@zwnne

Meldplichten en datalekken

Prof. mr. G-J. (Gerrit-Jan) ZWENNE | 20 januari 2022

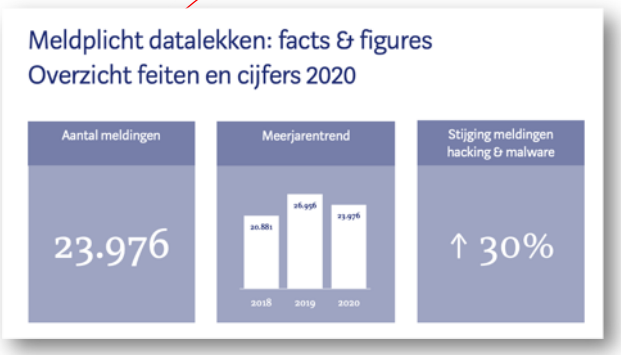
Studiecentrum voor Bedrijf en Overheid

eLaw Leiden

1

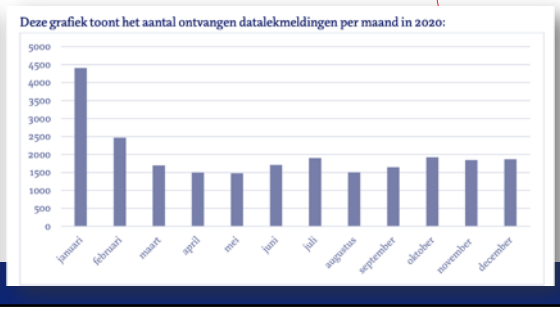
AUTORITEIT PERSOONSGEGEVENS

Meldplicht datalekken: facts & figures
Overzicht feiten en cijfers 2020



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



2

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

3

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

4


AUTORITEIT PERSOONSGEGEVENS
AP legt Uber boete op voor te laat melden datalek
Publicaties
Haga beboet voor onvoldoende interne beveiliging patiëntendossiers
Nieuwsbericht / 16 juli 2019
Het HagaZiekenhuis heeft de interne beveiliging van patiëntendossiers niet op orde. Dit blijkt uit onderzoek van de Autoriteit Persoonsgegevens (AP).
nrc
Transavia krijgt boete van vier ton voor datalek
Luchtvaart Een hacker omzeilde de beveiliging van Transavia en downloadde de privégegevens van 83.000 passagiers. Met een simpel wachtwoord kon hij de systemen van de luchtvaartmaatschappij binnendringen.
Luchtvaartmaatschappij Transavia heeft een boete van 400.000 euro opgelegd gekregen, omdat een hacker in 2019 de persoonsgegevens van 25 miljoen passagiers kon inzien.
de Rechtspraak
Home Onderwerpen Uitspraken en nieuws Registers de Rechtspraak Professionals
Rechtbank Den Haag > Nieuws > Boete voor ziekenhuis vanwege overtreden AVG
Boete voor ziekenhuis vanwege overtreden AVG
Den Haag, 16 april 2021
De rechtbank Den Haag heeft op 31 maart 2021 uitspraak gedaan in een zaak over een boete die de Autoriteit Persoonsgegevens (AP) heeft opgelegd aan een Haags ziekenhuis. Het ziekenhuis kreeg de boete vanwege het overtreden van de AVG, persoonsgegevens van patiënten werden namelijk niet voldoende beschermd. De AP had een boete opgelegd van 460.0000 euro maar die heeft de rechtbank teruggebracht naar 350.000 euro.

5


AUTORITEIT PERSOONSGEGEVENS
UWV krijgt boete voor slechte beveiliging bij verzending groepsberichten
AP: Boete orthodontiepraktijk vanwege onbeveiligde patiëntenwebsite
Boete PVV Overijssel vanwege niet melden datalek
De Autoriteit Persoonsgegevens (AP) legt de Partij voor de Vrijheid (PVV) Overijssel een boete op van 7.500 euro.
Boete Booking.com voor te laat melden datalek
De Autoriteit Persoonsgegevens (AP) legt Booking.com een boete op van 475.000 euro omdat het een datalek te laat meldde bij de AP.
Ziekenhuis OLVG beboet om onvoldoende beveiliging medische dossiers
De Autoriteit Persoonsgegevens (AP) legt een boete van 440.000 euro op aan het Amsterdamse ziekenhuis OLVG.

6

Allianz

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.

