@zwnne

RING NOORD NEDERLAND
GRONINGEN | 15 SEPTEMBER 2016

De Meldplicht Datalekken en de Privacywet & IoT & Datafication & Big Data

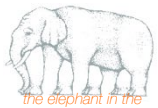
prof mr. Gerrit-Jan Zwenne

Universiteit Leiden

eLaw Leiden

roadmap

A. *Een eerste indruk van de Wet meldplichten datalekken*
B. *Een razendsnelle inleiding in de privacywet, nu en straks*
C. *Hoe IoT & Datafication & Big Data onze privacywetgever uitdagen*



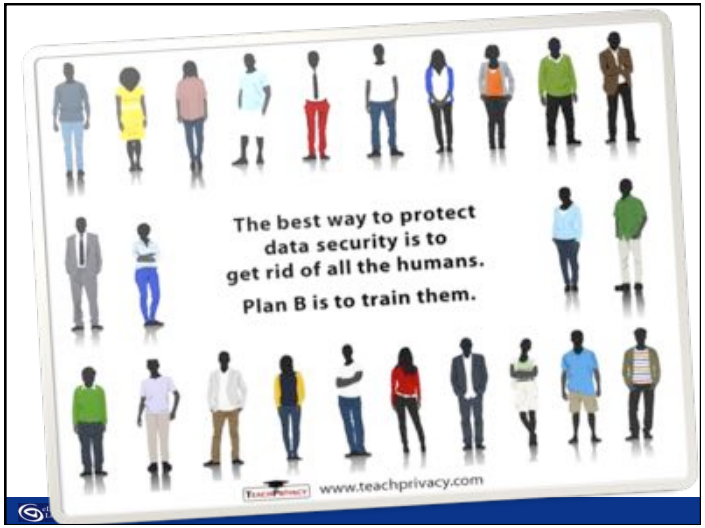
the elephant in the room

- *persoonsgegevens & bijzondere persoonsgegevens*
- *verwerkingsgrondslagen*
- *welbepaald uitdrukkelijk omschreven verzameldoel*
- *verdere verwerking niet onverenigbaar met verzameldoel*
- *vooraf informeren*
- *regels voor profilering*


telecompaper:::

Autoriteit Persoonsgegevens: 3.400 datalekken gemeld

A. *EEN EERSTE INDRUK VAN DE WET MELDPLICHTEN DATALEKKEN*



casus: gebruikersnaam en wachtwoord

Een werknemer geeft een kennis haar gebruikersnaam en wachtwoord die toegang geven tot de klantgegevens van het bedrijf waar zij werkt.

Dit wordt ontdekt. Het bedrijf past het wachtwoord aan. Daarmee heeft de kennis geen toegang meer.

Aan de hand van logbestanden gaat het bedrijf na of de derde daadwerkelijk toegang heeft gehad tot de klantgegevens.

Er kan redelijkerwijs worden uitgesloten dat er door middel van het betreffende account toegang is verkregen tot de gegevens

Melding..?

casus: passwords hack

op pastebin.com wordt een lijst gepubliceerd met 16,5 miljoen wachtwoorden van een populair sociaal netwerk

Melding..?


Update: LinkedIn Confirms Account Passwords Hacked

tweakers Nieuws Reviews Pricewatch Vraag & Aanbod Forum Meer

Gegevens 13.000 kinderen toegankelijk door lek Sinterklaas

Door Joost Schellevis, dinsdag 22 november 2011 10:17, 210 reacties • Feedback

Als gevolg van een be
gegevens van 13.000
2005 werd gebruikt en

De hacker claimt dat hij
kunnen inzien. De publ
gegevens van 13.000 k
online staat", zegt woor
bleek niet beveiligd op
De tool werd, ondanks

De tool gaf kinderen de mogelijkheid om
maar bleek ongewild tot meer in staat. Via
omzeilen, kon een databasedump worden ge
de database opgeslagen. De hacker, die anonie
gecensureerde dump van een tabel met administra
dan die informatie uit de database heeft gedownload. "Dat zou niet netjes zijn", zegt hij.

