@zwnne

Meldplichten en datalekken

Prof. mr. G-J. (Gerrit-Jan) ZWENNE | 28 april 2022 | Leiden

Universiteit Leiden

eLaw Leiden

1

AUTORITEIT PERSOONSGEGEVENS

Rapportage Datalekken 2020

Meldplicht datalekken: facts & figures
Overzicht feiten en cijfers 2020

Aantal meldingen	Meerjarentrend	Stijging meldingen hacking & malware
23.976		↑ 30%

Dit wetsvoorstel leidt voor het Cbp tot enkele nieuwe bestuurlijke lasten. De meldplicht bij doorbrekingen van beveiligingsverplichtingen leidt, naar thans wordt geschat tot 66.000 meldingen per jaar.

KST II 2012/13, 33662, nr. 3 p. 17

Onderstaande grafiek laat het verloop van het aantal datalekmeldingen sinds 2016 zien:

Deze grafiek toont het aantal ontvangen datalekmeldingen per maand in 2020:

2

AUTORITEIT PERSOONSGEGEVENS

Jaarverslag AP 2021, p. 20

Wat de AP niét kon doen

De AP heeft een zeer groot en divers toezichtsterrein. Daarnaast heeft de AP een omvangrijk pakket aan wettelijke taken. Om effectief te zijn als toezichthouder, is het van belang dat de AP voldoende middelen en capaciteit heeft om deze taken uit te voeren.

Door tekorten in capaciteit en middelen heeft de AP, net zoals in 2020, in 2021 scherpe keuzes moeten maken. De AP heeft gekozen voor de activiteiten waarbij de impact voor burgers het grootst is. Hierdoor heeft de AP andere activiteiten niet of minder kunnen doen. Ook nemen de achterstanden bij activiteiten nog steeds toe.

Klachten
Veel burgers dienen een klacht in over organisaties die de AVG niet naleven. De AP moet deze klachten behandelen, maar is onvoldoende in staat om organisaties waarover wordt geklaagd aan te spreken op hun gedrag. Of om er door middel van onderzoek en handhaving voor te zorgen dat zij de AVG alsnog gaan naleven.

Datalekmeldingen
Er kwamen in 2021 ongeveer 25.000 meldingen binnen van datalekken. Slechts bij enkele honderden meldingen kan de AP actie ondernemen, bijvoorbeeld door organisaties aan te spreken op hun werkwijze en hen te helpen deze te verbeteren. Of door een onderzoek te starten naar de mate waarin een bedrijf voldoende beveiligingsmaatregelen had getroffen.

Verkennende onderzoeken
De AP doet ook onderzoeken die niet direct gericht zijn op handhaving, maar die zijn bedoeld om te zien of bepaalde sectoren voldoen aan verplichtingen uit de AVG. De inzichten uit een verkennend onderzoek vormen onder andere input voor risicoanalyses ten behoeve van de risicosturing van de AP. Door de geringe capaciteit in 2021 heeft de AP slechts twee onderzoeken kunnen afronden en geen nieuwe verkennende onderzoeken op kunnen starten.

Innovatie
Door de beperkte capaciteit en middelen heeft de AP in 2021 niet kunnen investeren in de innovatie van haar toezicht door de inzet van technologie. Investeringen zouden het toezicht van de AP effectiever kunnen maken. Bijvoorbeeld door vaak voorkomende toezichtactiviteiten te automatiseren. Of door een diepgaande analyse van de aan de AP ter beschikking staande bronnen zoals de klachten en datalekmeldingen.

'slechts bij enkele honderden meldingen kan AP actie ondernemen'

'niet kunnen investeren in innovatie van toezicht'

API's

3

AG CONNECT
the amazing world of IT

GOVERNANCE

Stijgende werklast door datalekken zorgt voor frustraties bij gemeenten

'Meldingen moeten efficiënter kunnen.'

De werklast als gevolg van datalekken stijgt bij gemeenten al jaren. En dat blijft de komende jaren zo, toont gezamenlijk onderzoek van *Binnenlands Bestuur*, *AG Connect* en *iBestuur* aan. Een aantal gemeenten slaat alarm.

De hoeveelheid datalekken bij de overheid stijgt al jaren, en die stijging lijkt maar niet af te nemen. In 2017 werden er 484 datalekken bij het openbaar bestuur gemeld. In 2021 zijn dat er bijna 5.000. Vrijwel altijd gaat het om menselijke fouten, zoals een verkeerde bijlage in een mail, een e-mail naar een verkeerd odres of een verkeerd verstuurde brief, zo wordt duidelijk uit de antwoorden.

2,5 tot 4 uur werk

Uit het onderzoek wordt duidelijk dat de afhandeling van datalekken een werklast meebrengt van zo'n 2,5 tot 4 uur, afhankelijk van de ernst. In bijzondere gevallen kan de werklast veel verder oplopen. Daarbij neemt het aantal meldingen van datalekken bij de overheid jaarlijks fors toe, blijkt uit jaarlijkse cijfers van de AP. En vooral daar gaan veel uren in zitten.

