“1 jaar AVG: waar staan we?”

Marian ter Riet (Damsté)
Jor Muller (Sigmax ICT Specialisten)

Inhoud

- ✓ **Deel 1: AVG wat moet je er mee?**
  - Ratio van de AVG
  - Gevolgen voor uw bedrijf/organisaties
  - Privacyverklaring
  - Verwerkingsregister

- ✓ **Deel 2: AVG wat kan je er mee?**
  - Datalekken
  - Hoe te voorkomen?
  - Brexit
  - Tips en trucs

Wie zijn wij?

Marian ter Riet

- Advocaat Privacy recht
- Compliance Officer
- Damsté advocaten-notarissen

Wie zijn wij?

Jor Muller

- ✓ Security Officer
- ✓ Business Consultant
- ✓ Sigmax ICT Specialisten


WHY DO YOU GET THAT LOOK WHENEVER WE TALK ABOUT GDPR COMPLIANCE?
TOM FISH BURNE
© marketoonist.com


ZARA
THE STING

Terug naar 28 mei 2018

Europese regelgeving

- ✓ Regelt de verwerking van persoonsgegevens van natuurlijke personen
- ✓ In de EER (EU + Noorwegen, Liechtenstein en IJsland)
- ✓ Door een natuurlijk persoon, onderneming of organisatie

Nvt:

- ✓ Uitnodiging vrienden voor privé feestje
- ✓ Onderneming gevestigd buiten de EU die diensten verleent aan klanten buiten de EU

Verwerking van persoonsgegevens (I)

- Persoonsgegevens: *alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare levende natuurlijke persoon. Losse gegevens die samengevoegd kunnen leiden tot de identificatie van een bepaalde persoon vormen ook persoonsgegevens.*

- Vb: KVK nummer

- Verwerking: (handmatige of geautomatiseerd) verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken, verspreiden, ter beschikking stellen, wissen of vernietigen van persoonsgegevens.

Verwerking van persoonsgegevens (II)

Hoe moeten persoonsgegevens worden verwerkt?

- ✓ Wettig en transparant
- ✓ Specifiek doeleinde/doelbinding
- ✓ Minimale gegevensverwerking
- ✓ Opslagbeperking en beveiliging
- ✓ Technische en organisatorische waarborgen

Privacyverklaring

- ✓ Visitekaartje van je bedrijf
- ✓ Verplichte onderdelen
- ✓ Borging

Verwerking van persoonsgegevens

Persoonsgegevens moeten (…)

- ✓ voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld;
- ✓ Mogen vervolgens niet verder op een met die doeleinde onverenigbare wijze worden verwerkt;


GET ALL THE INFORMATION YOU CAN, WE'LL THINK OF A USE FOR IT LATER.

Voorbeeld

- ✓ Chatty receptionist

Oordeel

- ✓ Hoe wordt je geïnformeerd
- ✓ Wat is de inbreuk
- ✓ Gevolgen van de inbreuk
- ✓ Verhouding tussen betrokkene en inbreukmaker (wg-wn)
- ✓ Waar moet je op bedacht zijn

Voorbeeld 2

- ✓ Slimme meters
- ✓ Zwarte lijst

Oordeel

- ✓ Met welk doel verzameld
- ✓ Wat mag betrokkene verwachten
- ✓ Gevolgen van de inbreuk

Nijmeegse horecazaken filmen bezoekers op het toilet

NIJMEGEN / ARNHEM - Bij meerdere horecagelegenheden in Nijmegen worden bezoekers gefilmd op het toilet. In één kroeg hangt de camera zelfs zo, dat geslachtsdelen van plassende bezoekers in beeld komen. Gasten kunnen bij de ingang van de zaak meekijken. ,,Inbreuk op de privacy", aldus de Autoriteit Persoonsgegevens.

Onderzoek naar camera's in kleedruimte sauna na lekken naaktbeelden

De Autoriteit Persoonsgegevens gaat onderzoek doen naar camera's in sauna's. Nadat naaktbeelden van oud-speelsters van het Nederlandse handbalteam op internet waren verschenen, die door een bewakingscamera bij een sauna in Nederasselt zouden zijn gemaakt, zijn bij de toezichthouder veel klachten binnengekomen over camera's in sauna's.

Rechten van betrokkenen (I)

- ✓ Welke rechten heeft de betrokkene?
- ✓ Hoe borg je deze rechten?

Recht op inzage (I)

artikel 15 AVG:

“Betrokkene heeft recht om van de verantwoordelijke uitsluitsel te krijgen over het al dan niet verwerken van zijn persoonsgegevens en wanneer dat het geval is, om inzage te krijgen van die persoonsgegevens en van de overige informatie in dit artikel genoemd.”

