AUTORITEIT PERSOONSGEGEVENS

Autoriteit Persoonsgegevens

AUTORITEIT
PERSOONSGEGEVENS

NL | EN

Doorzoek de gehele site

TIP ONS

Home Actueel Over privacy Onderwerpen Zelf doen Publicaties Melden

18 mei 2017

AP presenteert jaarverslag 2016; nog 1 jaar tot nieuwe privacywet

BEKIJK HET NIEUWSBERICHT

Nieuwsberichten

Nieuwsbericht / 21 juni 2017
AP adviseert over Uitvoeringswet AVG

Nieuwsbericht / 20 juni 2017
Blijft het BSN straks een bijzonder persoonsgegeven?

Nieuwsbericht / 19 juni 2017
AP adviseert over ontwerpbesluit gebruik ANPR-gegevens door politie

→ Alle nieuwsberichten

INTERVIEW JACOB KOHNSTAMM

'Privacy wordt zeker chefsache, met boetes van 2% tot 4% van de omzet'

Bewaker van persoonsgegevens vertrekt na twaalf jaar bij toezichthouder

ranka Rolvink Couzy
msterdam

wee weken voordat zijn opvolger be-end wordt gemaakt, leest Jacob Kohn-tamm (66), de voorzitter van de Autori-eit Persoonsgegevens, in de Volkskrant at het op grote schaal aftappen van nternetverkeer vermoedelijk werkelijk-eid wordt. Inlichtingendiensten zou-en, zo blijkt uit geheime documenten, e data van onschuldige burgers vanaf olgend jaar net zo nauw in de gaten ogen houden als die van een verdachte n een misdrijf.

Dit moet een gruwel zijn voor de man ie twaalf jaar lang heeft gevochten voor e bescherming van persoonsgegevens. ij heeft overhoop gelegen met data-rslinders als Google en Facebook, gaf mroep NPO en academisch ziekenhuis Umc een reprimande nadat ze de rivacy hadden geschonden. En hij waar-huwde onlangs gemeenten voor hun ebrekkige verwerking van persoons-egevens.

Telkens benadrukt Kohnstamm dat egevens van mensen alleen mogen wor-en verzameld als er een rechtsgrond , zoals toestemming. Politie en justitie ogen dat ongevraagd van mensen die op de korrel hebben. Maar onschul-ige burgers hebben recht op privacy. aarin komt dus verandering, als de erichten kloppen en als de Raad van tate daarmee deze zomer akkoord gaat, lijkt het.

Wat vindt u van dit kabinetsvoorstel?
Gegevensverzameling moet proporti-neel zijn. Dat staat voorop. Of dat hier aat veranderen, weet ik niet, omdat ik et voorstel nog niet heb gelezen.'

aarmate het aantal aanslagen toe-

CV

1949
Geboren in Wassenaar

Studie rechten aan de Universiteit van Amsterdam (afgerond in 1977), daarna afwisselend advocaat, lid van de Tweede Kamer voor D66 en voorzitter van die partij

1994-1998
Staatssecretaris van Binnenlandse Zaken, verantwoordelijk voor grotestedenbeleid

1999-2004
Senator voor D66

2004-zomer 2016
Voorzitter van het College bescherming persoonsgegevens (CBP), dat sinds dit jaar Autoriteit Persoonsgegevens heet

2010-2014
Voorzitter van de Artikel 29-werkgroep, de Europese privacytoezichthouders

Sinds april
Coördinerend voorzitter van de Regionale Toetsingscommissies Euthanasie (parttime)

V Dus in Nederland hoeven we niet bang te zijn dat we te snel bij het kruisje tekenen. Daar waakt de Autoriteit over?
'Als we het vijfvoudige aan budget hebbe zo'n € 40 mln, komen we een eind. Goed is dat straks met de nieuwe Europese privacywetgeving de bewijslast bij de ander partij ligt. Bedrijven moeten aantonen

gehoord: onzichtbaar gevolgd worden in de winkelstraat omdat je wifi op je mobieltje aan hebt staan; een tv-provider die precies weet naar welke programma's je kijkt, op welke tijden én

der geval weten wat er met je gegevens gebeurt én daar bewust toestemming voor geven. Dat geldt nog sterker na 25 mei 2018. Dan gaat een nieuwe privacyverordening in.

toestemming weer in te trekken of een bedrijf te vragen om al jouw gegevens te verwijderen."

