



PIV Congres 2019

AVG in de praktijk

mr. ir. Jørgen Simons

Vrijdag 29 maart 2019

AVG in de praktijk

- Wat zijn inmiddels de ervaringen met de AVG, bijna 1 jaar later?
- Waar lopen verzekeraars, tussenpersonen, benadeelden, juristen, schade-experts, medisch adviseurs, arbeidsdeskundigen, herstelgerichte dienstverleners en werkgevers allemaal tegenaan?

Vraag 1

- Hoe streng wordt er gecontroleerd op de AVG?
- Wat zijn de belangrijke punten die op orde moeten zijn binnen deze branche?



Toezichtkader Autoriteit Persoonsgegevens 2018-2019

1. **Bevorderen** naleving

- bieden van guidance
- verstrekken van wetgevingsadviezen
- behandeling van klachten

Behandeling van klachten

Rapportage AP



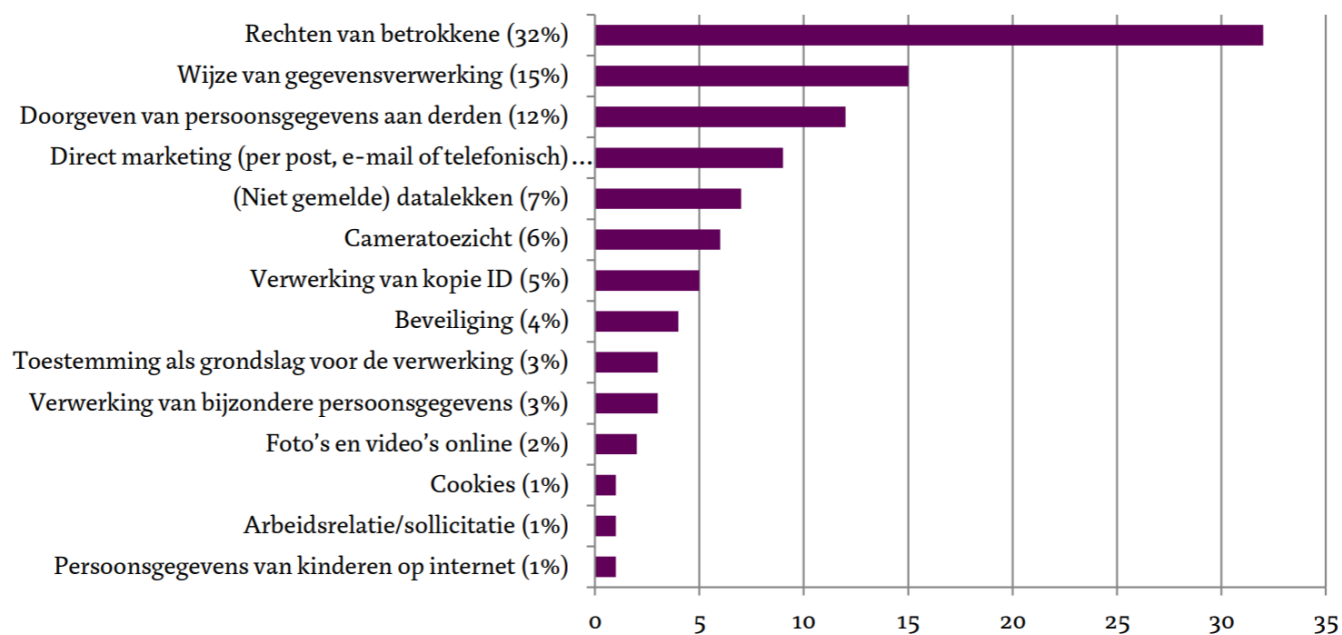
AUTORITEIT
PERSOONSGEGEVENS

Klachtenrapportage: facts & figures Overzicht 25 mei tot 25 november 2018



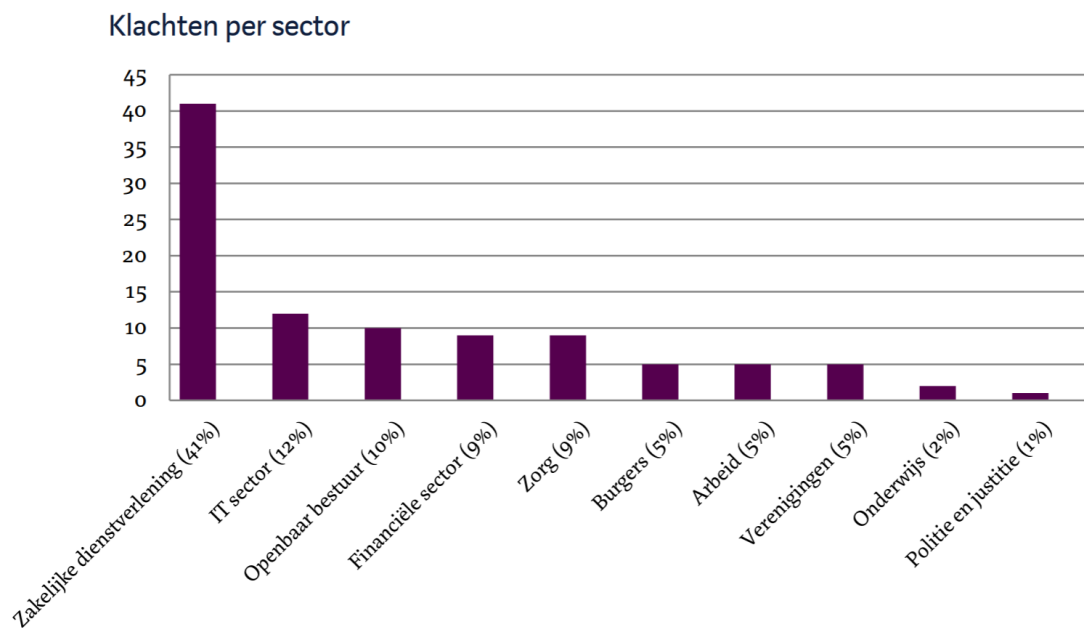
Behandeling van klachten

Klachten per onderwerp



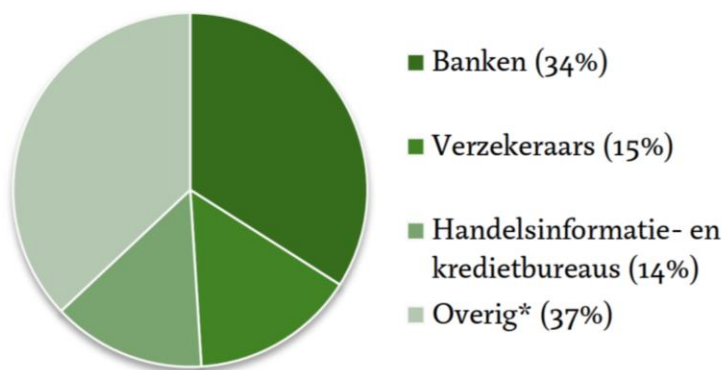
Behandeling van klachten

Klachten per sector



Behandeling van klachten

Financiële sector



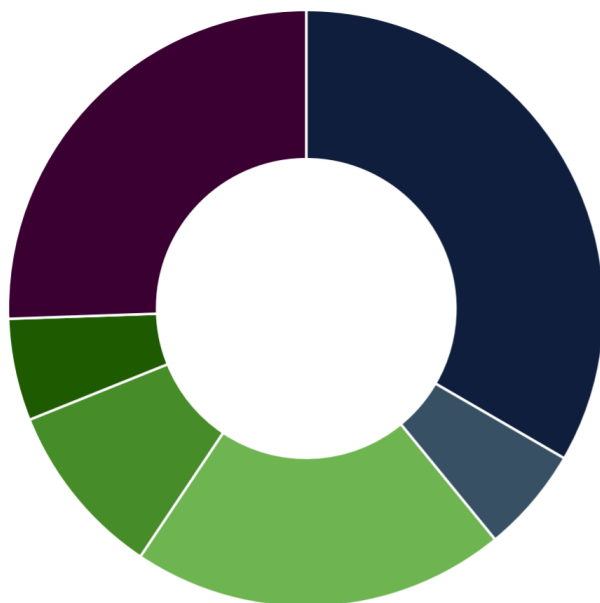
* Onder 'overig' bij financiële sector wordt verstaan betaalservices en investerings- en beleggingsmaatschappijen

