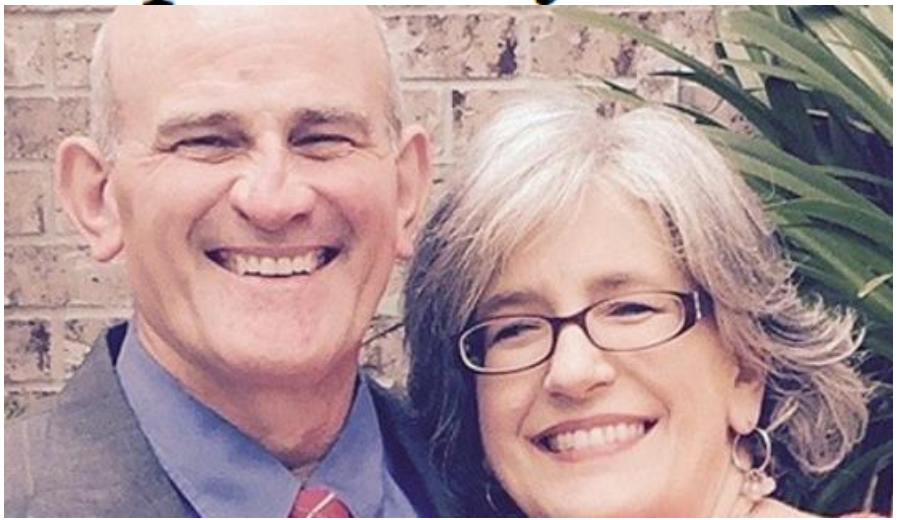
Bron: informationisbeautiful.net

Datalekken: breach level index

Bron: breachlevelindex.com

Datalekken: zelfmoorden door hack vreemdgangerssite

Ashley Madison Suicide? Married Baptist Teacher Exposed By Hack Takes Own Life



Bron: hollywoodlife.com

Datalekken: militairen en medewerkers veiligheidsdiensten

Hacking of Government Computers Exposed 21.5 Million People

By JULIE HIRSCHFELD DAVIS JULY 9, 2015

Bron: nytimes.com

Datalekken: klantenbestand webwinkel

Gegevens 157.000 klanten Mapp.nl gestolen

donderdag 16 april 2015, 13:44 door **Redactie**, 16 **reacties**

De webwinkel Mapp.nl heeft klanten gewaarschuwd nadat aanvallers een deel van het klantenbestand hebben gestolen. De aanval, waarbij 157.000 e-mailadressen en "gecodeerde wachtwoorden" werden buitgemaakt, vond plaats via SQL Injection, zo laat een woordvoerder tegenover Security.NL weten.

Bron: security.nl

Datalekken: gevoelige gegevens BN-ers

Ambtenaren verlekkeren zich aan privégegevens BN'ers

Door: Guido van Gorp
10-5-14 - 08:00 bron: AD

'Wat is er leuker dan snuffelen in besognes van de sterren?'

Bron: ad.nl

Datalekken: veroorzaken nieuwe datalekken

HRSDC privacy breach letters sent to wrong people

CBC News Posted: Feb 08, 2013 6:59 AM ET | Last Updated: Feb 08, 2013 8:07 AM ET

Former student loan recipients say letters from Human Resources and Skills Development Canada informing them their personal information may have been lost also include the contact information of complete strangers.

Bron: cbc.ca

Agenda

- Datalekken
- **Meldplicht**
- Beleidsregels
- Beheersen
- So what! We'll just pay the fine

Meldplicht: principle based

Meldplicht: wanneer is het een datalek?

- Inbreuk op de wettelijk verplichte beveiliging
- Beveiliging: passende maatregelen die persoonsgegevens beveiligen tegen:
  - Verlies
  - Onrechtmatige verwerking
- Kenmerkend voor inbreuk op de beveiliging:
  - Daadwerkelijk gevolgen voor persoonsgegevens, of
  - Niet redelijkerwijs uit te sluiten dat gegevens onrechtmatig zijn verwerkt, en
  - Repressieve en herstelmaatregelen niet voldoende om gevolgen weg te nemen
- Inbreuk op beveiliging onafhankelijk van of “passende maatregelen” zijn getroffen

Meldplicht: aan wie melden?

