



@zwnne

AVG & UAVG: toepassing en werking van de privacywet

Gerrit-Jan Zwenne | 11 mei 2023



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

en de spelregels

- verwerkingsgrondslagen
- doelbinding en bewaren
- bijzondere gegevens en bsn
- informatieplichten en rechten van betrokkenen
- 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 (voorsnog)
erg weinig
rechtspraak*

*en dus nog veel
onopgehelderde
begrippen en
rechtsonzekerheid*

*en een (soms wat)
grote rol voor (soms
wat) activistische
toezichhouders*





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

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."



Van je schulden hoeft de GGD niet te weten

De Algemene verordening gegevensbescherming wordt twee jaar na de invoering zijn verslag bevestigd. Met name en respecteren zijn zich veel beter van de privacy. Dit aspect wordt erin verwerkt tot de afname van de privacy van de consument.

De AVG dwingt tot nadenken vóór 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 locatiegegevens 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.

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



en 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



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



ASOPOS
DE VLIET



DAVILEX
LEDENADMINISTRATIE SOFTWARE



AUTORITEIT
PERSOONSGEGEVENS



«verwerkingsverantwoordelijke»

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

gezamenlijke verantwoordelijkheid

hoe gedetailleerd omschreven?

art. 4(7)
AVG

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

Oftewel: wie gaat erover...?



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?



*aan de hand van algemeen in het maatschappelijk
verkeer geldende maatstaven moeten worden gezien
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*



notaris (advocaat, belastingadviseur etc.)

Zijn het notarisbureau en/of de notaris jegens eisers aansprakelijk voor het doorzenden van een concept-leveringsakte met daarin opgenomen het geheime (nieuwe) woonadres van eiseres naar de kopers van de woning en naar de makelaar van eisers? *Vordering schade vergoeding o.g.v. art. 82 Avg*

Art. 17 Wna

1. De notaris oefent zijn ambt in onafhankelijkheid uit en behartigt de belangen van alle bij de rechtshandeling betrokken partijen op onpartijdige wijze en met de grootst mogelijke zorgvuldigheid.

Rechtbank Limburg 26 februari 2020, ECLI:NL:RBLIM:2020:1761

4.5.5. Naar het oordeel van de rechtbank moeten zowel de notaris als het notarisbureau worden aangemerkt als **verwerkingsverantwoordelijken** in de zin van de AVG. Zowel de notaris als het notarisbureau zijn immers verantwoordelijk voor de zorgvuldige totstandkoming van de te passeren akten. Zij moeten dan ook worden gekwalificeerd als de natuurlijke persoon en de rechtspersoon die **het doel van en de middelen voor de verwerking van persoonsgegevens vaststellen** (artikel 4, aanhef en onder 7 AVG). De rechtbank verwierpt derhalve het verweer dat de notaris ten onrechte is gedagvaard.



«verwerker»

art. 4(8)
AVG

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

onder de verantwoordelijkheid van de verantwoordelijke

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

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

[D]e verwerker [...] 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 gegevens-
bescherming of "FG"

verplicht voor

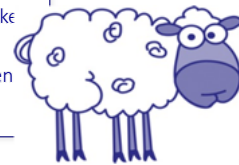
- overheden
- regelmatige en stelselmatige observatie op grote schaal
- grootschalige verwerking van bijzondere gegevens

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



én een specialisatieopleiding

Vereniging Privacyrecht Advocaten
(VPR-A)

toelatingseisen

- aantoonbaar diepgaande kennis van het privacyrecht



éérste specialisatievereniging

Vereniging Privacyrecht Advocaten
(VPR-A)

toelatingseisen

- aantoonbaar diepgaande kennis van het privacyrecht
- ten minste vijf jaar als advocaat een praktijk hebben gevoerd die voor ten minste 50% uit privacyrecht bestaat met een minimum van 500 uren aan privacyrecht per jaar





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



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'dam 15 september
2014
ECLI:NL:RBAMS:2014:5938

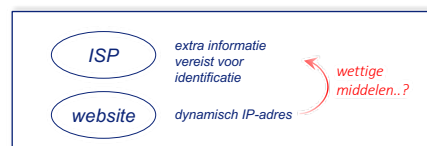


Breyer

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 mogelijkheden 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

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 één IP-adres is vastgeleed, ongeslaan 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 contact is gemaakt 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 verat, waardoor het gevaar voor identificatie in de praktijk onbeduidend is, kan het IP adres niet beschouwd worden als persoonsgegevens.