Volgens de hacker ging het trouwens om een tabel met de naam 'verlanglijstjes', maar Albada zegt dat dergelijke functionaliteit niet op de website van het Sinterklaasjournaal te vinden is. Die functionaliteit zat

De hacker, die anoniem wil blijven, plaatste op het internet een gedeeltelijke en gecensureerde dump van een tabel met administratieve logingegevens. Hij zegt dat hij bewust niet meer dan die informatie uit de database heeft gedownload. "Dat zou niet netjes zijn", zegt hij

casus: e-mail nieuwsbrief

melding...

Wie?	Wanneer?
verantwoordelijke	onverwijld d.w.z. in beginsel
Wat?	binnen 72 uur
inbreuk op	Hoe?
beveiliging van	bij Ap via Meldloket Datalekken
persoonsgegevens	bij data subject (zo-mogelijk individueel)

'datalek'

dus ook een brand in een servercentrum, tenzij er een goede back-up is

inbreuk op beveiliging met tot gevolg:

- *vernietiging, verlies of wijziging, of ongeoorloofde verstrekking van, of ongeoorloofde toegang tot, doorgezonden, opgeslagen of anderszins verwerkte gegevens*
- *hetzij per ongeluk hetzij onrechtmatig*

inbreuk of dreiging?

er is niet uitsluitend sprake van een dreiging of een tekortkoming in de beveiliging maar er heeft zich daadwerkelijk een beveiligingsincident voorgedaan

ransomware…?

daadwerkelijk gevolgen voor de persoonsgegevens:

- *er zijn persoonsgegevens verloren gegaan*
- *niet uit te sluiten dat de gegevens onrechtmatig zijn verwerkt*
- *beveiligings- en herstelmaatregelen onvoldoende om negatieve gevolgen weg te nemen*

twee meldplichten…

(1) melding bij toezichthouder

bij 'aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens'

(2) melding bij datasubject

bij 'waarschijnlijk ongunstige gevolgen voor diens persoonlijke levenssfeer'

?

aanzienlijke kans op ernstige nadelige en/of waarschijnlijk ongunstige gevolgen

gezondheid, etniciteit, sexuele orientatie, politieke voorkeur, geloof, strafrechtelijk, genetisch

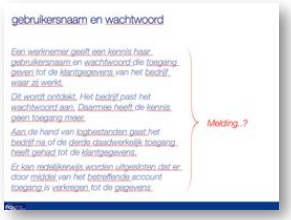
aard van de gegevens

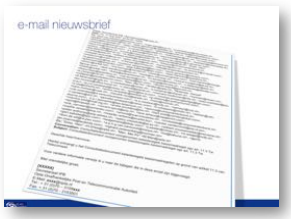
- gevoelige gegevens en financieel-economische gegevens
- stigmatiserings-, uitsluitingsrisico's
- gebruikersnamen, wachtwoorden, identiteitsfraude e.d.
- beroepsgeheim

andere criteria

- omvang van lek (aantal personen of hoeveelheid gegevens)
- ingrijpendheid van o.b.v. gegevens genomen beslissingen
- olievlek (bijv. bij keten-samenwerking)
- encryptie, hashing, remote-wipe, Mobile-Iron etc.

eventueel niet melden aan datasubject bij psychosociale hulpvragen van kinderen buiten medeweten van ouders, bedrijfsovernames of risico van een bank-run





wél melden

- technische storing in ziekenhuis waardoor medische gegevens zijn ingezien door onbevoegden
- kopieën paspoort of rijbewijs, bank- of creditcardnrs, wachtwoorden, enz.
- laptop met onversleutelde financiële gegevens
- tablet met versleutelde gegevens, maar geen back-up
- envelop met creditcardgegevens

niet melden

- foutief geadresseerde brief, ongeopend teruggestuurd
- zoekgeraakte en ongeopend teruggevonden koffer
- verloren ledenadministratie van tennisvereniging
- verpleegkundige 'leent' wachtwoord van co-assistent

bestand..?