- Aan: Autoriteit persoonsgegevens (Ap, voorheen Cbp)
  Als: “(aanzienlijke kans op) ernstige nadelige gevolgen”
- Aan: betrokkenen
  Als: “waarschijnlijk ongunstige gevolgen”
  Niet als: “onbegrijpelijk of ontoegankelijk voor eenieder die geen recht heeft”

  Beleidsregels:
  - Adequate encryptie
  - Adequate remote wipe
  - Adequaat gepseudonimiseerd

Meldplicht: wanneer melden?

- “Onverwijld”

Beleidsregels:

- Aan Autoriteit persoonsgegevens:
  - Tijd voor nader onderzoek
  - Hangt af van omstandigheden
  - Zonder onnodige vertraging
  - Uiterlijk 72 uur na ontdekken, tenzij gemotiveerd
- Aan betrokkene:
  - Rekening houden met maatregelen die betrokkene kan treffen

Meldplicht: wat melden?

- Aan Autoriteit persoonsgegevens èn betrokkenen:
  - Aard inbreuk
  - Vindplaats nadere informatie
  - Aanbevolen maatregelen

- Aan Autoriteit persoonsgegevens:
  - Gevolgen
  - Maatregelen

- Aan betrokkenen:
  - Alle andere noodzakelijke informatie

Agenda

- Datalekken
- Meldplicht

Beleidsregels

- Beheersen
- So what! We'll just pay the fine

Beleidsregels: opzet

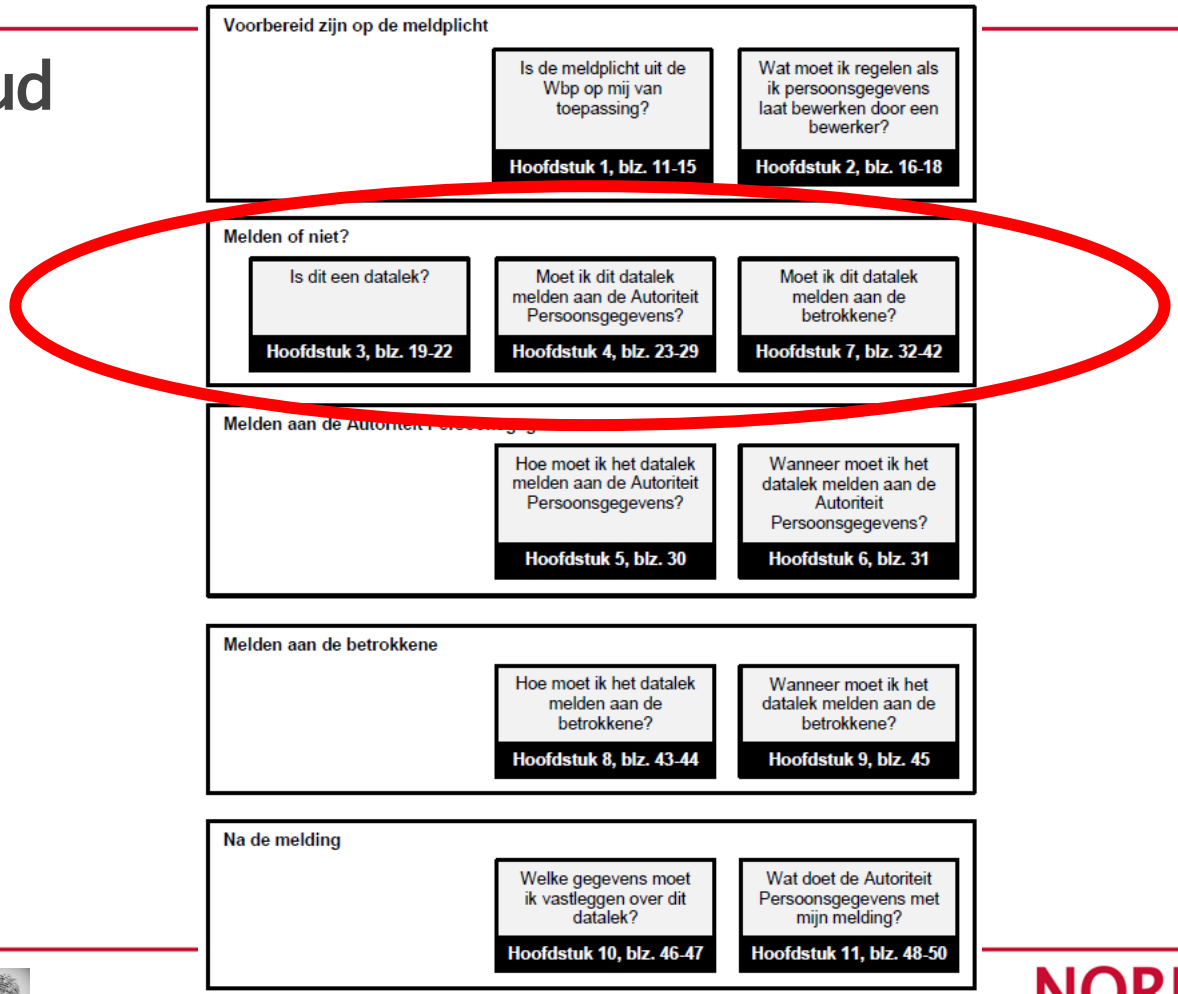
- Organisaties wegen meldplichtigheid zelf af
- Beleidsregels ondersteunen daarbij
- Beleidsregels zijn ook principle based
- Veel schema's
- Veel voorbeelden

