
@zwnne
De Algemene Verordening Gegevensbescherming
Meldplicht datalekken
5 april 2016
Wolters Kluwer


The best way to protect data security is to get rid of all the humans.
Plan B is to train them.
www.teachprivacy.com


Vanaf 1 januari 2016
Stb. 2015, 230
Meldplicht datalekken
Uitbreiding bestuurlijke boetebevoegdheid Cbp
Hoofdstuk 9. Toezicht
Paragraaf 1. Het College bescherming persoonsgegevens
Artikel 51
Wolters Kluwer

Wolters Kluwer

personal data breach

- *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*

GDPR

inbreuk i.v.m. persoonsgegevens

- *een inbreuk op de beveiliging met tot gevolg…*
- *vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig*

AVG

Wolters Kluwer

Meldplicht datalekken

Melding bij toezichthouder

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

Melding bij betrokkene

- bij 'waarschijnlijk ongunstige gevolgen voor diens persoonlijke levenssfeer'

Art. 34a Wbp

Melding bij toezichthouder

- 'unless the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals'

Melding bij betrokkene

- 'likely to result in a high risk [for] the rights and freedoms o individuals'

Art. 31-32 AVG

Wolters Kluwer

melding…

Wie? verantwoordelijke

Wat? inbreuk op beveiliging van persoonsgegevens

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

Hoe? Meldloket Datalekken (Ap) en zo-mogelijk individueel (betrokkenen)

Wolters Kluwer

'inbreuk op beveiliging van persoonsgegevens'

gegevens betreffende geïdentificeerde of identificeerbare natuurlijke personen

Wél: werknemers, ambtenaren, studenten, scholieren, zzp-ers, contactpersonen, patiënten, consumenten, kinderen, volwassenen, leden, treinreizgers, automobilisten, etc.

Niet: rechtspersonen, bedrijven, overledenen

- *passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.*
- *maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.*
- *maatregelen moeten onnodige verzameling en verdere verwerking van persoonsgegevens voorkomen*

Wolters Kluwer

beveiligingsmaatregelen

preventieve maatregelen
- voorkomen dat een dreiging leidt tot een incident

detectieve maatregelen
- vaststellen dat er een incident is geweest

repressieve maatregelen
- beperken van negatieve gevolgen van het incident

herstelmaatregelen
- herstel van negatieve gevolgen

dreiging

beveiligings-incident

gevolgen

correctieve maatregelen
- reparatie van tekortkomingen in de beveiliging

Wolters Kluwer

inbreuk

- er is niet uitsluitend sprake van een dreiging of een tekortkoming in de beveiliging maar er heeft zich daadwerkelijk een beveiligingsincident voorgedaan
- de preventieve maatregelen waren niet toereikend om dit te voorkomen.

verloren USB-stick
gestolen laptop
sql-hack
malware
ransomware
brand in datacentrum

- er zijn daadwerkelijk gevolgen voor de verwerkte persoonsgegevens:
- er zijn persoonsgegevens verloren gegaan
- niet uit te sluiten dat er gegevens onrechtmatig zijn verwerkt
- de getroffen repressieve maatregelen en de herstelmaatregelen waren onvoldoende om negatieve gevolgen geheel weg te nemen

Wolters Kluwer

datalek..?

Wolters Kluwer

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..?

Wolters Kluwer

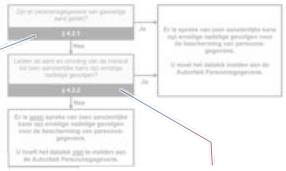
casus: accounts passwords hack

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

Wolters Kluwer

Melding bij Ap

- een (aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoons-gegevens



- *bijzondere gegevens (art. 16)*
- *financiële of economische gegevens*
- *stigmatiserings- c.q. uitsluitingsrisico's*
- *gebruikersnamen, wachtwoorden, identiteitsfraude e.d.*
- *beroepsgeheim, DNA-gegevens*

- *omvang van lek (aantal personen en/of hoeveelheid gegevens)*
- *ingrijpendheid van o.b.v. gegevens genomen beslissingen*
- *olievlek (bijv. ketensamenwerking)*

Wolters Kluwer

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

bestand i.d.z.v. art. 1(c) Wbp…?

Niet melden

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

Wolters Kluwer

'onverwijld'

wanneer

- vanaf moment van bekend worden van datalek
- bekend bij verantwoordelijke zelf
- of bekend bij bewerker(!)

idem art. 31(1) GDPR

zonder onnodige vertraging

- zo mogelijk niet later dan 72 uur na ontdekking
- maar later mag als dat kan worden uitgelegd

Wolters Kluwer

melding aan betrokkene

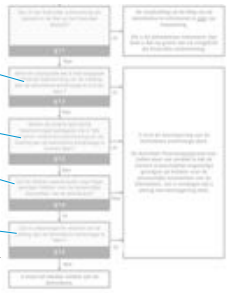
'waarschijnlijk ongunstige gevolgen voor diens persoonlijke levenssfeer'

(art. 34a(6) Wbp) encryptie, hashing beschermt tegen onbevoegde kennisneming (niet tegen vernietiging of aantasting)

bijv. tijdige remote wipe (Mobile-Iron)

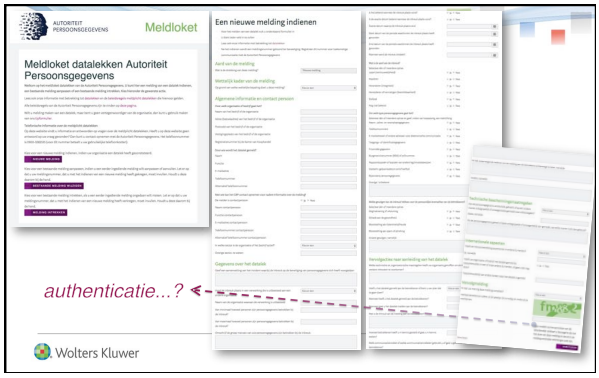
risico op schade voor betrokkenen, bijv. identiteitsdiefstal, chantage, aantasting eer en goede naam; bijzondere gegevens of anderzins gevoelige gegevens

psychosociale hulpvragen van kinderen buiten medeweten van ouders bedrijfsovername, bank-run



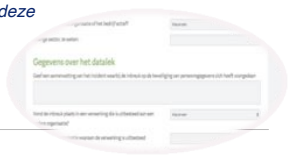
Wolters Kluwer

Wolters Kluwer



pro forma melding (tekstsuggestie)

"Er is naar oordeel van verantwoordelijke géén sprake van een inbreuk op de beveiliging van de persoonsgegevens. Voor het geval dat daarover verschil van inzicht kan bestaan wordt zekerheidshalve, en zonder aanvaarding van enige gehoudenheid daartoe, deze melding gedaan."



Wolters Kluwer


g.j. zwenne@law.leidenuniv.nl
@zwnne
Wolters Kluwer