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-

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.



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. Toeslik 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

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...?





Probleemloos op pad: Minder Hinder App

Reizigers via hun smartphone, pc of tablet informeren over verkeershinder door wegwerkzaamheden én betere routealternatieven aanbieden. De Minder Hinder App is een mooi voorbeeld van de mogelijkheden van dynamisch verkeersmanagement. De app heeft inmiddels zijn meerwaarde bewezen in verschillende steden.

De basis voor de informatie komt uit een verkeersmanagementsysteem, zoals Vialis dat aan bijvoorbeeld de gemeente Zwolle leverde. Dit systeem wint informatie in uit verkeersregelinstallaties van de gemeente, provincie en Rijkswaterstaat. Daarnaast verzamelt het reistijdinformatie via bluetooth. Actuele parkeerinformatie komt rechtstreeks vanuit het parkeerverwijssysteem van de gemeente.

Met de Minder Hinder App ziet de reiziger op zijn scherm via rode en groene lijnen realtime waar de doorstroming in de gemeente het beste is. Zo kan deze zijn reis beter plannen. Wil iemand bijvoorbeeld met de auto naar het centrum, dan kan deze via de app zien hoe vol de parkeergarage daar is, welke route hij het beste kan nemen en of er verkeershinder onderweg is. Bovendien kan de reiziger via de app, dankzij een verbinding met verschillende webcams, live zien hoe de situatie op de weg is bij bepaalde wegwerkzaamheden.

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



Gerechtshof Amsterdam 7 januari 2016, 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.

NL 44-RSH-R



overledenen

Rb A'dam 11 december 2003 LJN AN9893

*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.*

Overw. 27 AVG

De onderhavige verordening is niet van toepassing op de persoonsgegevens van overleden personen. **De lidstaten kunnen regels** vaststellen betreffende de verwerking van de persoonsgegevens van overleden personen.



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,

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

Overw. 18 AVG

Tot persoonlijke of huishoudelijke activiteiten kunnen behoren het voeren van correspondentie of het houden van adresbestanden, 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.



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.