De meeste datalekken komen voor

niet op orde heeft?

„Dan zijn ze in overtreding en kunnen ze een fikse boete verwachten. En ja, die boetes worden dan openbaar."

CHEFSACHE

Bestuurders aansprakelijk na ernstige cyberaanval

Axel Arnbak

All jaren lezen wij in de krant dat cybersecurity een groeiend maatschappelijk probleem is. Maar of de toenemende zorgen organisaties daadwerkelijk aanzetten tot actie bleef lang de vraag. Het antwoord wordt steeds duidelijker. Handhavingsboetes bij ernstige datalekken kunnen onder de nieuwe Europese datawetgeving oplopen tot 4% van de wereldwijde jaaromzet. Bovendien kunnen bestuurders persoonlijk aansprakelijk gesteld worden bij ernstige cyberaanvallen, en zijn de eerste schadeclaims al een feit. Cyberaanvallen kunnen zowel ondernemingen als individuele bestuurders diep in de portemonnee raken. Cybersecurity is chefsache.

Gregg Steinhafel stapte in mei 2015 op als ceo van de Amerikaanse retailer Target, na een creditcard-hack vlak voor kerst. Target moest de klanten een persoonlijke e-mail sturen en liep miljoenen mis omdat zij hun kerstinkopen vervolgens bij de concurrent deden. Later bleek de hack niet een kleine subgroep maar 70 miljoen klanten te hebben getroffen. Target had dit verzwegen. De koers kelderde, exit Steinhafel.

Door een zware hack in 2011 bij de kleine Beverwijkse certificatenaanbieder Diginotar lag het Nederlandse internet een week plat, vooral in de publieke sector. Daarop ging Diginotar vrij snel failliet. Kort voor de hack was Diginotar overgenomen. De nieuwe eigenaar wist in 2014 met succes bij de rechtbank Amsterdam de vorige bestuurders aansprakelijk te stellen, omdat zij de zwakke beveiliging hadden verzwegen voor de kopers. Via hun persoonlijke bv's moesten zij miljoenen euro's terugbetalen. Amerikaanse toestanden in de polder.

Sinds 1 januari 2016 heeft de wetgever bestuurdersaansprakelijkheid expliciet mogelijk gemaakt bij ernstige datalekken. Niet alleen een instructie tot onrechtmatig handelen kan daartoe leiden, ook het laten voortduren ervan of nalaten van preventieve maatregelen te treffen. Momenteel behandelt het parlement een meldplicht beveiligingsincidenten in brede zin, of er nu een datalek is of niet. Een cyberaanval die de energievoorziening, gezondheidszorg of het financiële verkeer lamlegt, leidt dan meteen tot vragen van toezicht- en aandeelhouders. Als blijkt dat een organisatie willens en wetens verouderde of verzwakte IT-systemen gebruikt, lopen onderneming en bestuurder een serieus risico. Vooral als het bestuur na interne escalatie pijnlijke feiten verzwijgt of verdraait om onder de radar te blijven.

Target en Diginotar tonen hoe cyberaanval grote en kleine onderneming diep in de problemen brengt

Niet alleen de media en IT-consultants, zelfs conventionele juridische vaktijdschriften publiceren nu over aansprakelijkheid bij cyberaanvallen. Vorige week verscheen een sterk overzichtsartikel van Eric Tjong Tjin Tai. De Tilburgse hoogleraar privaatrecht is alleen wat te voorzichtig waar hij vermoedt dat de schade na een datalek meevalt. Target en Diginotar tonen hoe een cyberaanval een grote en kleine onderneming diep in de problemen brengt of zelfs de nek omdraait, met miljoenenschade als gevolg.

