@zwnne

DINSDAG 17 MEI 13:30-18:00 | ~~ATRIUM~~ webinar ~~NTRE A'DAM~~

ontwikkelingen in privacywetgeving (AVG & UAVG)

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

iuris legal

eLaw Leiden

1

interessante debatten over de toepassing van de AVG en de rol van de toezichthouders

Bobek in Conclusie bij X vs AP

1. vragen over inzage

Prins in NJB

2. discussies over begrip «persoonsgegeven»

3. meldplicht datalekken

4. nog steeds het gerechtvaardigd belang

5. AVG en collectieve acties en schadevergoeding

6. wettelijke plicht of gerechtvaardigd belang

7. cookies en cookiemuren

(de rode draad)

2

if I go to a pub one evening

toepassing van de AVV

AG Bobek Opinion 6 October 2021, C-245/20 X v AP

56. If I go to a pub one evening, and I share with four of my friends around the table in a public place (thus unlikely to satisfy the private or household activity exception [..]) a rather unflattering remark about my neighbour that contains his personal data, which I just received by email (thus by automated means and/or is part of my filing system), do I become the controller of those data, and do all the (rather heavy) obligations of the GDPR suddenly become applicable to me? Since my neighbour never provided consent to that processing (disclosure by transmission), and since gossip is unlikely ever to feature amongst the legitimate grounds listed in Article 6 of the GDPR, (30) I am bound to breach a number of provisions of the GDPR by that disclosure, including most rights of the data subject

Prins over 'de toezichtreflex' (d.w.z. over AP)

rol van de toezichthouder

Vooraf 233

Rutte IV: toezichtreflex en Autoriteit Persoonsgegevens

Corien Prins

Het Vooraf staat ook op njb.nl/blogs

Sowieso is het [..] problematisch dat de AP nagenoeg zonder enige serieuze controle of reflectie standpunten uitdraagt die zich soms maar moeizaam verhouden met wat rechters of wetgever daarover hebben gezegd. Slechts spaarzaam kunnen deze standpunten door de rechter worden gecorrigeerd.

Reactie 749

De Autoriteit Persoonsgegevens als algoritme-waakhond; Toezichtreflex of...

Aleid Wolfsen[1]

De Autoriteit Persoonsgegevens is in inmiddels twee Voorjaarsnota's en een aantal moties met gebrekkige democratische legitimatie en onrechtmatig handelen. Dat zijn krasse standpunten. Alle reden dan ook om het grondrecht op bescherming van persoonsgegevens en de positie, taken en verantwoordelijkheden van de AP nog eens in een breder perspectief voor het voetlicht te brengen.

Het Coalitieakkoord benoemt 'digitalisering en (duurzame) technologieën' als een van de drie grote transities van de huidige tijd. Het bevat ambitieuze passages over de grondrechten die dat biedt 'voor onze samenleving en economie'. Maar het is ook waakzaam op de achterkant van deze transitie:

> 'Een digitale kloof en groeiende ongelijkheid in onze samenleving. Ook onze veiligheid, rechtsstaat, democratie, mensen- en grondrechten en concurrentievermogen staan onder druk. Dat vraagt om solide spelregels, toezicht en strategische autonomie.'

Hier is duidelijk oog voor het bewaken van de balans tussen de kansen van digitalisering voor economische groei en welvaartsgroei en de gevaren daarvan voor de belangen van iedere individuele burger. Terecht, want als gevolg van de sterk toenemende inzet van algoritmen en AI is de grens tussen 'Wat fantastisch dat dit kan' en 'Levensgevaarlijk wat hier gebeurt' nog nooit zo dun geworden.

Om die balans en die grens beter te kunnen bewaken heeft de coalitie besloten om de Autoriteit Persoonsgegevens (AP) in staat te stellen om actiever toezicht te kunnen houden op de inzet van algoritmen; de coalitie kwalificeert de AP expliciet als algoritme-waakhond.

Corien Prins heeft echter aarzelingen.[2] Die versterking van de AP lijkt haar een toezichtreflex, alhoewel de keuze op het eerste gezicht een logische lijkt'. De meest serieuze aarzelingen zijn van staatsrechtelijke aard. Ze wijst dan met name op 'het belang van ministeriële verantwoordelijkheid en parlementaire controle'. Want 'met het uitdijend arsenaal aan toezichthouders en activiteiten die daar worden belegd, kiift de ruimte voor ministeriële verantwoordelijkheid af'. En daarmee neemt ook de mogelijkheid van politieke beïnvloeding af. De zwakkere politieke positie van de AP wordt 'problematisch' genoemd, omdat dat tot gevolg heeft dat de AP nagenoeg zonder enige serieuze controle of reflectie standpunten uitdraagt die zich soms maar moeizaam verhouden met wat rechters of wetgever daarover hebben gezegd. Terecht, aldus Prins, vroeg ook de Raad van State in een rapport over de ministeriële verantwoordelijkheid[3] al aandacht voor deze zorgelijke ontwikkelingen. De Raad van State rept in dat rapport in relatie tot op EU recht gebaseerde 'regulatory' van 'zorgelijk makte politieke verantwoordelijkheid', omdat toezichthouders zoals de AP 'aan de nationale staatsrechtelijke verantwoordingsstructuren dreigen te worden onttrokken, terwijl tegelijkertijd onvoldoende duidelijk is welke Europese en/of nationale publieke verantwoordingsmechanismen daarvoor in de plaats zijn gekomen'. Met betrekking tot onder andere de AP zou moeten 'worden bezien hoe de publieke verantwoording kan worden verbeterd'. Prins concludeert dat de AP op de stoel van de politiek is gaan zitten.

> 'Dat betekent dat ze onafhankelijk van de politiek kunnen opereren.'

> 'Ingelijk handelen ze meer en meer op het terrein waar het primaat bij de wetgever en daarmee de politiek ligt. Daarmee ontstrekt de discussie en verantwoording over de normerende inkleuring – van rechtsnormen in het Handvest en de AVG, AIW – zich (vrijwel) volledig aan de bestaande mechanismen voor democratische controle en legitimiteit.'

> 'Illusoriteit' daarvoor zou zijn de wijze waarop deze autoriteiten in EU-verband bepijpen als 'grensbewaakingl belang, toestemming, (de voor gegevensverwerking) verantwoordelijke en dwingelte naar derde landen' invullen en voorzien van een "ruimte inkleuring".

Naschrift

750 Naschrift

Corien Prins[1]

Een ruim gooi woorden tellende reactie op mijn Vooraf van slechts 900 woorden. Laat ik het kort houden.

Mijn tekst is niet op een achternamiddag geschreven, maar ingegeven door talloze en al jarenlang consistente signalen en berichten vanuit de Hoge Colleges van Staat, de advocatuur en het privacywerkveld. Breed is de behoefte dat de AP zich openstelt voor meedenken, discussie en kritiek. Ik heb het voorbeeld in mijn redactieraad niet willen gebruiken, maar voor wie het nog niet had gemiskeerd (zowel in titel – *Meer en dichter door* – als in zijn conclusies) is een recent rapport van de Nationale ombudsman over de AP.[2] Een van diens observaties: 'De afhandeling van klachten lijkt bij de Autoriteit vooral gericht op het afhouden ervan.' Burgers vinden bij de AP al jaren geen gehoor en de Ombudsman concludeert dat' de manier waarop de Autoriteit nu werkt niet voldoet aan 'wat we van hen mogen verwachten.'

Juist vanwege het structurele karakter van dergelijke signalen is het jammer dat Wolfsen zich beperkt tot het verdedigen van de eigen positie en zich daarbij slechts beroept op formele en (institutionele (rechtsstatelijke) kaders; dat bij niet de gelegenheid aangrijpt tot kritische reflectie op de verantwoordelijkheid die de AP zelf binnen deze kaders heeft. Zo bespreekt Wolfsen het evenredigheidsbeginsel in het licht van de noodzakelijke zelfbeperking van de wetgever. Waardevol was het geweest als hij dat beginsel ook op de eigen organisatie had betrokken. Evenredigheid noopt immers ook de AP tot behoedzaamheid en zorgvuldigheid, gegeven de gevolgen die een besluit kan hebben. Het was interessant geweest te vernemen wat 'behoedzaamheid' en 'zorgvuldigheid' binnen de AP dan impliceren; niet alleen vanuit rechtsstatelijk redeneren, maar ook wat betreft concrete werkprocessen, communicatie en verantwoording.

Maar wie weet laat ik mijn oren te veel hangen naar het veld. Slaan zowel de Raad van State als ik de plank rechtsstatelijk volledig mis (hetgeen ik graag te betwijfelen).[3] We zullen het wellicht weten na de aankomende evaluatie waar Wolfsen naar verwijst. Daarbij ga ik er wel van uit dat de toetsingscriteria doelmatigheid en doeltreffendheid (artikel 39 Kaderwet ZBO's) worden uitgewerkt op basis van de zes principes van goed toezicht: naargelang de Rijksbrede kaderstellende visie op toezicht; dat het functioneren van de AP dus wordt beoordeeld langs de meetlat van: selectief, slagvaardig, samenwerkend, onafhankelijk, transparant en professioneel (Kamerstukken II 2005/06, 27831, nr. 15). ■

Evenredigheid noopt immers ook de AP tot behoedzaamheid en zorgvuldigheid, gegeven de gevolgen die een besluit kan hebben

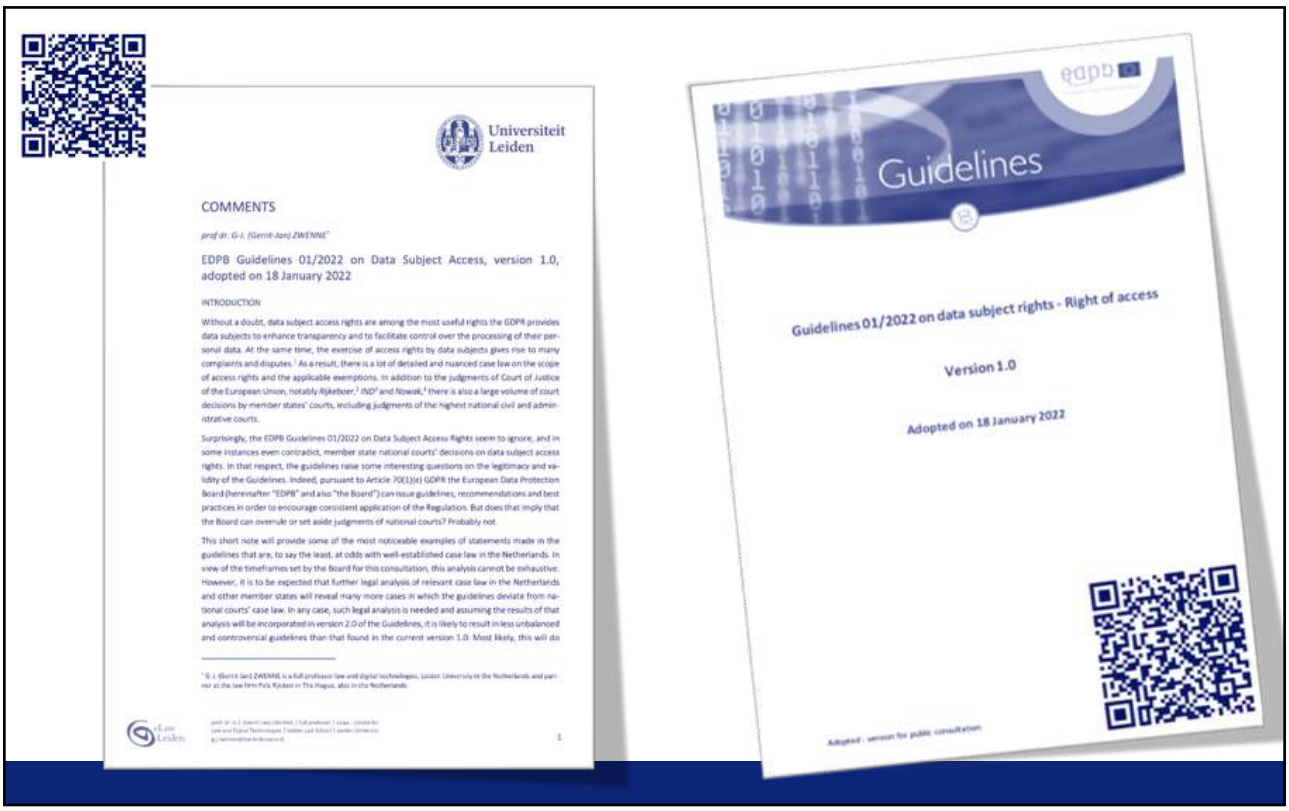
5

rol van de toezichthouder

[A]
VRAGEN OVER INZAGE

wat de European Data Protection Board ervan vindt en hoe dat zich (niet) verhoudt met nationale rechtspraak

6



7

wáár gaat het over?

art. 15 AVG

verzoek moet gepreciseerd zijn, maar behoeft niet te worden gemotiveerd

de natuurlijke persoon op wie de gegevens betrekking hebben

- *een recht van de betrokkene*
- *om op verzoek uitsluitsel te krijgen*
- *over het al dan niet verwerken van hem betreffende persoonsgegevens*
- *en als dat het geval is om inzage daarin te verkrijgen*
- *alsmede aanvullende relevante informatie*

gegevens waarover de verwerkingsverantwoordelijke beschikt (niet die hij kan samenstellen)

in beginsel een volledig overzicht, soms een kopie

herkomst, ontvangers etc.

8

EDPB over preciseren

35 In situations where the controller processes a large amount of data concerning the data subject, the controller may have doubts if a request of access, that is expressed in very general terms, really aims at receiving information on all kind of data being processed or on all branches of activity of the controller in detail. These may arise in situations, where there was no possibility to provide the data subject with tools to specify their request from the beginning or where the data subject did not make use of them. The controller then faces problems of how to give a full answer while simultaneously avoiding the creation of an overflow of information for the data subject that the data subject is not interested in and cannot effectively handle..

EDPB ziet te onbepaalde verzoeken vooral als probleem van de betrokkene, die geen wijs wordt uit de hem te verstrekken gegevens

hebben we daarvoor 'tools' nodig en is dat het probleem? waarom niet gewoon de betrokkene vragen zijn verzoek te preciseren?

volgens EDPB is het probleem dus vooral 'information overload'

9

EDPB over preciseren

35 There may be ways to solve this problem, depending on the circumstances and the technical possibilities, for example by providing self-service tools in online contexts […]. If such solutions are not applicable, a controller who processes a large quantity of information relating to the data subject may request the data subject to specify the information or processing to which the request relates before the information is delivered (see Recital 63 GDPR). This exceptional situation may exist for example in case of a company with several fields of activity or a public authority with different administrative units, if the controller found that numerous data relating to the data subject are processed in those branches as well as in cases where the controller has been collecting data upon frequent activities of the data subject for years.

myvodafone.nl; mijneneco.nl; mijnoverheid.nl etc.

ook voor camerabeelden, bezoekers-registratie, etc..?

uitzonderlijke situatie…?

10

'fishing expedition'

Art. 43 Wbp

De verantwoordelijke kan artikel 35 buiten toepassing laten voor zover dit noodzakelijk is in het belang van: […]

(e) de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

Hof Den Bosch 11 december 2014, ECLI:NL:GHSHE:2014:5221

7.12.8 [H]et hof [is] van oordeel dat het kennisnemingsverzoek van [appellanten] zo weinig concreet is dat gesproken moet worden van een ontoelaatbare 'fishing expedition'.

7.12.9. Het voorgaande betekent dat, voor zover daar door de Rabobank nog niet aan was voldaan, de verzoeken" van [appellanten] vanwege de onbepaaldheid daarvan moeten worden afgewezen.

Idem o.a.

Hof Den Bosch 1 februari 2018, ECLI:NL:GHSHE:2018:363

11

'fishing expedition'

Art. 43 Wbp

De verantwoordelijke kan artikel 35 buiten toepassing laten voor zover dit noodzakelijk is in het belang van: […]

(e) de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

AG Wuisman 15 januari 2016, ECLI:NL:PHR:2016:1

2.9.1 […] [V]eeleer valt aan te nemen dat het hof met 'fishing expedition' […] niet meer beoogt aan te geven dan dat het algemene verzoek van [verzoeker] c.s. een veel te omvangrijke en daarmee kostbare zoektocht binnen bij Rabobank aanwezige documenten, waaronder ook documenten van digitale aard, meebrengt en dat dit in redelijkheid niet van Rabobank valt te vergen. Dit vindt nog hierin bevestiging dat het hof […] over het kennisnemingsverzoek van [verzoeker] c.s. opmerkt dat het zo weinig concreet is.

