

JURIDISCH PAO ACTUALITEITEN WBP EA| LEIDEN 21 JUNI 2017

De belangrijkste ontwikkelingen m.b.t. privacy- & gegevensbescherming in Nederland

prof. mr. Gerrit-Jan Zwenne & mr. Ard Jan Dunnik



Universiteit Leiden



Miljoenenboete Facebook is kinderspel bij wat komen gaat

Grootste overtreders nieuwe privacyregels wachten boetes van enkele miljarden

Franka Robinsk Couzy
Dinsdag

De boete van enkele miljoenen euro's die Facebook boven het hoofd hangt voor het overtreden van de Nederlandse privacywet is kinderspel bij wat de toezichthouder ervan af volgt de komende jaren. Als de Autoriteit Persoonsgegevens (AP) dan, zoals twee weken geleden, oordeelt dat het socialemediabedrijf de gebruikers van het platform op meer punten niet duidelijk informeert over het gebruik van persoonsgegevens, kan ze een maximale boete opleggen van enkele miljarden euro's.

'Dit kan heel vervelend worden voor bedrijven', waarschuwt Aleid Wolfsen, voorzitter van de Autoriteit Persoonsgegevens. Nu heeft de privacywaakbond de mogelijkheid Facebook een last onder dwangsom op te leggen, wat neerkomt op een voorwaardelijke boete. Pas als het concreet binnen een bepaalde tijd niet toegenomen de overtredingen doet, wordt de boete onomroerbaarlijk.

Dat gaat veranderen. Als op 25 mei 2018 in Europa de Algemene Verordening Gegevensbescherming (AVG) van kracht wordt, dan worden er sneller boetes uitgedeeld, die bovendien hoger zijn. 'Fout is fout', zegt Wolfsen. 'We willen dat bedrijven de privacywet respecteren. De boetes kunnen oplopen tot € 20 mln, of 4% van de omzet als dat meer is dan die € 20 mln. Let wel, dat is per overtreding', zegt Wolfsen. 'En we geven geen kwantumschorting.'

In het geval van Facebook, met een omzet van \$ 26 miljard en drie overtredingen, zou dit neerkomen op maximaal € 2,5 miljard.

Volgens Daphne van der Knaaf van Bits of Freedom, een organisatie die zich inzet voor digitale privacy, ook in Amerikaans wetgeving, is de nieuwe Europese wet maar al te goed. 'De boetes zijn groot', zegt Van der Knaaf. 'Nu is de boete zo laag dat bedrijven bewust de randen opzoeken en overhoeren gaan.'



Dat kan straks niet meer. Dat weten ze. De pakkans is ook een stuk groter doordat de Europese toezichthouders gaan samenwerken. Dit is niet voor niets het meest belangrijke stuk wetgeving in jaren.

Het zijn niet alleen de grote tech-nologiebedrijven worden aangepakt. Ook een zorginstelling die data van patiënten verzamelt om met behulp van slimme apparatuur en een diagnose te kunnen stellen, is in overtreding als er geen expliciete toestemming of andere rechtsgeldige grondslag is. Hetzelfde geldt voor een bedrijf dat ongevraagd persoonlijke gegevens van sociale media als LinkedIn of Instagram haalt om daarmee klanten te werven.

Aleid Wolfsen: 'Iedereen moet in vrijheid kunnen leven, zonder op het web te worden achtervolgd door bedrijven.'

FOTO: WIEBE KUIJTER

'Ik zeg tegen bedrijven: jongens, je moet wel de boel op orde hebben'

Het zijn deze bedrijven die volgens de toezichthouder nog niet goed voor ogen hebben wat ze te wachten staat. 'Zij denken dat het wel loopt', zegt Wolfsen. 'Dat we niet zo snel een boete geven. Maar dat gaan we wel doen. We worden strenger. Daarom zeg ik tegen bedrijven: 'Jongens, je moet wel de boel op orde hebben'.'