Daarnaast breidt de nieuwe Nederlandse datawetgeving de handhavingsboetes uit tot maximaal 10% van de binnenlandse jaaromzet. De nieuwe EU-wet, die per mei 2018 de Nederlandse vervangt, maximeert de boete op 4% van de mondiale jaaromzet. Legt een toezichthouder zo'n heftige boete op, dan is er echt iets goed misgegaan en zullen aandeelhouders niet terugdeinzen hun schade op een bestuurder te verhalen. De EU-wet bevat ook een nieuw regime voor 'class action'-procedures. Net als in de financiële sector kunnen opportunistische stichtingen beperkte individuele dataschade gezamenlijk ophalen bij de rechter. Via internet zijn duizenden klanten van een groot bedrijf zo gevonden. De naderende beveiligingsnachtmerrie van het internet der dingen doet nog een flinke duit in het zakje. Zie als bestuurder een 'connected' cv-ketel, auto of televisie een jaar na aankoop maar beveiligd te houden tegen cyberaanvallen.

Beveiliging blijft moeilijk, maar bestuurders kunnen zich niet meer verschuilen achter de cybercomplexiteit. Vooral verdraaien en verzwijgen zal hard aangepakt worden. Verzekeraars houden hun beurzen dan gesloten. Als cybersecurity vanuit maatschappelijk oogpunt nog geen boardroom-issue was, zal de trend richting hoge boetes en bestuurdersaansprakelijk na ernstige cyberincidenten daarin het sluitstuk vormen.

Axel Arnbak is advocaat bij De Brauw Blackstone Westbroek en onderzoeker aan het Instituut voor Informatierecht (UvA). Reacties: **@axelarnbak**

pagina 11, 16-06-2016 © Het Financieele Dagblad

INTERVIEW ALEID WOLFSEN

Privacybaas dreigt gemeenten en bedrijven met hoge boetes

Torenhoge boetes wachten bedrijven die slordig omgaan met de privacy van hun klanten. Ook als er geen sprake is van 'grove schuld'.

Natasja de Groot
Den Haag

Bedrijven en vooral gemeenten springen nog steeds veel te slordig om met privacygevoelige informatie. Vanaf volgend jaar staan daar flinke boetes op.
Aleid Wolfsen moet ze gaan uitdelen. Als burgemeester van Utrecht, PvdA-Kamerlid én rechter besliste hij over privacy(inbreuk) van burgers, nu waakt hij over persoonsgegevens. Wolfsen (57) is sinds vorig jaar de baas van privacywaakhond Autoriteit

Ga uw gang als u uw naaktfoto's wilt delen met 20.000 vrienden

Persoonsgegevens.
In zijn nieuwste functie stuit Wolfsen soms op vormen van privacyschending waarvan hij nog nooit had gehoord: onzichtbaar gevolgd worden in de winkelstraat omdat je wifi op je mobieltje aan hebt staan; een tv-provider die precies weet naar welke programma's je kijkt, op welke tijden én hoe lang; een baas die zijn werknemer een *wearable* (een draagbare gadget) cadeau geeft en de informatie over diens leefpatroon wil 'uitlezen'.

Hoe belangrijk is privacy?
„Privacy is wat zich in je hoofd afspeelt, in je lichaam, in je huiskamer, je communicatie met anderen. Tegenwoordig vertaalt dit zich allemaal in data. Ik wed met jou dat Google meer over jouw gezondheid weet dan je huisarts. Privacy én data raken tegenwoordig aan alles, aan ons hele maatschappelijke leven."

Nederlanders lijken er niet wakker van te liggen dat ze hun privacy weggeven in ruil voor een gratis app...
„Mijn voorganger, Jacob Kohnstamm, zei altijd: 'Als u uw naaktfoto's wilt delen met uw 20.000 beste vrienden op Facebook en u weet wat u doet, ga vooral uw gang'. Echter, veel mensen zijn zich er niet van bewust dat hun persoonsgegevens het nieuwe betaalmiddel zijn. Hoe meer je van jezelf prijsgeeft – over je geloof, je voorkeuren, je inkomen of hobby's – hoe meer diensten je 'krijgt'."