Onderwerpen

1. Rechten van betrokkenen
2. Wijze van gegevensverwerking
3. Doorgeven van persoonsgegevens aan derden

Behandeling van klachten

Wijze van behandeling

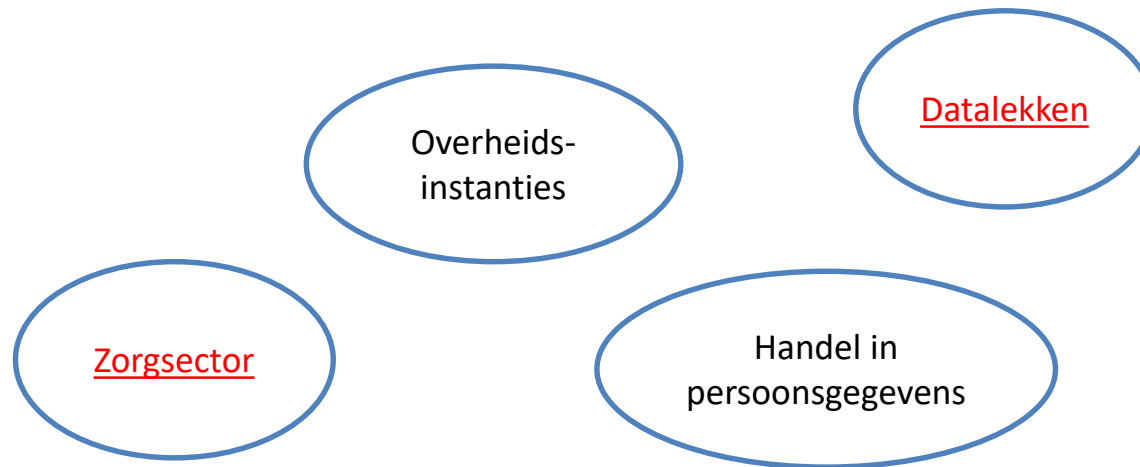


- Handreiking aan betrokkene (33%)
- Klacht ingetrokken (6%)
- Normuitleggende brief (20%)
- Normoverdragend gesprek (10%)
- Bemiddeling (5%)
- Geen (evidente) overtreding / Overig (26%)

Toezichtkader Autoriteit Persoonsgegevens 2018-2019

2. Controleren naleving

- controleren verschillende sectoren op één of meerdere nalevingsverplichtingen AVG
- risicogericht toezicht



Toezichtkader Autoriteit Persoonsgegevens 2018-2019

Zorgsector

Focus op:

- Beveiliging van medische gegevens
- Grondslag voor verwerking (met name bij uitwisseling van gegevens)
- Aanwezigheid/volledigheid verwerkingsregister
- Aanwezigheid Functionaris Gegevensbescherming en diens positie