De meldplicht datalekken
in de Wet bescherming persoonsgegevens (Wbp)

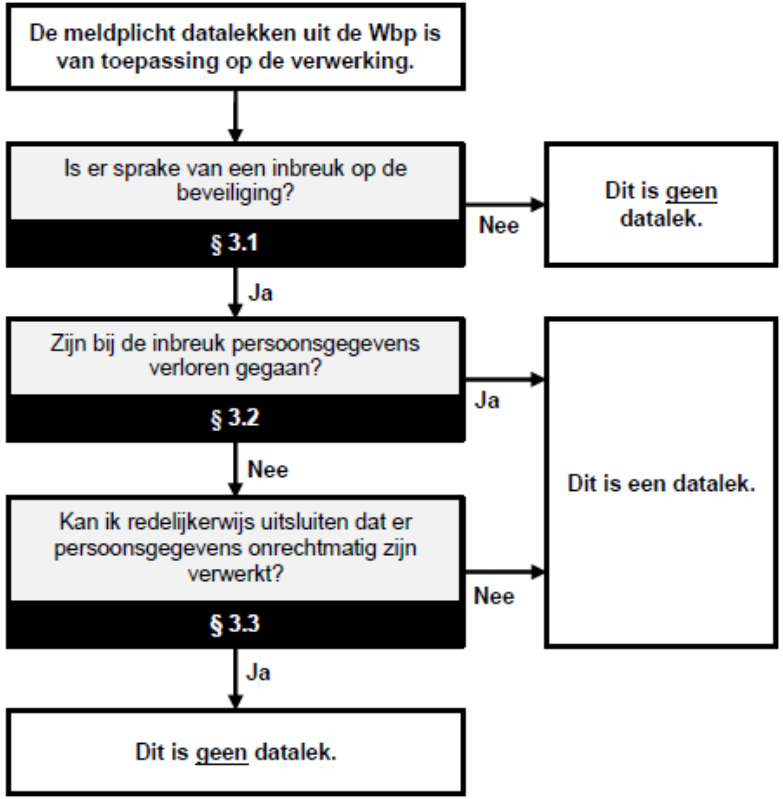
Beleidsregels voor toepassing van artikel 34a van de Wbp

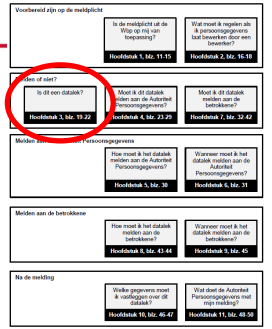
DATUM 8 december 2015

Beleidsregels: inhoud



Beleidsregels: is het een datalek?