Hoogleraar recht en de informatiemaatschappij Gerrit Jan Zwenne (Universiteit Leiden) sluit zich aan bij Terra. "De AP stelt nu dat een melding in vijftien tot dertig minuten kan worden gemaakt, maar binnen die tijd zal het vrijwel onmogelijk zijn om een melding af te ronden. Het zou heel plezierig zijn wanneer er API wordt ontwikkeld waarmee een organisatie datalekken in het eigen systeem kan verwerken en snel kan doorzetten naar het meldpunt."

AP: handmatig melden blijft nodig

De Autoriteit Persoonsgegevens stelt in een reactie dat er continu gewerkt wordt aan het verbeteren van het meldproces van een datalek. Het belang van een goede en volledige melding maken staat voorop. "We willen melden sneller en makkelijker maken, maar handmatig invullen blijft noodzakelijk, daar gaan we niets aan veranderen. Over de hoeveelheid werklast van een datalek heeft de AP geen gegevens beschikbaar. Een woordvoerder geeft aan dat de tijd die besteed wordt aan niet-gemelde datalekken momenteel "sowieso minder dan 5% bedraagt."

4

beveiligingsplicht

art. 32 AVG

- 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

5

beveiligingsplicht

art. 32 AVG

- 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

6

7

8

toetsvraag 1

Uber kreeg een boete van 600.000 euro voor het te laat melden van een datalek

A. Dit is juist

B. Dit is onjuist

9

Allianz Global Assistance

Uw gegevens in onze back-up

Update 19 augustus 2020: Om ervoor te zorgen dat wij bij brand of een andere calamiteit de continuïteit van onze bedrijfsvoering kunnen waarborgen hebben wij onder andere een back-up van onze gegevens opgeslagen op een externe beveiligde locatie. De kluis met back-up gegevens is eind 2019 uit de beveiligde locatie gestolen. De diefstal is direct bij de politie gemeld en het onderzoek loopt nog steeds.

In de back-up zaten zeer diverse en vooral oude gegevens, maar deels ook persoonsgevoelige informatie. Daarom hebben wij hiervan ook melding gedaan bij de Autoriteit Persoonsgegevens. De gestolen gegevens zijn alleen toegankelijk voor personen met de juiste specifieke apparatuur en kennis. Tot op heden hebben we geen signalen ontvangen dat er een poging is ondernomen om toegang te krijgen tot de gestolen gegevens. Desondanks hebben wij iedereen geïnformeerd die mogelijk betrokken is. En zijn alle noodzakelijke maatregelingen getroffen om de mogelijke gevolgen voor alle betrokkenen te beperken.

Wij betreuren uiteraard dat dit gebeurd is en nemen wij onze verantwoordelijkheid. Alle betrokkenen hebben daarom van ons bericht met meer informatie ontvangen. Heeft u geen bericht ontvangen, dan kunt u er van uit gaan dat het niet uw gegevens betreft.

Wij begrijpen dat u als klant hier vragen over heeft. Daarom hebben we de meest gestelde vragen voor u op een rij gezet. Mocht u na het lezen van dit bericht nog vragen hebben en staat uw vraag hier niet tussen, dan kunt u contact met ons opnemen. We hebben hier een apart e-mailadres voor open gesteld. Vanwege de corona pandemie is helaas onze reactietijd langer dan u van ons gewend bent. We vragen hiervoor uw begrip.

10

meldplichten

Algemene Verordening Gegevensbescherming
wie: verwerkingsverantwoordelijke
wat: inbreuk op beveiliging van persoonsgegevens
aan: Autoriteit persoonsgegevens én betrokkene

art. 33-34 AVG

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

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

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

Wet beveiliging netwerk- en informatie-systemen (Wbni)
Art. 8
wie: aanbieders van essentiële diensten en digitaledienstverleners
wat: inbreuk op beveiliging en verlies integriteit
aan: Bewindspersonen, DNB

11

Ratio

- betrokken weten niet dat persoonsgegevens zijn gelekt
- en de gevolgen ervan kunnen ernstig zijn
- en toezichthouders komt er niet vanzelf niet achter
- datalek is indicatie van niet-naleving AVG

- *identiteitsfraude*
- *reputatieschade*
- *financiële verliezen*
- *discriminatie*
- *etc.*

12

Ratio

- betrokken weten niet dat persoonsgegevens zijn gelekt
- en de gevolgen ervan kunnen ernstig zijn
- en toezichthouder komt er niet vanzelf niet achter
- datalek is indicatie van niet-naleving AVG

- *beveiligingsplicht (art. 32 AVG)*
- *bewaartermijnen e.d. (art. 5.1 AVG)*

13

Meldplicht datalekken

Melding bij toezichthouder

tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen

Melding bij betrokkene

waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen


AD Amersfoort

Datalek lang toegedekt

Wie?

verwerkings-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. 33 en 34 AVG

14

‘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*

15

inbreuk of dreiging?

‘incident’ *‘threat’*

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

16

inbreuk of dreiging?