7

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

8

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.*

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)*

Meldplicht datalekken


AD Amersfoort

Datalek lang toegedekt

Ambtenaren verzwegen blunder voor wethouder

Aanklager én verdachte speedbootdrama in hoger beroep

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

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

‘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?

'incident' 'threat'

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

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

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

15

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.*

16

'onverwijld'

vanaf moment van bekend worden van datalek

- door verwerkingsverantwoordelijke zelf
- door verwerker(?)

zonder onnodige vertraging

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

17

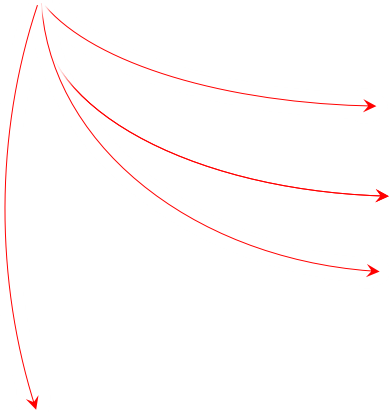
melding aan betrokkene

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

18

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

19

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

20

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

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

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.

23

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,

[redacted]

24

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..?

25

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

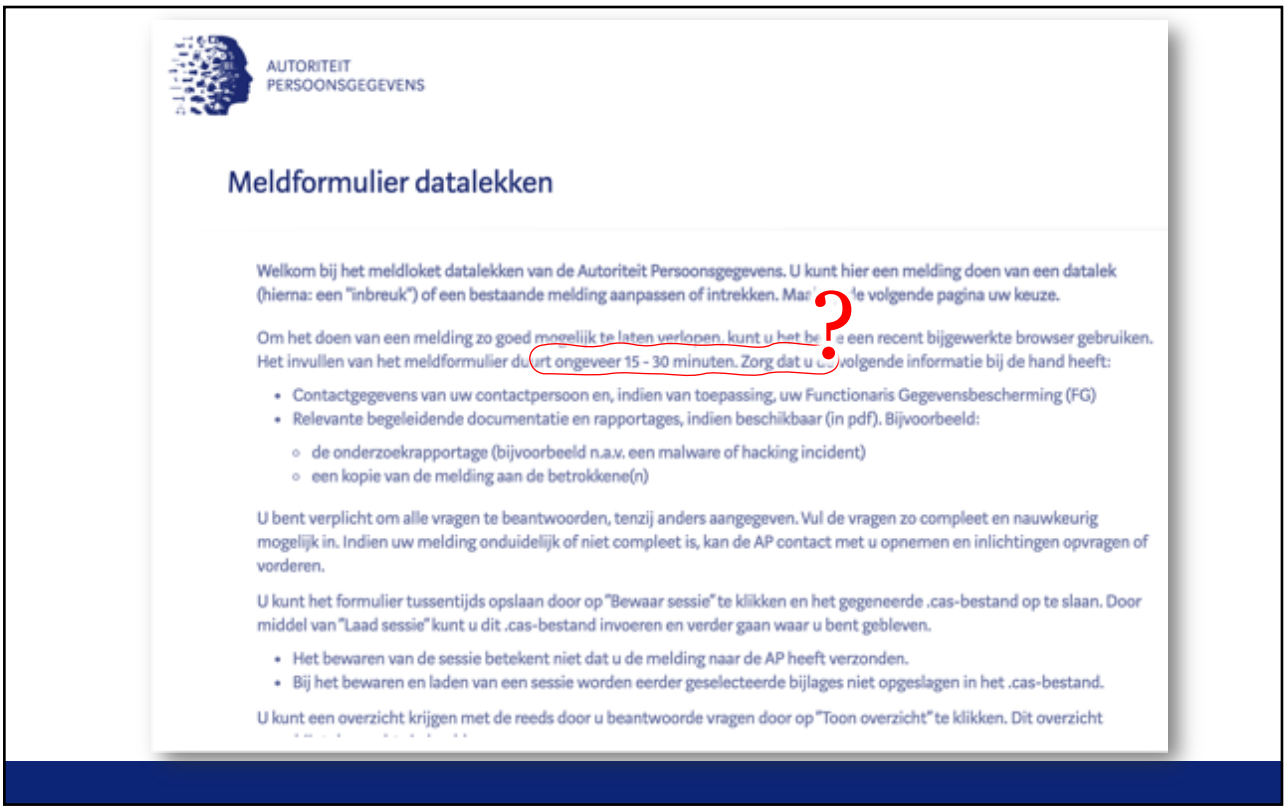
LinkedIn Wednesday confirmed that at least some passwords compromised in a major security breach correspond to LinkedIn accounts.

