@zwnne

AVG & UAVG: toepassing en werking van de privacywet

Gerrit-Jan Zwenne | 19 januari 2023

studiecentrum voor bedrijf en overheid SBO

eLaw Leiden

vandaag

achtergrond en context
- privacy en de privacywet

de spelers
- de betrokkene
- de verwerkingsverantwoordelijke
- de verwerker
- de autoriteit persoonsgegevens
- de functionaris gegevensbescherming

het speelveld
- de geheel of gedeeltelijk geautomatiseerde verwerking persoonsgegevens en het bestand
- persoonlijk of huishoudelijk en journalistiek, literair of academisch
- territoriale werking

en de spelregels
- verwerkingsgrondslagen
- doelbinding en bewaren
- bijzondere gegevens en bsn
- informatieplichten en rechten van betrokkenen
- internationale gegevensdoorgifte
- datalekken

ACHTERGROND EN CONTEXT

omnibus-wetgeving met grote reikwijdte, in een nogal dynamische context

het juridisch antwoord daarop: open begrippen en vage normen

want dat is toekomst-bestendig en flexibel

maar (vooralsnog) erg weinig rechtspraak

en dus nog veel onopgehelderde begrippen en rechtsonzekerheid

en een (soms wat) grote rol voor (soms wat) activistische toezichthouders

edpb
European Data Protection Board

POLITICO

Meet the Dutchman who cried foul on Europe's tracking technology

As European governments rushed to embrace technology to fight the coronavirus, a plainspoken Dutchman emerged as a thorn in their side. Aleid Wolfsen's message: Don't pretend your solutions are privacy-friendly.

In a group that normally keeps disagreements quiet, Wolfsen stands out. A former politician and mayor of Utrecht who had no formal [illegible] his role in 2016, he has repeatedly been at odds with other watchdogs, most of whom do not share his political background.

The official in charge of Europe's grouping of privacy regulators was also keen to play down any disagreements. There is "no difference in the position" [illegible] different privacy regulators and the "Dutch case was a specific case," Andrea Jelinek said, while a spokesperson for the group, the European Data Protection Board, added: "The legal concept of anonymization is not an absolute concept."

Europe's Data Protection Supervisor, who had OK'd the Commission's use of telecoms data to track the coronavirus, said: "There is a difference between the technical impossibility of doing something to the very end, and something which we would call an effective anonymization."

Van je schulden hoeft de GGD niet te weten

De AVG dwingt tot nadenken voor doen

dicht bij elkaar staan. De medische dossiers bij de huisarts van mensen die geen toestemming gaven voor gebruik ervan door anderen, zijn toegankelijk gemaakt voor huisartsenposten en eerste hulpen in het ziekenhuis. Het kabinet werkt aan een spoedwet om locatiegegevens van mobiele bellers te laten onderzoeken door het RIVM, om zo voorspellingen te doen over de verspreiding van het virus.

Wolfsen eist dat het om maatregelen gaat die de bescherming van persoonsgegevens zo goed mogelijk waarborgen. „Over die spoedwet hebben wij net advies uitgebracht aan het kabinet. Wij sluiten niet uit dat de analyse van die locatiedata op een privacy-vriendelijke manier kan, maar dan moet aan strenge normen worden voldaan. Onze adviezen worden meestal opgevolgd, omdat wij een wet buiten werking kunnen stellen als de AVG wordt geschonden", zegt Wolfsen.

[illegible] leven breder. „Het grootschalig volgen van mensen die daar geen toestemming voor hebben gegeven, is door de AVG echt *not done* geworden. Dat lijkt met die locatiedata nu weer aan de kant te worden geschoven", zegt Benaissa van Bits of Freedom. „Niets is zo permanent als een tijdelijke maatregel", reageert ook

nu even praktisch

http://bit.ly/AVG-taalversies
vergelijk (naar keuze) drie verschillende taalversies van de AVG

www.privacy-regulation.eu
artikelen met relevante overwegingen, in alle taalversies

toetsvraag 1

De Algemene verordening gegevensbescherming (Avg) is, volgens de docent van deze cursus, omnibuswetgeving met een grote reikwijdte, die moet werken in een nogal dynamische context

A. Dit is juist
B. Dit is onjuist

betrokkenen, verwerkingsverantwoordelijken, verwerker, functionaris en autoriteit persoonsgegevens

DE SPELERS

de spelers

- *betrokkenen ('data subjects')*
  de natuurlijke personen op wie de persoonsgegevens betrekking hebben
- *verwerkingsverantwoordelijken*
  degenen die doeleinden en middelen van de verwerking bepalen
- *verwerkers*
  verwerken persoonsgegevens ten behoeve van de verwerkingsverantwoordelijken
- *Autoriteit persoonsgegevens (AP)*
  toezichthoudende autoriteit, bedoeld in artikel 51, eerste lid, AVG

«verwerkingsverantwoordelijke»

- de natuurlijke persoon, rechtspersoon, bestuurs-orgaan, of ieder ander
- die/dat [...] alleen of tezamen met anderen
- het doel en middelen van de verwerking vaststelt

gezamenlijke verantwoordelijkheid

hoe gedetailleerd omschreven?

waarom vindt de verwerking plaats? en wie heeft deze geïnitieerd?

Oftewel: wie gaat erover...?

art. 4(7) AVG

---

aan de hand van algemeen in het maatschappelijk verkeer geldende maatstaven moeten worden bezien aan welke natuurlijke persoon, rechtspersoon of bestuursorgaan de betreffende verwerking moet worden toegerekend

binnen de overheid zullen als verantwoordelijke te kwalificeren zijn: de afzonderlijke ministers op rijksniveau, het college van gedeputeerde staten en de commissaris van de Koningin op provinciaal niveau en het college van B&W en de burgemeester op gemeentelijk niveau (MvT)

Kamerstukken II 1997/98, 25892, nr. 3, p. 57

wie gaat erover..?

wie gaat over de bewaartermijnen of beveiligingsniveau?

wie beslist over outsourcing of programmatuur?

en wie over inzage- en verwijder- of vergeetverzoeken?

met wie sluiten de betrokkenen een overeenkomst?

wie moet er melden in geval van een datalek?

«verwerker»

art. 4(8) AVG

- degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt,
- zonder aan zijn rechtstreeks gezag te zijn onderworpen

en onder de verantwoordelijkheid van de verantwoordelijke

dus geen interne ICT-afdeling, werknemer of iemand anders die deel uitmaakt van de organisatie van de verantwoordelijke

De bewerker is allereerst een buiten de organisatie van de verantwoordelijke staande persoon of instelling.

[D]e bewerker […] neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens etc."

Niettegenstaande SWIFT zichzelf als een gegevensverwerker voorstelt en de onderneming in het verleden, afgaande op sommige feiten, in sommige gevallen als gegevensverwerker voor de financiële sector is opgetreden, is de Groep rekening houdende met de daadwerkelijke handelingsruimte van SWIFT in de hierboven beschreven situaties van oordeel dat SWIFT een voor de verwerking verantwoordelijke is

verwerkersovereenkomst

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

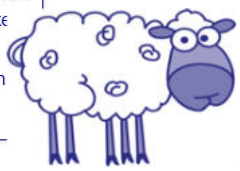
de functionaris

functionaris voor de gegevensbescherming of "FG"

verplicht voor
- overheden
- regelmatige en stelselmatige observatie op grote schaal
- grootschalige verwerking van bijzondere gegevens

taken:
- informeren en adviseren over AVG-verplichtingen
- toezicht houden op de naleving van die verplichtingen
- adviseren over DPIA's
- contact onderhouden met Ap
- samenwerken met Ap

vereisten:
- professionele kwaliteiten en, in het bijzonder, zijn (haar) deskundigheid op het gebied van de wetgeving en praktijk inzake gegevensbescherming
- vermogen om zijn (haar) taken vervullen



toetsvraag 2

De «verwerkingsverantwoordelijk» stelt doel en middelen van de verwerking van persoonsgegevens vast

