

@zwne

LEIDEN REVISITED | 2 SEPTEMBER 2016

actuele thema's op het gebied van privacy en
bescherming van persoonsgegevens en
cybersecurity

prof. mr. Gerrit-Jan Zwenne



Universiteit Leiden



gisteren in het
nieuws...



Programma

A. laatste ontwikkelingen bij de
privacytoezichthouder

'Cbq' heet nu 'Ap'
en meer...

B. van SafeHarbor naar
PrivacyShield

de houdbaarheid van
de nieuwe oplossing

C. de meldplicht datalekken

veel opwindend, maar
nog beperkte impact

D. opmerkingen over bulk-
aftappen en terughacken

twee controversiële
wetsvoorstellen

E. Algemene Verordening
Gegevensbescherming

- wat verandert er? wat niet? en
wat betekent dat?
- gezocht: functionaris voor de
gegevensbescherming (M/V)

de werkgelegenheids-
effecten van de nieuwe
wetgeving



A. DE LAATSTE ONTWIKKELINGEN BIJ DE PRIVACYTOEZICHTHOUDER

Artikel 51 Wet bescherming persoonsgegevens

- 4. Het College wordt in het
maatschappelijk verkeer aangeduid
als: Autoriteit persoonsgegevens.



sluit aan bij Europese ontwikkelingen en maakt
einde aan verwarring met het Centraal Planbureau
(CPB)

markeert een fase waarin we toegroeien naar een
in Europees verband verdergaand geharmoniseerd
systeem van bescherming van persoonsgegevens



Een bestuurlijke boete van €820.000

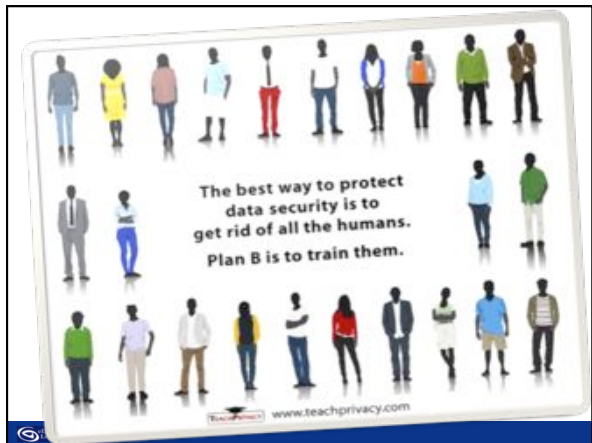
nog niet opgelegd (maar we houden hoop!)



normen	bepalingen
zorgvuldige verwerking, welbepaald gerechtvaardigd verzameldoel en doelbinding, bewaartermijnen, geen bovenmatige verwerking...	art. 6 tot en met 8, 9, 10, eerste lid, 11 t/m 12
beveiligingsverplichtingen (incl. meldplicht datalekken)	art. 13, 34a
verwerkingsverbod bijzondere gegevens (gezondheid, etniciteit, strafrechtelijk etc.) en BSN	art. 16 en 24
informatieplichten, inzage en correctierechten, opt-out-rechten bij direct marketing en profilering	art. 33, 34, 35, 36, 38 t/m 40, 41 en 42
internationale gegevensdoorgifte	art. 76 t/m 78
medewerking aan handhavingsonderzoeken	art. 5:20 Awb



B. MELDPlicht 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..?



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 beveiligingslek zijn gegevens van 13.000 kinderen in 2005 werd gebruikt en...

De hacker claimt dat hij de gegevens van 13.000 kinderen online staat", zegt woordvoerder van de politie. De tool werd, ondanks dat het mogelijk is om de gegevens in te sturen en kleurplaten te downloaden, maar bleek ongewild tot meer in staat. Via andere naam, e-mailadres en leeftijd werden in de database opgeslagen. De hacker, die anoniem blijft, plaatste op het internet een gedeeltelijke en gecensureerde dump van een tabel met administratieve loggegevens. Hij zegt dat hij bewust niet meer 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 de informatie 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 loggegevens. 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 binnen 72 uur

Wat? Hoe?
 inbreuk op beveiliging van persoonsgegevens bij Ap via Meldloket Datalekken bij data subject (zo-mogelijk individueel)

'datalek'

duis 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 er 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, seksuele oriëntatie, 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 ketensamenwerking)
- encryptie, hashing, remote-wipe, Mobile-Iron etc.

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



gebruikersnaam en wachtwoord

Een website heeft een kennisbaar gebruikersnaam en wachtwoord die toegang geeft tot de klantgegevens, en het bedrijf heeft al eens...

De account overheid: Het bedrijf heeft het wachtwoord van de klantgegevens, en het bedrijf heeft de klantgegevens...