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.

26


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,

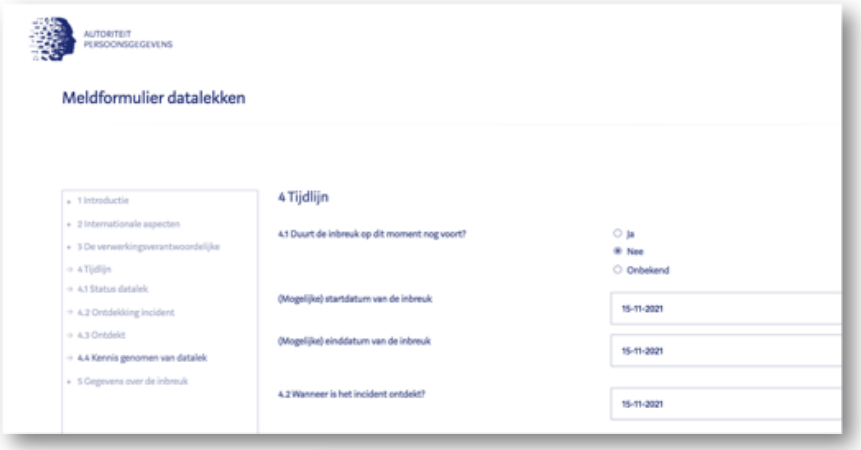
27

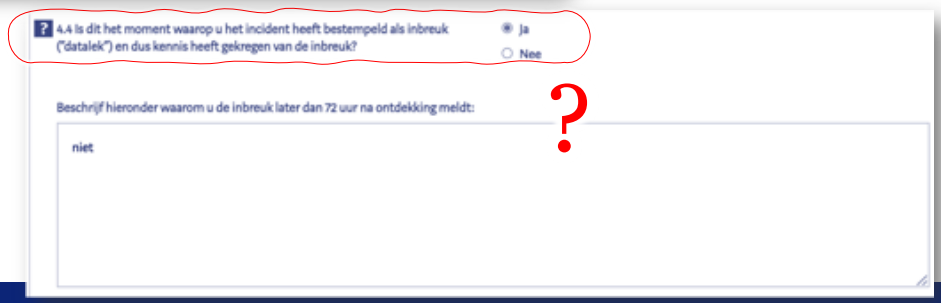

AUTORITEIT PERSOONSGEGEVENS
Meldformulier datalekken
Welkom bij het meldloket datalekken van de Autoriteit Persoonsgegevens. U kunt hier een melding doen van een datalek (hierna: een "inbreuk") of een bestaande melding aanpassen of intrekken.
Om het doen van een melding zo goed mogelijk te laten verlopen, kunt u het beste een recent bijgewerkte browser gebruiken. Het invullen van het meldformulier duurt ongeveer 15 - 30 minuten. Zorg dat u de volgende informatie bij de hand heeft:
Contactgegevens van uw contactpersoon en, indien van toepassing, uw Functionaris Gegevensbescherming (FG)
Relevante begeleidende documentatie en rapportages, indien beschikbaar (in pdf). Bijvoorbeeld:
de onderzoekrapportage (bijvoorbeeld n.a.v. een malware of hacking incident)
een kopie van de melding aan de betrokkene(n)
U bent verplicht om alle vragen te beantwoorden, tenzij anders aangegeven. Vul de vragen zo compleet en nauwkeurig mogelijk in. Indien uw melding onduidelijk of niet compleet is, kan de AP contact met u opnemen en inlichtingen opvragen of vorderen.
U kunt het formulier tussentijds opslaan door op "Bewaar sessie" te klikken en het gegeneerde .cas-bestand op te slaan. Door middel van "Laad sessie" kunt u dit .cas-bestand invoeren en verder gaan waar u bent gebleven.
Het bewaren van de sessie betekent niet dat u de melding naar de AP heeft verzonden.
Bij het bewaren en laden van een sessie worden eerder geselecteerde bijlages niet opgeslagen in het .cas-bestand.
U kunt een overzicht krijgen met de reeds door u beantwoorde vragen door op "Toon overzicht" te klikken. Dit overzicht