B. EEN RAZENDSNELLE INLEIDING IN DE PRIVACYWET, NU EN STRAKS

verwerking van persoonsgegevens

bewerking met betrekking tot persoonsgegevens

zoals raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens, etc.

alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, de betrokkene (of "het datasubject")

bijzondere persoonsgegevens

- *ras of etniciteit*
- *politieke opvattingen*
- *religieuze of levensbeschouwelijke overtuigingen, vakbondlidmaatschap*
- *genetische gegevens en biometrische gegevens (met het oog op de unieke identificatie)*
- *gezondheidsgegevens*
- *seksueel gedrag of seksuele gerichtheid*
- *strafrechtelijke gegevens*

Nieuw! in de Alg Gegevensbescherming (iwtr. 25 mei 2018)

verwerkingsverbod, tenzij…

verantwoordeliJke en bewerker

of: 'verwerkingsverantwoordelijke'
degene die die doel en wijze van verwerking bepaalt

of: 'verwerker'
degene die persoonsgegevens verwerkt ten behoeve van (en onder verantwoordelijkheid van) verantwoordelijke

verwerkingsgrondslagen

- *toestemming (van betrokkene)*
- *uitvoering overeenkomst*
- *naleving wettelijke verplichting*
- *behartiging vitaal belang*
- *publiekrechtelijke taak*
- *gerechtvaardigd belang*

doelbinding

welbepaald, uitdrukkelijke omschreven en gerechtvaardigd

verdere verwerking niet onverenigbaar met verzamel- en verwerkingsdoelen

vooraf informeren

- *identiteit van verantwoordelijke(n)*
- *verzamel- en verwerkings-doeleinden*
- *en al het overige dat nodig is om een zorgvuldige verwerking te waarborgen*

en straks ook: bewaartermijnen, inzagerechten, profilering, internationale doorgifte etc.

profileren

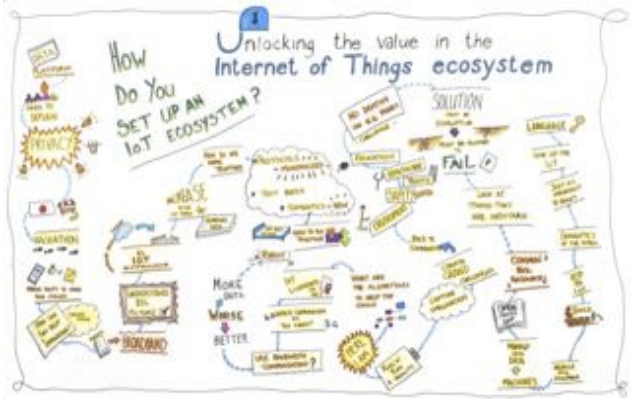
evaluatie (t.b.v voorspellingen) van:
- *beroepsprestaties, econo*
- *gezondheid, persoonlijke*
  interesses,
- *betrouwbaarheid, gedrag,*
  verplaatsing

recht niet te worden onderworpen aan een uitsluitend op profilering gebaseerd besluit met serieuze gevolgen

uitzonderingen
- *uitvoering overeenkomst*
- *wettelijke regeling*
- *toestemming*

C. HOE IOT & DATAFICATION & BIG DATA ONZE PRIVACYWETGEVER UITDAGEN

Internet of Things ("IoT")




theguardian

Forget the internet of things - we need an internet of people

[J. Judge & J. Powles 25 May 2015]

The internet of things is a vision of ubiquitous connectivity, driven by one basic idea: screens are not the only gateway to the ultimate network of networks.

With sensors, code and infrastructure, any object – from a car, to a cat, to a barcode - can become networked. But the question we need to ask is: should they be? And, if so, how?

It's hard to see what this [*ie* IoT] would look like, exactly. But imagining it shouldn't just be delegated to tech companies and opportunists riding the hype cycle.