'incident' *'threat'*

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*

17

Melding bij AP

Melding bij toezichthouder

tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen

18

Melding bij AP

Melding bij toezichthouder

tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen

- *bijzondere gegevens (art. 9 of 10 AVG)*
- *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)*
- *etc.*

19

toetsvraag 2

Een inbreuk op de beveiliging van persoonsgegevens moet worden gemeld bij AP als er waarschijnlijk een hoog risico is voor de rechten en vrijheden van natuurlijke personen

A. Dit is juist

B. Dit is onjuist

20

'onverwijld'

vanaf moment van bekend worden van datalek

- door ververwerkingsverantwoordelijke zelf
- door verwerker(?)

zonder onnodige vertraging

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

21

melding aan betrokkene

waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen

22

melding aan betrokkene

waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen

encryptie, hashing beschermt tegen onbevoegde kennisneming (maar niet tegen vernietiging of aantasting)

tijdige remote wipe (Mobile-Iron)

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

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

23

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

Níet melden

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

24

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

Níet melden

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

25

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

Níet melden

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

26

toetsvraag 3

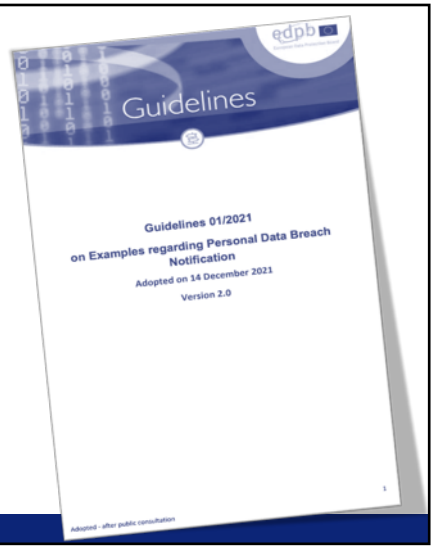
Volgens AP moet een foutief geadresseerde brief die ongeopend wordt teruggestuurd, niet worden gemeld.

A. Dit is juist

B. Dit is onjuist

27

- ransomware
- exfiltration attacks
- internal human risk source
- stolen or lost devices and paper documents
- postal mail mistake
- social enginering (incl. identity theft, email exfiltration



28

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@commit2law.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,

Hierbij attendeer ik jullie op het congres Implementatie Europese Privacy Verordening op 20 april 2016. VIRA leden ontvangen een korting van 20%. Onderstaand kort de belangrijkste informatie en aanmeldlink.

29

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,

Hierbij attendeer ik jullie op het congres Implementatie Europese Privacy Verordening op 20 april 2016. VIRA leden ontvangen een korting van 20%. Onderstaand kort de belangrijkste informatie en aanmeldlink.

Congres Implementatie Europese Privacy Verordening
Het congres Implementatie Europese Privacy Verordening (EPV) bereidt u voor op de nieuwe Europese regels. In sneltreinvaart ontdekt u hoe anderen de EPV aanpakken (o.a. Alliander, PostNL, NUON, PWN en T-Mobile).

Highlights:
- ✓ De vergaande gevolgen van de nieuwe Verordening
- ✓ Maak aantoonbaar dat u verantwoord omgaat met persoonsgegevens
- ✓ Hot topics: Data Protection Officer, Profiling, Meldplicht Datalekken, Security by Design, Cloud & risico's

Deelnemen met 20% VIRA korting!
Als lid van VIRA kunt u met 20% korting deelnemen. Vermeld hiervoor aanmeldcode 69752VIRA bij uw (online) aanmelding.

(te gebruiken link: http://iir.nl/events/europeseprivacyverordening/?utm_source=advertentie&utm_medium=website&utm_campaign=VIRA)

Met vriendelijke groet,

30

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..?

31

accounts passwords hack

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

Melding..?


Home / Security

Update: LinkedIn Confirms Account Passwords Hacked

By Ian Paul, PCWorld

47 COMMENTS

UPDATED 2:15 p.m. PT

LinkedIn Wednesday confirmed that at least some passwords compromised in a major security breach correspond to LinkedIn accounts.

Vicente Silveira, Director at LinkedIn, confirmed the hack on the company's blog Wednesday afternoon and outlined steps that LinkedIn is taking to deal with the situation. He wrote that those with compromised passwords will notice that their LinkedIn account password is no longer valid.

32

meldloket

Nieuw meldformulier datalekken is live

Nieuwsbericht / 1 juni 2021

Categorie:
Acties bij een datalek,
Meldplicht datalekken

De Autoriteit Persoonsgegevens (AP) heeft een nieuw meldformulier datalekken. Het nieuwe formulier maakt het voor de gebruiker makkelijker om een datalek bij de AP te melden.

Nieuwe functionaliteiten

Het nieuwe meldformulier heeft nieuwe functionaliteiten:

- Het formulier bepaalt op basis van de antwoorden die u invult welke vragen worden getoond. Zo hoeft u alleen de voor u relevante vragen te beantwoorden.
- U kunt het formulier tussentijds opslaan en op een ander moment verdergaan met uw melding.
- U kunt een sjabloon maken voor veelvoorkomende datalekken of een datalek dat zich in een korte tijd vaak voordoet. Zo hoeft u bepaalde delen van het formulier niet bij elke melding opnieuw in te vullen.
- Het aanvullen van een eerdere melding is eenvoudiger geworden. U hoeft hiervoor niet meer het hele meldformulier opnieuw in te vullen.

