@zwnne

Meldplichten en datalekken

Prof. mr. G-J. (Gerrit-Jan) ZWENNE | Leiden

Universiteit Leiden

eLaw Leiden

beveiligingsplicht

- 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
- de maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen

meldplichten

Wet bescherming persoonsgegevens
Art. 34a
wie: verantwoordelijke
wat: inbreuk op beveiliging van persoonsgegevens
aan: Autoriteit persoonsgegevens en betrokkene

Wet financieel toezicht
Art. 3:10(3); art. 4.11(4)
wie: financiële instellingen, banken enz.
wat: incident m.b.t. integriteit, vertrouwen etc.
aan: De Nederlandse Bank

Telecommunicatiewet
Art. 11a.2
wie: aanbieders openbare elektronische communicatie
wat: inbreuk op beveiliging en verlies integriteit
aan: De Minister (d.w.z. Agentschap telecom)

Algemene Verordening Gegevensbescherming
Art. 32
wie: verantwoordelijke
wat: inbreuk op beveiliging van persoonsgegevens
aan: Autoriteit persoonsgegevens en betrokkene

EIDAS-verordening
Art. 3:10(3); art. 4.11(4)
wie: verleners van vertrouwensdiensten
wat: inbreuk op beveiliging en verlies integriteit
aan: ACM (Ap, NCSC)

Wet gegevensverwerking en meldplicht cybersecurity
Art. 8
wie: vitale aanbieders (aan te wijzen bij Besluit meldplicht cybersecurity)
wat: inbreuk op beveiliging en verlies integriteit
aan: NCSC

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'

Wie?
verantwoordelijke

Wat?
inbreuk op beveiliging van persoonsgegevens

Wanneer?
onverwijld d.w.z. in beginsel binnen 72 uur na bekend worden van het datalek

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

art. 34a (1) en (2) Wbp

‘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*

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

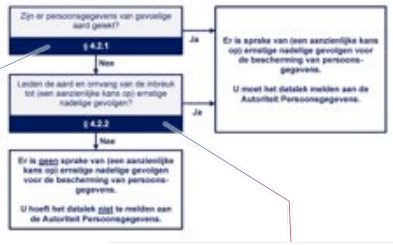
daadwerkelijk gevolgen voor de persoonsgegevens:

- *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*

Melding bij Ap

Melding bij toezichthouder

(aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens



- *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)*

'onverwijld'

vanaf moment van bekend worden van datalek

- door verantwoordelijke zelf
- door 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

melding aan betrokkene

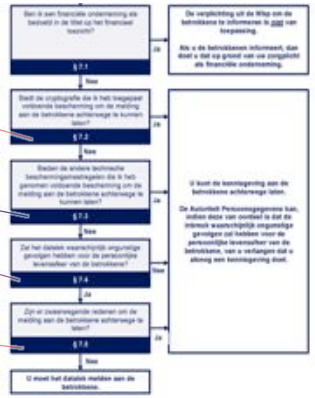
'waarschijnlijk ongunstige gevolgen voor diens persoonlijke levenssfeer'

(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



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…?