A. Dit is juist
B. Dit is onjuist

toetsvraag 3

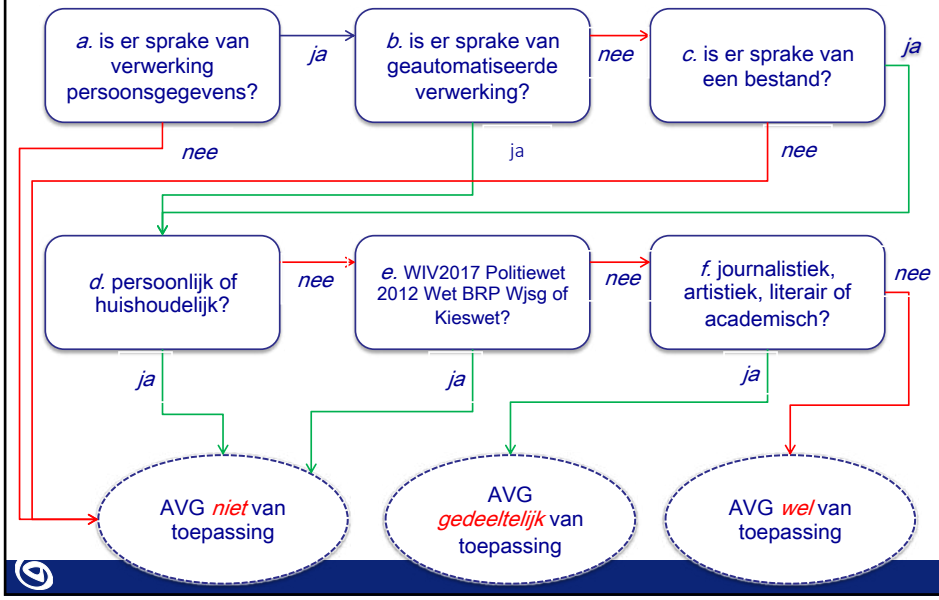
De «verwerker» verwerkt namens de verwerkingsverantwoordelijke persoonsgegevens

A. Dit is juist
B. Dit is onjuist

verwerking van persoonsgegevens, bestand, artistiek, literair journalistiek (en academisch), territoriale werking

HET SPEELVELD

toepassing (excl. territoriale werking)



de privacywet is van toepassing op

- de geheel of gedeeltelijk geautomatiseerd verwerkingen
- en soms ook op niet geautomatiseerde (handmatige) verwerkingen

"bestand"

verwerking van persoonsgegevens

gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon

kost het een onevenredige inspanning om aan de hand van het gegeven de desbetreffende natuurlijke persoon te identificeren..?

een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés

o.a. verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van ter beschikking stelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (enz.)

verwerking

GBA
Gegevensbeschermingsautoriteit

Mag een bedrijf of werkgever algemene en systematische controles van de lichaamstemperatuur van werknemers en/of bezoekers uitoefenen?

De Belgische Gegevensbeschermingsautoriteit beschouwt de loutere opname van de lichaamstemperatuur niet als een verwerking van persoonsgegevens. Voor zover dergelijke temperatuuropname dus niet gepaard gaat met een bijkomende registratie of verwerking van persoonsgegevens, is de AVG niet van toepassing. In het algemeen geldt hier dat een werkgever geen maatregelen kan nemen die het bestaande arbeidsrechtelijk regelgevend kader of instructies van bevoegde overheden te buiten gaan.

persoonsgegevens

KvK-nr

info@bedrijfsnaam.nl

IP-adres

vof, zzp-er, eenmanszaak

+31(6)2251 8338

@zwnne

070 3538800

postcode huisnr.

nationaal wanbetalersregister

[D]e naam en het kvk-nummer van [eiser] [kan] als de verwerking van persoonsgegevens [..] worden aangemerkt. [..] Met de (handels)naam en het kvk-nummer van de onderneming van [eiser] kan immers de voor- en achternaam van [eiser] eenvoudig worden achterhaald.

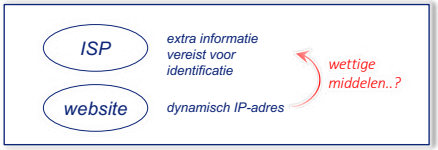
Rb A'dam15 september 2014
ECLI:NL:RBAMS:2014:5938

Breyer

Zie ook: HvJEU 17 juni 2021, C-597/19, ECLI:EU:C:2021:492, nr. 102

HJEU 19 oktober 2016 C-582/14 ECLI:EU:C:2016:779

[E]en dynamisch IP-adres dat door een aanbieder van onlinemediadiensten wordt geregistreerd telkens als een persoon een website bezoekt die door deze aanbieder toegankelijk wordt gemaakt voor het publiek, ten aanzien van die aanbieder [vormt] een persoonsgegeven [..], wanneer hij beschikt over wettige middelen waarmee hij de betrokken persoon kan identificeren aan de hand van extra informatie die bij de internetprovider van deze persoon berust.



Brein/Ziggo

Rechtbank Midden-Nederland 2 februari 2022 ECLI:NL:RBMNE:2022:297

Een IP-adres is dus een persoonsgeven voor degene die wettelijke mogelijkheden heeft om dat IP-adres met behulp van informatie van een isp aan een persoon te koppelen. Uit het [Breyer-]arrest lijkt te volgen dat het begrip "wettelijke mogelijkheden" door het Europese Hof ruim wordt opgevat. In het Breyer-arrest is immers overwogen dat van die wettelijke mogelijheden geen sprake is indien de identificatie van de betrokkene bij de wet verboden wordt of in de praktijk ondoenlijk is, bijvoorbeeld omdat zij – gelet op de [illegible] voor identificatie in werkelijkheid onbeduidend lijkt. De voorzieningenrechter concludeert daarom dat de mogelijkheid om (al dan niet via de rechter) NAW-gegevens van de gebruiker van een IP-adres bij de isp op te vragen, wel onder de in het Breyer-arrest bedoelde wettelijke middelen valt.

Haags fietsdepot

Rb. Den Haag 20 oktober 2020, ECLI:NL:RBDHA:2020:9590

7. *[V]erweerder [heeft] aannemelijk gemaakt dat binnen de gemeente Den Haag géén IP-adressen worden vastgelegd, opgeslagen en gekoppeld aan personen. Er is dan ook geen sprake van directe of indirecte herleidbaarheid naar personen. Daartoe is van belang dat verweerder heeft toegelicht dat IP adressen indirect herleidbaar kunnen zijn tot een persoon, maar dat daarvoor middelen moeten worden ingezet om dit te kunnen vaststellen. Verweerder heeft daarbij aangegeven dat het ondoenlijk qua tijd en mankracht is om van alle burgers met wie gecommuniceerd wordt, de identificatie via een IP-adres te achterhalen. Daarbij is van belang dat de gemeente niet zelf over de gegevens om een koppeling te kunnen maken tussen een IP-adres en een burger beschikt, maar zijn er gegevens nodig van een Internet Service Provider. Nu de verwerking een excessieve inspanning van verweerder vergt, waardoor het gevaar voor identificatie in de praktijk onbeduidend is, kan het IP adres niet beschouwd worden als persoonsgegeven.*

Haags fietsdepot

ABRvS 13 juli 2022
ECLI:NL:RVS:2022:1993

5.3 […] [D]e Afdeling [is] met de rechtbank van oordeel dat het college aannemelijk heeft gemaakt dat binnen de gemeente die IP-adressen niet worden opgeslagen, vastgelegd en gekoppeld aan personen en dat de gemeente zelf niet beschikt over de benodigde gegevens om een koppeling te kunnen maken tussen die IP-adressen en een burger. Een daadwerkelijk gevaar voor identificatie is onbeduidend.

AUTORITEIT PERSOONSGEGEVENS

Boete gemeente Enschede om wifitracking

De Autoriteit Persoonsgegevens (AP) geeft de gemeente Enschede een boete van 600.000 euro, omdat de gemeente wifitracking gebruikte in de binnenstad op een manier die niet mag. Daardoor was het mogelijk winkelend publiek en mensen die in de binnenstad wonen of werken te volgen.

Wifitracking in Enschede

De gemeente Enschede besloot in 2017 om via sensoren de drukte in de binnenstad te gaan meten. De gemeente huurde daarvoor een bedrijf in dat is gespecialiseerd in het tellen van passanten.

Meetkastjes in de winkelstraten vingen de wifisignalen op van de mobiele telefoons van passerende mensen. Ieders telefoon werd apart geregistreerd, met een unieke code.