PER E-MAIL

Autoriteit Persoonsgegevens
t.a.v. de heer mr. A. Wolfsen
Postbus 93374
2509 AJ DEN HAAG

Datum 8 november 2021
Inzake Meldingen datalekken via het meldloket – aanbevelingen voor verbetering

Geachte heer Wolfsen,

Namens de Vereniging Privacyrecht Advocaten (VPR-A) en de Vereniging Privacynet (VPR) richten wij ons hierbij tot de Autoriteit Persoonsgegevens (AP) met het verzoek aan de AP om een aantal belangrijke verbeteringen in de meldingsprocedure en het meldloket voor datalekken door te voeren. We hopen dat de AP onze aanbevelingen in overweging neemt en ook implementeert, zodat het melden en afhandelen van datalekken wordt verbeterd.

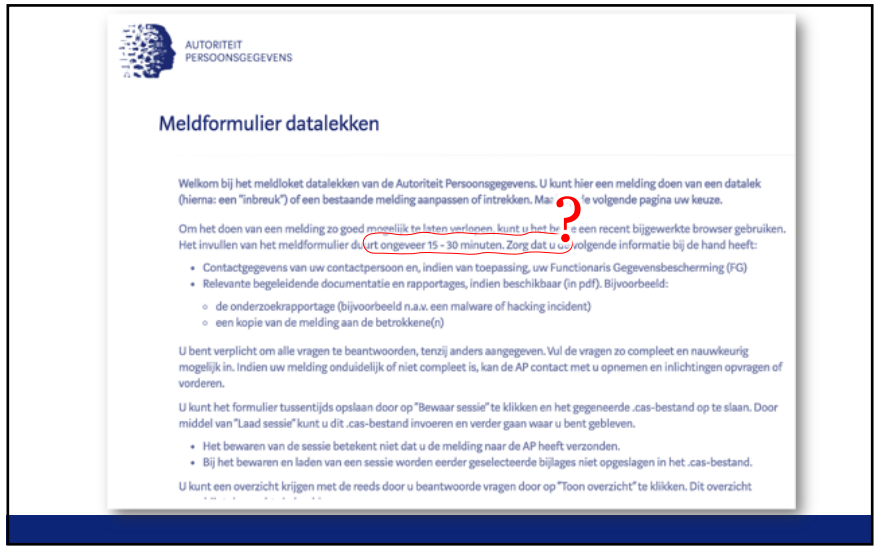
Als toezichthoudende instantie in Nederland voor het melden van datalekken (onder meer in de zin van artikel 33 AVG), heeft de AP ervoor gekozen een online meldloket in te richten om het melden van reeavante datalekken aan de AP te faciliteren. Op 1 juni 2021 heeft de AP haar meldprocedure aangepast in die zin dat zij het oude webformulier op haar website heeft vervangen door een nieuw interactief webformulier die voor drie verschillende situaties kan worden gebruikt, te weten voor het doen van (i) een (initiële) melding, (ii) een vervolgmelding, en (iii) om een melding in te trekken. Bij het publiceren van het nieuwe meldformulier heeft de AP aangegeven dat het doel van de wijzigingen is om een datalek sneller en makkelijker in te kunnen dienen.

Het is prijzenswaardig dat de AP het melden van datalekken probeert te vereenvoudigen. In de praktijk zien wij evenwel dat het nieuwe meldformulier maar ten dele daarin geslaagd is. Op belangrijke punten voelt met de nieuwe meldformulier ook tot verslechteringen geleid en staat het formulier zelfs op gespannen voet met de verplichtingen die op de AP als toezichthouder rusten. Ter ondersteuning van het doel van de AP om het doen van datalekmeldingen te vereenvoudigen, geven wij hierbij daarom graag aan de AP een aantal aanbevelingen alleen in overweging op basis van de ervaringen die wij daarmee hebben opgedaan. Deze aanbevelingen zien alleen op de (eerste) melding en meest noodzakelijke verbeteringen, zowel in relatie tot het indienen van een datalekmelding alsook de opvolging daarvan. Wij zijn uiteraard graag beschikbaar voor nadere toelichting.

1 Vermeide tijdsduur voor het invullen van de formulieren wekt onterechte verwachtingen

1.1 De AP geeft in haar instructie op het meldformulier aan dat de melding binnen ongeveer een kwartier (of half uur volstaat is. Wanneer een organisatie een (nieuw) datalek moet melden, wordt zij echter geconfronteerd met een uitgebreide lijst met gedetailleerde vragen waarop nauwkeurig, soms met exacte aantallen, moet antwoorden. Voor zover de gevraagde informatie al in een vroeg stadium beschikbaar is in verband met de vereiste waarborgen organisaties een (initiële) melding moeten indienen, is bovendien de gevraagde gedetailleerde informatie over het datalek vaak alleen