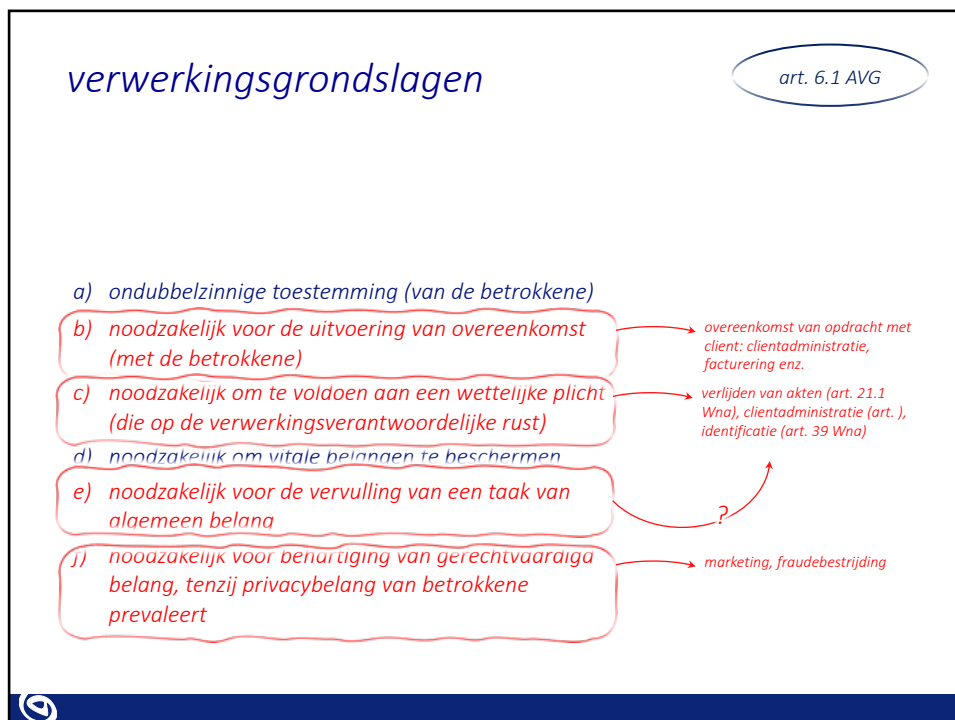
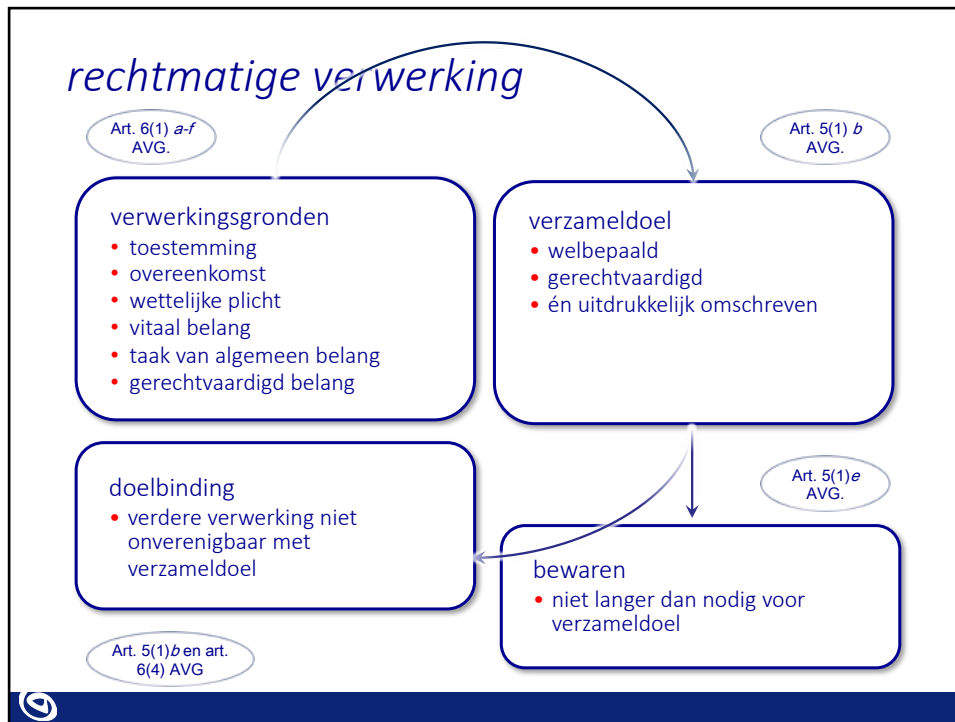
HJEU 11 december
2014 C-212/13



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

DE SPELREGELS





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 97/13/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 toestemmingvragers 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 toestemmingvragers en -gevers...

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 woordvoester 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 woordvoester 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 woordvoester.

verwerkingsgrondslagen

art. 6.1 AVG

- a) *ondubbelzinnige toestemming (van de betrokkene)*
- b) *noodzakelijk voor de uitvoering van overeenkomst (met de betrokkene)*
- c) *noodzakelijk om te voldoen aan een wettelijke plicht (die op de verwerkingsverantwoordelijke rust)*
- d) *noodzakelijk om vitale belangen te beschermen*
- e) *noodzakelijk voor de vervulling van een taak van algemeen belang*
- f) *noodzakelijk voor behartiging van gerechtvaardigd belang, tenzij privacybelang van betrokkene prevaleert*



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)



‘Toezichthouder gaat te ver met uitleg privacywet’
kritiek juristen op Autoriteit Persoonsgegevens

Privacytoezichthouder neemt heel opmerkelijk afstand van marktwerking



Boete voor tennisbond vanwege verkoop van persoonsgegevens

Nieuwsbericht / 3 maart 2020 Categorie: Direct marketing

De Autoriteit Persoonsgegevens (AP) legt tennisbond KNLTB een boete op van 525.000 euro voor het verkopen van persoonsgegevens. De KNLTB heeft in 2018 onrechtmatig tegen betaling persoonsgegevens van een paar honderdduizend van zijn leden verstrekt aan twee sponsors.