Door te tellen hoeveel telefoons er op een bepaald moment rond een meetkastje zijn, weet je hoe druk het is. Houd je over een langere periode bij welke telefoon langs welk meetkastje komt, dan verandert dit 'tellen' in

Uit onderzoek van de AP bij de gemeente Enschede blijkt dat dit aan de hand was. De privacy van burgers was dus niet goed gewaarborgd, omdat zij konden worden gevolgd zonder dat dit noodzakelijk was.

Het was niet de intentie van de gemeente om individuen te volgen. En de AP heeft ook geen aanwijzingen gevonden dat dit is gebeurd. Maar het inzetten van wifitracking die dit mogelijk maakt, is op zichzelf al een ernstige overtreding van privacywet AVG.

Enschede: geen onevenredige inspanning, zegt AP

Bij [LEVERANCIER] is [..] de exacte locatie van de sensoren bekend en heeft men toegang tot het werkgeheugen en de software die draait op elke sensor. Tegelijk met een nieuwe detectie van een mobiel apparaat door een sensor is het bijvoorbeeld voor iemand van [LEVERANCIER] mogelijk om ter plaatse of via een camera waar te nemen welke persoon binnen het bereik van de sensor komt lopen. Vooral op stille momenten in de binnenstad leidt dit direct tot identificatie van de natuurlijke persoon. Ter controle kan de persoon in werking gevraagd naar zijn/haar MAC-adres. Dezelfde manier van identificeren is mogelijk in geval van gepseudonimiseerde MAC-adressen en de bijbehorende locatiegegevens, omdat ook dan op het moment van detectie ter plaatse of via een camera de persoon in kwestie waargenomen kan worden

alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt…?

POLITICO

Meet the Dutchman who cried foul on Europe's tracking technology

As European governments rushed to embrace technology to fight the coronavirus, a plainspoken Dutchman emerged as a thorn in their side. Aleid Wolfsen's message: Don't pretend your solutions are privacy-friendly.

In a group that normally keeps disagreements quiet, Wolfsen stands out. A former politician and mayor of Utrecht who had no formal training in data protection when he took on his role in 2016, he has repeatedly been at odds with other watchdogs, most of whom do not share his political background.

The official in charge of Europe's grouping of privacy regulators was also keen to play down any disagreements. There is "no difference in the positions" of different privacy regulators and the "Dutch case was a specific case," Andrea Jelinek said, while a spokesperson for the group, the European Data Protection Board, added: "The legal concept of anonymization is not an absolute concept."

Europe's Data Protection Supervisor, who had OK'd the Commission's use of telecoms data to track the coronavirus, said: "There is a difference between the technical impossibility of doing something to the very end, and something which we would call an effective anonymization."

kenteken

ECLI:NL:GHAMS:2016:146

Uitgaande van de definitie van artikel 1, onderdeel a, Wbp vormt een kentekengegeven voor de heffingsambtenaar in beginsel wel een persoonsgegeven, omdat hij via Cition de beschikking krijgt over onversleutelde kentekengegevens van voertuigen die binnen de Gemeente Amsterdam geparkeerd zijn en die door hem, na gegevensverstrekking door de RDW, aan een natuurlijk persoon kunnen worden gerelateerd.

Rb A'dam 11 december
2003 LJN AN9893

overledenen

"De Wbp is slechts van toepassing op gegevens die betrekking hebben op identificeerbare natuurlijke personen die nog in leven zijn. Een identificeerbare persoon is blijkens de wetgeschiedenis een persoon wiens identiteit zonder onevenredige inspanning kan worden vastgesteld. Uit de enkele vermelding "overlevend kind" uit het gezin van haar wel op de website te vermelden vader kan haast onmogelijk -laat staan zonder onevenredige inspanning- worden afgeleid dat eiseres de dochter is van die in 1942 in Auschwitz vermoorde vader. Eiseres is dan ook geen identificeerbare persoon in de zin van de Wbp.

toetsvraag 4

De rechtbank Den Haag vond dat de Gemeente Den Haag geen inzage hoefde te geven in de IP-adressen die waren geregistreerd.

A. Dit is juist
B. Dit is onjuist

handmatige verwerking ('bestand')

- gestructureerd geheel van persoonsgegevens
- dat volgens bepaalde criteria toegankelijk is

onderlinge samenhang
- gemeenschappelijke bestemming of
- verzameling die in de praktijk als een geheel worden beschouwd, of
- vooraf aangebrachte structuur van de verzameling of raadpleeg-methodiek die samenhang brengt

Art. 4(6) AVG

uitzonderingen

Art. 2(1) AVG

- verwerking t.b.v. persoonlijke of huishoudelijke doeleinden
- Politiewet, Wjsg, WIV2017, Wet BRP, Kieswet,

Overw. 18. Tot persoonlijke of huishoudelijke activiteiten kunnen behoren het voeren van correspondentie of het houden van adres-bestanden, het sociaal netwerken en online-activiteiten in de context van dergelijke activiteiten.

Deze verordening geldt wel voor verwerkingsverantwoordelijken of verwerkers die de middelen verschaffen voor de verwerking van persoonsgegevens voor dergelijke persoonlijke of huishoudelijke activiteiten.

beperkte uitzondering voor verwerkingen met journalistieke, artistieke of literaire en academische doeleinden

het gebruik van een camera-systeem, dat door een natuurlijke persoon aan zijn gezinswoning werd bevestigd met als doel de eigendom, de veiligheid en het leven van de eigenaren van het huis te beschermen, maar ook de openbare ruimte in beeld brengt, en waarbij video-opnames van personen met behulp van opnameapparatuur doorlopend worden vastgelegd op bijvoorbeeld een harde schijf, wordt … niet aangemerkt als de verwerking van persoonsgegevens die in activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden wordt verricht.

HJEU 11 december 2014 C-212/13

verwerkingsgrondslagen, verzamel- en verwerkingsdoelen, doelbinding, kwaliteit en beveiliging van gegevens, transparantie

DE SPELREGELS

rechtmatige verwerking

toestemming

please do not tick the box if you do not want to receive our daily offers in your inbox

- eerst informeren
- aanvaarding algemene voorwaarden met instemmingsbepaling is onvoldoende
- intrekken 'te allen tijde' mogelijk
- jonger dan 16? dan toestemming door ouders
- vrijwillig gegeven…

Art. 4(11) en 6(1)a AVG

(32) Toestemming dient te worden gegeven door middel van een duidelijke actieve handeling, bijvoorbeeld een schriftelijke verklaring, ook met elektronische middelen, of een mondelinge verklaring, waaruit blijkt dat de betrokkene vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van zijn persoonsgegevens instemt. Hiertoe zou kunnen behoren het klikken op een vakje bij een bezoek aan een internetwebsite, het selecteren van technische instellingen voor diensten van de informatiemaatschappij of een andere verklaring of een andere handeling waaruit in dit verband duidelijk blijkt dat de betrokkene instemt met de voorgestelde verwerking van zijn persoonsgegevens. Stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit mag derhalve niet als toestemming gelden. De toestemming moet gelden voor alle verwerkingsactiviteiten die hetzelfde doel of dezelfde doeleinden dienen. Indien de verwerking meerdere doeleinden heeft, moet toestemming voor elk daarvan worden verleend. Indien de betrokkene zijn toestemming moet geven na een verzoek via elektronische middelen, dient dat verzoek duidelijk en beknopt te zijn en niet onnodig storend voor het gebruik van de dienst in kwestie.

duidelijke actieve handeling – dus niet stilzwijgend!

in vrijheid gegeven…

specifiek, geïnformeerd en ondubbelzinnig

afzonderlijke toestemming voor verschillende doeleinden

op duidelijke en beknopte wijze gevraagd en niet onnodig storend

(42) Indien de verwerking plaatsvindt op grond van toestemming van de betrokkene, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking. Met name in de context van een schriftelijke verklaring over een andere zaak dient te worden gewaarborgd dat de betrokkene zich ervan bewust is dat hij toestemming geeft en hoever deze toestemming reikt. In overeenstemming met Richtlijn 93/13/EEG van de Raad (10) stelt de verwerkingsverantwoordelijke vooraf een verklaring van toestemming op in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal; deze verklaring mag geen oneerlijke bedingen bevatten. Opdat toestemming met kennis van zaken wordt gegeven, moet de betrokkene ten minste bekend zijn met de identiteit van de verwerkingsverantwoordelijke en de doeleinden van de verwerking van de persoonsgegevens. Toestemming mag niet worden geacht vrijelijk te zijn verleend indien de betrokkene geen echte of vrije keuze heeft of zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen.