Toezichtkader Autoriteit Persoonsgegevens 2018-2019

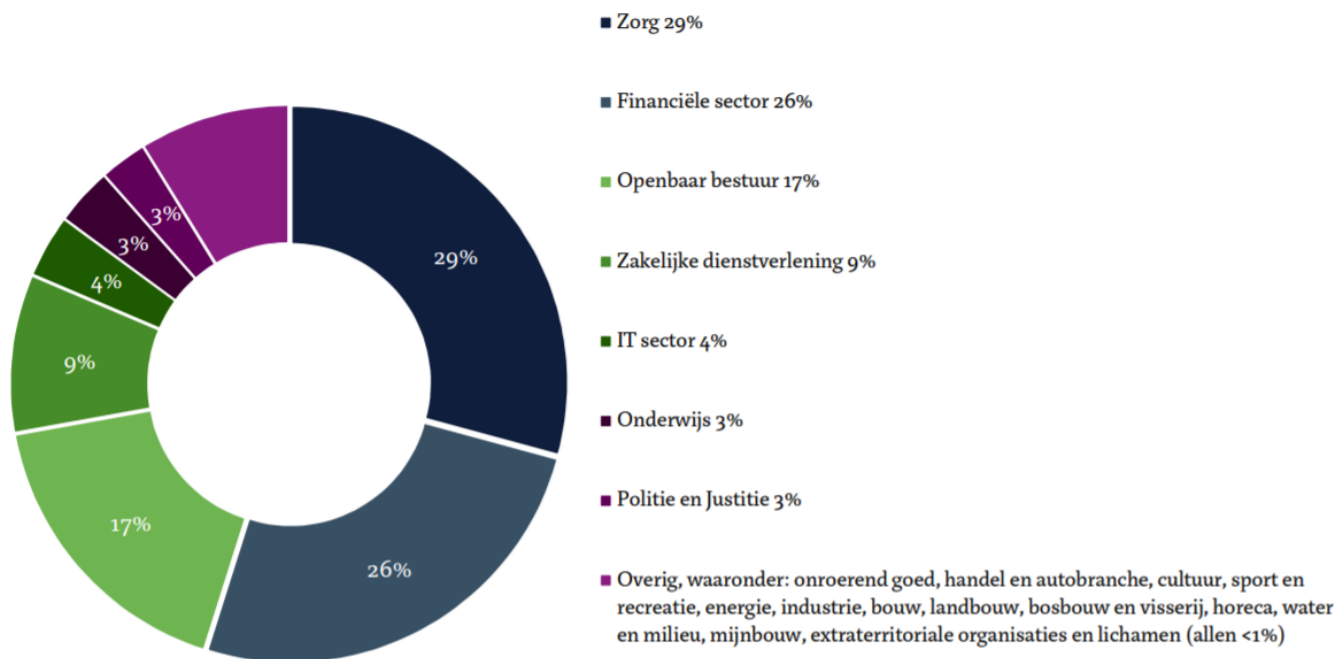
Datalekken

Sterke toename aantal meldingen:

- 2016: ≤ 6.000 meldingen
- 2017: > 10.000 meldingen
- 2018: > 20.000 meldingen

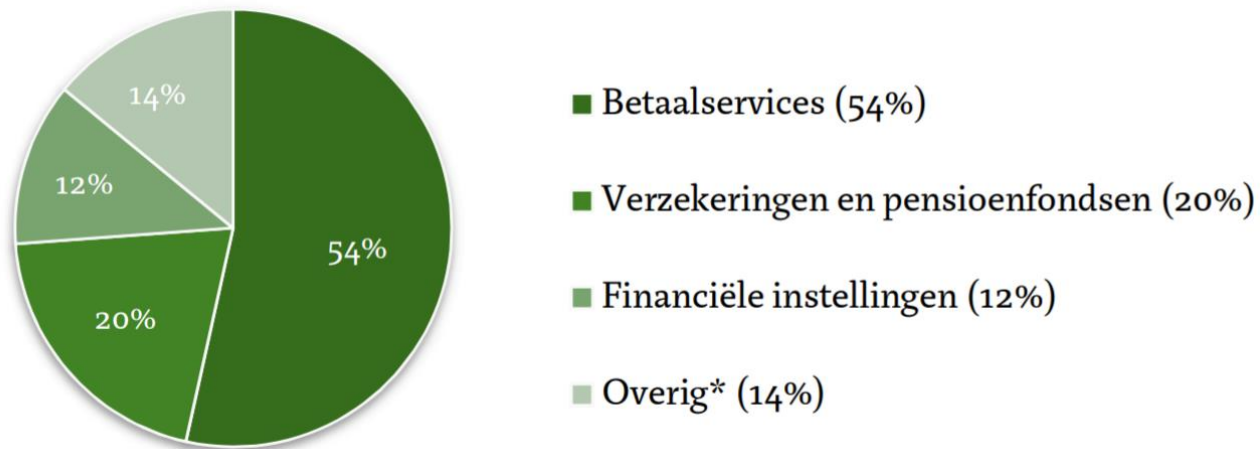
Meldplicht datalekken: facts & figures 2018