Als de klant een klantgegevens heeft het bedrijf zou of de klantgegevens toegang heeft, zodat het de klantgegevens...

Er zijn verschillende soorten gegevens die er door vallen, en het bedrijf heeft account gegevens of verstuurd het de gegevens.

Melding.?

passwords hack

no password.com heeft een lijst gepubliceerd met 18,5 miljoen wachtwoorden van een populair sociaal netwerk

Melding.?

Update LinkedIn Confirms Account Passwords Hacked

lekkers

Gegevens 13.000 kinderen toegankelijk door lek Sinterklaas

De hacker die anoniem wil blijven, zette op het internet een gedetailleerde en grootschalige dump van een tabel met administratieve gegevens. Hij zegt dat hij bewust niet meer dan de informatie uit de database heeft gelekt: "Dat zou niet reges zijn", zegt hij.

Melding.?

e-mail nieuwstrial

Document showing email content.

wél melden

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

niet melden

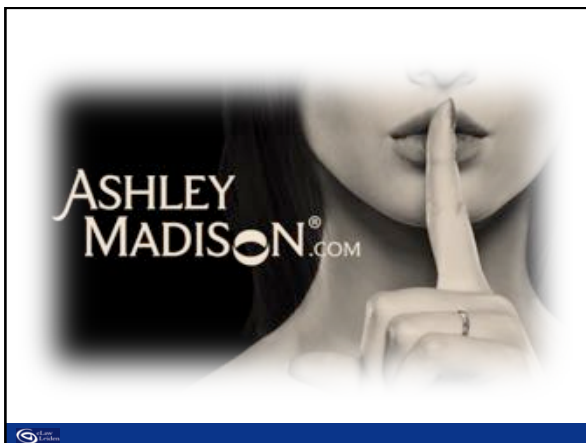
- foutief geadresseerde brief, ongeopend teruggestuurd
- zoekgeraakte en ongeopend teruggevonden koffer
- verloren ledenadministratie van tennisvereniging
- verpleegkundige "leent" wachtwoord van co-assistent

bestand.?



straks onder 'de verordening' ..?

	Art. 33(1) en 34(1) AVG	Art. 34a(1) en (2) Wbp
melding bij toezicht-houder	tenzij onwaarschijnlijk dat er een risico is voor de rechten en vrijheden natuurlijke personen	aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens
melding bij betrokkene	waarschijnlijk hoog risico voor rechten en vrijheden van natuurlijke personen	waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer



C. PRIVACY SHIELD



van Safe Harbor naar PrivacyShield

Facebook, Google, Amazon etc. verwerken veel persoonsgegevens van EU-ingezetenen

EU privacyregels verbieden doorgifte van die persoonsgegevens vanuit unie naar VS, tenzij...

Hof van Justitie EU: safe harbor vernietigd want niet passend.

gebruik wordt gemaakt van een instrument dat een 'passend beschermingsniveau' biedt, zoals

- modelcontracten (zg. "SCC's")
- binding corporate rules
- safe harbor self certificering
- toestemming, etc.

EU US PrivacyShield



PrivacyShield

- self-certification with monitoring by U.S. Dep. of Commerce
- regularly updated list of self-certified companies
- an ombudsperson mechanism
- no mass and indiscriminate collection of personal data, unless...

WP29 would have expected stricter guarantees concerning the independence and the powers of the ombudsperson
 WP29 regrets the lack of concrete assurances that such practice does not take place.

"Adherence to these Principles may be limited: [...] to the extent necessary to meet national security, public interest, or law enforcement requirements..."



HJEU 6 oktober 2015 vs PrivacyShield

onaanvaardbaar is dat:

- persoonsgegevens worden bewaard, zonder dat onderscheid wordt gemaakt op basis van het nagestreefde doel; én
- zonder een objectief criterium ter begrenzing van de toegang van bevoegde autoriteiten tot de gegevens en het gebruik ervan voor specifieke doeleinden, die strikt beperkt zijn, etc; én
- geen beroepsmogelijkheid voor de justitiabele om inzage in de hem betreffende persoonsgegevens te verkrijgen, of rectificatie of verwijdering etc.

én wat te zeggen van de Standard Contractual Clauses ("SCC's")...?



D. 'TERUGHACK-VOORSTEL' EN 'BULK-AFTAPPEN'



'terughacken'

- verdenking van misdrijf als bedoeld in art. 67 lid 1 WvSr
- een ernstige inbreuk op de rechtsorde, gezien de aard of de samenhang met andere door de verdachte begane misdrijven
- en indien het onderzoek dit dringend vordert

misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaren of meer is gesteld; en verder...

dan kan OvJ bevelen dat een daartoe aangewezen opsporingsambtenaar binnendringt in een geautomatiseerd werk van de verdachte....