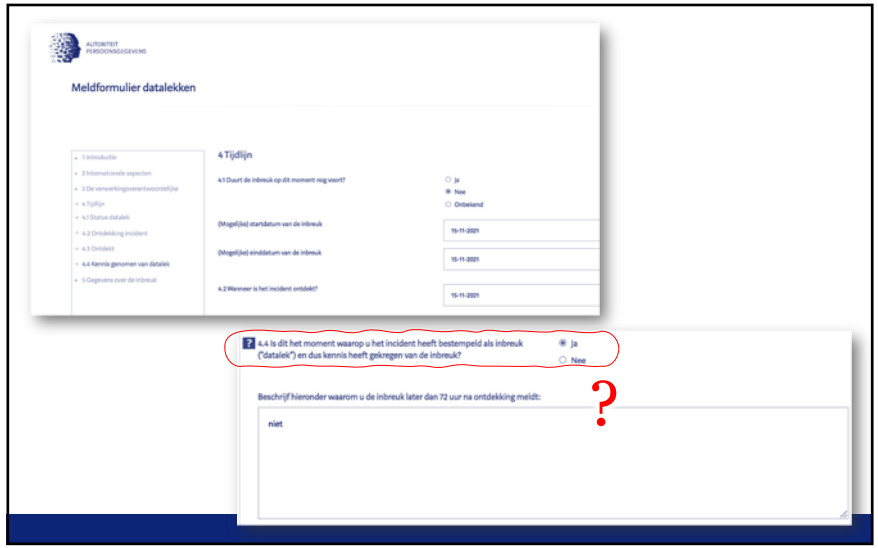
33



34

bulkmeldingen...