12

'fishing expedition'

Art. 43 Wbp

De verantwoordelijke kan artikel 35 buiten toepassing laten voor zover dit noodzakelijk is in het belang van: […]

(e) de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

Hof Den Bosch 1 februari 2018, ECLI:NL:GHSHE:2018:363

3.7.6.In het onderhavige geval is in ieder geval van een concreet en - mede in het licht van de al wel verstrekte informatie - nader onderbouwd verzoek geen sprake. Het voorgaande betekent dat het hof in het onderhavige geval eveneens sprake acht van een 'fishing expedition', nu [appellant] (althans geacht moet worden) slechts een algemeen verzoek heeft (te hebben) gedaan zonder ook maar een begin van verduidelijking te geven waar hij […] meer duidelijkheid over wenst.

13

preciseren

Overw. 63 AVG

[..] Wanneer de verwerkings-verantwoordelijke een grote hoeveelheid gegevens betreffende de betrokkene verwerkt, moet hij de betrokkene voorafgaand aan de informatieverstrekking kunnen verzoeken om te preciseren op welke informatie of welke verwerkingsactiviteiten het verzoek betrekking heeft.

Rb A'dam 20 juni 2019, ECLI:NL:RBAMS:2019:4404

4.11.Integrale honorering van het verzoek van [verzoeker] om alle verwerkte persoonsgegevens zou onder deze omstandigheden niet alleen welhaast praktisch ondoenlijk zijn maar ook een veel te omvangrijke en daarmee kostbare zoektocht van [verweerster] meebrengen.

Om aan dit algemene verzoek te voldoen zou [verweerster] , alle bij haar aan te treffen documenten – ook die van digitale aard – moeten doorzoeken ten einde daaruit vervolgens die stukken te halen waarin ten minste één persoonsgegeven met betrekking tot [verzoeker] voorkomt en daartoe kosten maken.

Daarbij komt dat in de door [verzoekers] verzochte stukken persoonsgegevens van derden zullen voorkomen, zodat [verweerster] ….

14

preciseren…

Overw. 63 AVG

[..] Wanneer de verwerkings-verantwoordelijke een grote hoeveelheid gegevens betreffende de betrokkene verwerkt, moet hij de betrokkene voorafgaand aan de informatieverstrekking kunnen verzoeken om te preciseren op welke informatie of welke verwerkingsactiviteiten het verzoek betrekking heeft.

Rechtbank NHLD 23 mei 2019, ECLI:NL:RBNHO:2019:4283

4.17.Gelet op de grote hoeveelheid gegevens die de rechtbank Amsterdam [verwerkingsverantwoordelijke] verwerkt mag van [verzoekers] worden verwacht dat zij preciseren op welke informatie of welke verwerkingsactiviteit het verzoek betrekking heeft. Dat hebben zij gedaan in het aanvullende verzoekschrift onder I tot en met IX. Voor zover hun verzoek zich ook richt op andere dan de daarin genoemde gegevens hebben [verzoekers] dat onvoldoende duidelijk gemaakt.

Verzoek behoeft niet te worden gemotiveerd. Maar bij veelomvattend verzoek moet verzoeker wél duidelijk maken wat hij/zij wenst in te zien. En waarom(..?)

15

algemene zoekslag of diepgravend onderzoek

Rechtbank NHLD 23 mei 2019, ECLI:NL:RBNHO:2019:4283

12. [D]e formulering van het verzoek [bepaalt] mede de door het bestuursorgaan te verrichten zoekslag [..]. In het geval van een algemeen geformuleerd verzoek kan in beginsel van het bestuursorgaan slechts een algemene zoekslag worden gevergd naar de meest gangbare persoonsgegevens (onder meer NAW-gegevens). Bij een concreter geformuleerd verzoek ligt dit anders. In zo'n situatie kan van een bestuursorgaan een meer diepgravend onderzoek worden gevergd.

In eisers geval is sprake van een zeer algemeen geformuleerd verzoek. Voor verweerder was er daarom geen aanleiding om, anders dan eiser meent, ook te zoeken naar andere - minder voor de hand liggende - persoonsgegevens, zoals mogelijk verwerkte IP-adressen van eiser. Dit kon gelet op formulering van het verzoek niet van verweerder worden gevergd. Het IP-adres van eiser is ook geen direct kenbaar persoonsgegeven, dat verweerder bij zijn algemene zoekslag naar eisers persoonsgegevens had moeten betrekken en in het verwerkingsoverzicht had moeten opnemen.

16

EDPB over het doel van het inzagerecht

13. Given the broad aim of the right of access, the aim of the right of access is not suitable to be analyzed as a precondition for the exercise of the right of access by the controller as part of its assessment of access requests. Thus, controllers should not assess "why" the data subject is requesting access, but only "what" the data subject is requesting […] and whether they hold personal data relating to that individual [..]. Therefore, for example, the controller should not deny access on the grounds or the suspicion that the requested data could be used by the data subject to defend themselves in court in the event of a dismissal or a commercial dispute with the controller.

→ *het doel waarvoor de verzoeker het inzagerecht gebruikt is niet relevant…*

betrokkene mag inzagerecht gebruiken t.b.v. een ontslagprocedure…

17

de uniewetgever over de bedoeling van het inzagerecht

Preambule AVG

(63) Een betrokkene moet het recht hebben om de persoonsgegevens die over hem zijn verzameld, in te zien, en om dat recht eenvoudig en met redelijke tussenpozen uit te oefenen, zodat hij zich van de verwerking op de hoogte kan stellen en de rechtmatigheid daarvan kan controleren.

Preambule Rl. 95/46/EG

(41) Overwegende dat een ieder over het recht moet kunnen beschikken toegang te verkrijgen tot de gegevens die het voorwerp van een verwerking vormen en hemzelf betreffen, zodat hij zich van de juistheid en de rechtmatigheid van de verwerking ervan kan vergewissen; […]

de betrokkene kan zijn inzagerecht gebruiken om te controleren of de hem betreffende gegevens kloppen en op een rechtmatige wijze worden verwerkt

18

doelstelling van het recht nu en vroeger

Rb A'dam 9 april 2020, ECLI:NL:RBAMS:2020:2250

4.20. Het inzagerecht was voorheen in artikel 12 van de Richtlijn persoonsgegevens vastgelegd. Dat inzagerecht had tot doel de betrokkene in staat te stellen kennis te nemen van de persoonsgegevens die over hem zijn verzameld en te controleren of die gegevens juist zijn en rechtmatig zijn verwerkt.

Er zijn geen aanwijzingen dat onder de AVG de doelstelling en omvang van dit inzagerecht ten opzichte van de Richtlijn persoonsgegevens is gewijzigd. De rechtbank neemt dan ook tot uitgangspunt dat de uitspraken van het Hof van Justitie van de Europese Unie (HvJEU) en de Hoge Raad die zijn gewezen over het inzagerecht ten tijde van de Richtlijn persoonsgegevens ook gelding hebben nu de AVG van kracht is.

rechtspraak over art. 35 Wbp of art. 12a Rl 95/46/EG heeft onverminderd betekenis voor art. 15 AVG

19

rechtspraak over misbruik van het inzagerecht

HR 16 maart 2018, ECLI:NL:HR:2018:365

3.3.3. […] Richtlijn 95/46/EG […] die door de Wbp is geïmplementeerd, [stelt] de betrokkene in staat te controleren of zijn persoonsgegevens juist zijn en rechtmatig zijn verwerkt, ter bescherming van het recht van betrokkene op eerbiediging van zijn persoonlijke levenssfeer. Die controle kan dan leiden tot rectificatie, uitwissing of afscherming van de gegevens. De onderhavige vordering van [eiseres] is gericht op verkrijging van informatie ten behoeve van de onderhavige procedure en niet op het doel waartoe Richtlijn 95/46/EG strekt. […] Het gaat hier dus niet om persoonsgegevens in de zin van die richtlijn.

Idem:

Rb. NHLD 23 april 2019, ECLI:NL:RBMNE:2019:3762

20

rechtspraak over misbruik van het inzagerecht

ABRvS 6 november 2019, ECLI:NL:RVS:2019:3754

8. De informatie die [appellant] door middel van de 96 Wob-verzoeken en de 35 Wbp-verzoeken heeft opgevraagd houdt verband met dit ontslag uit 2009. […] Zoals de rechtbank terecht heeft geoordeeld, is de Wob niet bedoeld om die procedure weer over te doen. Dit geldt eveneens voor de Wbp. [..]

10. De Afdeling [is] van oordeel dat de zwaarwichtige gronden, [die aanwezig zijn als rechten worden gebruikt zonder redelijk doel of voor een ander doel dan waarvoor zij zijn gegeven] zich voordoen. [appellant] heeft misbruik gemaakt van de bevoegdheid om Wob- en Wbp-verzoeken in te dienen en daarmee heeft de rechtbank terecht het beroep niet-ontvankelijk verklaard.

Raad vanState

21

rechtspraak over misbruik van het inzagerecht

Rb R'dam 21 januari 2020, ECLI:NL:RBROT:2020:515

4.8 […] Het inzagerecht heeft tot doel de betrokkene in staat te stellen kennis te nemen van de persoonsgegevens die over hem zijn verzameld en te controleren of die gegevens juist zijn en rechtmatig zijn verwerkt. Ter gelegenheid van de mondelinge behandeling heeft [verzoeker] verklaard dat hij deze verzoeken uitsluitend heeft ingediend om zijn onschuld te bewijzen met stukken die betrekking hebben op procesdossiers waarin hij als procespartij betrokken was. Voor zover moet worden geconstateerd dat het doel dat [verzoeker] nastreeft geen betrekking heeft op het controleren of zijn persoonsgegevens juis zijn en rechtmatig zijn verwerkt, maar het te doen is om informatie te verkrijgen die hij wil gebruiken om in een eventueel tegen de Staat te starten procedure (nader) bewijs van zijn onschuld te kunnen leveren.

Het doel van [verzoeker] bij zijn inzagerecht ziet niet op de bescherming van persoonsgegevens zodat sprake is van misbruik van recht.

22

identificeren verzoeker


Wilt u op grond van de Algemene verordening gegevensbescherming (AVG) inzage in uw persoonsgege
Dan is de organisatie waarbij u inzage vraagt wettelijk verplicht uw identiteit vast te stellen. Maar de wet geeft niet aan hoe een organisatie dat moet doen.

Identiteit vaststellen
De organisatie moet uw identiteit vaststellen om te voorkomen dat iemand door uw naam te gebruiken inzage in uw gegevens kan krijgen. Hoe gevoeliger de gegevens, hoe meer waarborgen er nodig zijn.

Identiteitsbewijs niet altijd nodig
De organisatie mag niet zomaar vragen om uw identiteitsbewijs, zoals uw paspoort of identiteitskaart. Kan de organisatie uw identiteit ook op een andere, minder vergaande manier vaststellen? Dan moet de organisatie voor die manier kiezen.

rechtsvragen

- *mag een kopietje paspoort worden gevraagd om de identiteit van verzoeker vast te stellen?*
- *en mag worden verlangd dat verzoeker zich in persoon identificeert door met ID-bewijs langs te komen?*

Art. 12 AVG
6. [D]e verwerkingsverantwoordelijke [kan], wanneer hij redenen heeft om te twijfelen aan de identiteit van de natuurlijke persoon die het [inzage]verzoek indient, om aanvullende informatie vragen die nodig is ter bevestiging van de identiteit van de betrokkene.

23

Raad van State

ABRvS 9 december 2020, ECLI:NL:RVS:2020:2833

5.1. [I]n beginsel [heeft het college] ten aanzien van de wijze waarop zij de identiteit van de verzoeker wil vaststellen beleidsruimte [..]. Die ruimte wordt mede bepaald door enerzijds het uitgangspunt dat de identiteitsvaststelling deugdelijk moet zijn. Anderzijds door het gegeven dat de identiteitsvaststelling niet zo belemmerend mag werken dat daarmee aan het recht van de betrokkene zich vrijelijk tot het college te wenden met een inzageverzoek afbreuk wordt gedaan.

5.2. Het uitgangspunt dat een kopie van een identiteitsbewijs wordt gevraagd bij een inzageverzoek, wordt niet onredelijk geacht. Dit waarborgt een deugdelijke identiteitsvaststelling zonder dat afbreuk wordt gedaan aan het recht van betrokkenen om zich vrijelijk tot het college te wenden. Het college heeft in dit geval opgemerkt dat de handtekening op het verzoek en op het paspoort niet overeen kwamen met de handtekening op eerder ingediende Wob-verzoeken van een persoon met dezelfde naam die woont op hetzelfde adres. Het kon zich daarom in redelijkheid op het standpunt stellen dat daardoor twijfel is ontstaan over de identiteit van de verzoeker en alleen een kopie van het paspoort in dit geval niet voldoende was

24

ABRvS 9 december 2020, ECLI:NL:RVS:2020:2915

5.1. Het college vraagt standaard [..] om langs te komen op het gemeentehuis om zich te identificeren. Voor [appellant], die aan de andere kant van het land woont, betekent dit dat hij heel ver zou moeten reizen. Er waren in dit geval ook andere mogelijkheden om de identiteit vast te stellen, die een lagere drempel opwerpen. Het overleggen van een kopie van een paspoort wordt bijvoorbeeld in beginsel als een redelijke maatregel aangemerkt om de identiteit te controleren. [...].

[appellant] had een kopie van een gewaarmerkte kopie van zijn paspoort overgelegd. Het college kon aan de hand hiervan zijn identiteit controleren. Zoals het college ter zitting heeft toegelicht, twijfelde het niet aan de identiteit van [appellant]. Er bestond daarom geen reden om aanvullende informatie te vragen of aanvullende eisen te stellen. Dat het mogelijk is om een kopie te vervalsen en dat de gewaarmerkte kopie niet op de juiste wijze gewaarmerkt is, zoals het college heeft aangevoerd, maakt dat niet anders, omdat het college zelf te kennen heeft gegeven dat het niet vermoedde dat de kopie vervalst was of dat er mogelijk een ander persoon achter het verzoek zou zitten. De eis van het college was in dit geval daarom geen redelijke maatregel. De rechtbank heeft ten onrechte geoordeeld dat het college in redelijkheid van [appellant] heeft mogen eisen om langs te komen op het gemeentehuis.

Raad van State

25

EDPB over het identificeren van de verzoeker

73. It should be emphasized that using a copy of an identity document as a part of the authentication process creates a risk for the security of personal data and may lead to unauthorised or unlawful processing, and as such it should be considered inappropriate, unless it is strictly necessary, suitable, and in line with national law. In such cases the controllers should have systems in place that ensure a level of security appropriate to mitigate the higher risks for the rights and freedoms of the data subject to receive such data. It is also important to note that identification by means of an identity card does not necessarily help in the online context (e.g. with the use of pseudonyms) if the person concerned cannot contribute any other evidence, e.g. further characteristics matching to the user account.

kopietje paspoort of ID-kaart is niet passend

maar wat mag dan wel…?

26

vragen over de taken van de EDPB (‘het Comité)

Art. 70 AVG

1. Het Comité zorgt ervoor dat deze verordening consequent wordt toegepast. Daartoe doet het Comité op eigen initiatief of, waar passend, op verzoek van de Commissie met name het volgende:
[..]
(e) onderzoeken, op eigen initiatief of op verzoek van een van zijn leden dan wel op verzoek van de Commissie, van kwesties die betrekking hebben op de toepassing van deze verordening, en uitvaardigen van richtsnoeren, aanbevelingen en beste praktijken om te bevorderen dat deze verordening consequent wordt toegepast

betekent dit dat de EDPB kan voorbijgaan aan de nationale rechter…?

of dat EDPB-richtsnoeren voorgaan op rechterlijke uitspraken…?

toetsvraag 1

De Afdeling vindt het uitgangspunt dat een kopie van een ID-bewijs wordt gevraagd bij een inzageverzoek, niet onredelijk

A. Dit is juist

B. Dit is onjuist

rol van de toezichthouder

[2]
persoonsgegeven, of niet?

over passententellingen en
wifitracking in Enschede

29

AUTORITEIT PERSOONSGEGEVENS

Boete gemeente Enschede om wifitracking

Persbericht / 29 april 2021 Categorie:

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 het volgen van mensen.