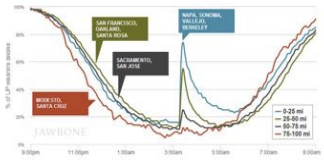
Artists, designers, philosophers, lawyers, psychologists and social workers must be just as involved as engineers and internet users in shaping our collective digital future

[J. Judge & J. Powles 25 May 2015]

every breath you take
every move you make
every bond you break
every step you take…

datafication [*dey•tuh•fi•key•shuh•n*]

a modern technological trend turning many aspects of our life into computerized data and transforming this information into new forms of value [Mayer-Schönberger & Cukier 2013]



Big Data
Big Brother?
Big Business!

Big Data is a generalized, imprecise term that refers to the use of large data sets in data-science and predictive analytics [Mayer-Schönberger & Cukier 2013]

Big Data
Big Bullshit?
Big Bucks!

Big data can be used to identify more general trends and correlations but it can also be processed in order to directly affect individuals [WP29 2013]

…a massive phenomenon that has rapidly become an obsession with entrepreneurs, scientists, governments and the media [Financial Times 2014]

unprecedented computational power and sophistication make possible unexpected discoveries, innovations, and advancements in our quality of life [Whitehouse 2014]

TARGET

ROLLS ROYCE

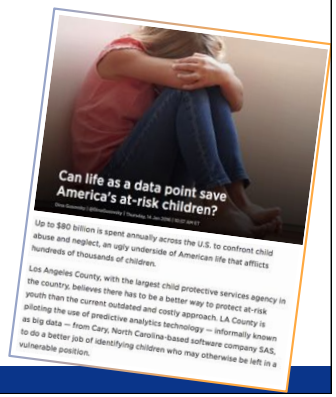
Probleemgezin kost 40.000 euro

Systeem Risico Indicatie (SyRI) is een instrument waarmee gegevensbestanden van gemeenten, UWV, SVB, Inspectie SZW en Belastingdienst kunnen worden gekoppeld ten behoeve van de bestrijding van fraude op het terrein van de sociale zekerheid en de inkomensafhankelijke regelingen, de belasting- en premieheffing en de arbeidswetten

sinds 2006 in gebruik onder de aanduiding 'Black Box'..

De aanleiding voor de uithuisplaatsingen was niet een calamiteit, zelfs geen incident, maar een risicoprofiel: moeder was getraumatiseerd door een oorlogsverleden in een ander land, en vader gebruikte trouw medicijnen voor een ggz-diagnose, waardoor de ziekte onder controle was.

Justine Pardoen 31 januari 2015 www.ouders.nl



The main advantage of Big Data is that it can reveal patterns between different sources and data sets, enabling useful insights

The use of Big Data by the top 100 EU manufacturers could lead to savings worth €425 billion, and by 2020, Big Data analytics could boost EU economic growth by an additional 1.9%, which means a GDP increase of €206 billion

[EC The EU Data Protection Reform and Big Data *Factsheet* April 2015]

correlatie & causaliteit

in a big-data age most innovative secondary uses [of data] haven't been imagined when the data is first collected. How can companies provide notice for a purpose that has yet to exist? How can individuals give informed consent to an unknown…?

[Mayer-Schönberger & Cukier 2013]

free, specific, informed and unambiguous 'opt-in' consent would almost always be required, otherwise further use cannot be considered compatible

[WP29 2013]

persoonsgegevens &
bijzondere gegevens

•

verwerkingsgrondslagen

•

doelbinding &
dataminimalisatie

•

vooraf informeren

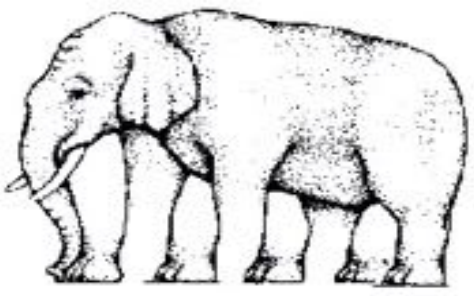
•

profilering

•

etc.

personalisering…
stigmatisering…
discriminatie…
onschuldpresumptie…
etc.



g.j.zwenne@law.leidenuniv.nl