Meldingen datalekken per sector



Meldplicht datalekken: facts & figures 2018

Financiële sector

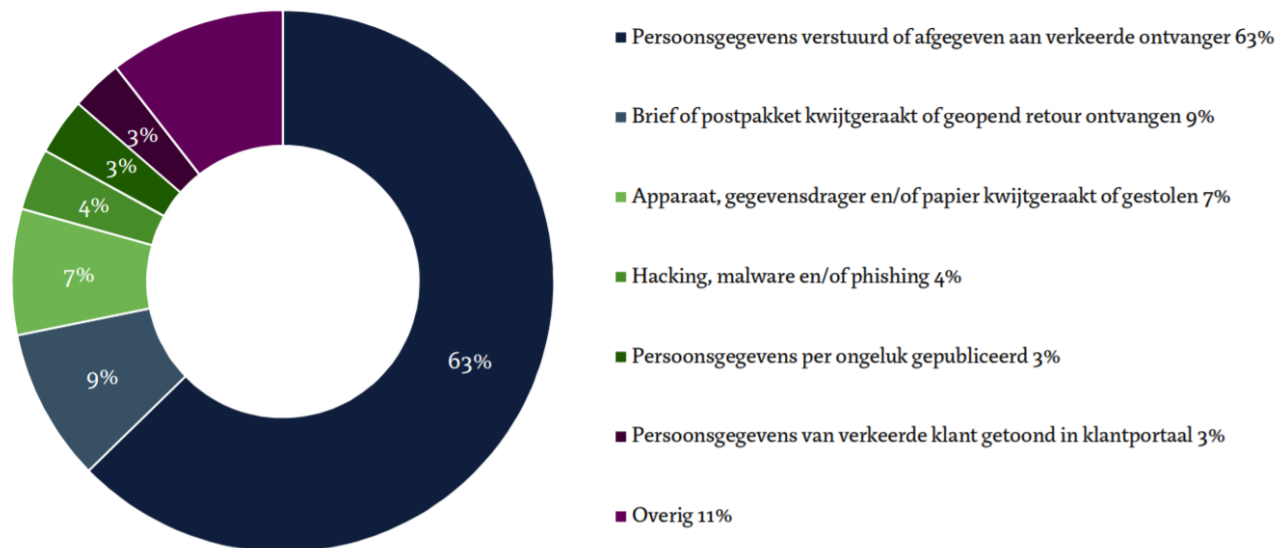


* Onder 'overig' bij financiële sector wordt o.a. verstaan financieel adviesbureaus en incassobureaus.

Meldplicht datalekken: facts & figures 2018

Type datalekken overall 2018

Type datalekken



Meldplicht datalekken: facts & figures 2018

Type datalekken financiële sector (eerste helft 2018)

Type datalekken



Meldplicht datalekken: facts & figures 2018

Datalekken: ondernomen acties 2018

- 14.489 datalekken beoordeeld door AP (op totaal > 20.000)
- 298 gevallen: actie ondernomen richting meldende organisatie
 - 39%: contact opgenomen met verzoek om aanvullende informatie
 - 35%: norm-uitleggende brief verzonden
 - 23%: norm-overdragend gesprek gevoerd
 - 3 gevallen: kortlopend onderzoek gestart naar achtergronden
 - 4 gevallen: uitgebreider onderzoek gestart naar oorzaak

Meldplicht datalekken: facts & figures 2018

Datalekken: in 2019 vaker sancties, met name in geval van:

- ten onrechte niet gemelde datalekken
- te late melding datalekken
- beveiligingsproblemen

Vraag 2

- Hoe zit het als de (computer)systemen van partijen niet op elkaar aansluiten (bijvoorbeeld met het beveiligd mailen)? Wiens verantwoordelijkheid is het dan?
- Hoe om te gaan met verzending en beveiliging van informatie per e-mail?