Goedgekeurd: venstertoppen in de algemene voorwaarden, wat bedrijven nu vaak doen, is niet langer meer voldoende. Toestemming kan alleen worden verkregen als duidelijk is waarvoor de persoonsgegevens worden gebruikt. Dat moet bijvoorbeeld op de website van het bedrijf met een button worden aangegeven. En die

magneit standaard op 'akkoord' staan.

'Privacy raakt de fundamentele van de rechtsorde', zegt Wolfsen. 'Iedereen moet invrijheid kunnen leven, zonder stiekem op het web te worden achtervolgd door bedrijven en instanties.'

Bedrijven die onzorgvuldig met de persoonlijke gegevens omgaan, kunnen ook te maken krijgen met een 'datarun', omdat vanaf volgend jaar iedereen zijn gegevens kan terugvragen, ongeacht een eerder verleende toestemming.

'Net als bij een bankrun betekent dit dat het bedrijf dan overmorgen niet meer bestaat', zegt Wolfsen. 'Vertrouwen wordt belangrijker dan ooit.'

De boete van enkele miljoenen euro's die Facebook boven het hoofd hangt voor het overtreden van de Nederlandse privacywet is kinderspel bij wat de toezichthouder vanaf volgend jaar kan uitdelen. Als de Autoriteit persoonsgegevens (AP) dan, zoals twee weken geleden, oordeelt dat het socialemediabedrijf de gebruikers van het platform op meer punten niet duidelijk informeert over het gebruik van persoonsgegevens, kan ze een maximale boete opleggen van enkele miljarden euro's.

Bedrijven die onzorgvuldig met de persoonlijke gegevens omgaan, kunnen ook te maken krijgen met een '**datarun**', omdat vanaf volgend jaar iedereen zijn gegevens kan terugvragen, ongeacht een eerder verleende toestemming. 'Net als bij een bankrun betekent dit dat het bedrijf dan overmorgen niet meer bestaat', zegt Wolfsen. 'Vertrouwen wordt belangrijker dan ooit.'

agenda

- A. Uitvoeringswet AVG: de stand van zaken en wat verwachten we ervan?
- B. handhavingsprioriteiten AP: waar liggen de accenten?
- C. onderzoek & handhaving door AP



A. Uitvoeringswet AVG

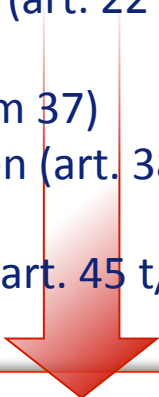
oUAVG: de stand van zaken

planning

- op 12 december 2016 werd het ontwerp wetsvoorstel gepubliceerd
- de reactietermijn eindigde op 20 januari 2017
- inmiddels ligt het bij de Raad van State
- en naar verwachting gaat het voor het zomerreces naar de Tweede Kamer
- na de zomer parlementaire behandeling
- inwerkingtreding uiterlijk 25 mei 2018...

onderwerpen

- toepassing (art. 1 t/m 5)
- regeling Autoriteit persoonsgegevens (art. 6 t/m 21)
- bijzondere persoonsgegevens (art. 22 t/m 31)
- rechtsbescherming (art. 32 t/m 37)
- uitzonderingen en beperkingen (art. 38 t/m 44)
- overgangs en slotbepalingen (art. 45 t/m 48)

- 
- *ras en etniciteit (art. 22)*
 - *gezondheid (art. 23)*
 - *genetische gegevens (art. 24)*
 - *uitzondering i.v.m. volksgezondheid (art. 25)*
 - *biometrische gegevens (art. 26)*
 - *uitzondering i.v.m. wetenschap (art. 27)*
 - *algemene uitzonderingen (art. 28)*
 - *religie en levensbeschouwing (art. 29)*
 - *politieke opvattingen*
 - *strafrechtelijke verodredelingen of feiten (art 31)*