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.

30

Is er sprake van «persoonsgegevens» …?

alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon

→ "de betrokkene" of "data subject"

kost het al dan niet een onevenredige inspanning om de betrokkene te identificeren?

maar, wat is identificeren eigenlijk..?

is alleen een uniek nummer (IP-adres, Mac-adres) voldoende om te spreken van identificatie..?

is «single-out» of «onderscheiden van anderen» voldoende om te spreken van identificeren?

31

«identificeerbaar»

Art. 4(1) AVG

als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator

bijvoorbeeld een naam, identificatienummer, locatiegegevens, online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon

IP-address, MAC-address

(26) […] Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken.

(30) Natuurlijke personen kunnen worden gekoppeld aan online-identificatoren via hun apparatuur, applicaties, instrumenten en protocollen, zoals internetprotocol (IP)-adressen, identificatiecookies of andere identificatoren zoals radiofrequentie-identificatietags. Dit kan sporen achterlaten die, met name wanneer zij met unieke identificatoren en andere door de servers ontvangen informatie worden gecombineerd, kunnen worden gebruikt om profielen op te stellen van natuurlijke personen en natuurlijke personen te herkennen.

32

«identificeren» wat is dat eigenlijk..?

~ **vaststellen wie iemand is**: *ze hebben de dode geïdentificeerd*

~ **aantonen wie je bent:** *kunt u zich identificeren?*

zich ~ *voorstellen dat hij een ander is: hij identificeert zich met het slachtoffe*

Art. 27a WvSv

De verdachte wordt ten behoeve van het vaststellen van zijn identiteit gevraagd naar zijn naam, voornamen, geboorteplaats en geboortedatum, het adres waarop hij in de basisregistratie personen is ingeschreven en het adres van zijn feitelijke verblijfplaats. Het vaststellen van zijn identiteit omvat tevens een onderzoek van een identiteitsbewijs

33

NN.PL133C.V.071030.100

HR 4 september 2012
ECLI:NL:HR:2012:BX4153

verdachte weigert bekend te maken wie zij is en daarom wordt zij in de stukken aangeduid met een nummer

zo een verdachte wordt aangemerkt als een anonieme, d.w.z. niet geïdentificeerde verdachte

34

deugdelijke vaststelling van identiteit

Artikel 12 AVG
6. [...] [D]e verwerkingsverantwoordelijke [kan], wanneer hij redenen heeft om te twijfelen aan de identiteit van de natuurlijke persoon die het verzoek indient als bedoeld in de artikelen 15 tot en met 21, om aanvullende informatie vragen die nodig is ter bevestiging van de identiteit van de betrokkene.


Alle antwoorden op mijn vragen

AUTORITEIT PERSOONSGEGEVENS

Vragen over het recht op inzage

Hoe weet een organisatie of ik het ben als ik een inzageverzoek doe?

Voordat de organisatie uw inzageverzoek in behandeling neemt, zal de organisatie meestal controleren wie u bent. Zij kan dat op verschillende manieren doen.

Minst privacygevoelig
Wil een organisatie uw identiteit controleren? Dan moet zij daarvoor die manier kiezen die het minst privacygevoelig is.

Het is bijvoorbeeld lang niet altijd noodzakelijk om een kopie van uw identiteitsbewijs te vragen. Vraagt u bijvoorbeeld om inzage bij een webshop? Dan is uw klantnum er in combinatie me uw naam en adres meestal genoeg om uw id ieren.

35

«single-out»...?

[data subject is] a natural person person who can be identified or singled out, directly or indirectly, alone or in combination with associated data, by means reasonably likely to be used by the controller ...

Draft LIBE-report of Albrecht January 2013

Art. 4(1) AVG

[data subject is] an identifiable natural person is one who can be identified, ~~or singled out~~, directly or indirectly, in particular by reference to an identifier ...

36

kamerbrief

Wat artikel 4 (begripsbepalingen) betreft, is er geen enkele steun voor het verder verfijnen van het begrip «persoonsgegevens» met categorieën als «singling out». De voorgestelde definitie lijkt Nederland en veel lidstaten al gecompliceerd genoeg.

Tweede Kamer der Staten-Generaal 2

Vergaderjaar 2012-2013

32 761 Verwerking en bescherming persoonsgegevens

Nr. 51 BRIEF VAN DE STAATSSECRETARIS VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 2 september 2013

In het algemeen overleg van 7 maart 2012 (Kamerstuk 32 761, nr. 27) heb ik toegezegd u periodiek op de hoogte te houden van de stand van zaken over de onderhandelingen in Brussel over de Algemene verordening gegevensbescherming en de richtlijn gegevensbescherming opsporing en vervolging.

In deze brief doe ik verslag van de onderhandelingsronden die in april, mei en juni 2013 hebben plaatsgevonden. Het betreft de tweede helft van de periode waarin iedere lidstaat het voorzitterschap van de Raad bekleedt. Ook deze periode heeft zich gekenmerkt door een hoge frequentie, lange duur en grote intensiteit van de onderhandelingen. In deze periode is de artikelsgewijze behandeling van verordening en richtlijn voortgezet. Ditmaal zijn de behandelingen achtereenvolgens gericht op het bereiken van een vorm van een akkoord in de JBZ Raad van 6 en 7 juni 2013. Het steeds verder verhogen van de druk op de delegaties om dat doel te bereiken, vooral in de allerlaatste periode van het Ierse voorzitterschap, is niet productief gebleken. Met name de grote lidstaten hebben uiting gegeven aan hun irritatie daarover. In deze verslagperiode is één vergadering aan de richtlijn gewijd. Alle overige vergaderingen betreffen de verordening.

Raadswerkgroep R, 10 en 11 april 2013

In deze raadswerkgroep is een begin gemaakt met de tweede behandeling van de tekst van de hoofdstukken I tot en met IV van de verordening op basis van een door het voorzitterschap opgestelde nieuwe tekst. Nederland blijft vragen houden bij artikel 1, derde lid. Het betreft een gebod om geen beperkingen of verboden op het vrij verkeer van persoonsgegevens binnen de Unie vast te stellen om redenen die verband houden met het beschermen ervan. Het is Nederland op zichzelf genomen duidelijk dat het beginsel van vrij verkeer van persoonsgegevens een geen andere beperkingen mag worden onderworpen dan de beperkingen die de verordening zelf vaststelt. Maar onduidelijk blijft of deze norm

Tweede Kamer, vergaderjaar 2012–2013, 32 761, nr. 51 1

Kamerstukken II 2012/13, 32761, nr. 51

37

HvJEU: Bodil Lindqvist

EHvJ 6 november 2003, C-101/01, ECLI:EU:C:2003:596

24. Het in […] begrip persoonsgegevens omvat volgens de definitie in artikel 2, sub a, daarvan iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Hieronder valt vanzelfsprekend iemands naam tezamen met zijn telefoonnummer of gegevens over zijn werksituatie en zijn liefhebberijen.
[..]
27. Derhalve moet op de eerste vraag worden geantwoord, dat het vermelden van verschillende personen op een internetpagina met hun naam of anderszins, bijvoorbeeld met hun telefoonnummer of informatie over hun werksituatie en hun liefhebberijen, als een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens [..] is aan te merken.

38

HvJEU: Scarlet SABAM

51 Het staat namelijk vast dat het rechterlijk bevel tot invoering van het litigieuze filtersysteem een systematische analyse van alle inhoud veronderstelt en de verzameling en identificatie van de IP-adressen van de gebruikers die illegale inhoud via het netwerk versturen. Aangezien *die IP-adressen* de precieze identificatie van die gebruikers mogelijk maken, vormen zij beschermde persoonsgegevens..

HJEU 24 november 2011, C-70/10

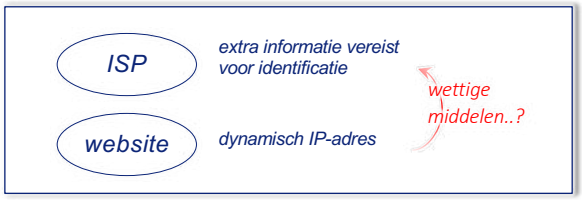
39

HvJEU: 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*.



40

Rb DHG: fietsendepot

Rechtbank 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.

41

Rb. MNL: Brein/Ziggo

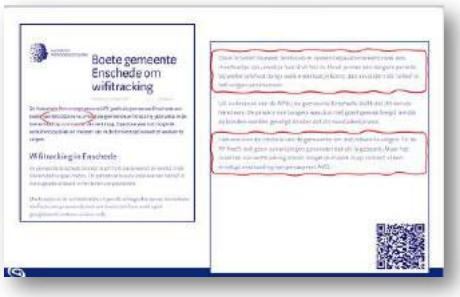
Rechtbank Midden NLD 2 februari 2022 ECLI:NL:RBMNE:2022:297

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 vereiste tijd, kosten en mankracht – een excessieve inspanning vergt, zodat het gevaar 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.

Dat Brein in het kader van de waarschuwingscampagne (nog) niet van plan is om NAW-gegevens bij Ziggo op te vragen (en, wanneer dat zonder succes blijft, deze van Ziggo te vorderen) en dat het niet zeker is dat – als zij dat wel doet – zij die gegevens ook verkrijgt, doet er niet aan af dat zij wel over dat wettelijke middel beschikt, dat de daarmee gemoeide tijd, kosten en mankracht niet excessief zijn in de genoemde zin en dat de IP adressen die Brein verzamelt dus ook ten aanzien van haar gelden als persoonsgegevens.

42

terug naar 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 worden 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…?

43

toetsvraag 2

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

44

rol van de toezichthouder

[3]
meldplicht datalekken

een vernieuwd en verbeterd meldloket

45

meldplicht datalekken

melding bij toezichthouder

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

Art. 33 AVG

melding bij betrokkene

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

Art. 34 AVG

Wie?

verwerkingsverantwoordelijke

Wat?

inbreuk op beveiliging van persoonsgegevens

Wanneer?

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

Hoe?

Meldloket Datalekken (AP)

zo-mogelijk individueel (betrokkenen)

46


AP legt Uber boete op voor te laat melden datalek
Haga beboet voor onvoldoende interne beveiliging patiëntendos
de Rechtspraak
Home Onderwerpen Uitspraken en nieuws Registers de Rechtspraak
Boete voor ziekenhuis vanwege overtreden AVG
Den Haag, 16 april 2021
De rechtbank Den Haag heeft op 31 maart 2021 uitspraak gedaan in een zaak over een boete die de Autoriteit Persoonsgegevens (AP) heeft opgelegd aan een Haags ziekenhuis. Het ziekenhuis kreeg de boete vanwege het overtreden van de AVG, persoonsgegevens van patiënten werden namelijk niet voldoende beschermd. De AP had een boete opgelegd van 460.0000 euro maar die heeft de rechtbank teruggebracht naar 350.000 euro.
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

47


UWV krijgt boete voor slechte beveiliging bij verzending groepsberichten
AP: Boete orthodontiepraktijk vanwege onbeveiligde patiëntenwebsite
Boete PVV Overijssel vanwege niet melden datalek
Boete Booking.com voor te laat melden datalek
Ziekenhuis OLVG beboet om onvoldoende beveiliging medische dossiers
AP beboet Transavia om slechte beveiliging persoonsgegevens

48

toetsvraag 3

Uber kreeg van AP een boete van 6.000.000 euro voor het te laat melden van een datalek

A. Dit is juist

B. Dit is onjuist

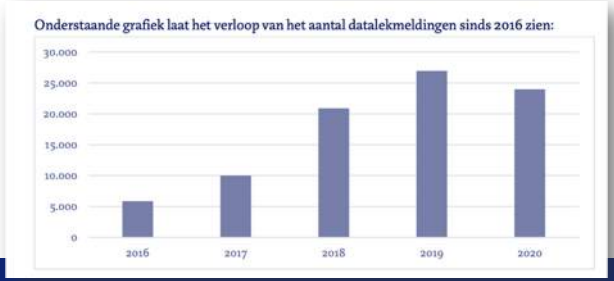
AUTORITEIT PERSOONSGEGEVENS

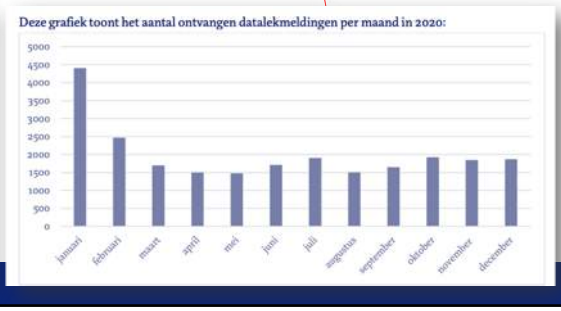
Rapportage Datalekken 2020

Meldplicht datalekken: facts & figures
Overzicht feiten en cijfers 2020

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

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





AUTORITEIT PERSOONSGEGEVENS

Jaarverslag AP 2021, p. 20

Wat de AP niét kon doen

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

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

Klachten
Veel burgers dienen een klacht[1] in over organisaties die de AVG niet naleven. De AP moet deze klachten behandelen, maar is onvoldoende in staat om organisaties waarover wordt geklaagd aan te spreken op hun gedrag. Of om er door middel van onderzoek en handhaving voor te zorgen dat zij de AVG alsnog gaan naleven.

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

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

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

d.w.z. 1 a 2 procent…

'slechts bij enkele honderden meldingen kan AP actie ondernemen'

'niet kunnen investeren in innovatie van toezicht'

API's kunnen helpen

51

AG CONNECT
the amazing world of IT

GOVERNANCE

Stijgende werklast door datalekken zorgt voor frustraties bij gemeenten

'Meldingen moeten efficiënter kunnen.'

22 APRIL 2022

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

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

2,5 tot 4 uur werk

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

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

AP: handmatig melden blijft nodig

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

?

52

VPR-A

55

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.

Vereniging Privacyrecht Advocaten (VPR-A)
Herenstraat 1/9
1621 JT Amsterdam

Vereniging Privacyrecht (VPR)
Postbus 21685
3001 AR Rotterdam

PER E-MAIL

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

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

Geachte heer Wolfsen,

Namens de Vereniging Privacyrecht Advocaten (**VPR-A**) en de Vereniging 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 opvolgen 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 (de voor- en 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 verplichtingen die op de AP als toezichthouder rusten. Ter ondersteuning van het doel van de AP om het doen van datalekmeldingen te vereenvoudigen, geven wij hierbij daarom graag aan de AP een aantal aanbevelingen 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 indienen van een datalekmelding alsook de opvolging daarvan. Wij zijn uiteraard graag beschikbaar voor nadere toelichting.