Verplichtingen AVG

- Passende organisatorische en technische maatregelen treffen ter beveiliging van de verwerking van persoonsgegevens (5 AVG)
 - Rekening houdend met de stand van de techniek en de uitvoeringskosten, alsmede met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen (overweging 32 AVG)
- Verplichting voor alle verantwoordelijken en hun verwerkers (nader vastgelegd in verwerkersovereenkomsten)
- Omvat tevens (in- en uitgaand) e-mailverkeer

Beveiliging e-mailverkeer

- Versleutelen bijlagen bij een e-mail
- Versleutelen van de inhoud van de e-mail zelf
- Versleutelen van de gehele e-mailverbinding (ook meta-date beveiligd, zoals identiteit verzender en ontvanger)
 - Zie website Nationaal Cyber Security Centrum (NCSC)
 - NCSC: 'Beveilig verbindingen van mailservers. STARTTLS en DANE beschermen e-mailverkeer op internet'



Factsheet FS-2017-01 | versie 1.1 | 4 april 2017

Vraag 3

- Hoe om te gaan met foto's van het letsel van de benadeelde en/of toegezonden camerabeelden?
- Wel of niet bewaren in technisch dossier?

Foto's letsel

- Kan om verschillende redenen een bijzonder persoonsgegeven zijn
- Foto litteken benadeelde betreft bijvoorbeeld gezondheidsgegeven betreffende een identificeerbare persoon
 - dus: behandelen net als andere gezondheidsgegevens
- Foto litteken kan daarnaast ook dienen ter vaststelling van ras of etnische afkomst; in dat geval betreft de foto om die reden eveneens een bijzonder persoonsgegeven, maar:
 - alleen toegestaan ter identificatie van de betrokkene
 - en slechts voor zover dit onvermijdelijk is voor dat specifieke doel

Camerabeelden en ander beeldmateriaal

- Kan om dezelfde redenen een bijzonder persoonsgegeven zijn als foto letsel benadeelde
- Indien dat niet het geval is, merkt de AP beeldmateriaal vooralsnog niet aan als bijzonder persoonsgegeven (Nippon Express, juni 2017), indien:
 - Het verwerkingsdoel niet de verwerking van bijzondere persoonsgegevens of het maken van onderscheid op basis daarvan betreft
 - Het voor de verantwoordelijke redelijkerwijs niet voorzienbaar is dat verwerking zal leiden tot het maken van onderscheid
 - En de verwerking onvermijdelijk is voor bereiken van het verwerkingsdoel

Vraag 4

- Mag er ook een (kopie van een) rijbewijs of paspoort worden gevraagd van de benadeelde?
- Hoe hiermee om te gaan?

Wel of geen verplichting tot vaststelling identiteit?

- WWFT?
- Zo ja, dan minst ingrijpende manier kiezen
 - Controleer identiteitsbewijs tijdens eerste gesprek en vermeldt het resultaat daarvan in het dossier
 - Indien dat niet kan, vraag dan slechts om een kopie waarop in ieder geval de pasfoto en het BSN-nummer zijn afgeschermd
- In alle gevallen: betrokkene informeren over doel identificatieverzoek en de aard van de verwerkte gegevens

Vraag 5

- Hoe om te gaan met strafrechtelijke gegevens in een letseldossier?

Strafrechtelijke gegevens

- Ook strafrechtelijke gegevens zijn bijzondere persoonsgegevens
- Er bestaan verschillende uitzonderingen op het verbod tot verwerking van strafrechtelijke gegevens: 32 en 33 UAVG

Strafrechtelijke gegevens

- 33 lid 2 UAVG:

Persoonsgegevens van strafrechtelijke aard mogen worden verwerkt door de verwerkingsverantwoordelijke die deze gegevens ten eigen behoefte verwerkt:

- a. ter beoordeling van een verzoek van betrokkene om een beslissing over hem te nemen of aan hem een prestatie te leveren; of
- b. ter bescherming van zijn belangen, voor zover het gaat om strafbare feiten die zijn gepleegd, of die op grond van feiten en omstandigheden naar verwachting zullen worden gepleegd, jegens hem of jegens personen die in zijn dienst zijn.

Overige vragen?



Dank u voor uw aandacht

Leijnse Artz
Blaak 555
3011 GB Rotterdam

T +31 10 244 43 44
F +31 10 244 00 91

www.leijnseartz.com
j.simons@leijnseartz.com