De Koninklijke Nederlandse Lawn Tennisbond (KNLTB) verstrekte de zoals naam, geslacht en adres, zodat zij een leden benaderen met tennisgerelateerde en sponsor ontving persoonsgegevens van aan 300.000 leden. Die sponsors benaderden per post of telefoon.

Het Parool

Privacywaakhond: VoetbalTV houdt zich op amateurvelden niet aan wetgeving

Via VoetbalTV, een initiatief van de KNVB en Talpa, kunnen professionele voetbalwedstrijden op amateurvelden volgen. Op meer dan 150 clubs zijn slimme camera's geplaatst die de bal volgen. Zo konden opmerkelijke acties of mooie doelpunten online worden teruggekeken en gedeeld.

In overzichtsbeeld

Vorig jaar november kwam de Autoriteit Persoonsgegevens (AP) met een negatief oordeel over de werkwijze van VoetbalTV. De privacywaakhond oordeelde dat de beelden een commercieel belang dienden en niet aan de privacywetten voldeden. Wat volgde waren maanden van onzekerheid, omdat onduidelijk bleef wat de consequenties van het oordeel van de AP waren.

Deur week stuurde VoetbalTV een mail aan de persbureaus, maar staat dat het platform uit de lucht wordt gehaald. Volgens het AP is VoetbalTV in overtreding, en hangt de dienst een sanctie boven het hoofd. 'Er rest ons daarom nu helaas niets anders dan onze dienstverlening per 27 augustus te stoppen, met pijn in ons hart aan te kondigen dat we de 'VoetbalTV'-app offline halen en ons op de verdere toekomst te beraden,' staat in de mail.

Sanctie

Maarten Hoeffler, directeur van VoetbalTV, wil de gevraagde niet toelichten hoe hoog de sanctie is die de AP heeft opgelegd. 'In aansluiting naar de rechtspraak die wij hier nog over gaan voeren kan ik daar nu niets over zeggen.'



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 persoonsgegevens

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 erkennen' (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;
- 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?

zgn. positieve toets

negatieve toets



DPS/Facebook

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

Rechtbank Amsterdam 15 maart 2023, ECLI:NL:RBAMS:2023:1407

12.68. Over de vraag of commerciële belangen een gerechtvaardigd belang kunnen vormen, heeft het HvJ EU zich nog niet uitgelaten. Over die vraag heeft de **bestuursrechter** aan deze rechtbank recent prejudiciële vragen gesteld aan het HvJ EU. [...]

Anders dan de Stichting heeft betoogd, ziet de rechtbank overigens vooralsnog **geen reden om aan te nemen dat commerciële belangen niet als een gerechtvaardigd belang [...] zouden kunnen worden aangemerkt.** Uit de rechtspraak van het HvJ EU blijkt dat niet en uit het advies van WP29 evenmin. **Integendeel, in het WP29-advies worden ook economische belangen van ondernemingen als voorbeeld genoemd.** Aan de door het HvJ en de in het WP29-advies genoemde eisen, dat het gestelde gerechtvaardigde belang bestaand, actueel (aanwezig), niet van hypothetische aard (werkelijk) en rechtmatig moet zijn, voldoet het door Facebook Ierland gestelde gerechtvaardigde belang in elk geval.

facebook



proportionaliteit & subsidiariteit

privacyinbreuk niet onevenredig in verhouding tot belang waarvoor gegevens worden verwerkt