Kunnen we eigenlijk nog wel om diensten als Google, Whatsapp of een parkeerapp heen?
„We beleven er plezier aan, het maakt ons leven gemakkelijker en draagt bij aan economische vooruitgang. Máár je moet wel weten dat je wordt getracked in winkels met wifi. Dat bedrijven een profiel van jou maken op basis van je persoonlijke gegevens. Wij zeggen: jij moet beheerder worden van jouw gegevens. Jij moet in ieder geval weten wat er met je gegevens gebeurt én daar bewust toestemming voor geven. Dat geldt nog sterker na 25 mei 2018. Dan gaat een nieuwe privacyverordening in.

▲ **Aleid Wolfsen: „90 procent van de bedrijven en gemeenten heeft hier nog geen weet van."**
FOTO MARCO DE SWART

Wat gaat die nieuwe Europese privacywet voor burgers betekenen?
„Europese burgers krijgen meer inzicht in en controle over hun persoonsgegeven

Ik wed dat Google meer over je gezondheid weet dan je huisarts

vens te verwerken, dan moet hij precies weten waar hij toestemming voor geeft. Het moet net zo simpel zijn om op een bepaald moment je toestemming weer in te trekken of een bedrijf te vragen om al jouw gegevens te verwijderen."

De meeste datalekken komen voor bij gemeenten. Zijn ze er straks klaar voor?
„Het eerlijke antwoord is dat we hier serieuze zorgen over hebben. Veel gemeenten, maar ook bedrijven hebben bijvoorbeeld nog geen functionaris gegevensbescherming aangesteld. We leggen nu pas boetes op als bij opzet of grove schuld informatie op straat is komen te liggen. Volgend jaar veranderen er drie dingen: instanties moeten sneller melden, de boetes worden draconisch hoger én de drempel van opzet of grove schuld komt te vervallen.
Ik denk dat 90 procent van alle bedrijven en gemeenten hier nog geen weet van heeft."

Wat als een gemeente of een verzekeraar op 25 mei zijn zaakjes niet op orde heeft?
„Dan zijn ze in overtreding en kunnen ze een fikse boete verwachten. En ja, die boetes worden dan openbaar."

Miljoenenboete Facebook is kinderspel bij wat komen gaat

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.

Geen kwantumkorting

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

Aleid Wolfsen, voorzitter van de Autoriteit Persoonsgegevens. Foto: Wiebe Kiestra

Volgen via mijn nieuws

- Boete
- Compliance
- EU
- Facebook
- Privacy
- Sociale media
- Technologie
- Toezichthouder

Laatste nieuws

21:37
Auteur Franse anti-corruptiewet blijkt zelf geen voorbeeld

21:23
Federal Reserve verhoogt rente ondanks tegenvallende inflatie

21:15
NVWA neemt exclusieve

Aleid Wolfsen

Wilbert Tomesen

Organigram Autoriteit Persoonsgegevens

locatie: Bezuidenhoutseweg 30 Den Haag

De AP in beweging

2001: voorlichter/adviseur

2007: handhavende toezichthouder

Anno 2017: handhavende toezichthouder in verbinding

Taken AP

- Toezicht
- Advisering
- Voorlichting, informatieverstrekking en verantwoording
- Internationale taken

Zienswijzen o.a.

- Landelijke verwerking medische gegevens

Richtsnoeren o.a.

- Richtsnoeren beveiliging van persoonsgegevens
- Richtsnoeren identificatie en verificatie van persoonsgegevens. Gebruik van ‘kopietje’ paspoort in de private sector

Richtlijnen o.a.

- Richtlijnen voor FG's
- Richtlijnen dataportabiliteit
- Richtlijnen leidende toezichthouder

Wat betekent een FG voor de AP:

- 'Verlengstuk' van de AP die belangrijke invloed uit kan uitoefenen op de naleving Wbp op de werkvloer.
- Signaalgever (mogelijke) overtredingen van de Wbp.