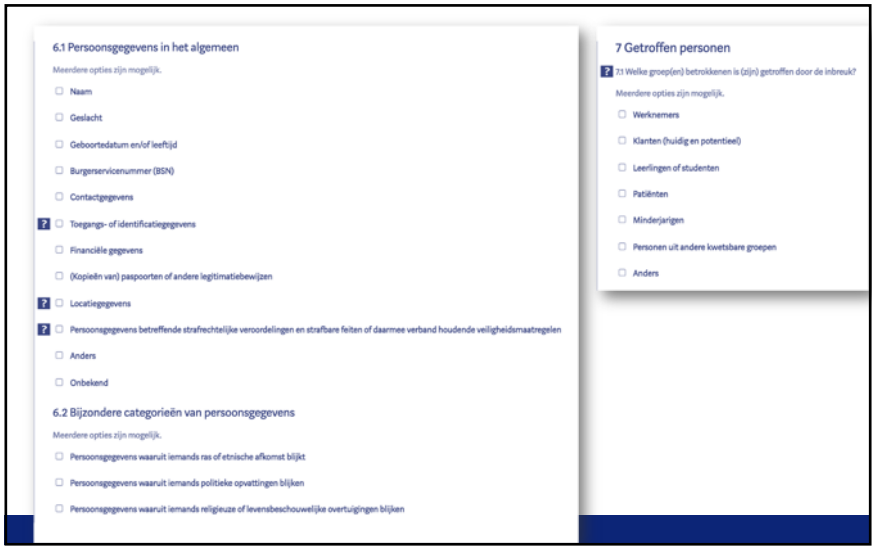
35



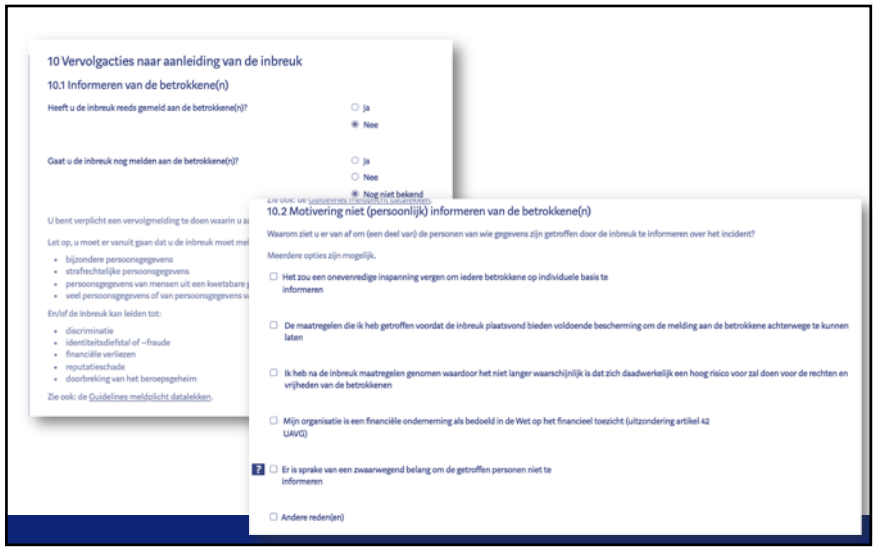
36


5 Gegevens over de inbreuk
5.1 Aard van de inbreuk
Meerdere opties zijn mogelijk.
Persoonsgegevens (mogelijk) ingezien door onbevoegden
Persoonsgegevens per ongeluk of onopzettelijk gewijzigd
Persoonsgegevens permanent niet beschikbaar (verloren/verwijderd)
Persoonsgegevens tijdelijk niet beschikbaar
5.2 Aard van het incident
Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?
Slechts één optie is mogelijk
Apparaat, gegevensdrager (bijv. USB-stick) en/of papier met persoonsgegevens kwijtgeraakt of gestolen
Autorisatie(s) van medewerker(s) verkeerd ingesteld
Brief of postpakket met persoonsgegevens geopend retour ontvangen
Brief of postpakket met persoonsgegevens kwijtgeraakt
Brief of postpakket met persoonsgegevens verstuurd of afgegeven aan de verkeerde ontvanger(s)
E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)
E-mail verstuurd met persoonsgegevens met ontvangers in het aan-veld of in de cc, in plaats van bcc
Hacking, malware (bijv. ransomware) en/of phishing
Netwerkmappen of -locaties met persoonsgegevens zijn te breed toegankelijk ingesteld binnen de organisatie
Overig
Persoonsgegevens bij oud papier gezet
Persoonsgegevens door storing (tijdelijk) niet beschikbaar
Persoonsgegevens per ongeluk gepubliceerd
Persoonsgegevens toegevoegd aan het verkeerde dossier

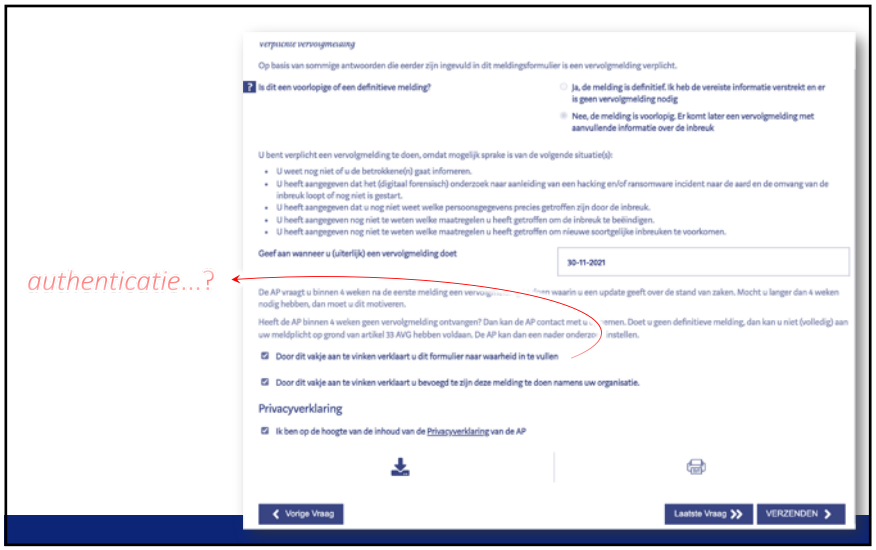
37


6.1 Persoonsgegevens in het algemeen
Meerdere opties zijn mogelijk.
Naam
Geslacht
Geboortedatum en/of leeftijd
Burgerservicenummer (BSN)
Contactgegevens
Toegangs- of identificatiegegevens
Financiële gegevens
(Kopieën van) paspoorten of andere legitimatiebewijzen
Locatiegegevens
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen
Anders
Onbekend
6.2 Bijzondere categorieën van persoonsgegevens
Meerdere opties zijn mogelijk.
Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt
Persoonsgegevens waaruit iemands politieke opvattingen blijken
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken
7 Getroffen personen
7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?
Meerdere opties zijn mogelijk.
Werknemers
Klanten (huidig en potentieel)
Leerlingen of studenten
Patiënten
Minderjarigen
Personen uit andere kwetsbare groepen
Anders

38


10 Vervolgacties naar aanleiding van de inbreuk
10.1 Informeren van de betrokkene(n)
Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?
ja
Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?
ja
Nee
Nog niet bekend
U bent verplicht een vervolgmelding te doen waarin u
Let op, u moet er vanuit gaan dat u de inbreuk moet
bijzondere persoonsgegevens
strafrechtelijke persoonsgegevens
persoonsgegevens van mensen uit een kwetsbare
veel persoonsgegevens of van persoonsgegevens
En/of de inbreuk kan leiden tot:
discriminatie
identiteitsdiefstal of –fraude
financiële verliezen
reputatieschade
doorbreking van het beroepsgeheim
Zie ook: de Guidelines meldplicht datalekken.
10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)
Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?
Meerdere opties zijn mogelijk.
Het zou een oneevenredige inspanning vergen om iedere betrokkene op individuele basis te informeren
De maatregelen die ik heb getroffen voordat de inbreuk plaatsvond bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten
Ik heb na de inbreuk maatregelen genomen waardoor het niet langer waarschijnlijk is dat zich daadwerkelijk een hoog risico voor zal doen voor de rechten en vrijheden van de betrokkenen
Mijn organisatie is een financiële onderneming als bedoeld in de Wet op het financieel toezicht (uitzondering artikel 42 UAVG)
Er is sprake van een zwaarwegend belang om de getroffen personen niet te informeren
Andere reden(en)