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

belang kan niet op andere, minder belastende wijze worden gerealiseerd



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



bron:
@despeld

Basis	Persoonlijk	Persoonlijk+
Een veilig gevoel. U deelt beperkt informatie met ons. U kunt terecht bij een beperkt aantal zorgverleners.	U geeft inzage in betalingsgegevens, medisch dossier, lichaamsvloeistoffen en rijstijl. U krijgt ter controle een kastje in huis, auto en toilet. U kunt terecht bij alle zorgverleners.	U vertelt alles wat u weet over de leefstijl van uw naasten en bent bereid ver te gaan voor deze informatie. Maximale korting!
106,96 p/maand Kiezen	84,95 p/maand ✓ Gekozen Kiezen	62,95 p/maand Kiezen

jouw zorg moeiteloos verzekerd

jouw voordeel bij HEMA

- ✓ 10% korting op bijna het gehele HEMA assortiment
- ✓ basispremie vanaf 73,- per maand
- ✓ gewoon naar jouw eigen huisarts en apotheek

bereken nu jouw premie >

steven 3 minuten online geregeld

bron:
hema.nl



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

H/EU 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)



Vyriausioji tarnybinės etikos komisija

H/EU 1 augustus 2022,
C-184/20,
ECLI:EU:C:2022:601



 hoge commissie voor de voorkoming van belangenconflicten in de openbare dienst

Feiten

in een openbaar register worden gegevens van ambtenaren én hu echtgenoten of partners vastgelegd

Rechtsvraag

is er sprake van bijzondere gegevens als het gaat om gegevens die indirect seksuele gerichtheid (politieke opvattingen etc.) van iemand kunnen onthullen..?

Uitgangspunt

ruime uitleg van het begrip «bijzondere gegevens»

- vanwege contextuele analyse van het begrip «gezondheidsgegevens» (art. 4(15) Avg)
- door richtlijn (overw. 10) en verordening (overw. 4 en 10) beoogd hoog beschermingsniveau

Antwoord: ja

128 [...] [D]e publicatie van persoonsgegevens die indirect de seksuele gerichtheid van een natuurlijke persoon kunnen onthullen [...] [vormt] een verwerking van bijzondere categorieën van persoonsgegevens



Meta vs Bundeskartellamt

AG Rantos 20 September
2022, C-252/21,
ECLI:EU:C:2022:704



Feiten

Meta neemt via Facebook-cookies en social plugins (e.d.) kennis van gebruik van 'flirting-apps, datingsites voor homoseksuelen, website voor politieke partij(en) gezondheidsgereleerde websites'

Rechtsvragen

is er sprake van verwerking van **bijzondere** gegevens..?

En maakt het uit of Meta de **bedoeling** heeft bijzondere gegevens af te leiden uit de verkregen gegevens..?

En maakt het uit of Meta haar gebruikers '**waarheidsgetrouw**' categoriseert?

Antwoorden

Ja, ook dit betreft verwerking van bijzondere gegevens.

Neen, dat maakt niet uit, want...

"[h]et doorslaggevende element [...] is het feit dat de verwerkte gegevens het mogelijk maken om de gebruiker te profileren aan de hand van een van de in [art. 9.1 Avg] opgesomde categorieën van gevoelige persoonsgegevens" (nr. 38)

Neen, ook dat maakt niet uit, want

"[w]aar het om gaat is de mogelijkheid dat een dergelijke categorisering een aanzienlijk risico voor de grondrechten en de fundamentele vrijheden van de betrokkene inhoudt.(nr. 40)



toezichthouders in Spanje en Denemarken over Grindr

AEPD 17 January 2022

Datatilsynet (Denmark)
21 September 2021

hub



Grindr did not process any special categories of personal data [...] because it does not directly collect information regarding a person's sexual orientation, and that the platform does not even have a field to specify this information on a user's profile. [...]

AEPD accepted that Grindr's denial that use of the application would reveal any specific sexual orientation due to the fact that the platform is open to all sexual orientations and gender identities, and in Grindr's own words, including heterosexuals "out of curiosity or to find a broader expression of self or to interact with other users".

Datatilsynet held that processing information about a data subject's sex life or sexual orientation involved the processing of special categories of personal data, regardless of whether the data subject explicitly revealed their sexual orientation.

Additionally, the DPA highlighted the company's role as a controller for any personal data revealed in a data subject's "biography" on the website. Datatilsynet also emphasized that the company's privacy policy mentioned processing of personal data regarding sexual orientation. Datatilsynet therefore concluded that the controller processed special categories of personal data.