B. handhavingsprioriteiten AP

enkele cijfers

Bezetting

	2015		2016	
	man	vrouw	man	vrouw
In dienst	2	4	2	3
Uit dienst	1	3	4	3
Bezetting einde jaar m/v	25	57	23	57
Bezetting einde jaar totaal	82		80	
Vast dienstverband	21	54	21	57
Tijdelijk dienstverband	7		2	
Totaal dienstverband	75		78	
Gemiddelde bezetting (jaar (fte's)	72,50		72,57	
Vacatures per einde jaar	1		3	
Bezetting einde jaar totaal (fte's)	74,70		73,10	

Ziekteverzuim

	2015	2016
Totaal ziekte excl. zwangerschap	7,80%	4,00%
Lang ziekteverzuim >28 dagen	3,94%	0,46%
Ouderschapsverlof	10	8
Verlof zwangerschap/bevalling	6	5
Seniorenregeling	4	3

Financiën

Begroting (bedragen x € 1.000)

	2015	2016
Begroting	8.188	8.103

Dirkzwager

	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Ambtshalve onderzoek	11	73	70	80	83	49	95	108	60	85	58	73	85	43
Boete (meldplicht)	0	1	35	9	3	0	0	0	0	0	0	0	0	0
Dwangsom	0	1	5	2	0	39	68	26	35	6	12	19	13	17
Bestuursdwang	1	1	1	1	2	0								
Bezwaar	1	2	8	15	2	5	5	6	10	6	7	6	11	15
Beroep	1	2	4	15	2	9	2	2	10	3	8	3	7	1

2016

197

0

20

15

7



verdrie(vijf)(tien)voudiging...?



De Correspondent 1 augustus 2016.

“Ik word altijd giechelend aangekeken als ik ervoor pleit ons budget te vervienvoudigen, maar dat zou nog maar een begin zijn. We moeten nu teveel laten liggen.”



Website AP 1 juni 2017.

handhavingsprioriteiten Ap 2017

Nieuwe EU-wetgeving
gegevensbescherming



Van verzamelen
tot profileren



Bijzondere
persoonsgegevens



Beveiliging van
persoonsgegevens

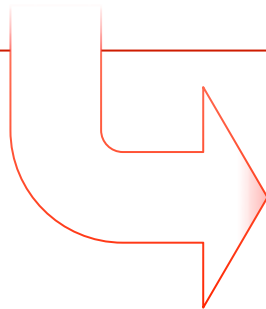


- op 25 mei 2018 gelijk speelveld voor organisaties die persoonsgegevens verwerken
- advies aan overheden en bedrijven te inventariseren welke aanpassingen nodig zijn om te voldoen aan de nieuwe regels
- tja...

Nieuwe EU-wetgeving
gegevensbescherming



- op basis van profielen kunnen mensen verschillend worden behandeld
- een toenemend gebruik van 'slimme technologieën' zoals wifi-tracking en big data
- (geautomatiseerde) conclusies mogelijk



focus op transparantie: mensen moeten worden geïnformeerd over welke gegevens van hen worden verwerkt, wat daarmee gebeurt en met welk doel (enz.)

Van verzamelen
tot profileren



- gegevens over gezondheid, ras, godsdienst, seksuele leven, politieke voorkeur, strafrechtelijk verleden (en BSN)
- ook deze gegevens belanden steeds vaker in databases

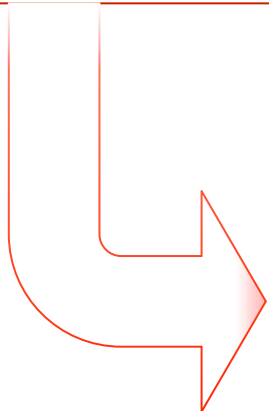
Bijzondere
persoonsgegevens



focus op naleving van het verbod op
verwerking van bijzondere persoonsgegevens

- privacy-by-design
- adequate beveiliging om te voorkomen dat mensen (financiële) schade ondervinden als hun persoonsgegevens op straat komen te liggen
- klantportalen goed beveiligen en zo nodig alleen toegang te verlenen tot gegevens d.m.v. tweefactorauthenticatie