- ✓ Kosteloos kopie gegevens (meerdere kopieën wel kosten)
- ✓ Pas na vaststelling identiteit!

Recht op inzage (II)

artikel 15 lid 3 AVG:

"*De verwerkingsverantwoordelijke verstrekt de betrokkene een kopie van de persoonsgegevens die worden verwerkt. Indien de betrokkene om bijkomende kopieën verzoekt, kan de verantwoordelijke op basis van de administratieve kosten een redelijke vergoeding rekenen. Wanneer de betrokkene zijn verzoek elektronisch indient, (..) wordt de informatie in een gangbare elektronische vorm verstrekt*"

Recht op inzage (III)

Wat volgt uit de huidige lijn van de rechtspraak en de AP?

- ✓ Of een inzageverzoek ongeclausuleerd kan worden gedaan zal afhangen van de hoeveelheid persoonsgegevens die de verantwoordelijke onder zicht heeft

- ✓ Of ook onderliggende stukken dienen te worden verstrekt zal afhangen van de inhoud van die stukken; interne notities zullen op grond van artikel 15 lid 4 AVG gevrijwaard blijven van verstrekking. Hetzelfde geldt voor informatie die afbreuk doet aan de rechten en vrijheden van anderen. Mogelijke optie: het weglakken van dit soort informatie

Recht op inzage (IV)

- ✓ Inzagerecht is niet onbeperkt!
- ✓ Doel van inzagerecht: om diegene van wie persoonsgegevens worden verwerkt toegang te verschaffen tot die gegevens "zodat hij zich de juistheid en de rechtmatigheid van de verwerking ervan kan vergewissen".

Praktijkvoorbeeld inzageverzoek

- ✓ *Vrouw stelt ziekenhuis en gynaecoloog aansprakelijk voor schade.*
- ✓ *Vrouw verzoekt om inzage o.g.v. privacywetgeving; volledig overzicht van elke verwerking van de persoonsgegevens van haar en haar zoon.*
- ✓ Namens ziekenhuis: misbruik van recht/oneigenlijk gebruik van privacywet.

Praktijkvoorbeeld: oordeel van het hof

Het hof oordeelt als volgt. Verzekeraar behoort als 'verantwoordelijke' in de zin van artikel 1 onder d Wbp, aan vrouw specifieke informatie te verstrekken waardoor zij in staat wordt gesteld behoorlijk kennis te nemen van haar en [de zoon van vrouw] betreffende gegevens en van de wijze waarop deze zijn verwerkt. Vrouw kan bij het vragen van deze informatie volstaan met een verwijzing naar art. 35 Wbp en behoeft geen nadere redenen op te geven.

Praktijkvoorbeeld 2

Casus: Bank zegt de relatie op met klant omdat klant de bank verzocht wekelijkse contante geldstortingen te faciliteren die afkomstig waren van een vennootschap actief in de raamprostitutie en waarvan de bestuurder banden zouden hebben met het criminele circuit.

Klant doet o.g.v. privacywetgeving verzoek om overzicht en afschrift van al zijn persoonsgegevens hoe ook genaamd en in welke vorm dan ook door de bank verwerkt, alsmede de ontvangers van deze gegevens en de beschikbare informatie

Praktijkvoorbeeld 2: oordeel van het hof

Er is geen sprake van een concreet en nader onderbouwd verzoek om inzage. Het voorgaande bekent dat het hof in het onderhavige geval eveneens sprake acht van een “fishing expedition”, nu de klant slechts een algemeen verzoek heeft gedaan zonder ook maar een begin van verduidelijking te geven waar hij meer duidelijkheid over wenst.

ECLI:NL:GHSHE:2018:363

Plichten van verantwoordelijke en verwerker

- ✓ Verantwoordingsplicht
- ✓ Documentatieplicht
- ✓ Informatieplicht

Documentatieplicht = registers

- ✓ Verwerkingen van persoonsgegevens
- ✓ Rechten van betrokkenen
- ✓ Verwerkersovereenkomsten
- ✓ DPIA's
- ✓ Meldingen datalekken
- ✓ etc

Verwerkingenregister

- ✓ Wat moet er in staan?
- ✓ Hoe pak je dit aan?

Voorbeeld van online register

Naam gegevensverwerking

Aanvraag individuele WMO–voorziening behandelen en beheren.

Rol gemeente

verantwoordelijke

Doel van de verwerking

Beoordelen welke voorziening de klant nodig heeft om zijn dagelijks leven in zijn eigen leefomgeving voort te zetten en het beheren van de verstrekte voorzieningen.

Grondslag van de verwerking

Uitvoering van een wettelijke taak.

Categorieën betrokkenen

De klant die zich aanmeldt, eventuele gezinsleden of huisgenoten die in hetzelfde huis wonen en zorgverleners ihkv PGB/hulp bij huishouden.