Wat kan de AP voor een FG betekenen:

- fg@autoriteitpersoonsgegevens.nl: vragen voldoende onderbouwd en gemotiveerd.
- Een maal per jaar aanwezig op vergaderingen FG's

Beleidsregels handhaving doorde AP

- ernstige overtredingen;
- structurele overtredingen;
- die veel mensen treffen;
- handhavingsinstrument effectief verschil kan maken.
- jaarlijkse aandachtpunten die door de AP bekend zijn gemaakt.

Speerpunten 2017
4 Thema's

- AVG
- Bijzondere persoonsgegevens
- Verzamelen en profileren
- Beveiliging van persoonsgegevens

1. Bronnen aanwijzingen overtredingen
   - Signaalfunctie
   - Verzoek om handhaving
   - Media
   - Contacten met en volgen ontwikkelingen in het 'veld'

2. Toepassen prioriteringscriteria

3. Beslissen over aanpak:
   - Alternatieve interventies; of
   - (Ambtshalve) onderzoek

a) Ambtshalve onderzoeken ex artikel 60 Wbp
   - Waterproof, recreatiewoningen, automatische kwijtschelding

b) Voorafgaande onderzoeken ex artikel 31 Wbp
   - Heimelijk cameratoezicht, BSN voor buitenwettelijke doeleinden, delen van strafrechtelijke gegevens met derden

c) Toetsen van gedragscodes ex art. 25 Wbp
   - Financiele Instellingen etc.

Bevoegdheden onderzoek

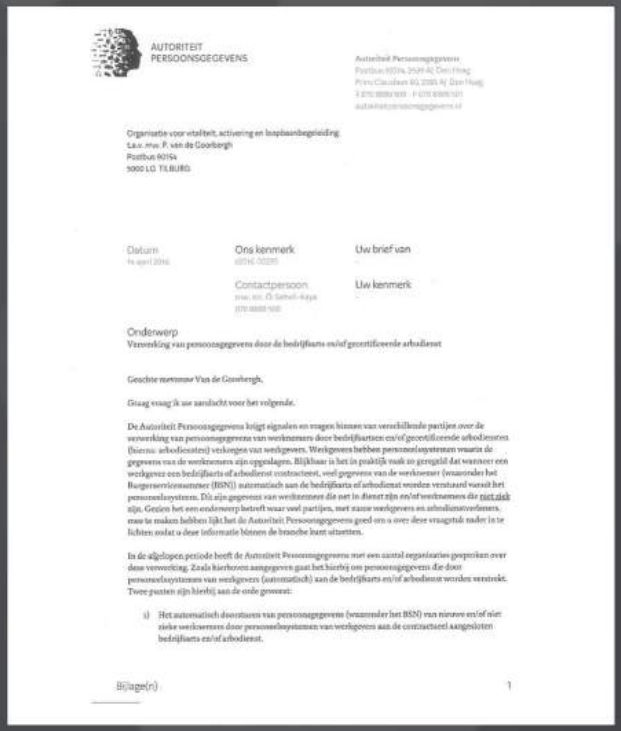
- Inlichtingen verzoeken (mondeling of schriftelijk) (5:16 AwB)
- Gegevens en bescheiden onderzoeken en kopiëren (5:17 AwB)
- Verantwoordelijken verplicht tot medewerking (5:20 AwB)
- Geen beroep op geheimhoudingsplicht (art 61, vijfde lid, Wbp)

Werkwijze ambtshalve onderzoeken

- Schriftelijk verzoek om inlichtingen (eventueel voorafgegaan door telefonisch contact)
- Aanvullende informatie opvragen zo nodig bij derden (bewerker of contractspartij)
- Mogelijk een onderzoek ter plaatse (gesprekken, papieren informatie, inzage in systemen)