Casus:

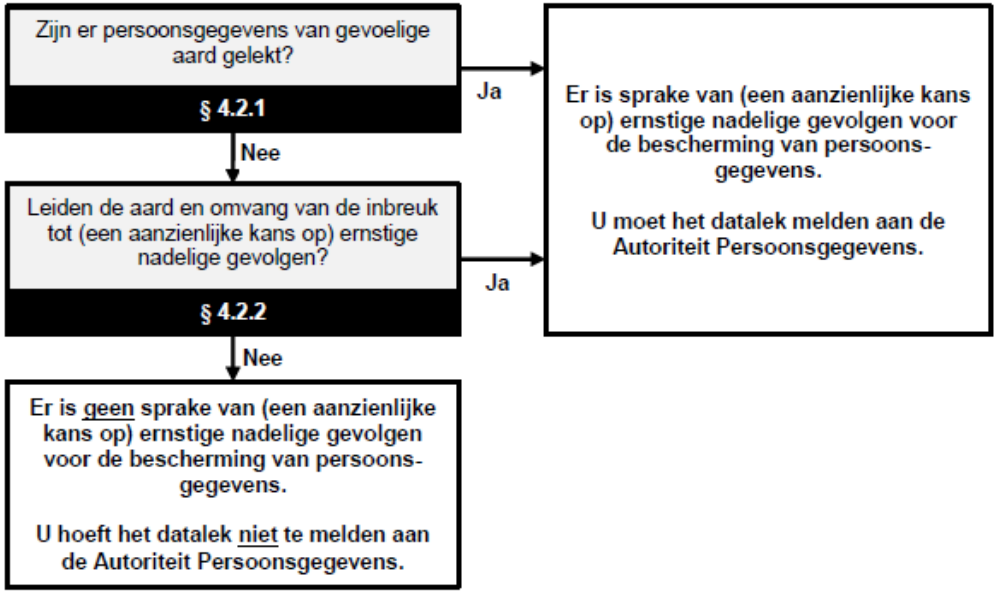
Webshop ≈ €400 miljoen omzet

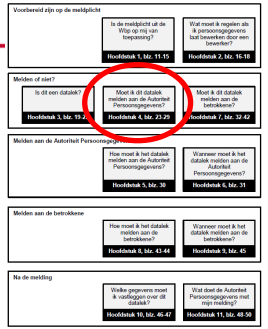
Toegang systeembeheerder gedeeld met partner voor checken email (partner vertelt dit tijdens een afdelingsuitje)

Geen:
- Klachten van betrokkenen

Wel:
- Toegang tot alle klantgegevens
- Toegang tot systeembeheer

Beleidsregels: melden aan Autoriteit persoonsgegevens?