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

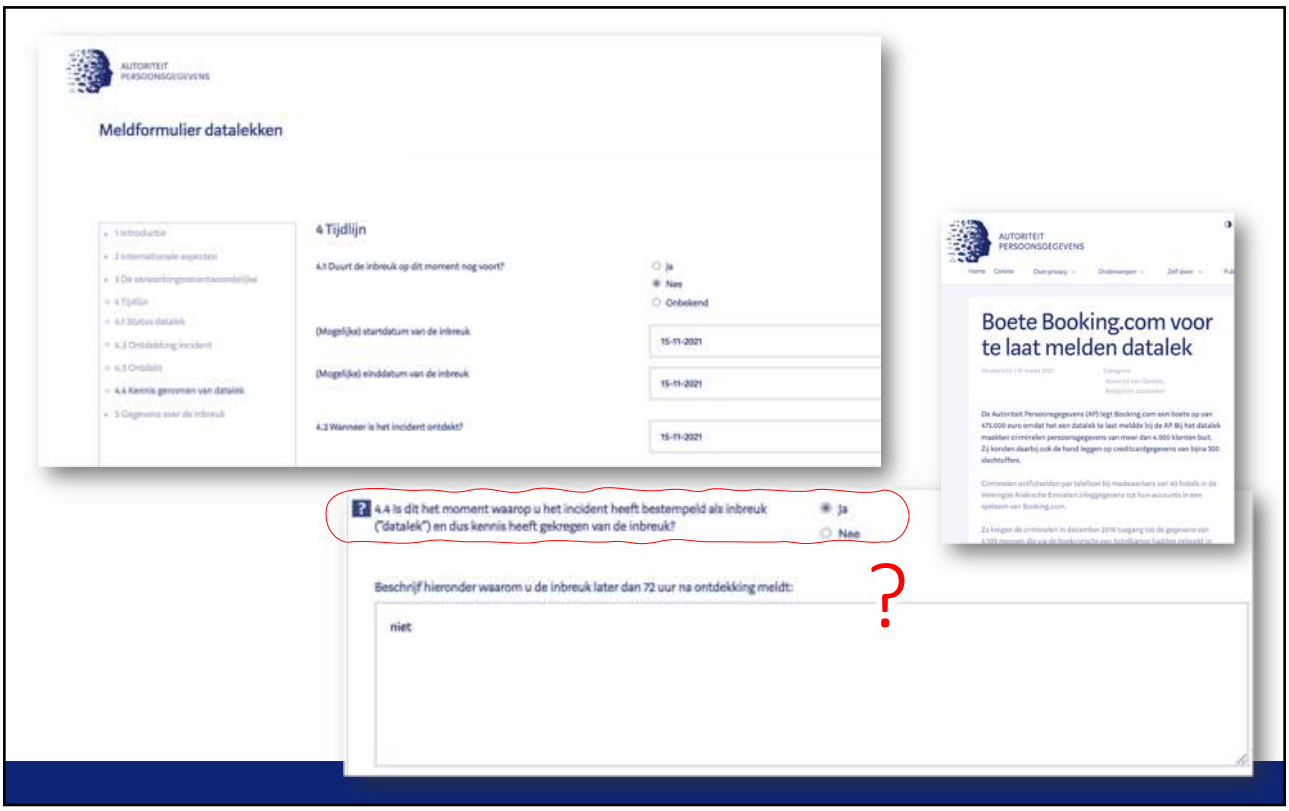
1.1 De AP geeft in haar instructie op het meldformulier aan dat de melding binnen ongeveer een kwartier en/of halfuur voltooid is. Wanneer een organisatie een (nieuw) datalek moet melden, wordt zij echter geconfronteerd met een uitgebreide lijst met gedetailleerde vragen waarop nauwkeurig, soms met exacte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

56

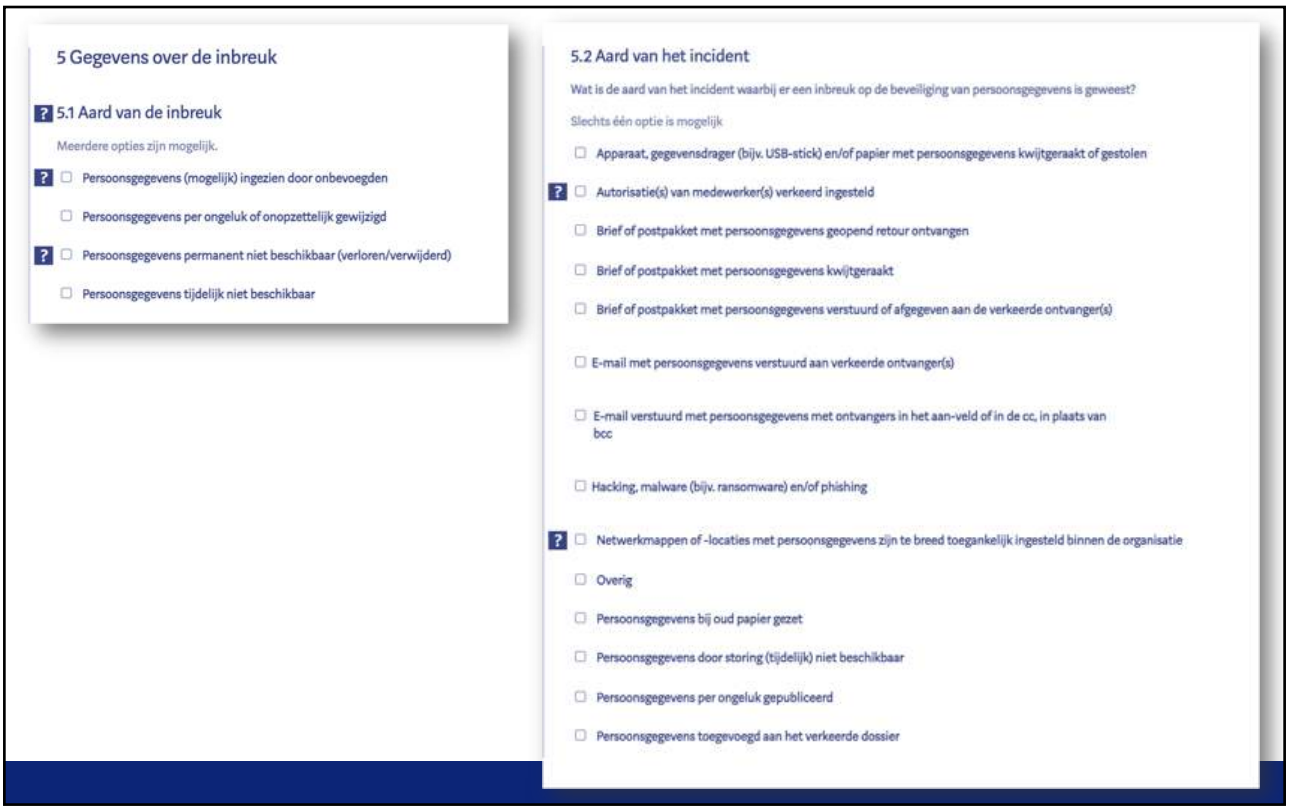
57

bulkmeldingen…

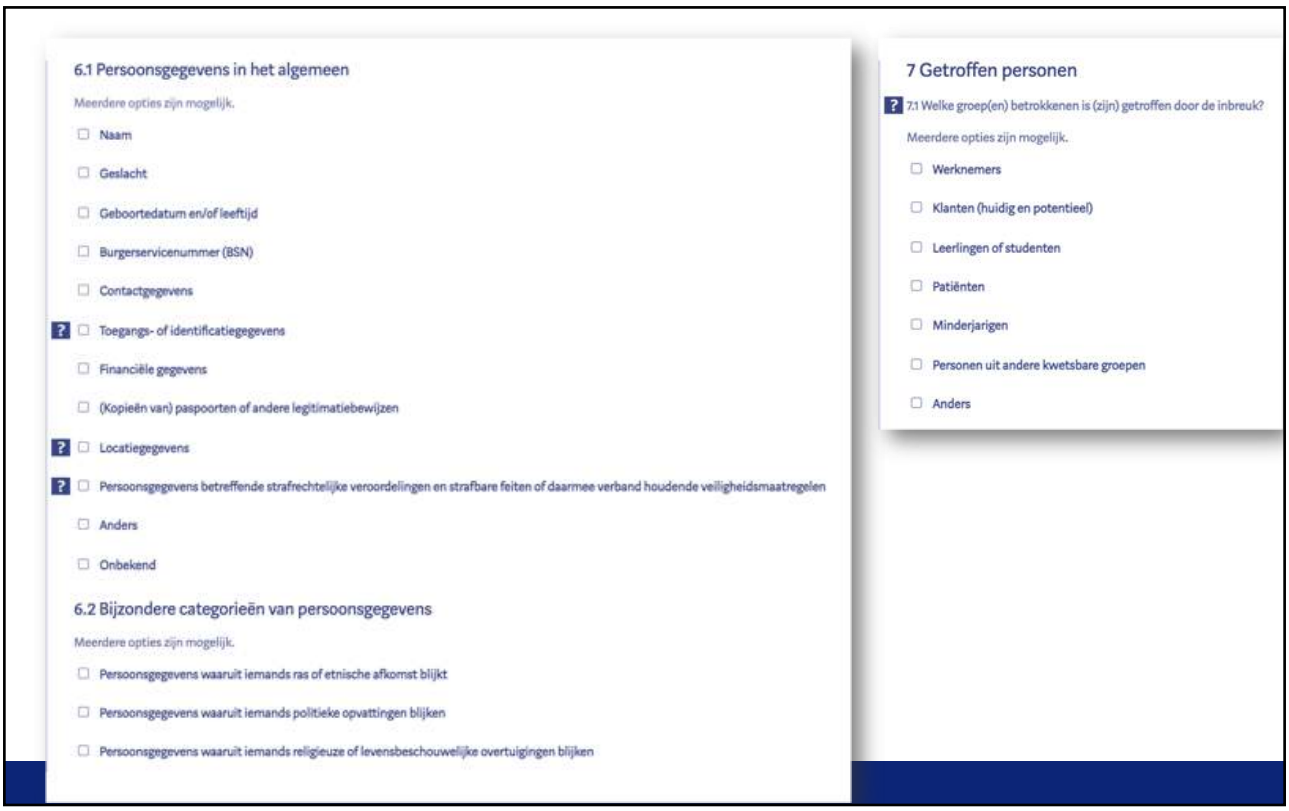
58


Meldformulier datalekken
4 Tijdlijn
4.1 Duurt de inbreuk op dit moment nog voort?
Ja
Nee
Onbekend
(Mogelijke) startdatum van de inbreuk
15-11-2021
(Mogelijke) einddatum van de inbreuk
15-11-2021
4.2 Wanneer is het incident ontdekt?
15-11-2021
Boete Booking.com voor te laat melden datalek
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:
niet
?