bewijsplicht m.b.t. toestemming

bewustheid dat toestemming is gegeven en hoever die reikt

begrijpelijk en gemakkelijk toegankelijk, duidelijke en eenvoudige taal

identiteit van de toestemmingvrager en de verwerkingsdoeleinden

'echte keuze' en weigering of intrekking kan zonder 'nadelige gevolgen'…

(43) Om ervoor te zorgen dat toestemming vrijelijk wordt verleend, mag toestemming geen geldige rechtsgrond zijn voor de verwerking van persoonsgegevens in een specifiek geval wanneer er sprake is van een duidelijke wanverhouding tussen de betrokkene en de verwerkingsverantwoordelijke, met name wanneer de verwerkingsverantwoordelijke een overheidsinstantie is, en dit het onwaarschijnlijk maakt dat de toestemming in alle omstandigheden van die specifieke situatie vrijelijk is verleend. De toestemming wordt geacht niet vrijelijk te zijn verleend indien geen afzonderlijke toestemming kan worden gegeven voor verschillende persoonsgegevensverwerkingen ondanks het feit dat dit in het individuele geval passend is, of indien de uitvoering van een overeenkomst, daaronder begrepen het verlenen van een dienst, afhankelijk is van de toestemming ondanks het feit dat dergelijke toestemming niet noodzakelijk is voor die uitvoering.

geen 'duidelijke wanverhouding' tussen toestemmingvrager en -gever…

afzonderlijke toestemming voor verschillende gegevensverwerkingen…

bij aangaan van overeenkomst geen toestemming verlangen voor verwerkingen die niet nodig zijn voor de uitvoering van die overeenkomst…

Echter, uit art. 7(4) AVG blijkt dat er in zo een geval alleen goed moet worden onderzocht of de toestemming in vrijheid is gegeven

vitaal belang…

Bonuskaart bleek van onschatbare waarde

Gepubliceerd: 22 augustus 2003 07:56
Laatste update: 22 augustus 2003 09:40

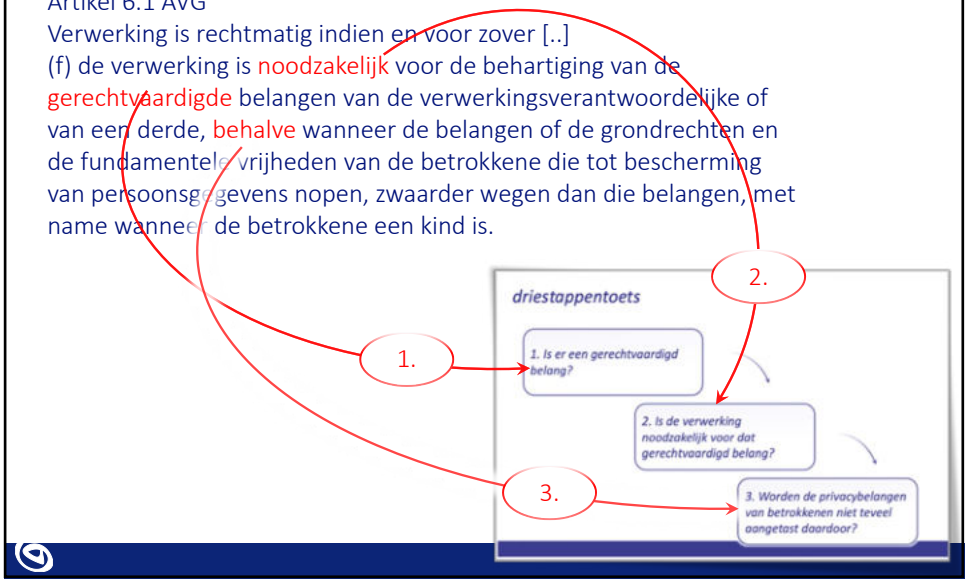
ZAANDAM - De bonuskaart van Albert Heijn is van "onschatbare waarde" gebleken bij het terughalen van Campina-producten die in een winkel van het supermarktconcern waren verkocht, aldus een woordvoerster van Albert Heijn, onderdeel van het Ahold.

"Met de klantgegevens konden we heel snel de mensen achterhalen die het product hadden gekocht", zei ze. Het ging om enkele tientallen stuks. Volgens de woordvoerster bleek na onderzoek dat één van de bij de klanten opgehaalde producten ook daadwerkelijk was "gemanipuleerd".

Albert Heijn ging tot actie over toen medio juni een vrouw ziek was geworden na het eten van het betreffende product, zogenoemde verwenkwark van het merk Mona. Het was de tweede keer dat Albert Heijn "handelend" moest optreden, aldus de woordvoerster.

gerechtvaardigd belang

Artikel 6.1 AVG
Verwerking is rechtmatig indien en voor zover [..]
(f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.



normuitleg gerechtvaardigd belang…

Wat ook niet als een gerechtvaardigd belang kwalificeert, is bijvoorbeeld: het enkel dienen van zuiver commerciële belangen, winstmaximalisatie, het zonder gerechtvaardigd belang volgen van het gedrag van werknemers of het (koop)gedrag van (potentiële) klanten, etc.

AP, Normuitleg 'gerechtvaardigd belang' 1 november 2019

AUTORITEIT PERSOONSGEGEVENS

Richtlijn 95/46 bevat wat het begrip „gerechtvaardigd belang" betreft geen definitie of opsomming. Dit begrip is tamelijk flexibel en open van aard. Mits op zichzelf wettig, bestaat er geen type van belang dat per se uitgesloten is.

AG Bobek 19 december 2018, C-40/17 (Fashion ID)

VoetbalTV

Opinion 06/2014 on legitimate interests, april 2014

Rigas, Volker und Markus Schecke en Eifert, en Ryneš, Promusicae

AG Bobek in FashionID

Rb Mid.NLD 23 november 2020, ECLI:NL:RBMNE:2020:5111

16. Gelet op de hiervoor aangehaalde Europese rechtspraak, conclusies van de advocaat-generaal en de opinie van de WP29, onderschrijft de rechtbank het standpunt van eiseres dat de vraag of een verwerker van persoonsgegevens een gerechtvaardigd belang heeft, aan de hand van een negatieve toets moet worden beoordeeld. Deze toets komt erop neer dat de verwerker geen belang mag nastreven dat in strijd is met de wet.

VoetbalTV

ABRvS 27 juli 2022, ECLI:NL:RVS:2022:2173

8. Met de rechtbank wordt geoordeeld dat in dit geval, gelet op de door VoetbalTV genoemde andere belangen, die niet van commerciële aard zijn, geen sprake is van een louter commercieel belang. De vraag of een uitsluitend commercieel belang op zichzelf een gerechtvaardigd belang in de zin van artikel 6, eerste lid, aanhef en onder f, van de AVG kan zijn, hoeft daarom niet te worden beantwoord.

Beslissing

De Afdeling bestuursrechtspraak van de Raad van State:

I. bevestigt de aangevallen uitspraak;

II. veroordeelt de Autoriteit Persoonsgegevens tot vergoeding van bij VoetbalTV B.V. in verband met de behandeling van het hoger beroep opgekomen proceskosten ...