28

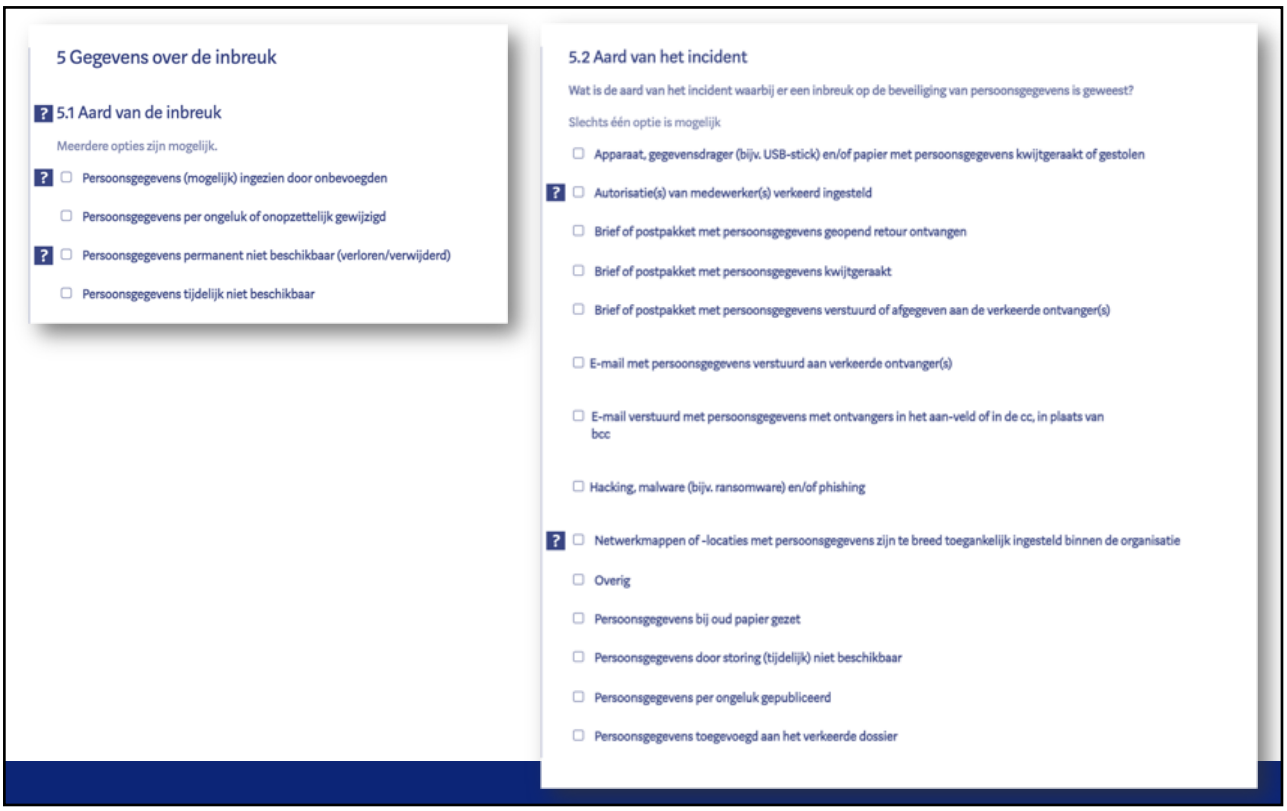
bulkmeldingen…

29

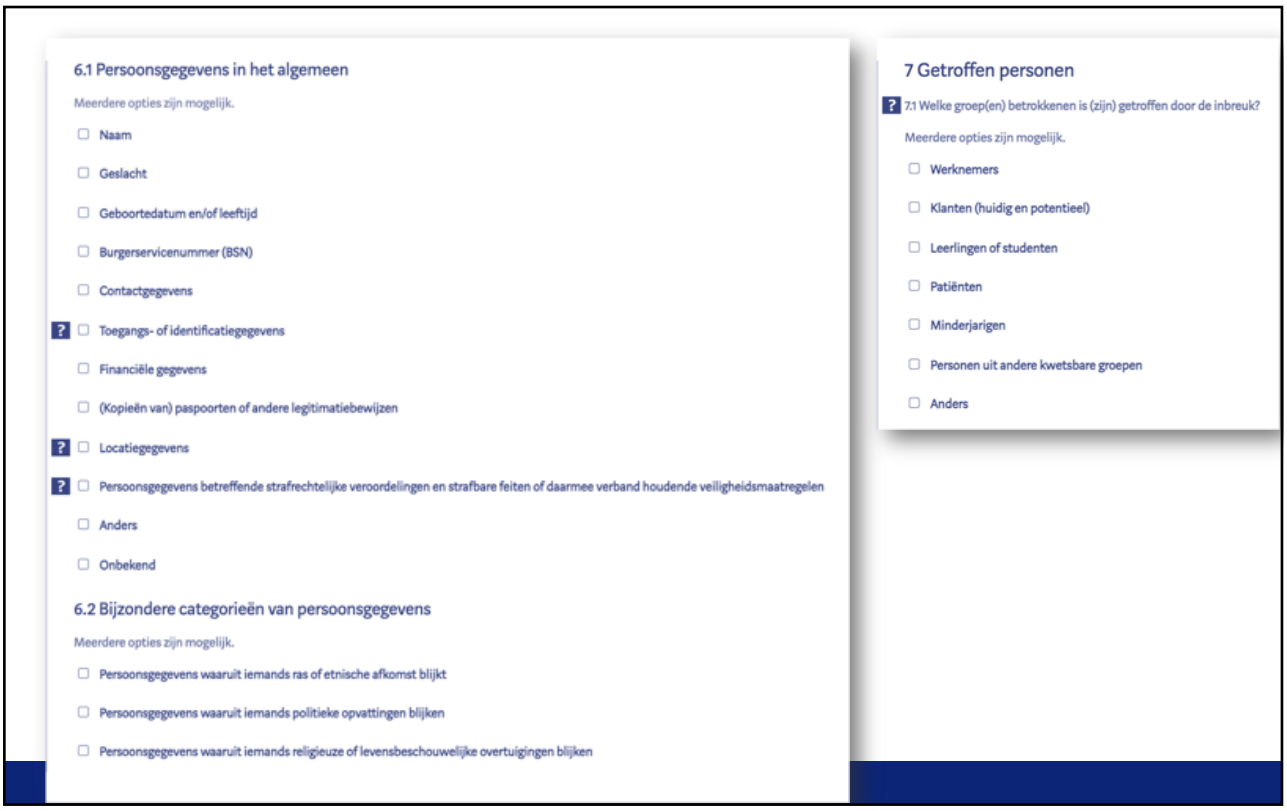