Beveiliging van
persoonsgegevens

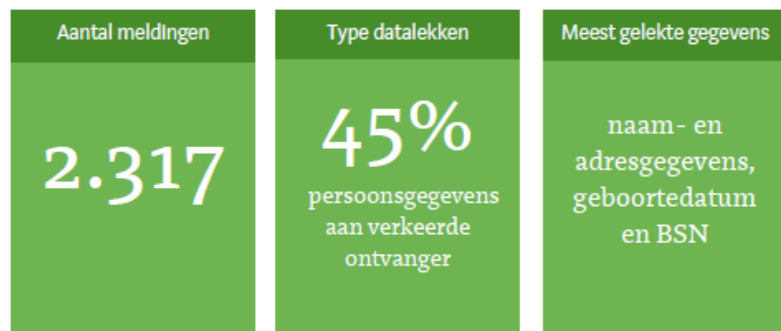


Ap houdt toezicht op naleving meldplicht datalekken en richt zich op situaties waarin de beveiliging overduidelijk niet op orde is

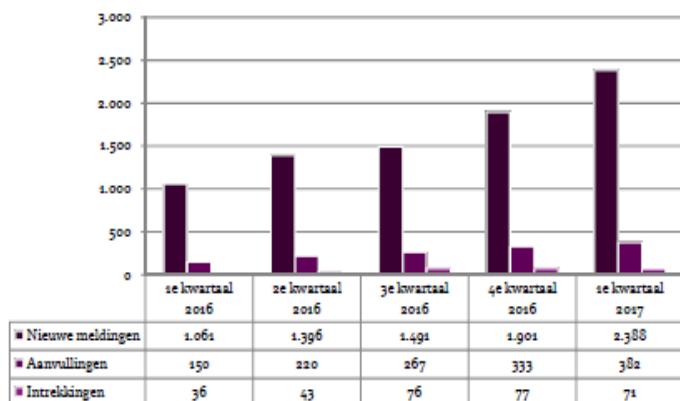
meldplicht datalekken

Meldplicht datalekken: facts & figures

Overzicht feiten en cijfers 1e kwartaal 2017



Aantal meldingen in het eerste kwartaal van 2017



soorten van datalekken



- Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger 45%
- Overig 16%
- Apparaat, gegevensdrager en/of papier kwijtgeraakt of gestolen 15%
- Hacking, malware en/of phishing 7%
- Brief of postpakket kwijtgeraakt of geopend retour ontvangen 7%
- Persoonsgegevens van verkeerde klant getoond in klantportaal 5%
- Persoonsgegevens per ongeluk gepubliceerd 5%
- Persoonsgegevens bij oud papier gezet <1%
- Persoonsgegevens nog aanwezig op afgedankt apparaat <1%



AUTORITEIT
PERSOONSGEGEVENS

C. onderzoek & handhaving door Ap

onderzoek & handhaving door Ap

- Hoffmann
- Uniper
- Bluetrace
- Facebook
- BSN in btw-nrs zzp'ers



Belastingdienst



- Hoffmann doet screening van (potentieel) personeel in opdracht van organisaties
- Hoffmann deed beroep op wettelijke grondslag ondubbelzinnige toestemming
- Bij de screenings verwerkte Hoffmann onder meer:
 - gegevens over **ras** en **afkomst** (door kopie identiteitsbewijs);
 - gegevens over **gezondheid**;
 - **strafrechtelijke** gegevens;
 - het **BSN** (door kopie identiteitsbewijs);
 - **financiële** gegevens;
 - gegevens afkomstig van **sociale media**; en
 - **relationele** gegevens.