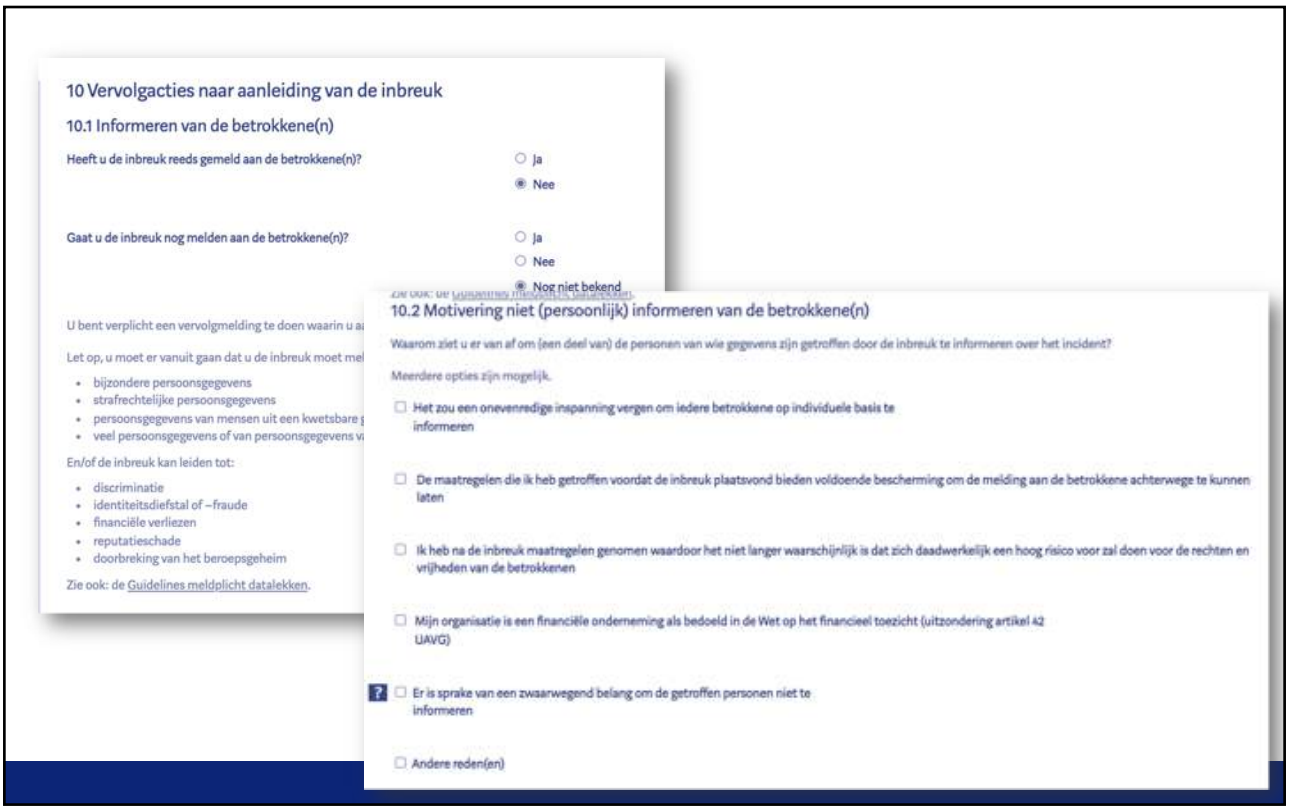
59


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

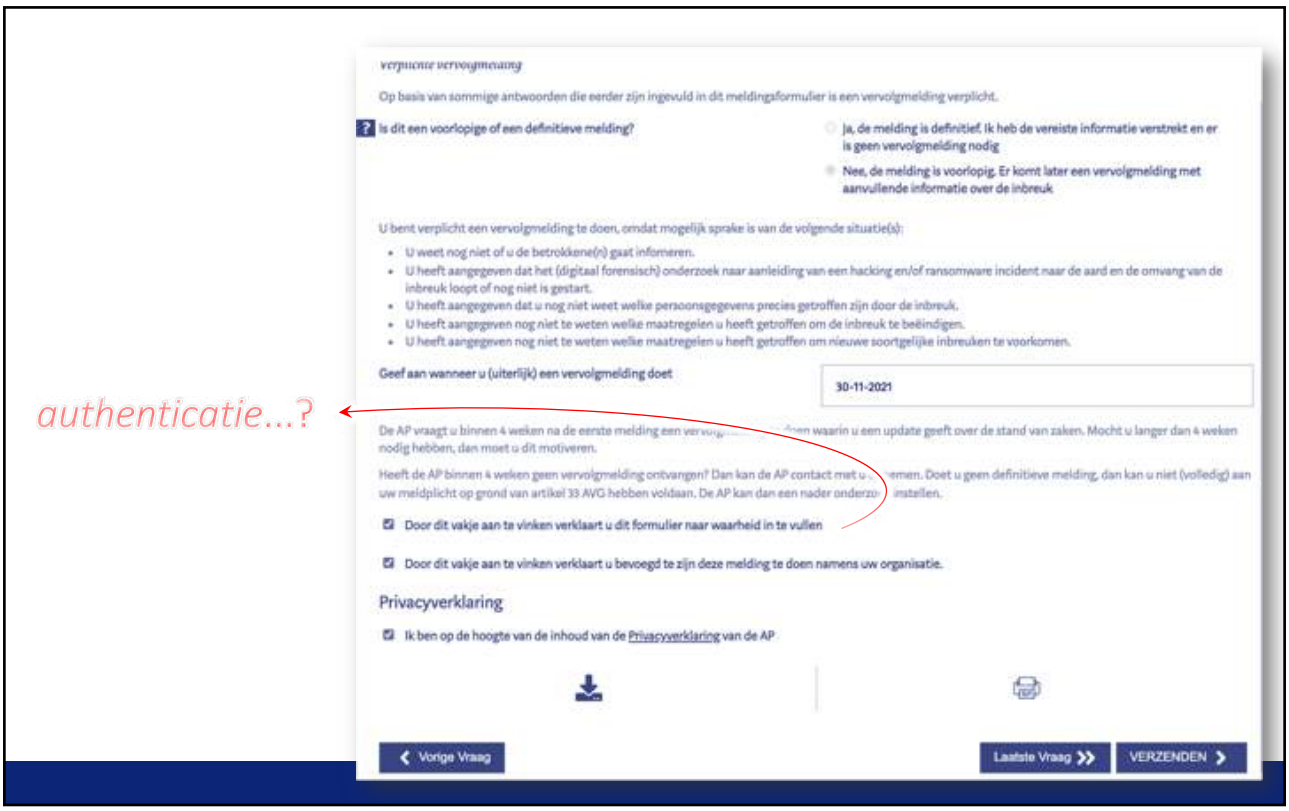
60


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

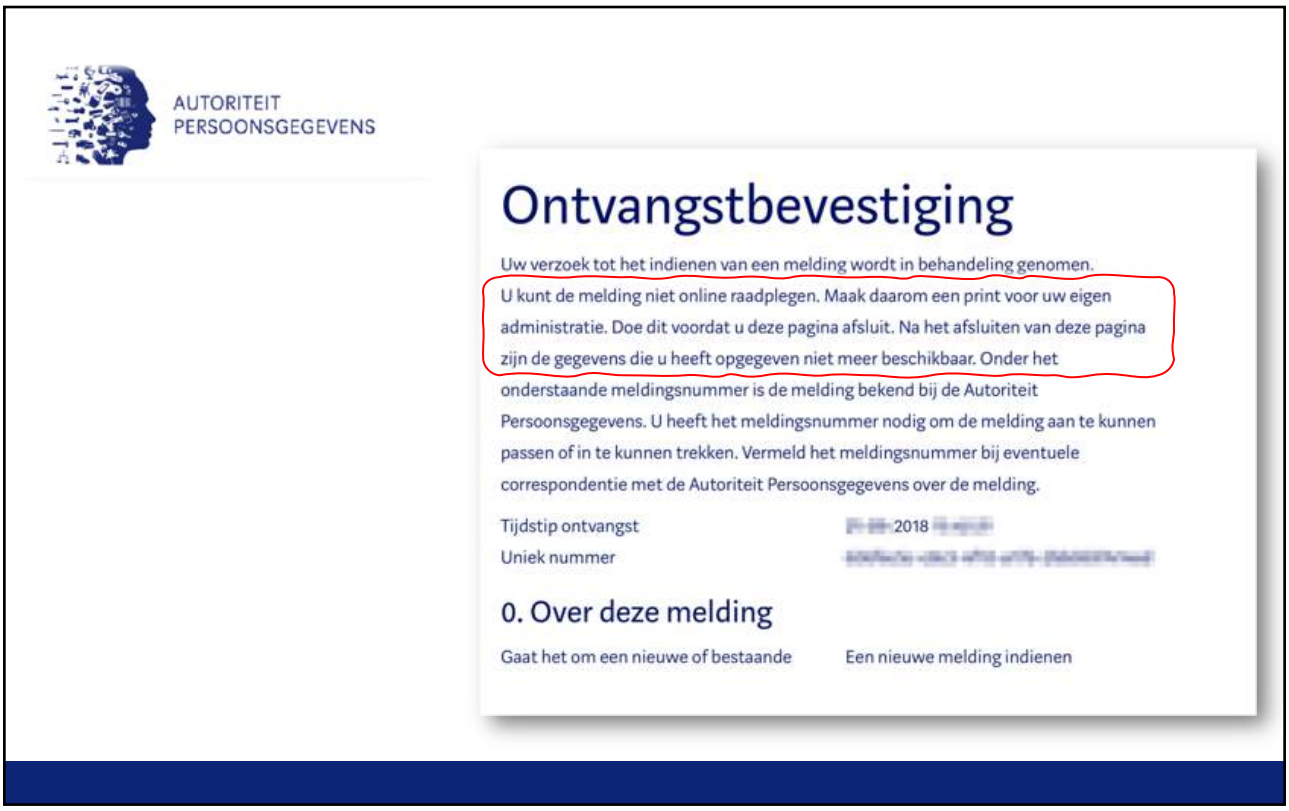
61


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 a
Let op, u moet er vanuit gaan dat u de inbreuk moet me
bijzondere persoonsgegevens
strafrechtelijke persoonsgegevens
persoonsgegevens van mensen uit een kwetsbare
veel persoonsgegevens of van persoonsgegevens v
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 onevenredige inspanning vergen om iedere betrokkene op individuele basis te informeren
De maatregelen die ik heb getroffen voordat de inbreuk plaatsvond bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten
Ik heb na de inbreuk maatregelen genomen waardoor het niet langer waarschijnlijk is dat zich daadwerkelijk een hoog risico voor zal doen voor de rechten en vrijheden van de betrokkenen
Mijn organisatie is een financiële onderneming als bedoeld in de Wet op het financieel toezicht (uitzondering artikel 42 UAVG)
Er is sprake van een zwaarwegend belang om de getroffen personen niet te informeren
Andere reden(en)

62


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

63


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
2018
Uniek nummer
0. Over deze melding
Gaat het om een nieuwe of bestaande
Een nieuwe melding indienen

64

pro forma melding (tekstsuggestie)

"Er is naar oordeel van verwerkingsverantwoordelijke 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."

65

toetsvraag 4

De Vereniging Privacyrecht Advocaten of VPR-A is een door de NOvA erkende specialisatievereniging

A. Dit is juist

B. Dit is onjuist

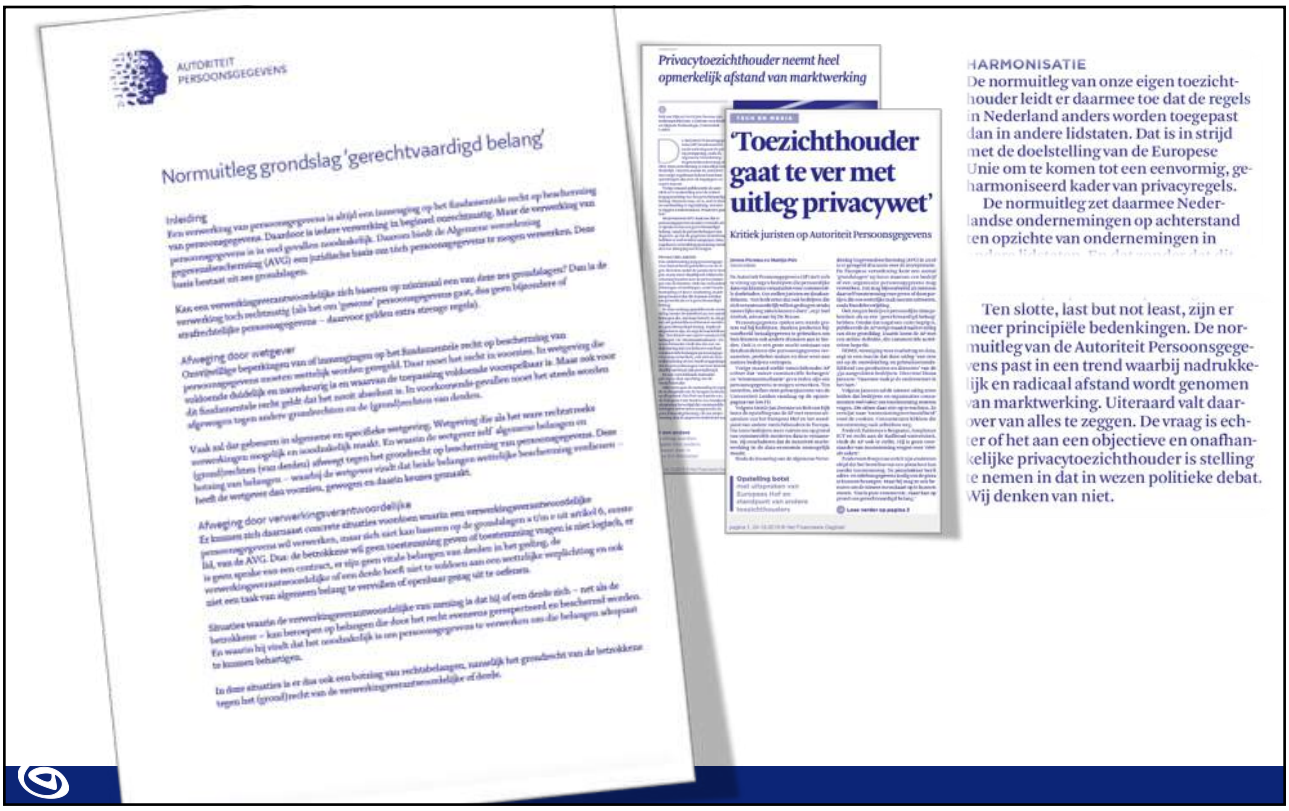
66

rol van de toezichthouder

[4]
nog steeds het gerechtvaardigd belang

deze maand VoetbalTV bij de Raad van State

67



68

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*

69

Art. 6.1 AVG

De 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.

70

driestappentoets

1. Is er een gerechtvaardigd belang?

2. Is de verwerking noodzakelijk voor dat gerechtvaardigd belang?

3. Worden de privacybelangen van betrokkenen niet teveel aangetast daardoor?

71

AP, Normuitleg 'gerechtvaardigd belang' 1 november 2019


AUTORITEIT PERSOONSGEGEVENS

Normuitleg grondslag 'gerechtvaardigd belang'

Inleiding

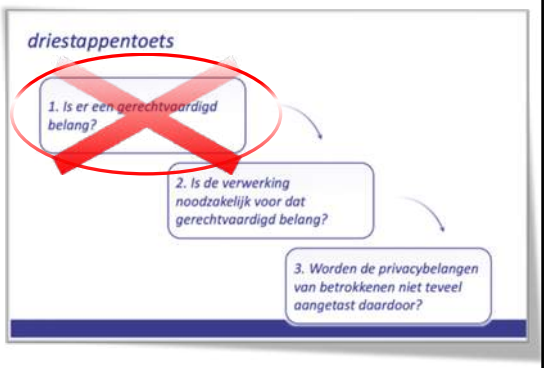
Afweging door verwerkingsverantwoordelijke

72

AUTORITEIT PERSOONSGEGEVENS

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



73

AUTORITEIT PERSOONSGEGEVENS

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 sponsoren.

De Koninklijke Nederlandse Lawn Tennisbond (KNLTB) verstrekte de sponsoren persoonsgegevens zoals naam, geslacht en adres, zodat zij een selectie van KNLTB-leden konden benaderen met tennisgerelateerde en andere aanbiedingen. De ene sponsor ontving persoonsgegevens van 50.000, de andere van meer dan 300.000 leden. Die sponsors benaderden een deel van die KNLTB-leden per post of telefoon.

74

VoetbalTV

Rb MNL 23 november 2020, ECLI:NL:RBMNE:2020:5111

18. Met de strikte toepassing die verweerder hier hanteert, is hij niet toegekomen aan zo'n beoordeling als het HvJ hier omschrijft. Daarmee heeft verweerder het gerechtvaardigd belang dus niet op een open en flexibele manier uitgelegd, zoals wel zou moeten. Hij miskent daarmee dat het begrip 'gerechtvaardigd' belang vooral als buitengrens dient voor de beoordeling en niet als een drempel. Er zijn de rechtbank verder ook geen uitspraken bekend waarin het HvJ, zonder nadere beoordeling van de belangen van zowel de verwerker als de betrokkene(n), constateert dat de verwerker in het geheel geen gerechtvaardigd belang heeft bij de verwerking en alleen al daarom onrechtmatig handelt. Verweerders uitleg dat het eiseres in de kern alleen maar gaat om het te gelde maken van persoonsgegevens en dat dit belang nooit een gerechtvaardigd belang kan zijn, gaat eraan voorbij dat het HvJ het op voorhand uitsluiten van bepaalde legitieme belangen nu juist verbiedt. Evenmin volgt de rechtbank de conclusie van verweerder dat de noodzakelijkheidstoets en de belangenafweging zinledig zijn, als wordt aangenomen dat het belang dat eiseres nastreeft een gerechtvaardigd belang is.

75

toetsvraag 5

AP vindt dat het enkel dienen van zuiver commerciële belangen en/of winstmaximalisatie niet kwalificeert als gerechtvaardigd belang (i.d.z.v. art.6.1(f) AVG)

A. Dit is juist
B. Dit is onjuist

76

toepassing van de AVV

[5]
collectieve acties en schadevergoeding

hoe de schade te verhalen die is veroorzaakt door een overtreding van de AVG?

77

78

lopende zaken…

Data Privacy Stichting vs. Facebook
- *grondslag- en transparantievereisten, verwerkingsverbod bijzondere gegevens, cookieregels*
- *verklaring voor recht*
- *Rb A'dam 30 juni 2021, ECLI:NL:RBAMS:2021:3307*

St. Onderzoek Marktinformatie, St. Take Back Your Privacy, st. Massaschade & Consument vs. TikTok
- *grondslag- en transparantievereisten, derde landendoorgifte (etc.)*
- *verklaring voor recht (etc.), schadevergoeding*

Privacy First vs Staat (Min, J&V)
- *rechtmatigheid van kenteken-registratie o.b.v. art. 126jj Sv*
- *verklaring voor recht, verbod kentekenregistratie*
- *RbDHG 1 december 2021, ECLI:NL:RBDHA:2021:13165*

St. The Privacy Collective vs. Oracle en Salesforce
- *cookieregels, profilering, grondslag- en transparantie-vereisten, doelbinding etc.*
- *verklaring voor recht, schadevergoeding*

Privacy First vs Staat (Min. Financiën)
- *rechtmatigheid van UBO-register, AMLD4, AMLD5, art. 15a Handelregisterwet*
- *verklaring voor recht, buitenwerkingstelling art. 15a Handelsregisterwet, prejudiciële vragen*
- *Rb DHG 18 maart 2021, ECLI:NL:RBDHA:2021:2457*

Amnesty International c.s. vs Staat (Min. Defensie en Minf. J&V)
- *controles i.h.k.v. Mobiel Toezicht Veiligheid (MTV) door de Koninklijke Marechaussee*
- *verwerkingsverbod bijzondere gegevens, profilering*
- *verklaring voor recht, resp. verbod*
- *Rb DHG 22 sept. 2021, ECLI:NL:RBDHA:2021:10280*

St. Stop Online Shaming en St. Expertisebureau Online Kindermisbruik vs [X] handelend onder de naam [Y]
- *rechtmatigheid website vagina.nl*
- *verwerkingsverbod bijzondere gegevens*
- *verklaring voor recht*

St. Stop Online Shaming vs St. Slachtoffers Iatrogene Nalatigheid-Nederland
- *rechtmatigheid website*
- *grondslag- en transparantievereisten*
- *verbod website*

79

lopende zaken: principieel

Privacy First vs Staat (Min, J&V)
- *rechtmatigheid van kenteken-registratie o.b.v. art. 126jj Sv*
- *verklaring voor recht, verbod kentekenregistratie*
- *RbDHG 1 december 2021, ECLI:NL:RBDHA:2021:13165*

Privacy First vs Staat (Min. Financiën)
- *rechtmatigheid van UBO-register, AMLD4, AMLD5, art. 15a Handelregisterwet*
- *verklaring voor recht, buitenwerkingstelling art. 15a Handelsregisterwet, prejudiciële vragen*
- *Hof DHG 16 november 2021, ECLI:NL:GHDHA:2021:2176*

80

lopende zaken: ontvankelijkheid en bevoegdheid (pre-WAMCA)

geen openbaarmaking dagvaarding en geen vermelding rechtspraak.nl

Data Privacy Stichting vs. Facebook
- grondslag- en transparantievereisten, verwerkingsverbod bijzondere gegevens, cookieregels
- verklaring voor recht (geen schadevergoeding!)
- Rb A'dam 30 juni 2021, ECLI:NL:RBAMS:2021:3307

'procedure tegen verwerkingsverantwoordelijke [..] wordt ingesteld bij de gerechten van de lidstaat waar de verwerkingsverantwoordelijke [..] een vestiging heeft.

Een dergelijke procedure kan ook worden ingesteld bij de gerechten van de lidstaat waar de betrokkene gewoonlijk verblijft'

- rechtbank A'dam is bevoegd o.g.v. Brussels I bis-vo. en Rv, alsmede a(rt). 79.2 AVG (overw. 147)
- geen aanleiding tot het stellen van prejudiciële vragen
- weldegelijk sprake van gelijksoortige belangen i.d.z.v. art. 305a BW
- voldaan aan de vereisten van art. 80.2 AVG

o.b.v. zgn. opt-out mechanisme

collectieve actie kan 'onafhankelijk van de opdracht van betrokkene' worden ingesteld

81

lopende zaken…

Data Privacy Stichting vs. Facebook
- grondslag- en transparantievereisten, verwerkingsverbod bijzondere gegevens, cookieregels
- verklaring voor recht
- Rb A'dam 30 juni 2021, ECLI:NL:RBAMS:2021:3307

St. Onderzoek Marktinformatie, St. Take Back Your Privacy, st. Massaschade & Consument vs. TikTok
- grondslag- en transparantievereisten, derde landendoorgifte (etc.)
- verklaring voor recht (etc.), schadevergoeding

Privacy First vs Staat (Min, J&V)
- rechtmatigheid van kentekenregistratie o.b.v. art. 126jj Sv
- verklaring voor recht, verbod kentekenregistratie

St. The Privacy Collective vs. Oracle en Salesforce
- cookieregels, profilering, grondslag- en transparantie-vereisten, doelbinding etc.
- verklaring voor recht, schadevergoeding

Privacy First vs Staat (Min. Financiën)
- rechtmatigheid van UBO-register, AMLD4, AMLD5, art. 15a Handelregisterwet
- verklaring voor recht, buitenwerkingstelling art. 15a Handelsregisterwet, prejudiciële vragen
- Rb DHG 18 maart 2021, ECLI:NL:RBDHA:2021:2457

Amnesty International c.s. vs Staat (Min. Defensie en Minf. J&V)
- controles i.h.k.v. Mobiel Toezicht Veiligheid (MTV) door de Koninklijke Marechaussee
- verwerkingsverbod bijzondere gegevens, profilering
- verklaring voor recht, resp. verbod MTV
- Rb DHG 22 sept. 2021, ECLI:NL:RBDHA:2021:10280

St. Stop Online Shaming en St. Expertisebureau Online Kindermisbruik vs [X] handelend onder de naam [Y]
- rechtmatigheid website vagina.nl
- verwerkingsverbod bijzondere gegevens
- verklaring voor recht

St. Stop Online Shaming vs St. Slachtoffers Iatrogene Nalatigheid-Nederland
- rechtmatigheid website
- grondslag- en transparantievereisten
- verbod website

82

lopende zaken: representativiteit

Wrakingsverzoek tegen rechter-plaatsvervanger, tevens hoogleraar, toegewezen. [..] rechter heeft als wetenschapper onvoldoende distantie betracht tot de zaak van verzoekers o.a. door een tweet.