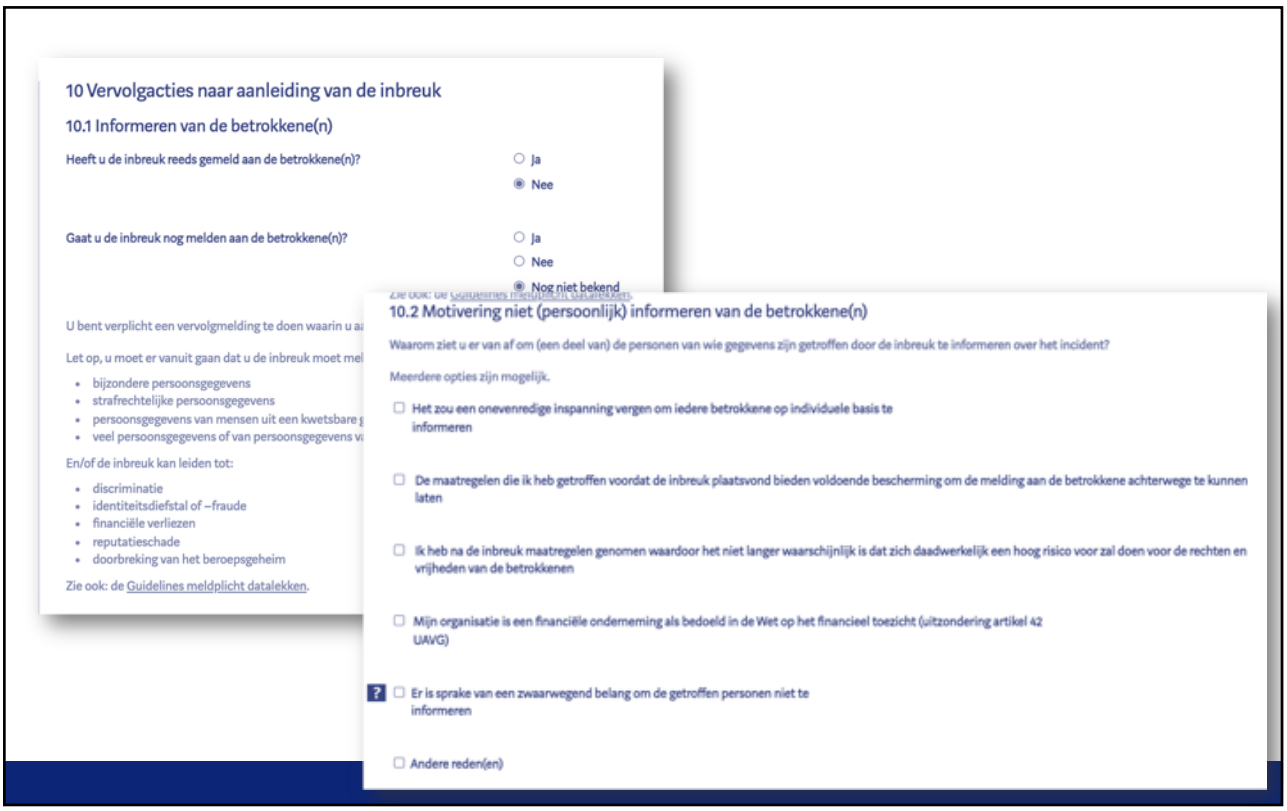
30


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