KNLTB

Art. 8 Handvest: recht op bescherming persoons-gegevens → *AP: iedere gegevensverwerking is een inbreuk: 'natuurlijke personen dienen controle over hun eigen persoonsgegevens te hebben' (overw. 7 Avg)*

inbreuk bij wet, duidelijk en nauwkeurig, en voorspelbaar overeenkomstig rechtspraak HvJEU en EHRM (overw. 41 Avg)

gerechtvaardigd belang moet 'op zijn minst doelstellingen van algemeen belang raken die worden erkend in de EU of nodig zijn om rechten en vrijheden van anderen erkennnen' (r.o. 3.3 uitspraak)

Rb A'dam 22 september 2022, ECLI:NL:RBAMS:2022:5565

6. De rechtbank vindt zich daarom genoodzaakt om de volgende prejudiciële vragen aan het Hof van Justitie te stellen:

- *Hoe dient de rechtbank de term 'gerechtvaardigd belang' uit te leggen?*
- *Dient die term te worden uitgelegd zoals verweerder dat uitlegt? Zijn dat uitsluitend tot de wet behorende, wet zijnd, in een wet vastgestelde belangen? Of;* → *zgn. positieve toets*
- *Kan elk belang een gerechtvaardigd belang zijn, mits dat belang niet in strijd is met de wet? Meer specifiek gesteld: is een zuiver commercieel belang en het belang zoals hier aan orde, het verstrekken van persoonsgegevens tegen betaling zonder toestemming van de betreffende persoon, onder omstandigheden aan te merken als een gerechtvaardigd belang? Zo ja, welke omstandigheden bepalen of een zuiver commercieel belang een gerechtvaardigd belang is?* → *negatieve toets*

proportionaliteit & subsidiariteit

privacyinbreuk niet onevenredig in verhouding tot belang waarvoor gegevens worden verwerkt

belang kan niet op andere, minder belastende wijze worden gerealiseerd

Art. 5(1)a, 6(1) b-f AVG

verzamel- en verwerkingsdoelen

verzameldoel welbepaald uitdrukkelijk omschreven gerechtvaardigd

verdere verwerking niet onverenigbaar

Art. 5(1)b en 6(4) AVG

- relatie verzamel- en verwerkingsdoelen
- aard van de gegevens
- gevolgen voor betrokkene
- verkregen bij betrokkene of bij derden
- passende waarborgen

toetsvraag 5

In de KNLTB —zaak heeft de rechtbank Amsterdam prejudiciele vragen gesteld aan het Hof van Justitie van de EU

A. Dit is juist
B. Dit is onjuist

toetsvraag 6

In de VoetbalTV-zaak heeft de rechtbank Midden-Nederland de aan VoetbalTV opgelegde boete vernietigd

A. Dit is juist
B. Dit is onjuist

verwerkingsverbod voor «bijzondere gegevens»

- levensovertuiging of godsdienst
- politieke gezindheid
- lidmaatschap vakbond
- ras, etniciteit
- seksuele leven
- gezondheid
- biometrische ID-gegevens
- genetische gegevens

Art. 9 AVG

Art. 22-31 UAVG

- strafrechtelijke gegevens

Art. 10 AVG

Art. 32-33 UAVG

verwerking bijzondere gegevens verboden, tenzij…

- specifieke uitzonderingen: door bepaalde verwerkers en voor bepaalde doeleinden
- algemene uitzonderingen: met uitdrukkelijke toestemming, duidelijke openbaar gemaakt door betrokkene, (enz.),
- enz…

vraagstukken

- gegevens betreffende ras of etniciteit
- gegevens betreffende gezondheid
- biometrische ID-gegevens
- etc.

- *foto's. video-opnames*
- *nationaliteit*

?

- *leeftijd, geboortedatum*
- *gewicht, lengte*

?

- *toetsaanslagen*
- *stemgeluid*
- *foto..?*

?

Overw. 51 AVG: foto's vallen alleen onder de definitie van biometrische gegevens wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken.

Bodil Lindqvist

HJEU 6 November 2003, C-101/01, ECLI:EU:C:2003:596

Feiten

Bodil knutselt een website en vermeldt daarop dat "een van haar collega's haar voet had bezeerd en met gedeeltelijk ziekteverlof was"

Rechtsvraag

Is de mededeling op een homepage, dat een bij name genoemde collega haar voet heeft bezeerd en met gedeeltelijk ziekteverlof is, een persoonsgegeven over de gezondheid?

Antwoord

Ja. "Gelet op het doel van de richtlijn, moet aan de uitdrukking «gegevens die de gezondheid betreffen»[…] een ruime uitlegging worden gegeven, zodat informatie over alle — zowel fysieke als psychische — aspecten van iemands gezondheid daaronder valt.

[D]e vermelding van het feit dat iemand zijn voet heeft bezeerd en met gedeeltelijk ziekteverlof is, een persoonsgegeven betreffende de gezondheid" (nrs. 50-52)

toetsvraag 7

Volgens AP zegt het feit dat iemand onder invloed is iets over de gezondheid van die persoon op dat moment, ongeacht de context, namelijk dat deze persoon op dat moment zowel geestelijk als lichamelijk niet goed functioneert (het evenwichtsgevoel en beoordelingsvermogen is verslechterd, er is sprake van tunnelzicht, etc.

A. Dit is juist
B. Dit is onjuist

persoonsnummers

Art. 46 UAVG

- nummer ter identificatie van betrokkene bij wet voorgeschreven
- alléén gebruiken ter uitvoering van betreffende wet of voor doeleinden bij wet bepaald

discussies over uitlener en inlener aannemer en onderaannemer

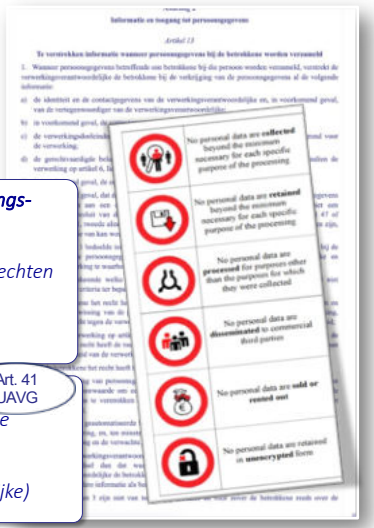
transparantie en rechten van betrokkenen

Art. 12-23 AVG

rechten van betrokkenen
- inzage
- verbetering
- bezwaar
- wissing (vergeten)
- gegevensover-draagbaarheid

verplichtingen verwerkings-verantwoordelijken
- informatieplichten
- voldoen aan inzagerechten

enz.



Art. 41 UAVG

uitzonderingen
- staatsveiligheid, gewichtige financiële en economische belangen van de staat
- voorkoming opsporing vervolging strafbare feiten
- rechten en vrijheden van derden (incl. verantwoordelijke)

verbod op derde-landen-doorgifte

Art. 44-45 AVG

landen buiten de Europese Unie c.q. Europese Economische Ruimte (EER)

EU én IJsland Liechtenstein Noorwegen

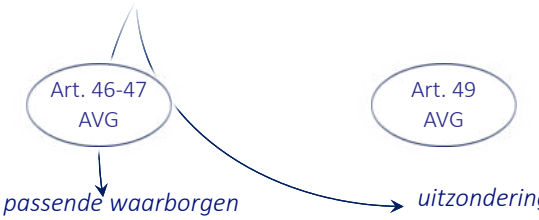
doorgifte mag alleen naar derde landen met passend beschermingsniveau

Schrems II: 'essentially equivalent'

EC Adequacy Decisions

- Andorra
- Argentinië
- Canada (bedrijven)
- Faroe Islands
- Guernsey
- Isle of Man
- Israel
- Japan
- Jersey
- New Zealand
- Uruguay
- Verenigd KOninkrijk
- ~~VS Privacyshield~~
- Zuid Korea
- Zwitserland

uitzonderingen op doorgifteverbod



passende waarborgen

- *modelcontracten ('standard contractual clauses' – SCC's)*
- *bindende bedrijfsvoorschriften ('Binding Corporate Rules – BCR's)*
- *gedragscodes*
- *certificering*

uitzonderingen voor specifieke situaties

- *toestemming van betrokkene*
- *uitvoering overeenkomst*
- *gewichtige reden van algemeen belang*
- *instelling uitoefeing rechtsvordering*
- *vitale belangen*
- *openbaar register*
- *incidentele, niet repitieve doorgifte m.b.t. beperkt aantal betrokkenen*

melding bij toezichthouder en betrokkene, meldloket en boetes

MELDPLICHT DATALEKKEN

Meldplicht datalekken

Art. 33-34
AVG

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. binnen 72 uur na bekend worden van het datalek

Hoe?
Meldloket Datalekken (AP)
zo-mogelijk individueel


AP legt Uber boete op voor te laat melden datalek
Haga beboet voor onvoldoende interne beveiliging patiëntendossiers
Het HagaZiekenhuis heeft de interne beveiliging van patiëntendossiers niet op orde. Dit blijkt uit onderzoek van de Autoriteit Persoonsgegevens (AP). Dit onderzoek volgde toen bleek dat tientallen medewerkers van het ziekenhuis onnodig het medisch dossier van een bekende Nederlander hadden ingezien. De AP legt het HagaZiekenhuis voor de onvoldoende beveiliging een boete op van 460.000 euro.
Rb DHG 31 maart 2021, ECLI:NL:RBDHA:2021:3090
[Haga heeft] ten tijde van belang wel maatregelen [...] genomen om te voorkomen dat persoonsgegevens in het digitale patiëntendossier worden ingezien door onbevoegde medewerkers, zoals onder meer de invoering van een extra waarschuwing die in beeld komt als een medewerker een dossier opent, de verplichtstelling van een e-learningcursus voor alle medewerkers die toegang hebben tot het elektronische patiëntendossier, de aanscherping van de arbeidsovereenkomsten en het waar mogelijk aanscherpen van autorisaties.
€110.000
de Rechtspraak
Boete voor ziekenhuis vanwege overtreden AVG
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 Haagse 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.