Categorieën persoonsgegevens

Klant:
– BSN
– Naam
– Geslacht
– Adres
– Geboortedatum
– Telefoonnummer
– Telefoonnummer en naam contactpersoon (eventueel)
– E–mailadres
– Medische gegevens/beperkingen/aandoeningen

– Geslacht
– Adres
– Geboortedatum
– Telefoonnummer
– Telefoonnummer en naam contactpersoon (eventueel)
– E–mailadres
– Medische gegevens/beperkingen/aandoeningen

Bij Hulp bij huishouden:
– Naam en geboortedatum huisgenoten.

Bij Persoonsgebondenbudget:
– Rekeningnummer

Ontvangers buiten de gemeente

– Hulpmiddelen leveranciers
– Zorgleveranciers
– Medisch advies instituut (Treve, systeem Regas waarin we gegevens delen)
– SVB
– Buurtteams
– Aannemers
– Ergotherapeuten
– Woningcorporaties
– Overige hulpverleners

Bewaartermijn

Bewaartermijnen:
1) Verstrekt: 15 jaar (ingang na vervallen belang)
2) Geweigerd: 5 jaar (ingang direct)
3) Beëindigd: 15 jaar (ingang direct)
4) Afgebroken: 1 jaar (ingang direct)

Worden de gegevens doorgezonden naar landen buiten de EU?

nee

Samenvatting eerste gedeelte

AVG: wat moet je er mee?

- ✓ Privacyverklaring (verantwoordingsplicht)
- ✓ Registers (documentatieplicht)
- ✓ Awareness en organisatie (informatieplicht)

Hoe doe je dat?

- ✓ Opstellen door jurist/plaatsen op website/onder aan mailberichten
- ✓ Inrichten met behulp van jurist/ict specialist. Bijhouden in geautomatiseerd systeem


Pause

Recent

30 april 2019 12:06
Laatste update: 30 april 2019 14:07

28

De gemeente Assen heeft de persoonsgegevens van 530 inwoners met een gebiedsverbod gelekt. Het gaat daarbij om mensen met lopende en inmiddels verlopen gebiedsverboden en anderen die een waarschuwing hebben ontvangen.

Een greep uit de meest pijnlijke datalekken 2018 & 2019

Groot datalek bij Jeugdzorg: dossiers duizenden kwetsbare kinderen gelekt

Belastingdienst meldt 1275 datalekken, 84 met 'hoog risico'

05 juni 2018 17:58
Aangepast: 06 juni 2018 06:40

Menzis krijgt boete van 50.000 euro vanwege onzorgvuldigheid met privacy

Nieuws 04-04-2019 Print dit artikel

Erasmus MC lekt mailadressen jonge hiv-patiënten

19 maart 2018 16:31
Aangepast: 21 april 2018 21:59

Facts 2018

- ✓ 20.881 datalekken
- ✓ 63% (13.155x of 36 meldingen per dag): **versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger;**
- ✓ 14% (2923x of ruim 8 meldingen per dag): **kwijtraken of de diefstal van een laptop of USB-stick**


gettyimages
James Worrell
200432721-001


gettyimages
artpartner-images


gettyimages
Vicente Méndez
979036606

Beveiligingsincident en datalek

- ✓ Verschil
- ✓ **Persoonsgegevens**

- ✓ Geëncrypte of niet tot persoon herleidbare gegevens

Hoe voorkom ik datalekken?

- ✓ Met name:
  - E-mail naar naar verkeerde geadresseerde
  - Gegevensdragers verliezen