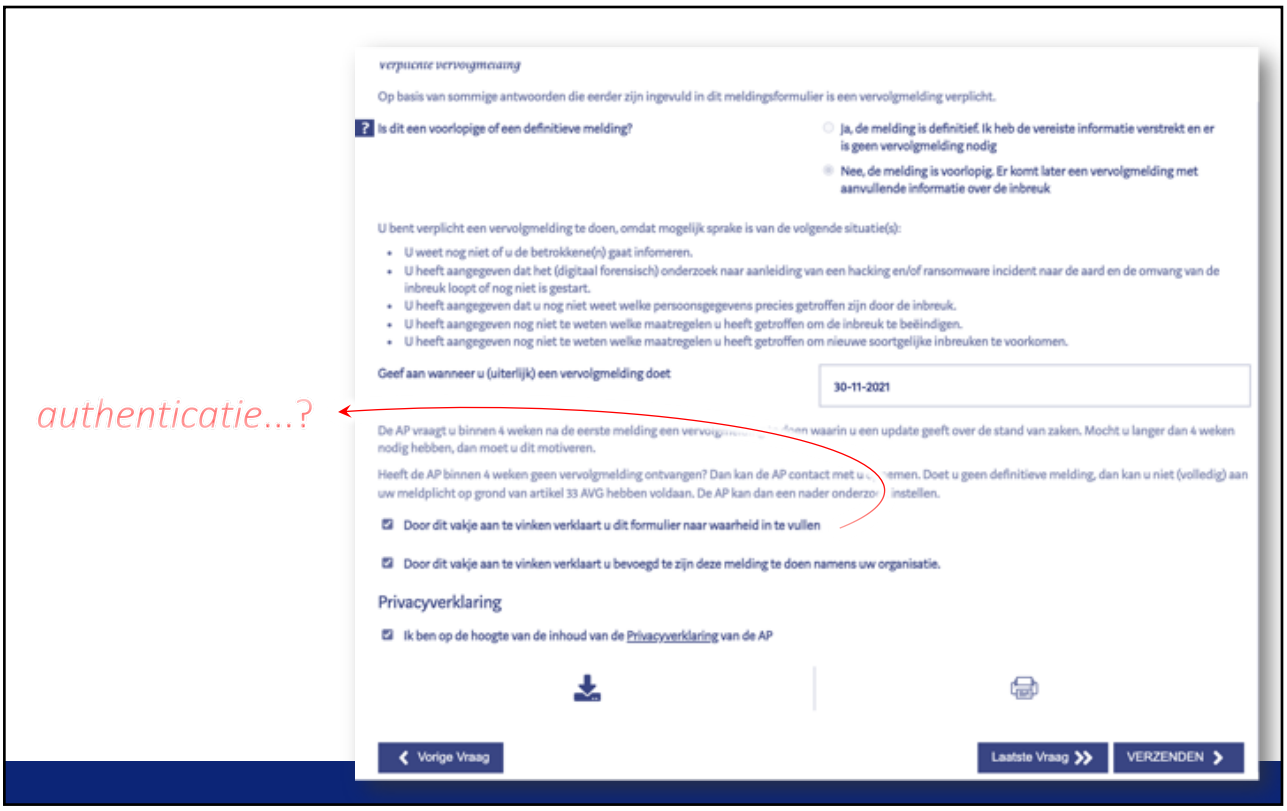
31


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

32



33



authenticatie...?