Het Parool
Datalek KvK: privéadressen van Kamerleden gelekt
De Kamer van Koophandel (KvK) heeft de
van zo'n 1800 mensen gelekt, waaronder
Kamerleden van D66, GroenLinks en Bij1.
privéadressen zijn opgevraagd door een v
advocaat die nog toegang had tot deze ge
gegevens, meldt RTL Nieuws.
AD
Oud-advocaat onder vuur na datalek KvK, privéadressen van Kamerleden op straat
Door een fout van de Kamer van Koophandel (KvK) zijn privéadr
van 1800 bestuurders van verschillende organisaties gelekt aan
advocaat. De instantie vraagt de gedupeerden het te melden als
ongewone activiteiten zijn rond hun woning, staat in een brief die op
sociale media circuleert.
deVolkskrant
Privégegevens 1.800 Kamerleden en bestuurders op straat door datalek KvK
Zo'n 1.800 privéadressen van politici en bestuurders van politieke organisaties zijn mogelijk in verkeerde handen gevallen. Dat heeft de Kamer van Koophandel (KvK) dinsdag bekendgemaakt. Een oud-advocaat had toegang tot deze afgeschermde persoonsgegevens in het Handelsregister, terwijl hij daartoe niet (meer) bevoegd was. Meerdere Kamerleden willen een debat over dit datalek.

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*

'onverwijld'

vanaf moment van bekend worden van datalek

- *door ververwerkingsverantwoordelijke zelf*
- *door verwerker(?)*

zonder onnodige vertraging

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

Evaluatie UAVG, alsmede Meldplicht datalekken en boetebevoegdheid

it's déjà vu all over again

De Uitvoeringswet AVG (UAVG) heeft slechts een beperkte toegevoegde waarde ten opzichte van de Algemene verordening persoonsgegevens (AVG). Dat komt vooral door het gebrek aan verdere invulling van de open normen in de UAVG. Dat draagt niet bij aan duidelijkheid voor de uitvoeringspraktijk.

Daarnaast zou de toezichthouder, de Autoriteit persoonsgegevens, de werkwijze rondom de bestuurlijke boete meer transparant kunnen vormgegeven en bij de meldplicht datalekken het toezicht op niet-melders kunnen intensiveren.

in het toezicht meer evenwicht tussen gemelde en niet-gemelde datalekken

onduidelijk hoe de hoogte van de boetes wordt vastgesteld

toetsvraag 8

De rechtbank Den Haag matigde de bestuurlijke boete die AP had opgelegd aan het Haga Ziekenhuis met €110.000

A. Dit is juist
B. Dit is onjuist

toetsvraag 9

In de evaluatie van de UAvg en Wet Meldplicht datalekken wordt de aanbeveling gedaan dat de toezichthouder de werkwijze rondom de bestuurlijke boete meer transparant maakt.

A. Dit is juist
B. Dit is onjuist

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.

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).

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.

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]

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.

melden..?

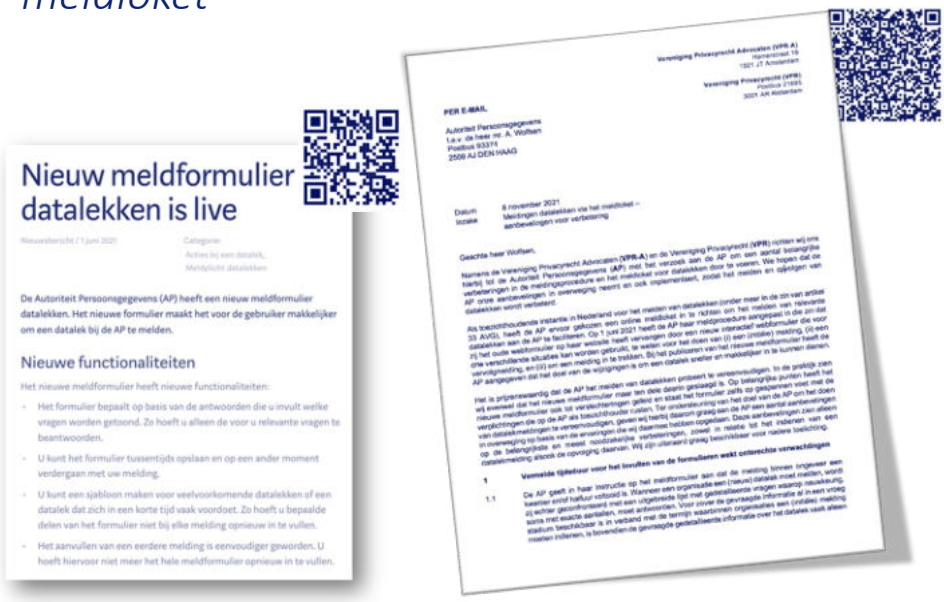
accounts passwords hack

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

melden..?


Update: LinkedIn Confirms Account Passwords Hacked

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 – verbeteringen voor verbetering

Geachte heer Wolfsen,

Namens de Vereniging Privacyrecht Advocaten (VPR-A) en de Vereniging Privacyrecht (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 oplossen 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 relevante 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 ons 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 heeft het nieuwe meldformulier ook tot verslechteringen geleid en staat het formulier zelfs op gespannen voet met de vergelijkingen 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 in overweging op basis van de ervaringen die wij daarmee hebben opgedaan. Deze aanbevelingen zien alleen op de belangrijkste en meest noodzakelijke verbeteringen, zowel in relatie tot het inbrengen van een datalekmelding alsook de opvolging daarvan. Wij zijn uiteraard graag bereikbaar voor nadere toelichting.

1 **Vermeide tijdsdruk 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 eenvoudig afgerond kan worden. 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 termijn waarbinnen organisaties een (initiële) melding moeten indienen, is bovendien de gevraagde gedetailleerde informatie over het datalek vaak alleen

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. Maa[illegible]'s volgende pagina uw keuze.

Om het doen van een melding zo goed mogelijk te laten verlopen, kunt u het be[illegible] een recent bijgewerkte browser gebruiken. Het invullen van het meldformulier du[illegible]urt ongeveer 15 - 30 minuten. Zorg dat u d[illegible]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)

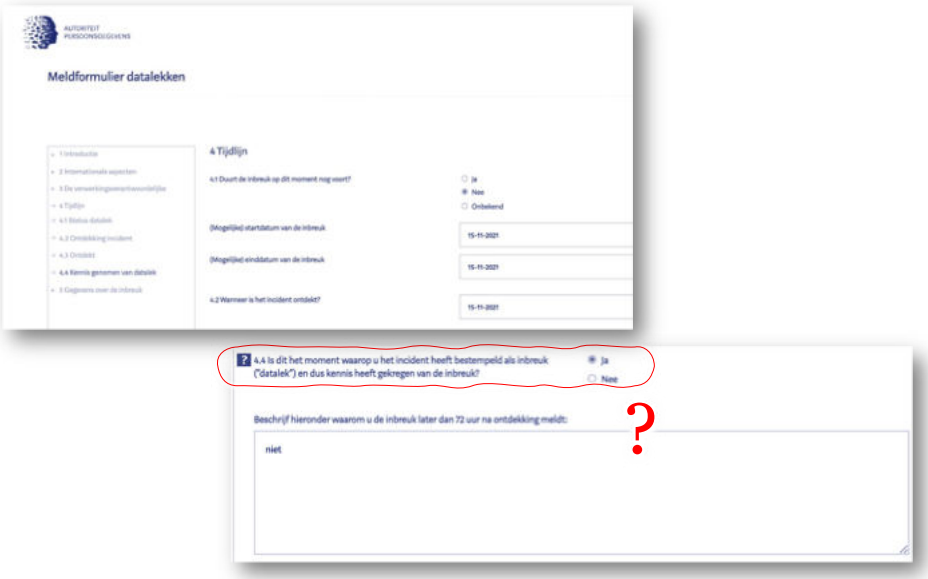
U bent verplicht om alle vragen te beantwoorden, tenzij anders aangegeven. Vul de vragen zo compleet en nauwkeurig mogelijk in. Indien uw melding onduidelijk of niet compleet is, kan de AP contact met u opnemen en inlichtingen opvragen of vorderen.