St. The Privacy Collective vs. Oracle en Salesforce

- *cookieregels, profilering, grondslag- en transparantie-vereisten, doelbinding etc.*
- *verklaring voor recht, schadevergoeding*

5.11 TPC dient feitelijk te onderbouwen hoeveel gedupeerden deze actie daadwerkelijk ondersteunen en aldus wat de omvang is van de door haar vertegenwoordigde vordering. Dat heeft TPC niet gedaan.

Op de website van TPC konden en kunnen bezoekers de steunknop aanklikken. Ten tijde van de mondelinge behandeling had TPC ruim 75.000 keer op deze manier een steunbetuiging verkregen. […] Het enkel klikken op de steunknop betekent nog niet dat daarmee een steunbetuiging is verkregen zoals is beoogd met het representativiteitsvereiste. Informatie over de aard en de inzet van de procedure ontbreekt in het scherm. Hierin staat niet vermeld tegen welke partijen de actie is gericht. Oracle en Salesforce worden niet genoemd. Evenmin volgt hieruit dat een persoon door het aanklikken van de steunknop zich als gedupeerde aanmeldt voor deze collectieve actie of zal worden gerekend tot de achterban voor wie TPC in deze procedure opkomt. Een omschrijving van de gedupeerden voor wie TPC opkomt, ontbreekt. De conclusie van TPC dat meer dan 75.000 personen uit haar achterban hun steun kenbaar hebben gemaakt door te klikken op de steunknop, kan dan ook niet worden gevolgd.

83

lopende zaken: schadevergoeding

St. Onderzoek Marktinformatie, St. Take Back Your Privacy, st. Massaschade & Consument vs. TikTok

- *grondslag- en transparantievereisten, derde landendoorgifte (etc.)*
- *verklaring voor recht (etc.), schadevergoeding*

St. The Privacy Collective vs. Oracle en Salesforce

- *cookieregels, profilering, grondslag- en transparantie-vereisten, doelbinding etc.*
- *verklaring voor recht, schadevergoeding*

op welke wijze, en in hoeverre, moet de betrokkene aantonen dat de geleden schade het gevolg is van de overtreding van de verordening..?

84

Pieter Baan Centrum: €300

Rb Gelderland 19 december 2018
ECLI:NL:RBGEL:2018:5551

5.1 Naar het oordeel van de rechtbank is de privacy van eiser geschonden omdat rapportages over eiser naar het Tuchtcollege zijn verstuurd en de daarin opgenomen strikt vertrouwelijke persoonlijke gegevens bij medewerkers en leden van het Tuchtcollege terecht zijn gekomen. Eiser heeft er in dit verband terecht op gewezen dat voor de aanspraak op schadevergoeding niet is vereist dat sprake is van psychische schade. [..]

5.2 Het voorgaande betekent dat eiser ingevolge artikel 49, tweede lid, van de Wbp recht heeft op een naar billijkheid vast te stellen schadevergoeding.

6. Ten aanzien van de hoogte van de vast te stellen schadevergoeding acht de rechtbank van belang dat de privacygevoelige persoonsgegevens bij een kleine groep professionals terecht zijn gekomen, te weten bij medewerkers en leden van het Tuchtcollege, en dat zij uit hoofde van hun functie een geheimhoudingsplicht hebben. Dit neemt niet weg dat van een schending van de privacy van eiser sprake is, en dat dit begrijpelijkerwijs door eiser als naar en nadelig is ervaren. Alles afwegend acht de rechtbank een schadevergoeding van € 300 billijk.

kleine groep professionals met geheimhoudingsplicht

85

Deventer: €500

Rb Overijssel 28 mei 2019
ECLI:NL:RBOVE:2019:1827

9. Naar het oordeel van de rechtbank is eiser als gevolg van dat onrechtmatige besluit in zijn persoon aangetast wegens verlies van controle over zijn persoonsgegevens. Dat is een persoonlijkheidsrecht. Dit betekent dat eiser op grond van artikel 82 van de Avg in samenhang met artikel 6:106 van het BW recht heeft op een naar billijkheid vast te stellen schadevergoeding. Wat betreft de hoogte van die vergoeding neemt de rechtbank in acht dat in het onrechtmatige besluit geen rechtvaardiging is gegeven voor de verwerking van de persoonsgegevens van eiser. De rechtbank neemt mede in aanmerking het gestelde onder 75, 85 en 146 van de preambule bij de Avg.

[..]

11. Nu door de verspreiding van zijn persoonsgegevens sprake is geweest van een schending van de privacy van eiser acht de rechtbank een schadevergoeding van € 500,- billijk.

86

UWV: €250

Rb A'dam 2 september 2019
ECLI:NL:RBAMS:2019:6490

18. [..] Als gevolg van die schending heeft [eiseres] reële en niet verwaarloosbare nadelen geleden. De belangen waarin zij is getroffen zijn de belangen die de voorschriften van de AVG juist beoogt te beschermen. Art. 82 AVG bepaalt dat degene die materiële of immateriële schade heeft geleden als gevolg van een inbreuk op deze verordening, het recht heeft om van de verwerkingsverantwoordelijke [..] schadevergoeding te ontvangen voor de geleden schade. Alle schade moet worden vergoed en het begrip schade moet – overeenkomstig de doelstellingen van de AVG – ruim worden uitgelegd (par. 146 Considerans), [..]

18. Nu het verlies van controle over haar persoonsgegeven betreffende de langdurige ziekte blijvend is, dit anderzijds uitsluitend (medewerkers van) [werkgever 2] betreft en dit geen gevolgen heeft gehad voor haar economische of maatschappelijke positie, terwijl de als gevolg van de inbreuk opgetreden angst en stress in tijd beperkt is geweest, wordt een schadevergoeding van € 250,00 passend en billijk geacht. [..]

kleine groep medewerkers, geen economische en maatschappelijke gevolgen, angst en stress beperkt

87

Gronings Stadsblog: €250

Rb Nrd NLD 15 januari 2020
ECLI:NL:RBNNE:2020247

4.106. [Er is] sprake [..] van een schending van een fundamenteel recht, die naar zijn aard en gelet op de ernst daarvan meebrengt dat aanspraak bestaat op vergoeding van schade. Dit laatste volgt ook uit de AVG. Art. 82 AVG bepaalt dat degene die materiële of immateriële schade heeft geleden als gevolg van een inbreuk op de verordening, het recht heeft om van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade. Alle schade moet worden vergoed en het begrip schade moet – overeenkomstig de doelstellingen van de AVG – ruim worden uitgelegd (par. 146 van de preambule bij de AVG), hetgeen betekent dat het enkele feit dat de schade niet exact gepreciseerd kan worden en mogelijk relatief gering van omvang is geen grond kan vormen om elke aanspraak daarop af te wijzen.

4.107. Het verlies van controle van [gedaagde 2] over zijn persoonsgegevens is enerzijds blijvend. Anderzijds beperkt het verlies van controle zich (vooralsnog) tot e medewerker van [eiser 1] ([naam A]) en één derde. [gedaagde 2] stelt weliswaar dat hij negatieve gevolgen heeft gehad van het handelen van [eiser 1] , maar niet duidelijk is waar die negatieve gevolgen uit hebben bestaan. Het lag, gelet op zijn daarop gerichte vordering, op de weg van [gedaagde 2] dat inzichtelijk te maken. Nu [gedaagde 2] dat niet heeft gedaan, maar het schadebegrip ruim uitgelegd moet worden en de rechtbank het aannemelijk acht dat [gedaagde 2] als gevolg van het handelen van [eiser 1] negatieve effecten heeft ervaren, bijvoorbeeld angst en stress, wordt een schadevergoeding van € 250,00 passend en billijk geacht.

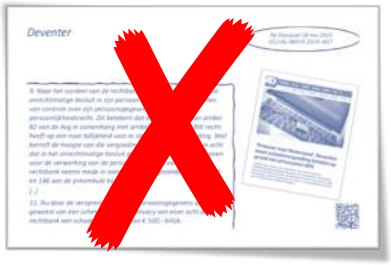
88

Deventer hoger beroep: nihil

ABRvS 1 april 2020
ECLI:NL:RBNNE:2020:899

33. [..]Het algemene uitgangspunt dat schade moet worden onderbouwd, geldt ook hier. Er is geen grond voor het oordeel dat een inbreuk op de AVG zonder meer aantasting van de integriteit van een persoon impliceert en daarmee tot vergoedbare schade leidt. Anders dan [appellant sub 2] betoogt, kan dit niet worden afgeleid uit overwegingen 85 en 146 van de AVG. Dat een inbreuk op persoonsgegevens kan resulteren in (im)materiële schade en dat een betrokkene volledige en daadwerkelijke vergoeding van de door hem geleden schade moet ontvangen, betekent niet dat een normschending per definitie tot schade leidt en dat schade niet reëel en zeker moet zijn geleden. [..]

34. In dit geval doet zich niet een situatie voor waarbij de nadelige gevolgen van de normschending voor de hand liggen. [..] Het gaat niet om ernstig verwijtbaar gedrag met zo ernstige gevolgen, dat dit als een inbreuk op een fundamenteel recht moet worden gekwalificeerd.



Idem:

- *ABRvS 1 april 2020, ECLI:NL:RBNNE:2020:900*
- *ABRvS 1 april 2020, ECLI:NL:RBNNE:2020:901*

89

Pieter Baan Centrum hoger beroep

ABRvS 1 april 2020
ECLI:NL:RVS:2020:898

32. […] Ook als het bestaan van geestelijk letsel in voornoemde zin niet kan worden aangenomen, is niet uitgesloten dat de aard en de ernst van de normschending en van de gevolgen daarvan voor de benadeelde, meebrengen dat van de in artikel 6:106, aanhef en onder b, BW bedoelde aantasting in zijn persoon 'op andere wijze' sprake is. In zo een geval zal degene die zich hierop beroept de aantasting in zijn persoon met concrete gegevens moeten onderbouwen. Dat is slechts anders indien de aard en de ernst van de normschending meebrengen dat de in dit verband relevante nadelige gevolgen daarvan voor de benadeelde zo voor de hand liggen, dat een aantasting in de persoon kan worden aangenomen. Van een aantasting in de persoon 'op andere wijze' als bedoeld in artikel 6:106, aanhef en onder b, BW is niet reeds sprake bij de enkele schending van een fundamenteel recht.

schade behoeft niet te worden onderbouwd als de nadelige gevolgen zo voor de hand liggen dat 'aantasting in de persoon' kan worden aangenomen

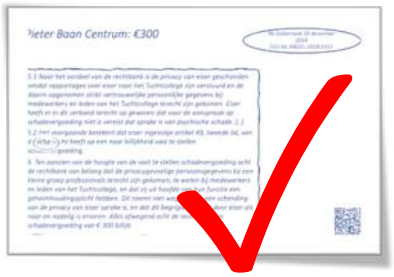
Zie:

HR 15 maart 2019, ECLI:NL:HR:2019:376 (EBI)

90

Pieter Baan Centrum hoger beroep: €500

ABRvS 1 april 2020
ECLI:NL:RVS:2020:898



36. [appellant] [heeft] recht heeft op toekenning van een vergoeding voor immateriële schade. [..]

Gelet op de omstandigheden van dit geval, waaronder de aard, duur en ernst van de inbreuk, zal de Afdeling deze schade naar billijkheid vaststellen op € 500. Daartoe neemt de Afdeling in aanmerking de bijzondere gevoeligheid van de aard van de persoonsgegevens die in dit geval zonder toestemming van [appellant] zijn verwerkt. Voor de verwerking van bijzondere (gevoelige) persoonsgegevens als bedoeld in artikel 9 van de AVG, is in de AVG een hoger beschermingsniveau is neergelegd dan voor gewone persoonsgegevens. De nadelige gevolgen van de verstrekking van de gevoelige persoonsgegevens liggen voor de hand. [..]

91

Oldambt: €500

Rb Nrd NLD 12 januari 2021,
ECLI:NL:RBNNE:2021:106

4.27 [eiser] heeft naar het oordeel van de kantonrechter niet, althans onvoldoende, gesteld dat hij als gevolg van het onrechtmatig handelen van de gemeente op objectieve gronden vastgesteld psychisch letsel heeft opgelopen, in de zin van een in de psychiatrie erkend ziektebeeld. [..]

4.28.De kantonrechter is wél van oordeel dat [eiser] anderszins in zijn persoon is aangetast. De persoonlijke levenssfeer van [eiser] is bij herhaling door de gemeente geschonden vanwege het - in strijd met de AVG - meermalen publiceren van het BSN-nummer, het e-mailadres en het telefoonnummer van [eiser] op de gemeentelijke website, zonder dat [eiser] daarvoor toestemming aan de gemeente had verleend (vgl. r.o. 36 van de uitspraak van de Afdeling). Het gaat hierbij ook om naar hun aard gevoelige gegevens, zeker waar het betreft het BSN-nummer van [eiser] . De nadelige gevolgen van het lekken daarvan, zoals identiteitsfraude, liggen voor de hand. [..]

Gelet op de omstandigheden van het onderhavige geval, waaronder de aard, duur, frequentie en ernst van de inbreuk, afgezet tegen de omstandigheid dat niet is gebleken dat de datalekken tot concrete negatieve gevolgen hebben geleid, zal de kantonrechter deze schadevergoeding naar billijkheid vaststellen op een bedrag van € 500,00.

92

zwartelijstartsen.com: €5000(!)

Hof Arnhem-Lw. 6 april 2021, ECLI:NL:GHARL:2021:3206

minus €1000, nl. het bedrag dat al in de strafzaak was toegewezen

5.1 [Het hof zal de] Stichting SIN veroordelen om binnen veertien dagen na het wijzen van dit arrest al de persoonsgegevens van appellant, waaronder ook de verwijzing naar de uitspraken van het CTG van 2 september 2010, van de websites www.sin-nl.org en www.zwartelijstartsen.nl te verwijderen en verwijderd te houden [..]

Het gevorderde bedrag van € 5.000,- voor immateriële schade [..] zal het hof toewijzen minus het bedrag van € 1.000,- dat al door de strafrechter aan appellant als benadeelde partij is toegekend. [...]

Nu het hier gaat om langdurige aantasting in eer en naam, waarvan appellant (evenals zijn partner) naar aan te nemen valt aanzienlijke hinder heeft ondervonden in zijn privéleven en in zijn mogelijkheden om een betaalde baan te vinden, is het hof van oordeel, ook gezien andere uitspraken van Nederlandse rechters, dat het gevorderde bedrag gezien de maatstaf van artikel 6:106 lid 1 aanhef, sub b BW een billijk bedrag is.