Artikel 120ter, eerste lid, TK 34372, nr. 1.



hoe erg is het..?

- voorzienbaarheid van de privacyinbreuk...?
- wat wij kunnen, kunnen anderen ook..!
- voldoende kennis bij politie?
- worden kwetsbaarheden verholpen?
- misbruik

Hollywood en Pirate Bay
VS en Wikileaks
Iran en Diginotar



'ongericht onderzoek in kabelgebonden infrastructuur'

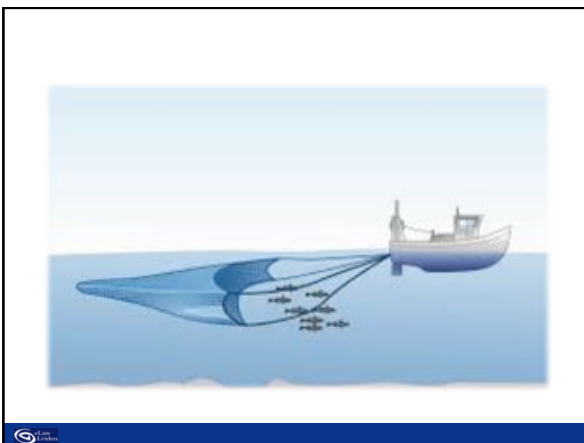
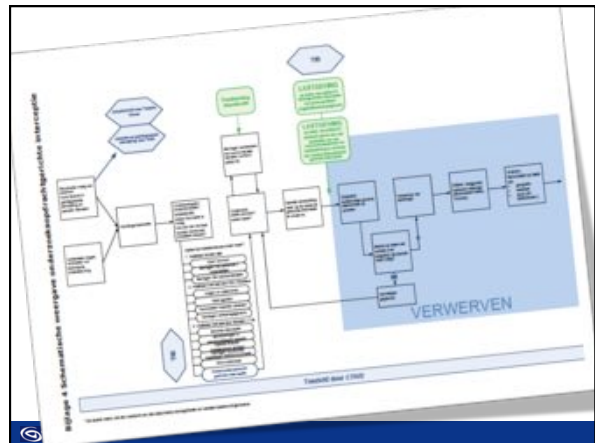
- onderzoeksoopdrachtgericht aftappen, ontvangen, opnemen etc. van elke vorm van telecommunicatie of gegevensverdracht
- alleen met toestemming van minister

- *verlengd voor een periode van ten hoogste een jaar*
- *kan telkens op een daartoe strekkend verzoek worden verlengd voor zelfde periode*

'geen zorgen over kosten'

De rijksoverheid neemt de kosten van de modernisering van de bevoegdheden op zich. [...]

De investeringen die de telecomsector moet doen, worden naar redelijkheid vergoed. De sector hoeft zich geen zorgen te maken over kosten of concurrentienadeel.



E. EEN NIEUWE (EUROPESE) PRIVACYWET:
DE ALGEMENE VERORDENING GEGEVENS-
BESCHERMING

Algemene Verordening Gegevensbescherming

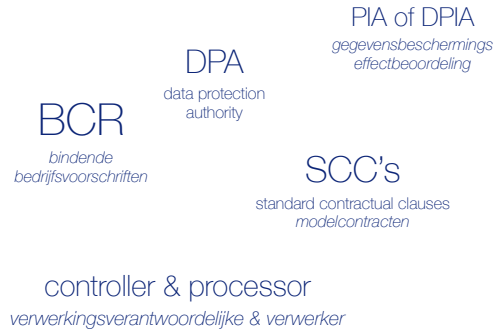
veel van hetzelfde, maar ook nieuwe rechten en verplichtingen en wellicht ook meer bescherming

- verplichtingen voor verwerkingsverantwoordelijken én verwerkers
 - recht op beperking van verwerking, recht op vergetelheid, gegevensoverdraagbaarheid, etc.
 - gegevensbeschermingseffectbeoordeling en veel andere formaliteiten
 - boetes van 2-4 procent wereldwijde omzet
- én serieuze werkgelagenheidseffecten
vaak verplichte 'functionaris voor de gegevensbescherming'

afkortingen: 'AVG' of 'AVGB' of desnoods 'GDPR', maar niet: 'EPV'!



jargon...



lost in translation

Artikel 23

1. De reikwijdte van de verplichtingen en rechten als bedoeld in de artikelen 12 tot en met 22 en artikel 34, alsmede in artikel 5 kan, voor zover de bepalingen van die artikelen overeenstemmen met de rechten en verplichtingen als bedoeld in de artikelen 12 tot en met 20, worden beperkt door middel van Unierechtelijke of lidstaatrechtelijke bepalingen die op de verwerkingsverantwoordelijke of de verwerker van toepassing zijn ...