AP over een glas bier

Rapport definitieve
bevindingen november
2015 (Uniper)

[H]et feit dat iemand onder invloed is [zegt] 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). **Dit betekent niet perse dat deze persoon ziek is, maar zegt wel iets over zijn huidige geestelijke en lichamelijke gezondheid.**

dus niet één glas bier maar
wel drie of meer..(?)



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

rechten van betrokkenen

- inzage
- verbetering
- bezwaar
- wissing (vergeten)
- gegevensoverdraagbaarheid

Art. 12-23
AVG

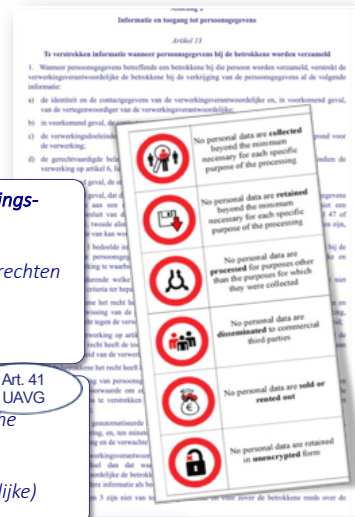
verplichtingen verwerkingsverantwoordelijken

- informatieplichten
- voldoen aan inzagerechten enz.

uitzonderingen

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

Art. 41
UAVG



melding bij toezichthouder en betrokkene, meldloket en boetes

BEVEILIGING EN MELDPLICHT DATALEKKEN



passende beveiligingsmaatregelen

Art. 32
AVG

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

- de pseudonimisering en versleuteling van persoonsgegevens;
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

2. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

open begrippen,
vage normen



Ik kreeg net een mailje van een notaris waarin stond dat mijn koopovereenkomst online voor me klaarstond. In de aanhef stond "aan meneer <mijn achternaam> en mevrouw <een andere achternaam die ik niet ken>". Oftewel, ze hebben de andere meneer "Albantar" dus willen aanschrijven, maar mijn emailadres gebruikt.

In de email stond een link naar een fileshare systeem. Dat blijkt beveiligd te zijn door een simpel "de laatste twee cijfers van uw telefoonnummer zijn <XX>; typ ter authenticatie de laatste vier cijfers van uw telefoonnummer in" dus ik heb geen toegang tot de toegestuurde gegevens anders dan dat ik nu weet dat ene meneer "Albantar" en mevrouw "onbekende achternaam" een huis aan het kopen zijn. Voor de duidelijkheid, ik was niet van plan om die documenten daadwerkelijk te gaan inzien of te downloaden, maar ik wilde alleen controleren of er nog een extra beveiliging op zat. Dat bleek dus het geval, maar een beveiliging van dit type is natuurlijk niet erg sterk; ik ga natuurlijk geen poging doen om via doxxen achter het juiste telefoonnummer te komen, hoewel dat vrij triviaal zou kunnen zijn waardoor een kwaadwillende wel toegang tot die gegevens had kunnen krijgen.

Nu is mijn vraag... Is dit een datalek volgens de AVG? Want ik vind het toch wel vrij zorgelijk dat een notaris zomaar zulke belangrijke documenten, waarin zonder twiifel veel persoonsgegevens staan, naar een onbekende derde partij stuurt door het gebruiken van een verkeerd emailadres, waar in ieder geval de slachtoffers (die meneer "Albantar" en mevrouw "onbekend") van op de hoogte gesteld zouden moeten worden door die notaris.



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



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**.

Haga beboet voor onvoldoende interne beveiliging patiëntendossiers

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 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 466.000 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 advocaat die nog toegang had tot deze gegevens, meldt *RITL Nieuws*.
 Het Parool 24 augustus 2020, 12:20

de Volkskrant
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 afgeschermd persoonsgegevens in het Handelsregister, terwijl hij daartoe niet (meer) bevoegd was. Meerdere Kamerleden willen een debat over dit datalek.
 Yvonne Hofst 24 augustus 2021, 15:05

Oud-advocaat onder vuur na datalek KvK, privéadressen van Kamerleden op straat
 Door een fout van de Kamer van Koophandel (KvK) zijn privéadressen 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.
 Sebastiaan Quast@innenredactie 24-08-21, 10:56 Laatste update: 24-08-21, 11:16



inbreuk of dreiging?