93

SVB: nihil

Rb. Mid-NNLD 4 mei 2021, ECLI:NL:RBMNE:2021:1865

ABRvS 4 maart 2020, ECLI:RVS:2020:674

onrechtmatige verstrekking van persoonsgegevens door Svb aan Belastingdienst/Toeslagen

36. De aard en de ernst van de privacyinbreuk zijn in dit geval niet zodanig dat de nadelige gevolgen zo voor de hand liggen dat een aantasting in de persoon kan worden aangenomen. Het uitgangspunt is dan dus dat eiser moet bewijzen dat zijn dochter in haar persoon is aangetast en dat hij de geleden schade met concrete gegevens moet onderbouwen. De rechtbank oordeelt dat eiser daarin niet is geslaagd. Op de zitting heeft hij erop gewezen dat de met het startbericht verstrekte persoonsgegevens digitaal heel lang kunnen blijven bestaan en dat dit schadelijk kan zijn voor zijn dochter. Eiser heeft op deze manier slechts in algemene bewoordingen gesteld dat schade is geleden en heeft dat niet kunnen concretiseren. Hij heeft dan ook niet aannemelijk gemaakt dat het verstrekken van de persoonsgegevens van zijn dochter aan de Belastingdienst/Toeslagen heeft geleid tot de aantasting van haar persoon en dat de gevolgen van de inbreuk haar rechtstreeks hebben getroffen.

37. De rechtbank overweegt hierbij dat de algemene vrees voor identiteitsfraude onvoldoende is voor een veroordeling in immateriële schade. Hoewel deze vrees voorstelbaar is en identiteitsfraude als gevolg van de privacyinbreuk niet uit te sluiten is, is dat onvoldoende concreet om nu uit te kunnen concluderen dat eisers dochter in haar persoon is aangetast.

- *schade ligt niet voor de hand*
- *eiser moet schade aantonen*
- *met concrete gegevens*
- *algemene vrees voor ID-fraude is onvoldoende*

94

Almelo: 2 x €125

Rb. Overijssel 31 mei 2021, ECLI:NL:RBOVE:2021:2264

besluit van gemeente om niet te voldoen aan verwijderingsverzoek o.g.v. art. 17.1 AVG

15. Naar het oordeel van de rechtbank is [naam] als gevolg van het bestreden besluit, dat een onrechtmatig karakter heeft, in zijn persoon aangetast door verlies van controle over zijn persoonsgegevens. Het betreft een aantasting van een persoonlijkheidsrecht. Dat betekent dat eiseres op grond van artikel 82 van de AVG in samenhang met artikel 6:106 van het Burgerlijk Wetboek recht heeft op een naar billijkheid vast te stellen schadevergoeding.

16. Het uitgangspunt is dat eiseres de door haar gestelde schade met concrete gegevens moet onderbouwen. Gelet op de omstandigheden van het geval en het langdurig verzet van verweerder tegen een redelijk verzoek tot vernietiging van het Jeugdwet-dossier van [naam] , heeft de gemachtigde van eiseres in het aanvullend beroepschrift van 9 september 2020 aangevoerd het billijk te achten dat zowel voor [naam] als voor zijn wettelijk vertegenwoordigster een bedrag van € 1.500,- wordt toegekend wegens immateriële schade.

17. De rechtbank volgt de gemachtigde van eiseres hierin niet vanwege het ontbreken van concrete gegevens. De rechtbank acht een schadevergoeding van € 125,- voor eiseres en eenzelfde bedrag aan schadevergoeding voor [naam] redelijk en zal verweerder hiertoe veroordelen.

95

Rotterdam: €2500

Rb. Rotterdam 12 juli 2021, ECLI:NL:RBROT:2021:6822

besluit van gemeente om medische gegevens niet uit dossier te verwijderen (art.17.1 AVG?)

4.2.Verzoekster stelt als gevolg van het handelen van verweerder ten minste €25.000,- aan schade te hebben geleden.

4.3.Ten aanzien van de hoogte van de vast te stellen schadevergoeding is van belang dat de privacygevoelige persoonsgegevens gedurende een periode van ongeveer tien jaar door verweerder zijn bewaard, ondanks verschillende verzoeken van verzoekster tot vernietiging van de gegevens. De rechtbank acht voldoende aannemelijk dat in die tien jaar de persoonlijke gegevens van verzoekster zijn verwerkt en meerdere personen en/of instanties van de inhoud kennis hebben kunnen nemen zonder dat zij daartoe gerechtigd waren en dat verzoekster op grond daarvan immateriële schade heeft geleden. De schade begroot de rechtbank, met inachtneming van de in 4.1. genoemde uitspraak van de Afdeling (waarin een schadevergoeding is toegekend van € 500,- voor een kortdurende onrechtmatige verwerking van medische gegevens) en de lengte van de periode dat de gegevens onrechtmatig zijn bewaard en verwerkt, op € 2.500,-.

4.4.De stelling van verzoekster dat door het onrechtmatig bewaren en bewerken van haar gegevens haar carrière is beschadigd en zij daardoor onder andere inkomensverlies heeft geleden, acht de rechtbank niet aannemelijk gemaakt. Het verzoek om materiële schadevergoeding wordt daarom afgewezen.

- medische gegevens
- ten onrechte bewaard 10 jaar bewaard
- toegankelijk voor meerdere personen en instanties

96

Dus…

In beginsel moet met concrete gegevens worden aangetoond dat er schade is geleden als gevolg van de overtreding

tenzij de schade zo voor de hand ligt dat 'aantasting in de persoon' kan worden aangenomen

relevant zijn

- verwijtbaarheid gedrag en ernst van gevolgen (Deventer)
- aard duur en ernst van de overtreding (Pieter Baan)
- gevoeligheid van de gegevens (Pieter Baan)
- bij een datalek ligt ID-fraude voor de hand (Oldambt)

97

intussen in Duitsland en Oostenrijk

Bundesverfassungsgericht 14 January 2021, ECLI:DE:BVerfG:2021:rk20210114.1bvr285319

The facts to be assessed in the main proceedings raised the question under which conditions Art. 82(1) GDPR grants a claim for monetary damages and which understanding of this provision is to be given in particular with regard to recital 146, third sentence, which requires a broad interpretation of the concept of damage in light of the case law of the Court of Justice of the European Union that fully complies with the objectives of the GDPR

Oberster Gerichtshof 12 May 2021 questions asked to CJEU

- Does the award of compensation under Article 82 GDPR […] also require, in addition to infringement of provisions of the GDPR, that an applicant must have suffered harm, or is the infringement of provisions of the GDPR in itself sufficient for the award of compensation?
- Does the assessment of the compensation depend on further EU-law requirements in addition to the principles of effectiveness and equivalence?
- Is it compatible with EU law to take the view that the award of compensation for non-material damage presupposes the existence of a consequence of the infringement of at least some weight that goes beyond the upset caused by that infringement?

wordt vervolgd…

98

[6]
wettelijke plicht of gerechtvaardigd belang?

beantwoording prejudiciële vragen in HR 3 december 2021, ECLI:NL:HR:2021:1814

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*

BKR-registratie: c- of f-grond..?

het belang van de verwerkingsgrondslag

om een zgn. bijzonderheidcodering uit het Centraal Krediet Informatiesysteeem van BKR te verwijderen maken consumenten gebruik van hun wissingsrecht en/of hun recht van bezwaar

bijv. betalingsachterstand, roodstaan, studieschuld

art. 17.1 AVG

art. 21.1 AVG

dat kan evenwel alleen als de kredietaanbieder dit niet doet ter naleving van een wettelijke plicht maar ter behartiging van een gerechtvaardigd belang

art. 6.1(f) AVG

art. 6.1(c) AVG

de vraag is dus:

is de registratie van bijzonderheidscodes door de bank in CKI van BKR inherent aan het voldoen aan de wettelijke plicht om deel te nemen aan BKR?

- ❑ *ja, want een bank kan niet deelnemen aan BKR zonder deze registraties*
- ❑ *neen, want de registratie is vereist door het CKI-reglement, niet door de wet*

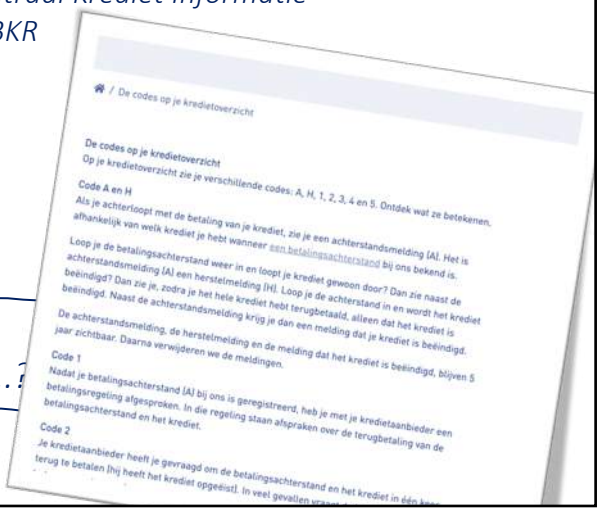
let op: geen toetsvraag!

verwerkingsgrondslag voor de kredietaanbieder

zeg: een bank, postorderbedrijf, mobiele telecomaanbieder

waarvan een kredietaanbieder gebruik maakt als hij van iemand persoonsgegevens opneemt in het Centraal Krediet Informatie Systeem (CKI) van BKR

bijv. bijzonderheidscode "A" d.w.z. de aanduiding dat sprake is van een betalingsachterstand



- *wettelijke plicht (art. 6.1c AVG) of*
- *gerechtvaardigd belang (art. 6.1f AVG)..?*

103

verwerkingsgrondslag voor de kredietaanbieder

- *d.w.z. art. 4:32 en 4:34 Wet financieel toezicht (Wft) én*
- *art. 114 Besluit Gedragstoezicht financiële ondernemingen (Bgfo) én*
- *Reglement CKI*

géén wissingsrecht (art. 17.3b AVG) en géén recht van bezwaar (art. 21.1 AVG)

wél Santander-toets (HR 9 september 2011, ECLI:NL:HR:2011:B08097)

- *wettelijke plicht (art. 6.1c AVG) of*
- *gerechtvaardigd belang (art. 6.1f AVG)*

wél een wissingsrecht (art. 17.1 AVG) en een recht van bezwaar (art. 21.1 AVG)

104

verwerkingsgrondslag voor bank

- art. 4:32 en 4:34 Wft én
- art. 114 Bgfo
- Reglement CKI

deelnemers aan BKR moeten eigen kredietovereenkomsten opnemen in CKI

kredietaanbieder moet deelnemen aan kredietregistratiestelsel, zoals BKR

kredietaanbieder moet informatie inwinnen over financiële positie van consument, om overkreditering te voorkomen

voordat hij met een consument een kredietovereenkomst (meer dan €250) aangaat, moet kredietaanbieder het kredietregistratiestelsel raadplegen

wettelijke plicht (art. 6.1c AVG) ?

105

BKR-registratie door kredietaanbieder: c- of f-grond?

hof Den Bosch 6 augustus 2020, ECLI:NL:GHSHE:2020:2536 én
hof Arnhem-L. 17 december 2020, ECLI:NL:GHARL:2020:10564

- bank moet voldoen aan wettelijke plicht om deel te nemen aan een stelsel van kredietregistratie o.g.v. art. 4:32 Wft
- bank verwerkt ter uitvoering van haar wettelijke plicht de persoonsgegevens van de verzoeker, dus o.b.v. c-grond
- verzoeker kan geen gebruik maken van art. 17.1 en art. 21.1 AVG, wèl geldt de Santander-toets
- de termijn van art. 35.2 AVG is niet van toepassing; verzoeker is niet niet-ontvankelijk

hof Den Haag 8 september 2020, ECLI:NL:GHDHA:2020:2068

- bank moet voldoen aan wettelijke plicht om deel te nemen aan een stelsel van kredietregistratie o.g.v. art. 4:32 Wft
- maar bank is o.g.v. die wettelijk plicht niet gehouden om een concrete registratie te doen in een individueel geval: bank verwerkt niet o.b.v. c-grond maar f-grond
- verzoeker kan wel gebruik maken van art. 21.1 AVG
- maar wel binnen de termijn van art. 35.2 AVG, anders niet-ontvankelijkheid

rechtbank A'dam 21 januari 2021, ECLI:NL:RBAMS:2021:174

prejudiciele vragen aan de Hoge Raad (art. 392, eerste lid, onderdeel b, Rv)

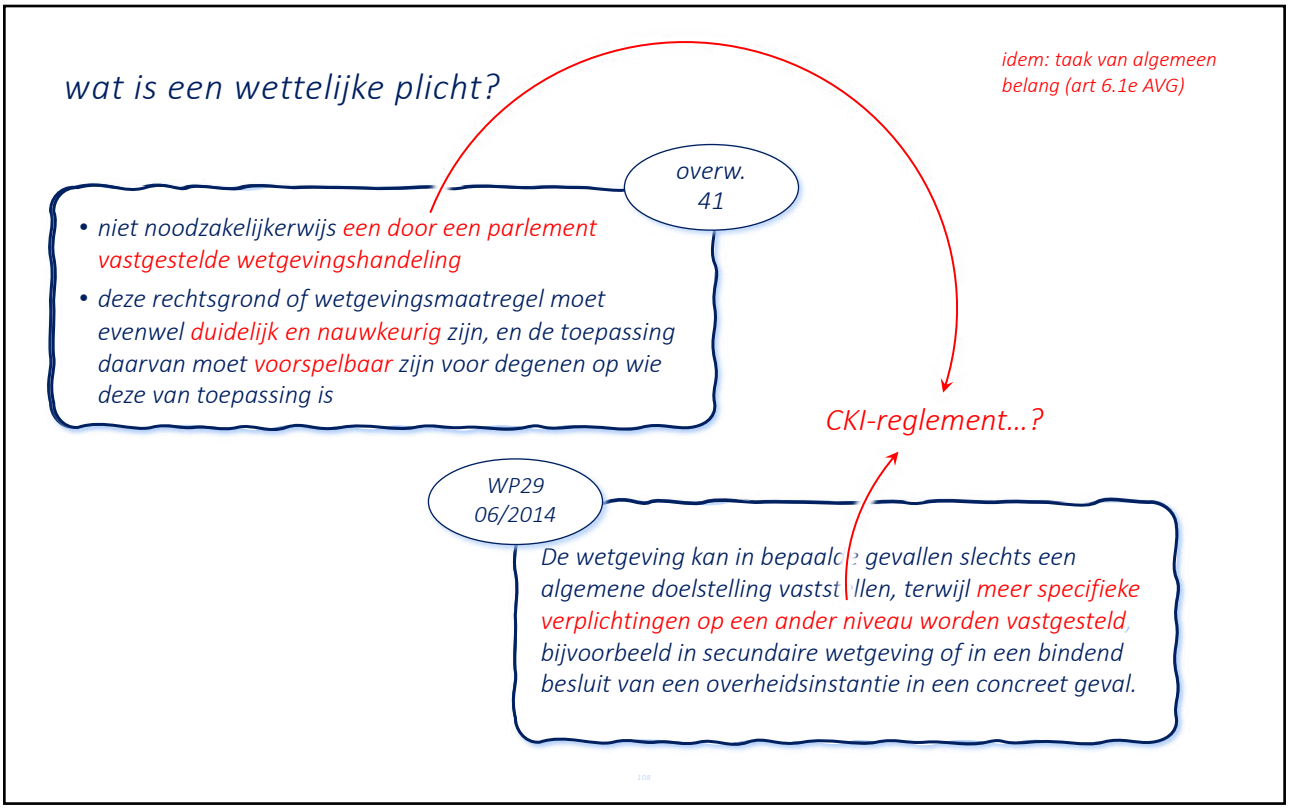
- verwerkt bank om te voldoen aan een wettelijke verplichting (c-grond) of ter behartiging van een gerechtvaardigd belang (f-grond)..?
- komt aan de betrokkene een beroep toe op het recht van gegevenswissing en het recht van bezwaar (art. 17 resp 21 AVG)..?
- als hem geen recht op bezwaar toekomt, leidt dat er dan toe dat art. 35 UAVG geen rol speelt..?

?