Níet melden

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

Van: Edward de Lange^Summit Legal
Datum: 25 maart 2016 09:04:25 CET
Aan: : christiaan.alberdingkthijm@bureaubrandeis.com; wieke.vanangeren@brinkhof.com; juliette.van.balen@ipadvocaat.nl; c.beijer@vandiepen.com; robertboekhorst@vbk.nl; bieneke.braat@legaltree.nl; dtbrink@plp.nl; gijsbert@wenckebach.com; b.cordemeyer@cordemeyerslager.nl; dekhuijzen@whitebridge.nl; don@gmsadvocaten.nl; n.vanduuren@declercq.com; linda.eijpe@skoopadvocaten.nl; eijsvogelsf@hoyngmonegier.com; peter.eijsvoogel@allenovery.com; Marc.Elshof@boekel.com; essen@solv.nl; irene.feenstra@projectmoore.com; joachim.fleury@cliffordchance.com; m.gerritsen@vandiepen.com; Marjolein Geus; lgdegier@degierstam.nl; serge.gijrath@commitzlaw.com; tycho.degraaf@nautadutilh.com; hardenbroek@delissenmartens.nl; Ruprecht Hermans - External; taco.huizinga@thelawfactor.nl; Friederike.vanderJagt@Stibbe.com; dejong@louwersadvocaten.nl; herald.jongen@allenovery.com; jonker@van-doorne.com; kerkvoorden@solv.nl; r.ketting@nysingh.nl; jeroen.koeter@projectmoore.com; konings@zennlaw.nl; korpershoek@louwersadvocaten.nl; koster@abc-legal.com; nynke.koster@nklc.nl; Kramer@boelszanders.nl; judica.krikke@stibbe.com; info@wiseman.nl; kubbenga@kubbenga-advocatuur.nl; arend.lagemaat@lagemaatadvocatuur.nl; edward.delange@summitlegal.nl; Jeroen Van Der Lee; elievens@planet.nl; ambition@ziggo.nl; Joost.Linnemann@kvdl.nl; louwers@louwersadvocaten.nl; vanmanenj@hoyngmonegier.com; alfred.meijboom@kvdl.nl; dj@micta.nl; lmoerel@mofo.com; joost.mosselman@dvan.nl; f.mutsaerts@banning.nl; Roelien van Neck; mnoordermeer@nexavelo.nl; joost.vanooijen@akzonobel.com; dinant.oosterbaan@itlawyers.nl; m.den.Otter@ojw-advocaten.nl; tjeerd.overdijk@vondst-law.com; vandepas@dirkzwager.nl; vanderperk@parickadvocatuur.nl; polo.vanderputt@vondst-law.com; bart.vanreeken@debrauw.com; rijnveld@rijnveldlaw.nl; reinout.rinzema@ventouxlaw.com; l.ritzema@live.nl; sars@csadvocaten.nl; mw.scheltema@pelsrijcken.nl; regine.scholten@rechtspraktijkscholten.nl; info@sitelaw.nl; christian.vanseeters@projectmoore.com; wouter.seinen@bakermckenzie.com; j.slager@cordemeyerslager.nl; otto.sleeking@kvdl.nl; sprey@vwsadvocaten.nl; hendrik.struik@cms-dsb.com; stuurman@van-doorne.com; jaap.tempelman@cliffordchance.com; melissa.theunissen@bayer.com; thole@van-doorne.com; m.topsarneel@ploum.nl; lieneke.viergever@projectmoore.com; eliane.devilder@brinkhof.com; eva.visser@projectmoore.com; volgenant@boekx.com; t.de.weerd@houthoff.com; wbettink@xs4all.nl; weij@solv.nl; caspar@wenckebach.com; reinoud.westerdijk@kvdl.nl; p.vdwiel@telfort.nl; hugo@wijnandsadvocaat.nl; joris.willems@dlapiper.com; patrick.wit@kvdl.nl; dewit@louwersadvocaten.nl; avanderwolk@mofo.com; nicole.wolters.ruckert@kvdl.nl; dzieren@plp.nl; roelof.zomer@zomeradvocaten.com; serge.zwanen@loyensloeff.com; Gerrit-Jan Zwenne
Onderwerp: FW: IIR Congres Implementatie Europese Privacy Verordening - 20 april 2016

Beste (aspirant)leden,

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.

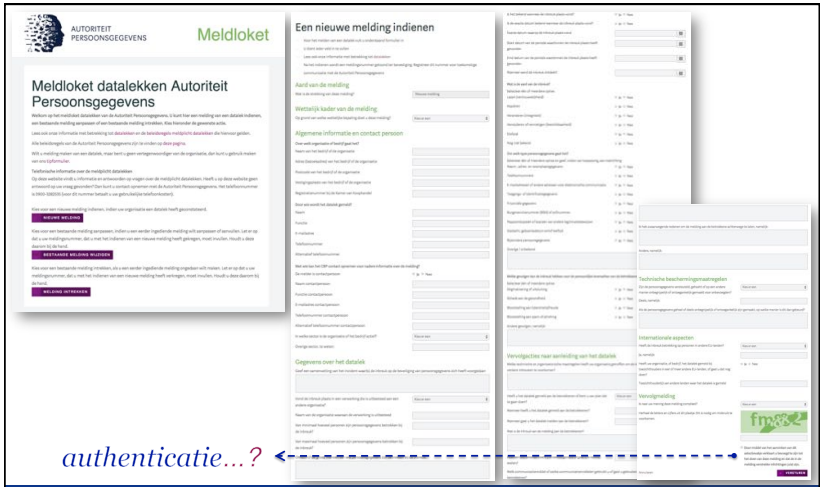
Er kan redelijkerwijs worden uitgesloten dat er door middel van het betreffende account toegang is verkregen tot de gegevens.

Melding..?

accounts passwords hack

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

Melding..?

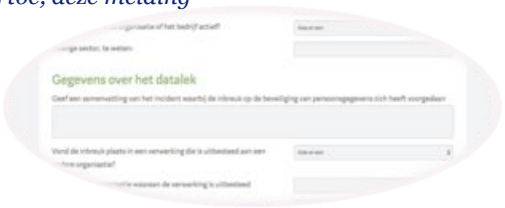


authenticatie…?

vooralsnog alleen voor organisaties aangesloten bij de Pensioen-federatie, Verbond van Verzekeraars, de Nederlandse Vereniging van Banken alsmede voor een beperkt aantal andere organisaties….

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."



@zwenne

vragen?

g.j.zwenne@law.leidenuniv.nl

Universiteit Leiden

eLaw Leiden