MINISTERIE VEILIGHEID & JUSTITIE
LUNCHLEZING 11 OKTOBER 2016

Van Wbp naar AVG in minder dan 60 minuten

Universiteit Leiden
The Netherlands

eLaw Leiden

tien veranderingen

1. géén richtlijn maar een verordening
2. handvol nieuwe begrippen
3. vergrote materiële werkingssfeer (?)
4. uitbreiding territoriale werkingssfeer
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

bedoeling: minder fragmentatie

minder minder…?

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 artikel~~en~~ overeenstem~~t~~men 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)

'without undue delay'
'without delay'

'onverwijld' of 'onverwijld'

overw. 86, 87, art.17(1), art. 33(1) en (2), art. 70(1)(g)

'zonder onredelijke vertraging'

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),

1. géén richtlijn maar een verordening
2. handvol nieuwe begrippen
3. vergrote materiële werkingssfeer (?)
4. uitbreiding territoriale werkingssfeer
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

'data subject' means an identified natural person or a natural person who can be identified or ~~singled out~~, directly or indirectly, alone or in combination with associated data…

1. geen richtlijn maar een verordening
2. handvol nieuwe begrippen
3. vergrote materiële werkingssfeer (?)
4. uitbreiding territoriale werkingssfeer
5. meer verplichtingen voor bewerkers (of: verwerkers)
6. veel meer rechten voor betrokkenen
7. nogal wat formaliteiten, zoals PIA's, DPO's etc.
10. substantiële boetes

(26) […] To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.

(26) […] Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken.

(26) […] To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.

1. géén richtlijn maar een verordening
2. handvol nieuwe begrippen
3. vergrote materiële werkingssfeer (?)
4. uitbreiding territoriale werkingssfeer
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

- *aanwijzen vertegenwoordiger*
- *verplichtingen m.b.t. gebruik van sub-bewerkers*
- *bijhouden verwerkingsregister*
- *samenwerking met toezichthouder*
- *informeren van verantwoordelijke bij beveiligingsinbreuk*
- *gegevensbeschermingseffectbeoordeling (?) en voorafgaand onderzoek*
- *functionaris voor de gegevensbescherming*
- *regels m.b.t. doorgifte naar derde landen*
- *aansprakelijk t.o.v. betrokkenen*
- *…*

verwerkers- of bewerkersovereenkomst

- *onderwerp en duur, aard en doel, van verwerking, soort persoonsgegevens, categorieën van betrokkenen, rechten en verplichtingen van verwerkingsverantwoordelijke;*
- *instructiebevoegdheid verwerkingsverantwoordelijke (schriftelijk)*
- *vertrouwelijkheid en beveiliging, vereisten m.b.t. sub-verwerkers*
- *medewerking t.b.v. voldoen aan rechten van betrokkenen*
- *accountability & audits*

1. géén richtlijn maar een verordening
2. handvol nieuwe begrippen
3. vergrote materiële werkingssfeer (?)
4. uitbreiding territoriale werkingssfeer
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

- *gegevensbeschermingeffectbeoordeling*
- *documentatie- en registerplichten*
- *aanwijzen functionaris voor de gegevensbescherming*
- *certificering, gedragscodes, model gegevensdoorgifte-contracten, etc.*

gegevensbeschermings-effectbeoordeling

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

- *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)*

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*

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 handelspraktijk…?

1. géén richtlijn maar een verordening
2. handvol nieuwe begrippen
3. vergrote materiële werkingssfeer (?)
4. uitbreiding territoriale werkingssfeer
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

	Art. 33(1) en 34(1) AVG	Art. 34a(1) en (2) Wbp
melding bij toezichthouder	tenzij onwaarschijnlijk dat er een risico is voor de rechten en vrijheden van 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

3. vergrote materiële werkingssfeer (?)
4. uitbreiding territoriale werkingssfeer
5. meer verplichtingen voor bewerkers (of: verwerkers)
8. meer instrumenten voor internationale doorgifte
9. iets andere uitgangspunten bij de meldplicht datalekken
10. substantiële boetes

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..?

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 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

e-mail nieuwsbrief

melding...

Wie?

verantwoordelijke

Wat?

inbreuk op beveiliging van persoonsgegevens

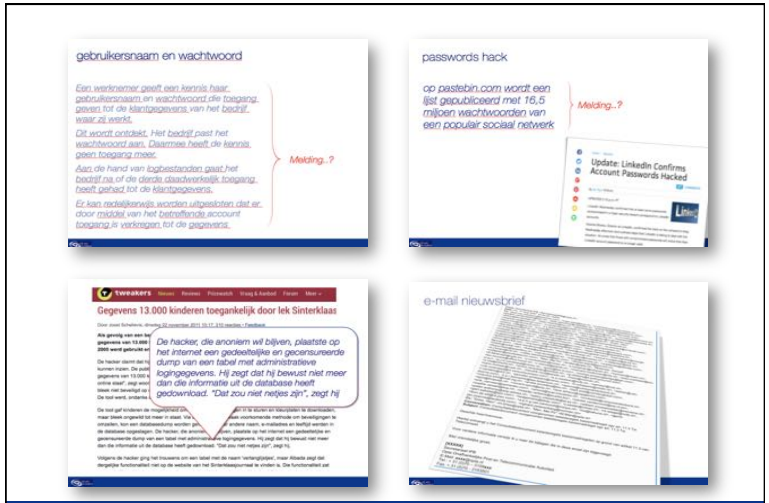
Wanneer?

onverwijld d.w.z. in beginsel binnen 72 uur

Hoe?

bij Ap via Meldloket Datalekken

bij data subject (zo-mogelijk individueel)



g.j.zwenne@law.leidenuniv.nl