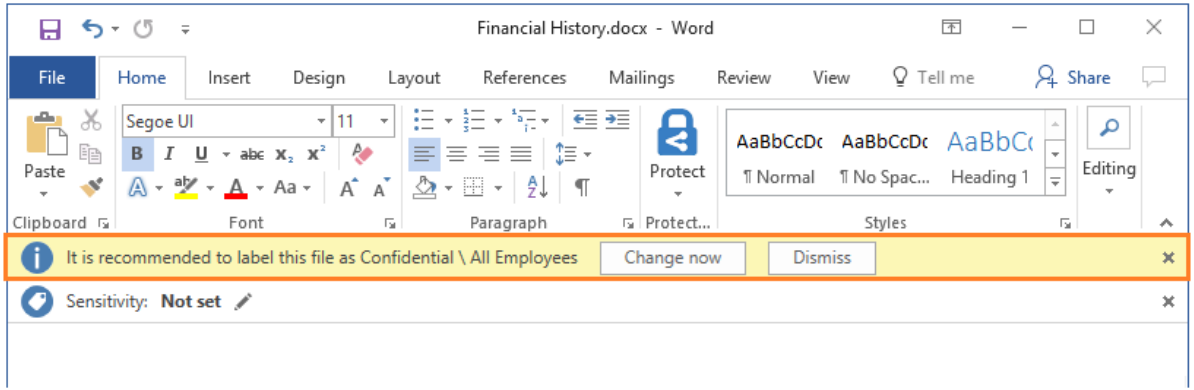
E-mail naar verkeerde geadresseerde

- ✓ ‘Reply to all’
- ✓ Nieuwe contactpersonen → check e-mail

- ✓ Versleuteling
- ✓ Technische policies

Azure Information Protection

- ✓ Beveiligt documenten en mails van je organisatie



Azure Information Protection

- ✓ Beveiligde e-mail per ongeluk verzonden naar verkeerde geadresseerde?
- ✓ Gevoelige data of vertrouwelijke mail doorsturen, kopiëren, afdrukken etc?
- ✓ Maatwerk mogelijk!

Azure Information Protection

- ✓ Je houdt altijd grip op je data!

Kwijtraken/diefstal gegevensdragers

Windows 10
BitLocker

Beleid

- ✓ Geen USB-sticks?
- ✓ **Geen data lokaal op de laptop**

Microsoft InTune

- MDM: Mobile Device Management
- iOS, Android, Windows, macOS


fn
delete
gettyimages
LisaValder
157504374

Awareness – bewustwording!

- ✓ Ontwikkel een awareness-programma over een langere termijn
- ✓ Combineer training met toetsen
- ✓ Moedig melden van incidenten aan!
- ✓ AVG: artikel 39 onder b: "Toezien op naleving van deze verordening, [..] bewustwording en opleiding van het bij de verwerking betrokken personeel[..]".

Van bewustwording naar gedragsverandering


FORTNITE


gettyimages
John Dominis


1
©PHOTO Rienk Mebius 2007

Melden datalek

- ✓ Niet ieder datalek hoeft gemeld te worden.
- ✓ Persoonsgegevens van gevoelige aard altijd melden!
- ✓ Bijzondere persoonsgegevens.
- ✓ Zijn er veel gegevens gelekt?

De te nemen stappen

1. Start onmiddellijk met de bestrijding
2. Maak een afweging of er gemeld moet worden
3. Indien er gemeld moet worden, start de procedure (72 uur)
4. Leg alle handelingen vast in een systeem/register

Melden aan betrokkene

- ✓ Afweging
- ✓ Wat is het doel van de wetgever?
- ✓ Hoe pak je dit aan?

Brexit en het data-export verbod

- *"Onze gemeente heeft delen van haar administratie, waarin ook persoonsgegevens zijn verwerkt, ondergebracht bij een databedrijf dat is gevestigd in het VK. Het databedrijf geeft aan dat het per 25 mei 2018 zal voldoen aan de voorwaarden van de Algemene Verordening Gegevensbescherming (AVG). Ook heeft het bedrijf de intentie om aan de AVG te blijven te voldoen na de Brexit. Kan de gemeente er vanuit blijven gaan dat het verwerken van persoonsgegevens bij het databedrijf in het VK 'AVG-proof' zal blijven ondanks de Brexit?"*

Brexit en het data-export verbod

- Nee,: VK is dan een derde land binnen het wettelijke kader van de AVG. In beginsel geen wisseling van persoonsgegevens mogelijk!
- Persoonsgegevens mogen dan alleen geoorloofd worden verwerkt in het VK, mits de Europese Commissie (EC) een zogenaamde adequaatheidsbeslissing neemt of dat de verwerker in het VK toeziet op passende waarborgen (is al aangekondigd)
- EU modelcontract: “standard contractuel clauses” verplichten de partij in het VK om hetzelfde beschermingsniveau als dat van de AVG toe te passen.
- Binding Corporate Rules: geldt voor concernverband: schrijven voor het hele concern voor hoe wordt omgegaan met persoonsgegevens.

Samenvatting tweede gedeelte

AVG: wat kan je er mee?

- ✓ Voorkomen van datalekken
- ✓ Voorbereiden op Brexit

Hoe doe je dat?

- ✓ Juiste technische maatregelen
- ✓ Bewustwording → Gedragsverandering
- ✓ AVG toepassen op jouw Brexit-situatie

Voordelen van de AVG!

- ✓ Transparantie = vertrouwen
- ✓ Aantrekkelijk voor andere partijen (keurmerk/certificaat)
- ✓ Registreren = weten
- ✓ Inzicht in eigen procesvoering
- ✓ Geldbesparingsmethode

Tips en trucs

Meer informatie? Advies nodig?

- ✓ Damsté Advocaten en Notarissen
- ✓ Sigmax ICT Specialisten

- ✓ Ook mogelijk in samenwerking
- ✓ Vraag naar de mogelijkheden