lost in translation

Artikel 23

1. De reikwijdte van de verplichtingen en rechten als bedoeld in de artikelen 12 tot en met 22 en artikel 34, alsmede in artikel 5 kan, voor zover de bepalingen van die dat artikelen overeenstemmen met de rechten en verplichtingen als bedoeld in de artikelen 12 tot en met 20, kan worden beperkt door middel van Unierechtelijke of lidstaatrechtelijke bepalingen die op de verwerkingsverantwoordelijke of de verwerker van toepassing zijn ...

Article 23

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22...

lost in translation (..?)

overw. 59, 85, art. 12(3), art. 16, art. 34(1), art. 61(2), art. 64(4) en (5), art. 65(5) en (6) overw. 86, 87, art. 17(1), art. 33(1) en (2), art. 70(1)(g)

'without undue delay' 'onverwijld' of 'zonder onredelijke vertraging'
'without delay' 'onverwijld'

overw. 127, art. 5(1)(d), 12(4), 51(4), 56(3), 60(3), 62(2), 65(5), 66(1), 83(9), 84(2), 85(3), 88(3), 90(2)



tien veranderingen

geen parlementaire geschiedenis maar 173 overwegingen en allerlei concept-versies

1. géén richtlijn maar een verordening
2. handvol nieuwe begrippen
3. vergrote materiële werkingsfeer (?)
4. uitbreiding territoriale werkingsfeer
5. meer verplichtingen voor bewerkers (of: verwerkers)
6. veel meer rechten voor betrokkenen
7. nogal wat formaliteiten, zoals PIA's, DPO's etc.
8. meer instrumenten voor internationale doorgifte
9. iets andere uitgangspunten bij de meldplicht datalekken
10. substantiële boetes



géén nationale privacywetten, maar één verordening, in verschillende (soms inhoudelijk afwijkende) taalversies

1. géén richtlijn maar een verordening

2. handvol nieuwe begrippen

3. vergrote materiële werkingsfeer (?)

4. uitbreiding territoriale werkingsfeer

5. meer verplichtingen voor bewerkers (of: verwerkers)

6. veel meer rechten voor betrokkenen

7. nogal wat formaliteiten, zoals PIA's, DPO's etc.

8. meer instrumenten voor internationale doorgifte

9. iets andere uitgangspunten bij de meldplicht datalekken

10. substantiële boetes


bedoeling: minder fragmentatie

minder minder...?




1. géén richtlijn maar een verordening
2. handvol nieuwe begrippen
3. vergrote materiële werkingsfeer (?)
4. uitbreiding territoriale werkingsfeer
5. meer verplichtingen voor bewerkers (of: verwerkers)
6. veel meer rechten voor betrokkenen
7. nogal wat formaliteiten, zoals PIA's, DPO's etc.
8. meer instrumenten voor internationale doorgifte
9. iets andere uitgangspunten bij de meldplicht datalekken
10. substantiële boetes

- gegevensbeschermingseffectbeoordeling
- documentatie- en registerplichten
- aanwijzen functionaris voor de gegevensbescherming
- certificering, gedragscodes, model gegevensdoorgiftecontracten, etc.



gegevensbeschermings-effectbeoordeling

dat wil zeggen: een systematische beschrijving van beoogde verwerkingen en doeleinden:

wanneer vereist?

- profilering met rechtsgevolgen voor natuurlijke personen of die natuurlijke personen wezenlijk treft;
- grootschalige verwerking van bijzondere persoonsgegevens
- stelselmatige grootschalige monitoring van openbaar toegankelijke ruimten

- gerechtvaardigde belangen van verwerkingsverantwoordelijke en beoordeling van noodzaak en evenredigheid
- beoordeling van risico's voor de rechten en vrijheden van betrokkenen
- beoogde maatregelen om de risico's aan te pakken
- maatregelen om compliance aan te tonen (accountability)



Tja...




functionaris voor de gegevensbescherming of "FG"

verplicht voor

- overheden
- regelmatige en stelselmatige observatie op grote schaal
- grootschalige verwerking van bijzondere gegevens

taken:

- informeren en adviseren over AVG-verplichtingen
- toezicht houden op de naleving van die verplichtingen
- adviseren over DPIA's
- contact onderhouden met Ap
- samenwerken met Ap

vereisten:

- professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming, en
- vermogen om zijn taken te vervullen.



oneerlijke handelspraktijken...?



@zwnne

g.j.zwenne@law.leidenuniv.nl

DANK VOOR UW AANDACHT!