39


authenticatie...?
Op basis van sommige antwoorden die eerder zijn ingevuld in dit meldingsformulier is een vervolgmelding verplicht.
Is dit een voorlopige of een definitieve melding?
ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig
Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk
U bent verplicht een vervolgmelding te doen, omdat mogelijk sprake is van de volgende situatie(s):
U weet nog niet of u de betrokkene(n) gaat informeren.
U heeft aangegeven dat het (digitaal forensisch) onderzoek naar aanleiding van een hacking en/of ransomware incident naar de aard en de omvang van de inbreuk loopt of nog niet is gestart.
U heeft aangegeven dat u nog niet weet welke persoonsgegevens precies getroffen zijn door de inbreuk.
U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om de inbreuk te beëindigen.
U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om nieuwe soortgelijke inbreuken te voorkomen.
Geef aan wanneer u (uiterlijk) een vervolgmelding doet
30-11-2021
Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen
Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.
Privacyverklaring
Ik ben op de hoogte van de inhoud van de Privacyverklaring van de AP
Vorige Vraag
Laatste Vraag
VERZENDEN

40


AUTORITEIT
PERSOONSGEGEVENS
Ontvangstbevestiging
Uw verzoek tot het indienen van een melding wordt in behandeling genomen.
U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.
Tijdstip ontvangst
Uniek nummer
0. Over deze melding
Gaat het om een nieuwe of bestaande
Een nieuwe melding indienen

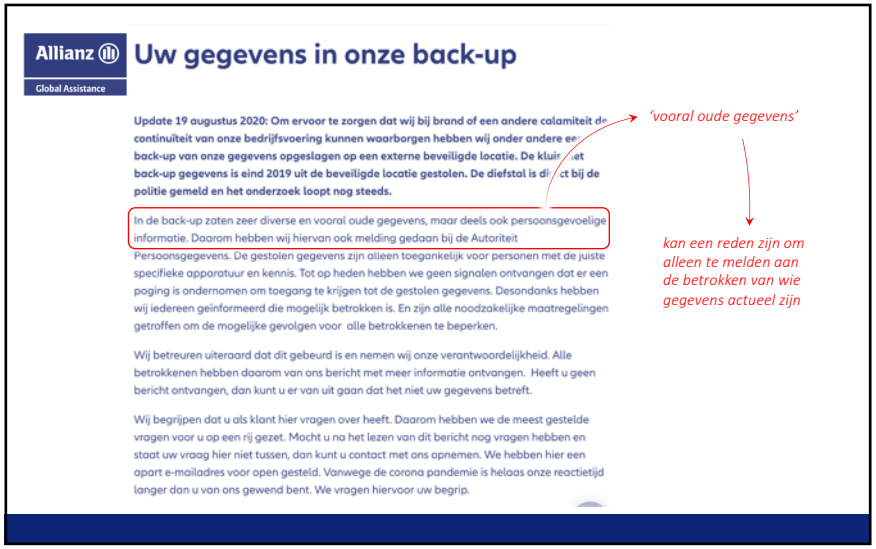
41


Allianz
Global Assistance
Uw gegevens in onze back-up
Update 19 augustus 2020: Om ervoor te zorgen dat wij bij brand of een andere calamiteit de continuïteit van onze bedrijfsvoering kunnen waarborgen hebben wij onder andere een back-up van onze gegevens opgeslagen op een externe beveiligde locatie. De kluis met back-up gegevens is eind 2019 uit de beveiligde locatie gestolen. De diefstal is direct bij de politie gemeld en het onderzoek loopt nog steeds.
In de back-up zaten zeer diverse en vooral oude gegevens, maar deels ook persoonsgevoelige informatie. Daarom hebben wij hiervan ook melding gedaan bij de Autoriteit Persoonsgegevens. De gestolen gegevens zijn alleen toegankelijk voor personen met de juiste specifieke apparatuur en kennis. Tot op heden hebben we geen signalen ontvangen dat er een poging is ondernomen om toegang te krijgen tot de gestolen gegevens. Desondanks hebben wij iedereen geïnformeerd die mogelijk betrokken is. En zijn alle noodzakelijke maatregelingen getroffen om de mogelijke gevolgen voor alle betrokkenen te beperken.
Wij betreuren uiteraard dat dit gebeurd is en nemen wij onze verantwoordelijkheid. Alle betrokkenen hebben daarom van ons bericht met meer informatie ontvangen. Heeft u geen bericht ontvangen, dan kunt u er van uit gaan dat het niet uw gegevens betreft.
Wij begrijpen dat u als klant hier vragen over heeft. Daarom hebben we de meest gestelde vragen voor u op een rij gezet. Mocht u na het lezen van dit bericht nog vragen hebben en staat uw vraag hier niet tussen, dan kunt u contact met ons opnemen. We hebben hier een apart e-mailadres voor open gesteld. Vanwege de corona pandemie is helaas onze reactietijd langer dan u van ons gewend bent. We vragen hiervoor uw begrip.