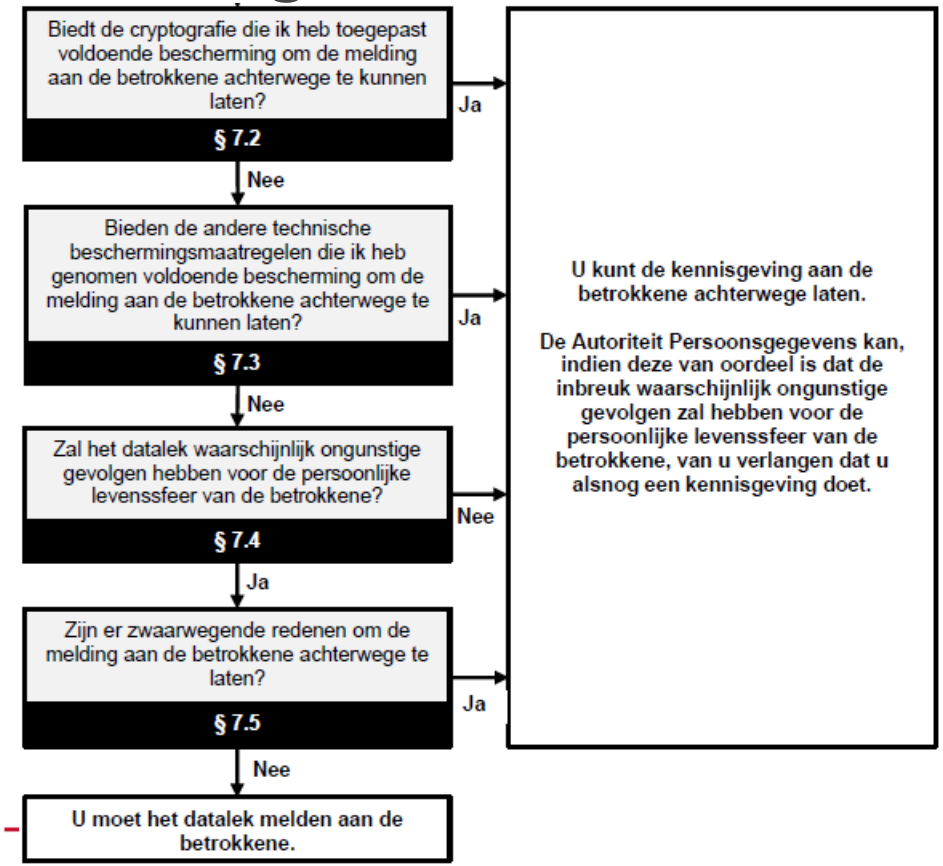
Casus:

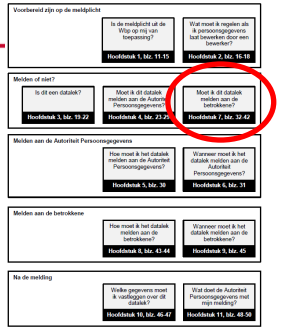
Toegang systeembeheerder gedeeld

Geen:
- Ziekenhuis, kerkgenootschap, Blijf-van-m'n-lijf huis, politieke partij, …

Wel:
- Veel personen
- O.a. webshop voor bloeddrukmeters
- O.a. betalingshistorie

Beleidsregels: melden aan de betrokkene?





Casus:

Toegang systeembeheerder gedeeld

Geen:
- Verdachte items in raadpleeglogging van systeembeheerder

Wel:
- Adequaat versleutelde wachtwoorden
- Pro-actieve monitoring van de logging, (maar kan ongelogd geschoond worden door systeembeheerder)