106


wanneer is sprake van een wettelijke plicht?
geldt oook voor taak van algemeen belang of uitoefening openbaar gezag
art. 6.3
de rechtsgrond van de plicht is vastgesteld bij unierecht of lidstatelijk recht dat van toepassing is op de verwerkingsverantwoordelijke
in die rechtsgrond moet het doel van de verwerking staan
die rechtsgrond kan specifieke bepalingen bevatten om de toepassing van de regels van deze verordening aan te passen
unierecht of het lidstatelijke recht moet beantwoorden aan een doelstelling van algemeen belang en moet evenredig zijn met het nagestreefde gerechtvaardigde doel
bijv.
types van gegevens; betrokkenen; entiteiten waaraan en doeleinden waarvoor de persoonsgegevens mogen worden verstrekt; doelbinding; opslagperioden etc.
overw. 45
de verwerking moet een grondslag te hebben in unierecht of lidstatelijke recht.
geen specifieke wetgeving vereist is voor elke afzonderlijke verwerking
voldoende is wetgeving die als basis fungeert voor verscheidene verwerkingen o.gv. een wettelijke verplichting die op de verwerkingsverantwoordelijke rust
unierecht of het lidstatelijke recht moet het doel van de verwerking bepalen

107


wat is een wettelijke plicht?
idem: taak van algemeen belang (art 6.1e AVG)
overw. 41
niet noodzakelijkerwijs een door een parlement vastgestelde wetgevingshandeling
deze rechtsgrond of wetgevingsmaatregel moet evenwel duidelijk en nauwkeurig zijn, en de toepassing daarvan moet voorspelbaar zijn voor degenen op wie deze van toepassing is
CKI-reglement…?
WP29 06/2014
De wetgeving kan in bepaalde gevallen slechts een algemene doelstelling vaststellen, terwijl meer specifieke verplichtingen op een ander niveau worden vastgesteld, bijvoorbeeld in secundaire wetgeving of in een bindend besluit van een overheidsinstantie in een concreet geval.

108

wat is een wettelijke plicht?

Kst II 2017/18, 34 851, nr. 3, p. 35

Deze wettelijke verplichting behoeft niet noodzakelijkerwijs te bestaan uit een expliciete verplichting om (bepaalde) persoonsgegevens te verwerken. Het komt namelijk ook voor dat de verwerking van persoonsgegevens een basis vindt in een ruimer geformuleerde zorgplicht of wettelijke verplichting. In dat geval heeft de verwerkingsverantwoordelijke een grotere eigen verantwoordelijkheid inzake het beoordelen van de noodzakelijkheid van de verwerking in het licht van het voldoen aan de wettelijke verplichting. Zonder verwerking van de gegevens moet het uitvoeren van een wettelijke verplichting redelijkerwijs niet goed mogelijk zijn.

109

109

Conclusie AG Rank-Berenschot

Conclusie 15 september 2021, ECLI:NL:PHR:2021:831

Mijns inziens moet de verwerking van persoonsgegevens door een kredietinstelling, door middel van een registratie in het CKI van het BKR, worden getoetst aan het bepaalde in artikel 6 lid 1, aanhef en onder f, AVG.

Het bepaalde in art. 6 lid 1, aanhef en onder c, AVG leent zich mijns inziens bij de huidige stand van de wet- en regelgeving niet voor toepassing op de verwerking van persoonsgegevens in het CKI van het BKR.

110

110

Hoge Raad

HR 3 december 2021
ECLI:NL:HR:2021:1814

Art. 4:32 lid 1 Wft en art. 4:34 lid 1 Wft, zoals nader uitgewerkt in art. 114 BGfo, verplichten kredietaanbieders weliswaar tot deelname aan en raadpleging van een stelsel van kredietregistratie, maar deze wettelijke bepalingen zijn niet voldoende duidelijk en nauwkeurig en de toepassing ervan is niet voldoende voorspelbaar voor degenen op wie deze wettelijke bepalingen van toepassing zijn, zoals art. 6 lid 3 AVG eist [...].

Uit die wettelijke bepalingen blijkt immers niet welke persoonsgegevens in het CKI geregistreerd moeten of mogen worden, wat de voorwaarden voor een dergelijke registratie zijn en onder welke voorwaarden en binnen welke termijnen tot verwijdering van persoonsgegevens moet worden overgegaan. Een en ander wordt wel geregeld in het CKI-reglement, maar dat reglement berust niet op een wettelijke grondslag; de registratie van persoonsgegevens in het CKI vindt plaats op grond van een overeenkomst tussen het BKR en kredietaanbieders

111

de vraag is dus:

is de registratie van bijzonderheidscodes door de bank in CKI van BKR inherent aan het voldoen aan de wettelijke plicht om deel te nemen aan BKR?

- ❑ *ja, want een bank kan niet deelnemen aan BKR zonder deze registraties*
- ☑ *neen, want de registratie is vereist door het CKI-reglement, niet door de wet*

112

toetsvraag 6

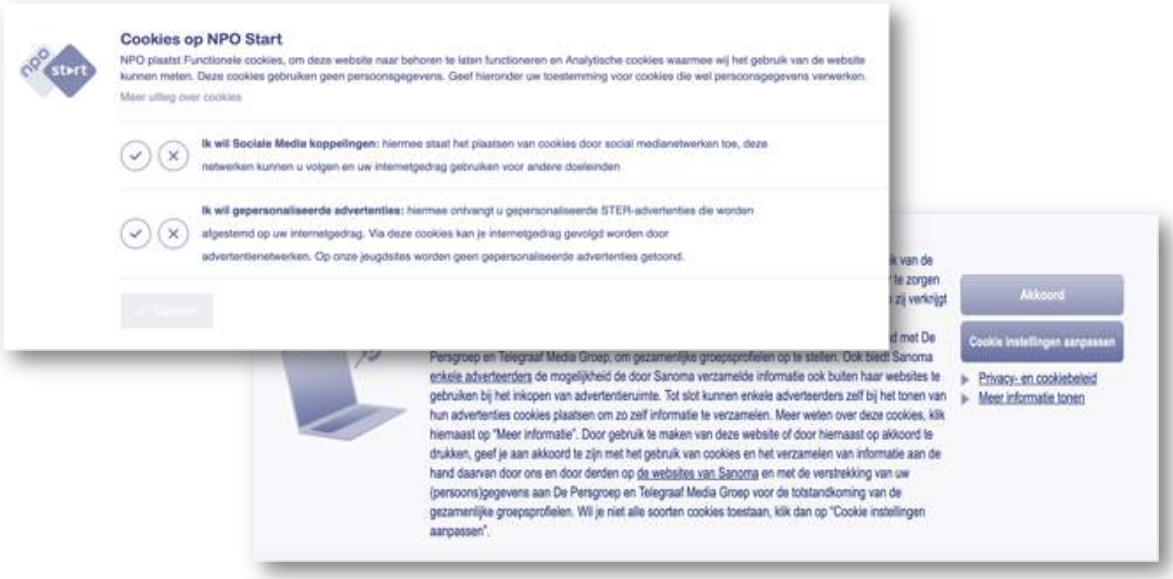
Volgens de Hoge Raad vindt de registratie van persoonsgegevens in het CKI van BKR plaats op grond van een overeenkomst tussen het BKR en kredietaanbieders en niet ter naleving van een wettelijke plicht (i.d.z.v. art. 6.1(c) AVG)

A. Dit is juist
B. Dit is onjuist

[7]
over cookies en cookiemuren

mag het of mag het niet? en wie bepaalt dat dan?

cookies e.d.



115

cookiebepaling

Art. 11.7a Telecomwet

Onverminderd de Algemene verordening gegevensbescherming is het via een elektronisch communicatienetwerk opslaan van of toegang verkrijgen tot informatie in de randapparatuur van een gebruiker, alleen toegestaan op voorwaarde dat de betrokken gebruiker:

a) is voorzien van duidelijke en volledige informatie overeenkomstig de Algemene verordening gegevensbescherming, in ieder geval over de doeleinden waarvoor deze informatie wordt gebruikt, en

b) daarvoor toestemming heeft verleend.

plaatsen en uitlezen van cookies


ICTRecht incasseert €8200 dankzij cookiepopup met incassotoestemming

Dankzij het gemak waarmee mensen online akkoord gaan met cookiepopups heeft ICTRecht een bedrag van €8200 mogen incasseren via automatische incasso. Dat maakte het juridisch adviesbureau vandaag bekend. Naast de bekende teksten over Analyticscookies en sociale media bevatte de cookiepopup ook de tekst "Tevens geeft u toestemming €100 van uw bankrekening te laten afschrijven". Een dergelijke tekst is rechtsgeldig, nu bezoekers expliciet op "Akkoord" moesten klikken.

Art. 13-14 AVG: o.a. eigen identiteit, doeleinden en 'nadere informatie voor zover nodig om zorgvuldige verwerking te waarborgen'

is de toestemming rechtsgeldig als er sprake is van een cookiemuur..?

is de toestemming in vrijheid gegeven...?

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 (overw. 42 Preambule AVG)

116

cookiemuren-verbod (voor overheid e.d.)

Art 11.7 lid 5 Tw

De toegang van de gebruiker tot een dienst van de informatiemaatschappij die wordt geleverd door of namens een krachtens publiekrecht ingestelde rechtspersoon wordt niet afhankelijk gemaakt van het verlenen van toestemming

a contrario: geen verbod op cookiemuren voor niet krachtens publiekrecht ingestelde rechtspersonen…

119

parl. geschiedenis

Een cookiemuur is over het algemeen dan ook een rechtmatige manier om aan het toestemmingsvereiste in de cookiebepaling te voldoen. Ook al is dit niet de meest gebruiksvriendelijke manier en is het technisch ook nooit noodzakelijk, het staat de websitehouder in beginsel wel vrij om te bepalen of hij een bezoeker die geen toestemming geeft voor het gebruik van cookies, al dan niet toegang geeft tot zijn website. Dit kan anders zijn als de bezoeker zo afhankelijk is van de via een bepaalde website aangeboden diensten en informatie, dat er door het gebruik van de cookiemuur geen sprake meer kan zijn van een «vrije» wilsuiting wanneer de bezoeker vervolgens het vakje «ik geef toestemming» aanklikt.

Kamerstukken II 2013/14, 33902, nr. 3, p. 29

120

AUTORITEIT
PERSOONSGEGEVENS

Wettelijke regels voor cookies

Voor het gebruik van cookies gelden wettelijke regels. Dat zijn in de eerste plaats regels uit de Telecommunicatiewet (Tw).

Maar op tracking cookies (in combinatie met overige gegevens die over het websitebezoek worden verzameld) is ook de Algemene verordening gegevensbescherming (AVG) van toepassing.

Uitleg over de wettelijke eisen aan andere soorten cookies is te vinden op de website van de Autoriteit Consument en Markt (ACM).

Cookiewalls

Op grond van de AVG zijn cookiewalls niet toegestaan. Dat komt omdat de AVG bepaalde eisen stelt aan de benodigde toestemming voor het plaatsen van tracking cookies.

Met een cookiewall (cookiemuur) kunnen websites, apps of andere diensten géén geldige toestemming krijgen van hun bezoekers of gebruikers.

??

121

discussie over invoering van een verbod op cookiewalls

Text proposed by the Commission

(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, **end-users** are increasingly requested to provide consent to store such tracking cookies. As a result, end-users may be overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. The choices made by **end-users** when establishing **its** general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the **end-user** and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as **gatekeepers**, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

Amendment

(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, **users** are increasingly requested to provide consent to store such tracking cookies. ***This Regulation should prevent the use of so- called "cookie walls" and "cookie banners" that do not help users to maintain control over their personal information and privacy or become informed about their rights.*** The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by ***technical specifications, for instance by*** using the appropriate settings of a browser or other application. ***Those settings should include choices concerning the storage of information on the user's terminal equipment as well as a signal sent by the browser or other application indicating the user's preferences to other parties.*** The choices made by **users** when establishing **the** general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the **user** and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers, ***or applications or operating systems*** may be used as ***the executor of a user's choices***, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

122

Text proposed by the Commission

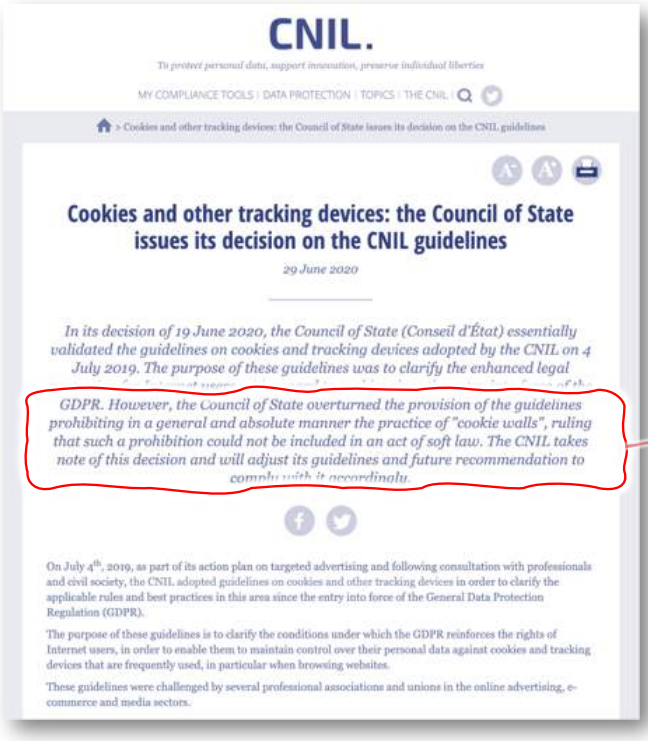
(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, ***end-users*** are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. The choices made by ***end-users*** when establishing ***its*** general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the ***end-user*** and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as ***gatekeepers***, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

123

Amendment

(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, ***users*** are overloaded with requests to provide consent. ***This Regulation should prevent the use of so- called "cookie walls" and "cookie banners" that do not help users to maintain control over their personal information and privacy or become informed about their rights***. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by ***technical specifications, for instance by*** using the appropriate settings of a browser or other application. ***Those settings should include choices concerning the storage of information on the user's terminal equipment as well as a signal sent by the browser or other application indicating the user's preferences to other parties.*** The choices made by ***users*** when establishing ***the*** general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the ***user*** and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers, ***or applications or operating systems*** may be used as ***the executor of a user's choices***, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

124



CNIL.

To protect personal data, support innovation, preserve individual liberties

MY COMPLIANCE TOOLS | DATA PROTECTION | TOPICS | THE CNIL |

> Cookies and other tracking devices: the Council of State issues its decision on the CNIL guidelines

Cookies and other tracking devices: the Council of State issues its decision on the CNIL guidelines

29 June 2020

In its decision of 19 June 2020, the Council of State (Conseil d'État) essentially validated the guidelines on cookies and tracking devices adopted by the CNIL on 4 July 2019. The purpose of these guidelines was to clarify the enhanced legal

GDPR. However, the Council of State overturned the provision of the guidelines prohibiting in a general and absolute manner the practice of "cookie walls", ruling that such a prohibition could not be included in an act of soft law. The CNIL takes note of this decision and will adjust its guidelines and future recommendation to comply with it accordingly.

On July 4th, 2019, as part of its action plan on targeted advertising and following consultation with professionals and civil society, the CNIL adopted guidelines on cookies and other tracking devices in order to clarify the applicable rules and best practices in this area since the entry into force of the General Data Protection Regulation (GDPR).

The purpose of these guidelines is to clarify the conditions under which the GDPR reinforces the rights of Internet users, in order to enable them to maintain control over their personal data against cookies and tracking devices that are frequently used, in particular when browsing websites.

These guidelines were challenged by several professional associations and unions in the online advertising, e-commerce and media sectors.

[T]he Council of State overturned the provision of the guidelines prohibiting in a general and absolute manner the practice of "cookie walls", ruling that such a prohibition could not be included in an act of soft law.

125

ePrivacy Regulation

- *requirement to obtain the explicit consent from end-users before using cookies and trackers on your website, or any other technology that stores personal data on users' terminal equipment (hardware and software)*
- *cookie walls are allowed, if the user is offered an equivalent that does not involve giving consent to cookies and trackers*
- *possibility to whitelist cookie providers in their browser settings and encourage providers to make it easy for users to amend whitelists and to withdraw their consent at any time*

Council of the European Union

Brussels, 10 February 2021
(OR. en)

6087/21

Interinstitutional File:
2017/0003(COD)

TELECOM 52
COMPET 90
MI 80
DATAPROTECT 34
CONSOM 38
JAI 131
DIGIT 20
FREMP 26
CYBER 33
CODEC 178

OUTCOME OF PROCEEDINGS
From: General Secretariat of the Council
To: Delegations
No. prev. doc.: 5840/21
No. Cion doc.: 5358/17
Subject: Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)
- Mandate for negotiations with EP

Delegations will find in the Annex the Mandate on the above mentioned Proposal for a Regulation adopted by the Permanent Representative Committee on 10 February 2021.

6087/21 TREE.2.B PB/ek 1 EN

126

DANK VOOR UW AANDACHT

g.j.zwenne@law.leidenuniv.nl