34

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 [redacted]2018 [redacted]
Uniek nummer [redacted]

0. Over deze melding

Gaat het om een nieuwe of bestaande — Een nieuwe melding indienen

35

Allianz

Uw gegevens in onze back-up

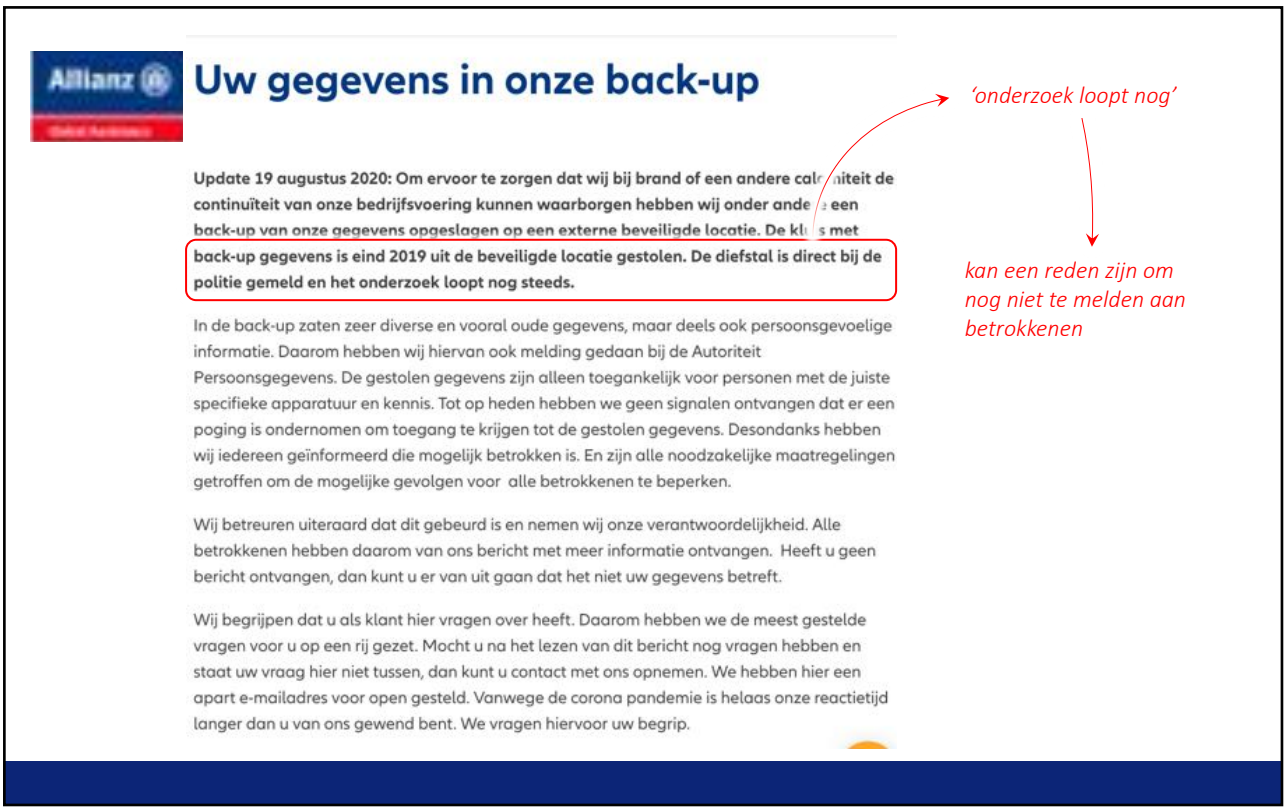
Update 19 augustus 2020: Om ervoor te zorgen dat wij bij brand of een andere calamiteit de continuïteit van onze bedrijfsvoering kunnen waarborgen hebben wij onder andere een back-up van onze gegevens opgeslagen op een externe beveiligde locatie. De kluis met back-up gegevens is eind 2019 uit de beveiligde 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.