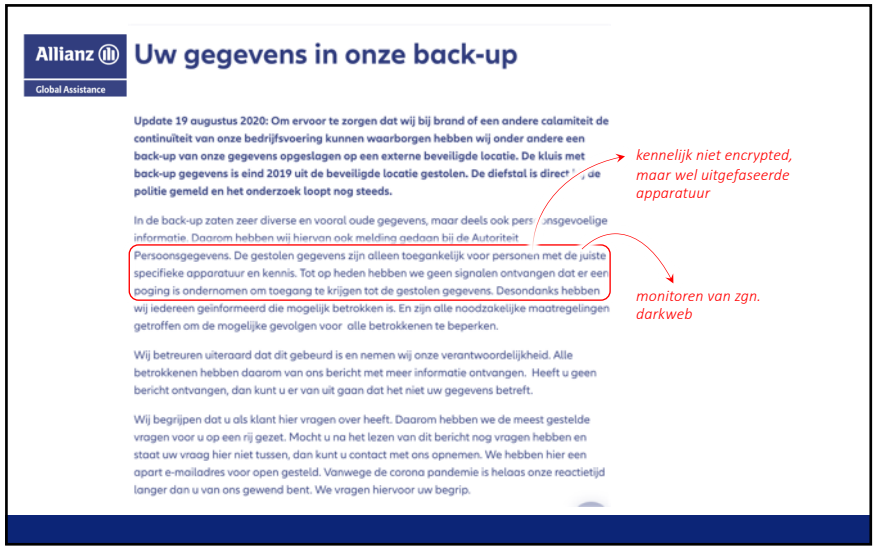
42


Allianz
Global Assistance
Uw gegevens in onze back-up
'onderzoek loopt nog'
kan een reden zijn om nog niet te melden aan betrokkenen
Update 19 augustus 2020: Om ervoor te zorgen dat wij bij brand of een andere calamiteit de continuïteit van onze bedrijfsvoering kunnen waarborgen hebben wij onder andere een back-up van onze gegevens opgeslagen op een externe beveiligde locatie. De kluis met back-up gegevens is eind 2019 uit de beveiligde locatie gestolen. De diefstal is direct bij de politie gemeld en het onderzoek loopt nog steeds.
In de back-up zaten zeer diverse en vooral oude gegevens, maar deels ook persoonsgevoelige informatie. Daarom hebben wij hiervan ook melding gedaan bij de Autoriteit Persoonsgegevens. De gestolen gegevens zijn alleen toegankelijk voor personen met de juiste specifieke apparatuur en kennis. Tot op heden hebben we geen signalen ontvangen dat er een poging is ondernomen om toegang te krijgen tot de gestolen gegevens. Desondanks hebben wij iedereen geïnformeerd die mogelijk betrokken is. En zijn alle noodzakelijke maatregelingen getroffen om de mogelijke gevolgen voor alle betrokkenen te beperken.
Wij betreuren uiteraard dat dit gebeurd is en nemen wij onze verantwoordelijkheid. Alle betrokkenen hebben daarom van ons bericht met meer informatie ontvangen. Heeft u geen bericht ontvangen, dan kunt u er van uit gaan dat het niet uw gegevens betreft.
Wij begrijpen dat u als klant hier vragen over heeft. Daarom hebben we de meest gestelde vragen voor u op een rij gezet. Mocht u na het lezen van dit bericht nog vragen hebben en staat uw vraag hier niet tussen, dan kunt u contact met ons opnemen. We hebben hier een apart e-mailadres voor open gesteld. Vanwege de corona pandemie is helaas onze reactietijd langer dan u van ons gewend bent. We vragen hiervoor uw begrip.

43


Allianz
Global Assistance
Uw gegevens in onze back-up
'vooral oude gegevens'
kan een reden zijn om alleen te melden aan de betrokken van wie gegevens actueel zijn
Update 19 augustus 2020: Om ervoor te zorgen dat wij bij brand of een andere calamiteit de continuïteit van onze bedrijfsvoering kunnen waarborgen hebben wij onder andere een back-up van onze gegevens opgeslagen op een externe beveiligde locatie. De kluis met back-up gegevens is eind 2019 uit de beveiligde locatie gestolen. De diefstal is direct bij de politie gemeld en het onderzoek loopt nog steeds.
In de back-up zaten zeer diverse en vooral oude gegevens, maar deels ook persoonsgevoelige informatie. Daarom hebben wij hiervan ook melding gedaan bij de Autoriteit Persoonsgegevens. De gestolen gegevens zijn alleen toegankelijk voor personen met de juiste specifieke apparatuur en kennis. Tot op heden hebben we geen signalen ontvangen dat er een poging is ondernomen om toegang te krijgen tot de gestolen gegevens. Desondanks hebben wij iedereen geïnformeerd die mogelijk betrokken is. En zijn alle noodzakelijke maatregelingen getroffen om de mogelijke gevolgen voor alle betrokkenen te beperken.
Wij betreuren uiteraard dat dit gebeurd is en nemen wij onze verantwoordelijkheid. Alle betrokkenen hebben daarom van ons bericht met meer informatie ontvangen. Heeft u geen bericht ontvangen, dan kunt u er van uit gaan dat het niet uw gegevens betreft.
Wij begrijpen dat u als klant hier vragen over heeft. Daarom hebben we de meest gestelde vragen voor u op een rij gezet. Mocht u na het lezen van dit bericht nog vragen hebben en staat uw vraag hier niet tussen, dan kunt u contact met ons opnemen. We hebben hier een apart e-mailadres voor open gesteld. Vanwege de corona pandemie is helaas onze reactietijd langer dan u van ons gewend bent. We vragen hiervoor uw begrip.

44



45

46

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."

47

@zwnne

vragen?
g.j.zwenne@law.leidenuniv.nl

48