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

ransomware

daadwerkelijk gevolgen voor de persoonsgegevens:

- er zijn persoonsgegevens verloren gegaan
- niet uit te sluiten dat er gegevens onrechtmatig zijn verwerkt
- beveiligings- en herstelmaatregelen onvoldoende om negatieve gevolgen weg te nemen

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

Niet 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; gijbert@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@allenoverly.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@allenoverly.com; jonker@van-doorne.com; kerkvoorden@solv.nl; r.ketting@nysingh.nl; jeroen.koeter@projectmoore.com; konings@zenlaw.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; vanmanen@hoyngmonegier.com; alfred.meijboom@kvdl.nl; dj@micta.nl; lmoerel@mofo.com; joost.mosselman@dvan.nl; f.mutsaerts@banning.nl; Roelien van Neck; mmoordermeer@naxavelo.nl; joost.vanoijen@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; rijneveld@rijneveldlaw.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; spreij@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@ploom.nl; lieneke.viergever@projectmoore.com; eliane.devilder@brinkhof.com; eva.visser@projectmoore.com; volgenant@boeckx.com; t.de.weerd@houthoff.com; wbettink@xs4all.nl; weij@solv.nl; caspar@wenckebach.com; reinoud.westerdijk@kvdl.nl; p.vdviel@telfort.nl; hugo@wijnantsadvocaat.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. Allander, 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; rijneveld@rijneveldlaw.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; spreij@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@ploom.nl; lieneke.viergever@projectmoore.com; eliane.devilder@brinkhof.com; eva.visser@projectmoore.com; volgenant@boeckx.com; t.de.weerd@houthoff.com; wbettink@xs4all.nl; weij@solv.nl; caspar@wenckebach.com; reinoud.westerdijk@kvdl.nl; p.vdviel@telfort.nl; hugo@wijnantsadvocaat.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. Allander, 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 signature]



accounts passwords hack

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

Melding..?



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 gesteld. 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.





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. Maar **?** volgende pagina uw keuze.

Om het doen van een melding zo goed mogelijk te laten verlopen, kunt u het best 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



bulkmeldingen...



Meldformulier datalekken

→ 1 Introductie

→ 1.1 De melding van een inbreuk

1.1 De melding van een inbreuk

Wat wilt u doen?

- Een nieuwe melding doen van een inbreuk
- Een bestaande melding aanvullen of aanpassen
- Een bestaande melding intrekken

Wat voor soort datalek melding wilt u doen?

- Ik wil één inbreuk melden (reguliere melding)
- Ik wil meerdere gelijkaartige inbreuken, als gevolg van een grootschalige postverzending, tegelijk melden (bulkmelding)

? Heeft uw organisatie uitdrukkelijke schriftelijke toestemming ontvangen van de AP om inbreuken in bulk te melden?

- Ja
- Nee

U bent niet bevoegd om een bulkmelding te doen. Selecteer bij de vorige vraag de optie "Ik wil een inbreuk melden (Reguliere melding)".



AUTORITEIT PERSOONSgegevens

Meldformulier datalekken

1 Introductie
2 Internationale aspecten
3 De verwerkingsprocesvoordelen
4 Tijdlijn
4.1 Status datalek
4.2 Ontdekking incident
4.3 Onthald
4.4 Kennis genomen van datalek
5 Gegevens over de inbreuk

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort? Ja
 Nee
 Onbekend

(Mogelijk) startdatum van de inbreuk

(Mogelijk) einddatum van de inbreuk

4.2 Wanneer is het incident ontdekt?

4.4 Is dit het moment waarop u het incident heeft bestempeld als inbreuk ("datalek") en dus kennis heeft gekregen van de inbreuk? Ja
 Nee

Beschrijf hieronder waarom u de inbreuk later dan 72 uur na ontdekking meldt:

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

21 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

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)? Ja Nee

Gaat u de inbreuk nog melden aan de betrokkene(n)? Ja Nee Nog niet bekend

U bent verplicht een vervolgmelding te doen waarin u aangeeft of u de betrokkene gaat informeren.