Agenda

- Datalekken
- Meldplicht
- Beleidsregels

Beheersen

- So what! We'll just pay the fine

Beheersen: Risico's afwegen

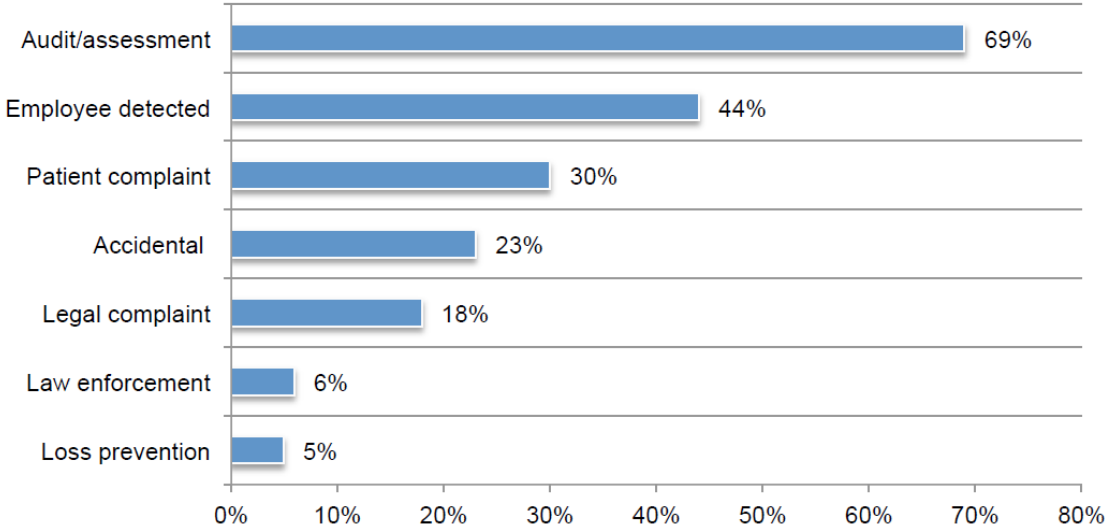
Beheersen: Welke rol heeft IT security

- Voorkomen
  - Nut & Noodzaak
  - Risico management
- Detecteren
- Opvolgen

Beheersen: Niet alléén IT security

- Voorkomen
- Detecteren
  - IT management
  - Klanten
  - Medewerkers
  - Hackers
  - …
- Opvolgen

Q& A, 15: How the data breach was discovered (healthcare organizations)



Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data
Ponemon Institute 2015

Beheersen: Wees voorbereid

- Voorkomen
- Detecteren
- Opvolgen
  - Beoordelen en afwegen
  - Registreren
  - Stoppen
  - Melden
  - Voorkomen

Beheersen: haak in op bestaande processen en structuren

- IT–operations
  - Security, Event, Incident, Problem
- Business operations
  - Inkoop / Outsourcing / Contract management
  - Customer Services / klant contact centrum
- Governance
  - Risk management
  - Public relations management
  - Stakeholder management

Agenda

- Datalekken
- Meldplicht
- Beleidsregels
- Beheersen

So what! We'll just pay the fine

Boetes: uitbreiding bevoegdheid per 1/1/2016

- Op belangrijke delen van de Wbp geldboete van de zesde categorie
- Direct bij opzettelijkheid en ernstig verwijtbare nalatigheid
- Anders pas nadat aanwijzing met termijn niet is opgevolgd

Boete van de zesde categorie:

- Maximaal: €820.000
- Indien maximum niet passend: maximaal 10% jaaromzet vorig boekjaar

Boetes: zesde categorie, onder andere voor

- Ontbreken rechtmatige grondslag (incl. bijzondere persoonsgegevens)
- Onverenigbaar gebruik
- Langer bewaren dan noodzakelijk
- Bovenmatig verwerken
- Geen passende beveiliging
- Onrechtmatig verwerken BSN
- …

Boetes: zesde categorie, onder andere voor

- …
- Geen, onvolledige, onjuiste of ontijdige informatie aan betrokkene
- Verzuim meldplicht datalekken
- Geen invulling rechten van betrokkenen (o.a. inzage, correctie)
- Geen invulling aan opt-out bij commerciële doelen
- Doorsturen naar landen zonder passend beschermingsniveau

Boetes: wat brengt de Europese toekomst?

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

Boete: tot maximal € 1 miljoen / €100 miljoen of 2% / 5% omzet?

Status: triloog Commissie, Parlement, Raad van Ministers

Boetes: dus als ik aan de wet voldoe heb ik geen issue?

Directeur particulieren ING vertrekt

Pieter Lalkens
vrijdag 14 november 2014, 14:04
Update: vrijdag 14 november 2014, 21:46

Directeur particulieren Hans Hagenaars (53) van ING Nederland vertrekt bij de bank. Hij gaat per 1 december weg en wordt opgevolgd door marketingdirecteur Vincent van den Boogert (45).

Volgens een woordvoerder van ING heeft het vertrek van Hagenaars niets te maken met de onrust over het gebruik van betaalgegevens van klanten. 'Het is een reguliere directiewisseling en dit is een natuurlijk moment om deze bekend te maken', aldus de woordvoerder. Tot het vertrek is volgens haar 'in goed overleg' besloten. Zij wil verder niet kwijt of Hagenaars zelf het initiatief heeft genomen voor zijn vertrek.

Bedankt

Voor meer informatie kun je contact opnemen met:

drs. Erik König EMITA
Privacy Officer Global Markets
Koninklijke Philips N.V.

+31 6 11 95 78 17
erik.konig@philips.com

Wolter Karssenberg RE, CIPP/E, CIPM
Management Consultant Privacy
EigenRuimte Advies

+31 6 22 39 37 49
wolter.karssenberg@eigenruimteadvies.nl
@WolterKarss

10 december 2015