Conclusies AP:

- geen toestemming als wettelijke grondslag voor screenings van sollicitanten en werknemers
- screening mag alleen plaatsvinden op onderdelen die noodzakelijk zijn om de in kaart gebrachte risico's te verkleinen.
- verwerkte informatie tijdens screenings moet voldoen aan beginselen van proportionaliteit en subsidiariteit
- Hoffmann heeft haar werkwijze aldus aangepast

- Uniper had (voorgenomen) beleid:
 - alle personeel tekent voor at random alcoholtesten (blaastest) en drugstesten (wangslijmtest, drugshond, controle werkplek en auto) bij vermoeden
 - alle personeel die deelnemen aan verkeer of installatie bedienen melden medicijnverbruik met gele sticker bij leidinggevende
- wie niet tekende liep risico sanctie

Conclusies AP t.a.v. testen:

- Verwerking gegevens betreffende iemands gezondheid, dus
 - art. 16 Wbp (verwerkingsverbod) van toepassing,
 - dus uitzondering op verwerkingsverbod nodig
- toestemming van werknemer is niet rechtmatig
- voor het overige geen uitzonderingsgrond in de wet te vinden voor Uniper

Conclusies AP t.a.v. medicijngebruik:

- werkgevers mag medicijnverbruik niet verwerken
- wel bedrijfsarts in het kader van de begeleiding en re-integratie van zieke werknemers
- ... en dan uitsluitend bij werknemers die werkzaamheden uitvoeren waarbij gevaar voor de werknemer of omstanders bij gebruik medicijnen.

- Bluetrace verzamelt via wifi-tracking locatiegegevens van
 - winkelbezoekers,
 - voorbijgangers en
 - omwonenden
- identificatie via Mac-adres van telefoon
- voorbijgangers t.b.v. conversiemeting
- omwonenden is ongewenste bijvangst
- Bluetrace doet beroep gerechtvaardigd belang

Conclusies AP:

- betreffen persoonsgegevens (identificatie zonder onevenredige inspanning)
- winkelbezoekers moeten beter worden geïnformeerd (art. 34 Wbp), tracking kenbaar, opt-out
- geen grondslag voor tracking omwonenden
- passanten niet meer volgen, maar slechts tellen, en beter informeren met borden
- Last onder dwangsom (6 maanden)

Facebook



- Facebook verzamelt gegevens over gedrag van gebruikers
 - binnen de Facebookomgeving
 - én op andere website via cookies
- daarmee maakt Facebook profielen
- deze worden ingezet om gericht advertenties te tonen

constateringen

- informatie welke soorten gegevens worden gebruikt voor staat niet op een centrale plek, maar verspreid over allerlei bronnen.
- Facebook zegt niet dat het bijzondere persoonsgegevens seksuele geaardheid wordt gebruikt en maakt onvoldoende duidelijk dat surfgedrag en app-gebruik ook buiten Facebook gevolgd wordt, zelfs als men is uitgelogd.
- weinig informatie over controlemogelijkheden voor gericht adverteren
 - gebruikers hebben geen mogelijkheid om alle verwerkingen voor dit doeleinde te weigeren.

conclusies

- gebruikers worden niet adequaat geïnformeerd over wat het Facebook met hun gegevens doet.
- voor de verwerking van bijzondere gegevens moet beroep worden gedaan op een uitzondering (art. 16 jo 23 Wbp), zoals
 - uitdrukkelijk toestemming van gebruikers of
 - duidelijke openbaarmaking door gebruikers zelf.
- beide zijn niet van toepassing

BSN in btw-nummers ZZP'ers



- recent onderzoek of de Belastingdienst een wettelijke grondslag heeft voor het verwerken van het BSN in btw-identificatienummers van zzp'ers
- BSN van ZZP'ers is integraal opgenomen in btw-identificatienummer
- ZZP'ers hebben verplichting om hun btw-nummer aan (potentiële) klanten bekend te maken, bijv. op facturen
- BSN is een bijzonder persoonsgegeven, want het is een uniek en tot de persoon herleidbaar nummer
- verwerking vereist daarom wettelijke grondslag