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.

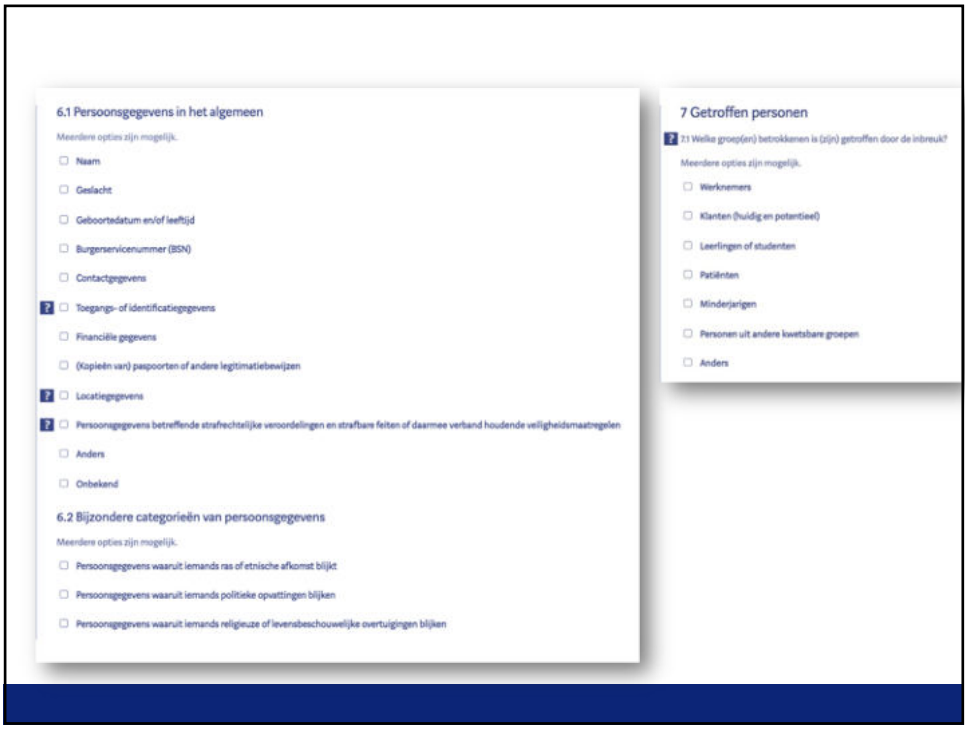
- Het bewaren van de sessie betekent niet dat u de melding naar de AP heeft verzonden.
- Bij het bewaren en laden van een sessie worden eerder geselecteerde bijlages niet opgeslagen in het .cas-bestand.

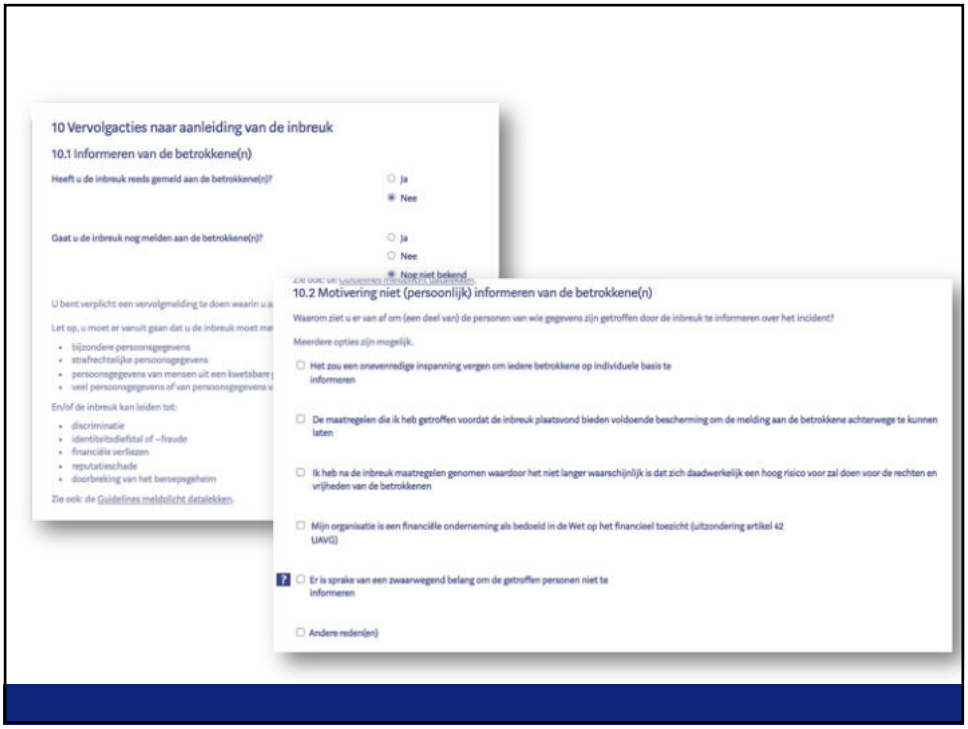
U kunt een overzicht krijgen met de reeds door u beantwoorde vragen door op "Toon overzicht" te klikken. Dit overzicht