Let op, u moet er vanuit gaan dat u de inbreuk:

- bijzondere persoonsgegevens
- strafrechtelijke persoonsgegevens
- persoonsgegevens van mensen uit een kwetsbare groep
- veel persoonsgegevens of van persoonsgegevens van een kwetsbare groep

En/of de inbreuk kan leiden tot:

- discriminatie
- identiteitsdiefstal of -fraude
- financiële verliezen
- reputatieschade
- doorbreking van het beroepsgeheim

Zie ook de [Guidelines meldplicht datalekken](#)

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

- Het zou een onovermatige inspanning vergen om iedere betrokkene op individuele basis te informeren
- De maatregelen die ik heb getroffen voordat de inbreuk plaatsvond bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten
- Ik heb na de inbreuk maatregelen genomen waardoor het niet langer waarschijnlijk is dat zich daadwerkelijk een hoog risico voor zal doen voor de rechten en vrijheden van de betrokkenen
- Mijn organisatie is een financiële onderneming als bedoeld in de Wet op het financieel toezicht (uitzondering artikel 42 LAAG)
- Er is sprake van een zwaarwegend belang om de getroffen personen niet te informeren
- Andere reden(en)



verplichte vervolgmelding

Op basis van sommige antwoorden die eerder zijn ingevuld in dit meldingsformulier is een vervolgmelding verplicht.

1 Is dit een voorlopige of een definitieve melding?

Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig.

Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk.

U bent verplicht een vervolgmelding te doen, omdat mogelijk sprake is van de volgende situatie(s):

- U weet nog niet of u de betrokkene(n) gaat informeren.
- U heeft aangegeven dat het (digitaal forensisch) onderzoek naar aanleiding van een hacking en/of ransomware incident naar de aard en de omvang van de inbreuk loopt of nog niet is gestart.
- U heeft aangegeven dat u nog niet weet welke persoonsgegevens precies getroffen zijn door de inbreuk.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om de inbreuk te beëindigen.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om nieuwe soortgelijke inbreuken te voorkomen.

Geef aan wanneer u (uiterlijk) een vervolgmelding doet

30-11-2021

De AP vraagt u binnen 4 weken na de eerste melding een vervolgmelding te doen waarin u een update geeft over de stand van zaken. Mocht u langer dan 4 weken nodig hebben, dan moet u dit motiveren.

Heeft de AP binnen 4 weken geen vervolgmelding ontvangen? Dan kan de AP contact met u opnemen. Doet u geen definitieve melding, dan kan u niet (volledig) aan uw meldplicht op grond van artikel 33 AVG hebben voldaan. De AP kan dan een nader onderzoek instellen.

Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

Ik ben op de hoogte van de inhoud van de [Privacyverklaring](#) van de AP

[← Vorige Vraag](#) [Laatste Vraag >>](#) [VERZENDEN >](#)

authenticatie...?

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 maatregelen getroffen om de mogelijke gevolgen voor alle betrokkenen te beperken.

Wij betreuen uiteraard dat dit gebeurt 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.



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 kluit 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 maatregelen 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



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 kluit 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 maatregelen 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



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 persoonsgegevens. Daarom hebben wij hiervan ook melding gedaan bij de Autoriteit Persoonsgegevens.

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 maatregelen 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 vgn. darkweb

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 persoonsgegevens. Daarom hebben wij hiervan ook melding gedaan bij de Autoriteit Persoonsgegevens.

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 maatregelen 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

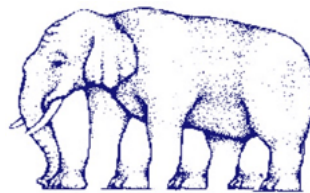


pro forma melding (tekstsuggestie)

“Er is naar oordeel van de verwerkingsverantwoordelijke géén sprake van een (meldingsplichtige) 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