- Opstellen voorlopige bevindingen met verzoek om reactie
- Vaststellen definitieve bevindingen met een openbaarmakingsbesluit
- Persmoment; voor openbaarmaking contact met verantwoordelijke

- Bij in onderzoek vastgestelde overtredingen overdracht naar afdeling Juridische zaken voor het formele handhavingstraject
- Handhaving bestaat uit last onder dwangsom
- Vanaf 1 januari 2016 ook een boete mogelijk geworden (max €820k)
- Per 25 mei 2018 boete mogelijk van max €20 mio



AUTORITEIT
PERSOONSGEGEVENS

Organisatie voor vitaliteit, activering en loopbaanbegeleiding
t.a.v. mw. P. van de Goorbergh
Postbus 90154
5000 LG TILBURG

Datum
14 april 2016

Ons kenmerk

Uw brief van

Contactpersoon

Uw kenmerk

Onderwerp
Verwerking van persoonsgegevens door de bedrijfsarts en/of gecertificeerde arbodienst

Geachte mevrouw Van de Goorbergh,

Graag vraag ik uw aandacht voor het volgende.

De Autoriteit Persoonsgegevens krijgt signalen en vragen binnen van verschillende partijen over de verwerking van persoonsgegevens van werknemers door bedrijfsartsen en/of gecertificeerde arbodiensten (hierna: arbodienst(en)) verkregen van werkgevers. Werkgevers hebben personeelssystemen waarin de gegevens van de werknemers zijn opgeslagen. Blijkbaar is het in praktijk vaak zo geregeld dat wanneer een werkgever een bedrijfsarts of arbodienst contracteert, veel gegevens van de werknemer (waaronder het Burgerservicenummer (BSN)) automatisch aan de bedrijfsarts of arbodienst worden verstrekt via het personeelssysteem. Dit zijn gegevens van werknemers die niet in dienst zijn en/of werknemers die niet ziek zijn. Gezien het een onderwerp betreft waar veel partijen, met name werkgevers en arbodienstverleners, mee te maken hebben lijkt het de Autoriteit Persoonsgegevens goed om u over deze vraagstuk nader in te lichten zodat u deze informatie binnen de branche kunt uitzetten.

In de afgelopen periode heeft de Autoriteit Persoonsgegevens met een aantal organisaties gesproken over deze verwerking. Zoals hierboven aangegeven gaat het hierbij om persoonsgegevens die door personeelssystemen van werkgevers (automatisch) aan de bedrijfsarts en/of arbodienst worden verstrekt. Twee punten zijn hierbij aan de orde geweest:

i) Het automatisch doorsturen van persoonsgegevens (waaronder het BSN) van nieuwe en/of niet zieke werknemers door personeelssystemen van werkgevers aan de contractueel aangesloten bedrijfsarts en/of arbodienst.

Bijlage(n)

1

Beleidsregels actieve openbaarmaking
vanaf 12 januari 2016
uitgangspunt; openbaar tenzij..
tenzij;

- onevenredige benadeling
- bedrijfsvertrouwelijkheid

Boetebeleidsregels 15 december 2015

WP 29

- 27 nationale toezichthouders, EDPS en Europese Commissie
- Vijf vergaderingen per jaar
- Interpretatie open normen via opinies
- Coördinatie standpunten
- Gezamenlijk onderzoek

  - Opinies worden voorbereid in subgroepen
  - Plenaire vergadering: ca 30 delegaties aan tafel
  - Merkbare verschillen West/Oost of Noord/Zuid
  - Subgroep: gemiddeld 10 delegaties aan tafel

Europees toezicht op politie en justitie

- Niet één overkoepelende vergadering van toezichthouders
- Gemeenschappelijk toezicht op centrale delen systeem, nationaal toezicht op nationale delen systeem
- Eén gemeenschappelijk orgaan per databank/soort verwerking
  - JSB Europol
  - JSA Douane (Douane Informatiesysteem)
  - JSA Eurodac (Vingerafdrukken)
  - JSA Schengen (Schengen Informatiesysteem)