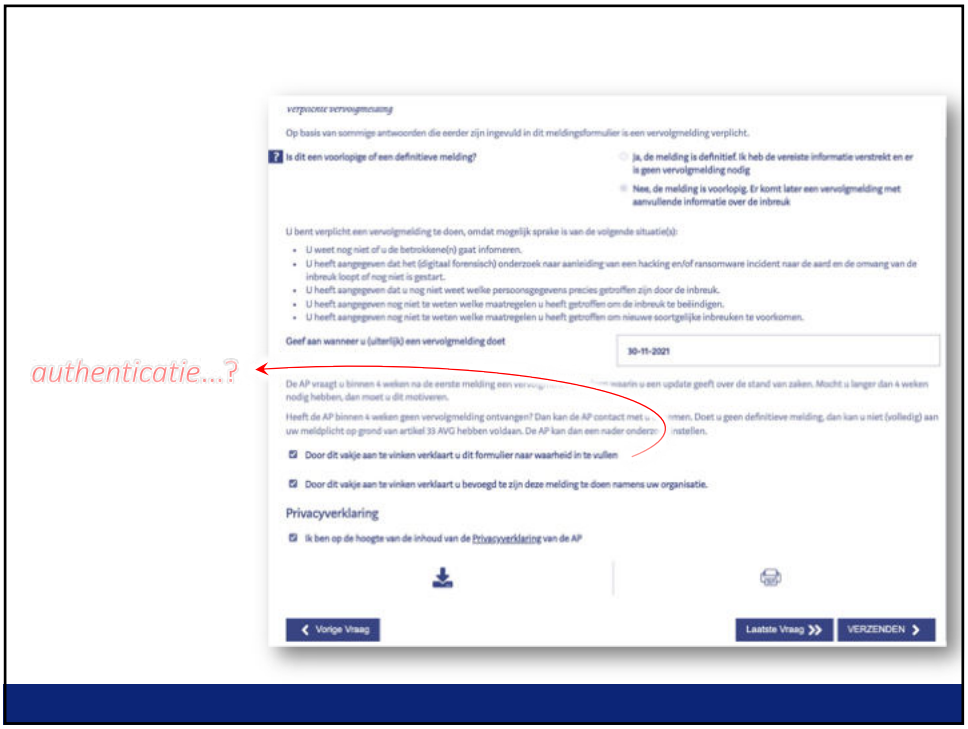
bulkmeldingen…



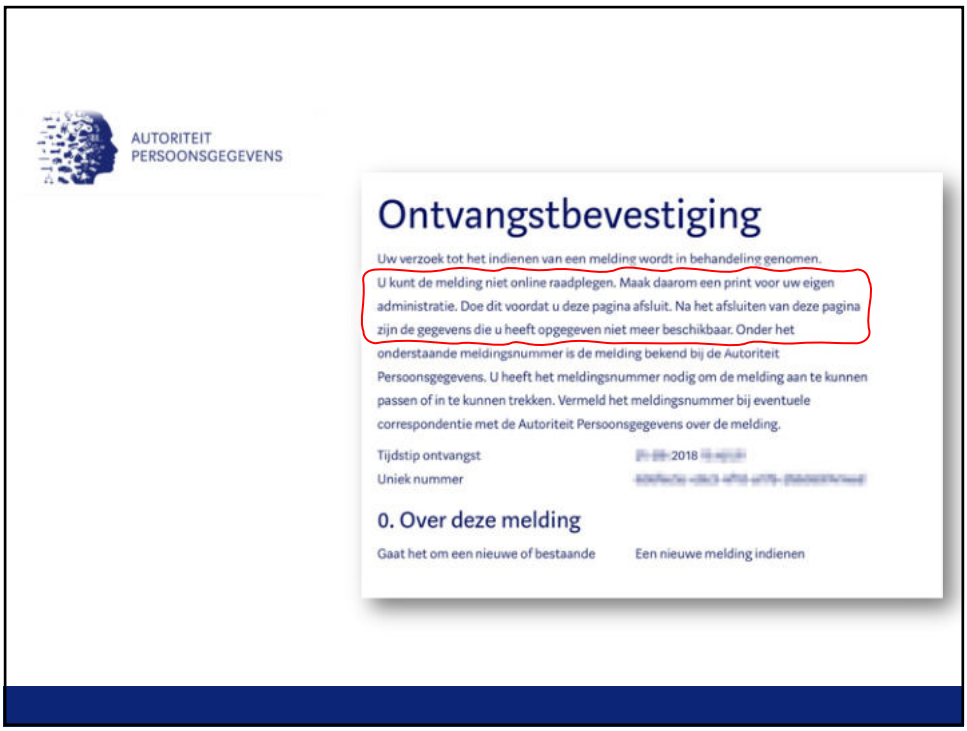

5 Gegevens over de inbreuk
5.1 Aard van de inbreuk
Meerdere opties zijn mogelijk.
Persoonsgegevens (mogelijk) ingezien door onbevoegden
Persoonsgegevens per ongeluk of onopzettelijk gewijzigd
Persoonsgegevens permanent niet beschikbaar (verloren/verwijderd)
Persoonsgegevens tijdelijk niet beschikbaar
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


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





authenticatie...?



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

Allianz
Global Assistance

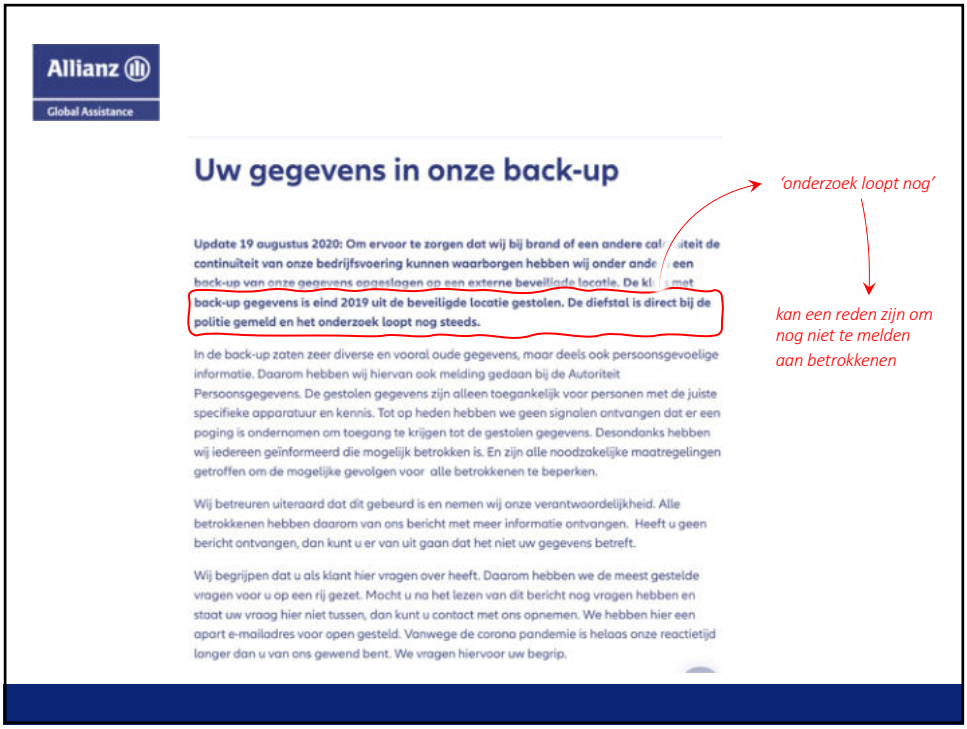
Uw gegevens in onze back-up

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.

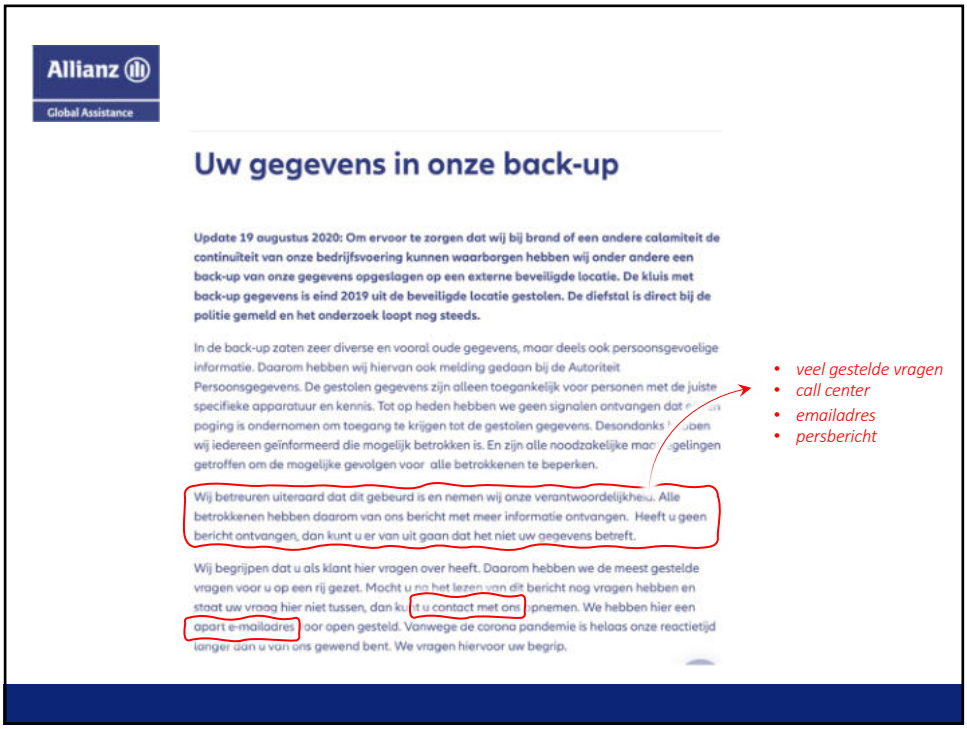
Wij betreuren uiteraard dat dit gebeurd is en nemen wij onze verantwoordelijkheid. Alle betrokkenen hebben daarom van ons bericht met meer informatie ontvangen. Heeft u geen bericht ontvangen, dan kunt u er van uit gaan dat het niet uw gegevens betreft.

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.


Allianz
Global Assistance
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 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


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.
'vooral oude gegevens'
kan een reden zijn om alleen te melden aan de betrokken van wie gegevens actueel zijn


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.
kennelijk niet encrypted, maar wel uitgefaseerde apparatuur
monitoren van zgn. darkweb


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
poging is ondernomen om toegang te krijgen tot de gestolen gegevens. Desondanks
wij iedereen geïnformeerd die mogelijk betrokken is. En zijn alle noodzakelijke
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

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."

vragen?

g.j.zwenne@law.leidenuniv.nl