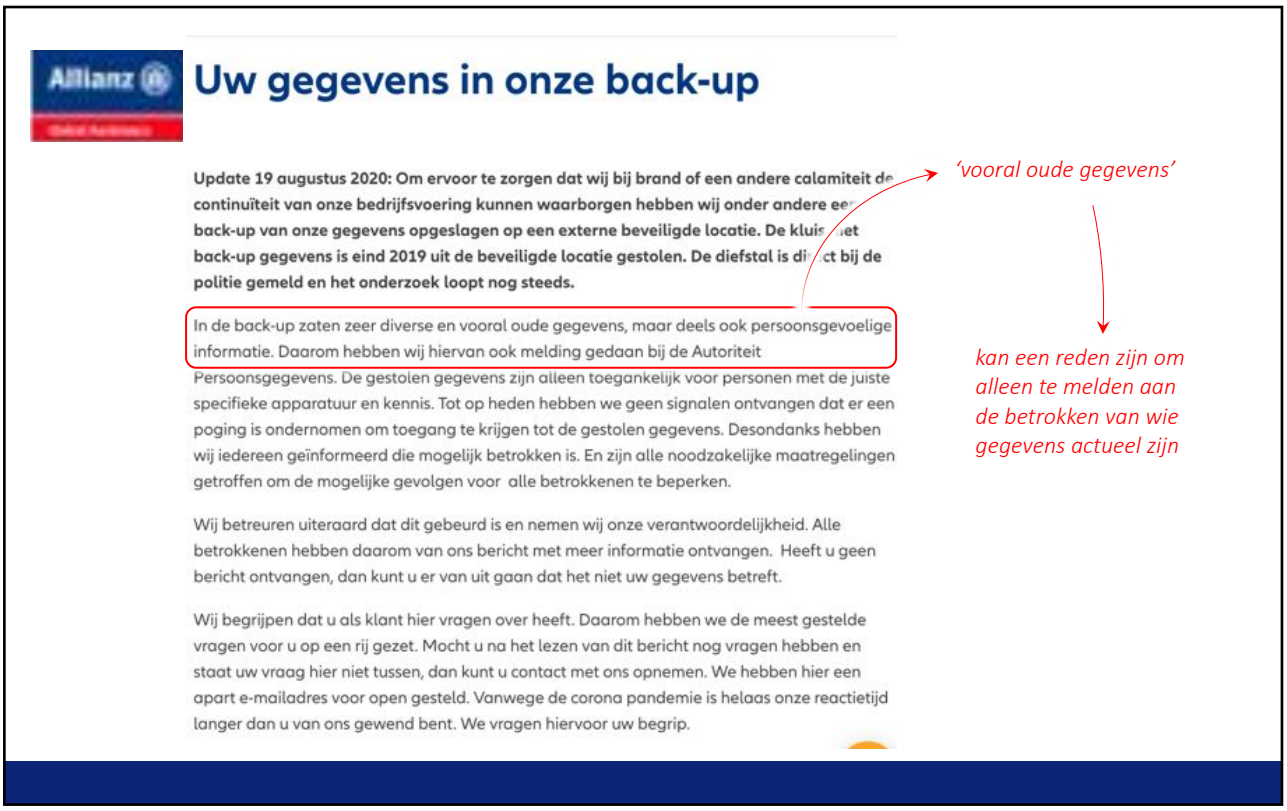
Wij betreuren uiteraard dat dit gebeurd is en nemen wij onze verantwoordelijkheid. Alle betrokkenen hebben daarom van ons bericht met meer informatie ontvangen. Heeft u geen bericht ontvangen, dan kunt u er van uit gaan dat het niet uw gegevens betreft.

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.

36


Allianz
Uw gegevens in onze back-up
Update 19 augustus 2020: Om ervoor te zorgen dat wij bij brand of een andere cal iteit de continuïteit van onze bedrijfsvoering kunnen waarborgen hebben wij onder ande een back-up van onze gegevens opgeslagen op een externe beveiligde locatie. De kl s 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.
'onderzoek loopt nog'
kan een reden zijn om nog niet te melden aan betrokkenen

37


Allianz
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 ee back-up van onze gegevens opgeslagen op een externe beveiligde locatie. De kluis et back-up gegevens is eind 2019 uit de beveiligde locatie gestolen. De diefstal is di ct 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.
'vooral oude gegevens'
kan een reden zijn om alleen te melden aan de betrokken van wie gegevens actueel zijn

38

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.

kennelijk niet encrypted, maar wel uitgefaseerde apparatuur

monitoren van zgn. darkweb

39

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.

- *veel gestelde vragen*
- *call center*
- *emailadres*
- *persbericht*

40

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."

41

@zwenne

vragen?

g.j.zwenne@law.leidenuniv.nl

Studiecentrum voor Bedrijf en Overheid

eLaw Leiden

42