Aan de slag met AVG

Bob Hulsebosch

value through innovation

Wie ben ik?

- Senior adviseur Identity, Privacy & Trust bij InnoValor
- > 15 jaar ervaring
- Opdrachten:
  - Min. SZW: PIA SUWInet en Frauderegister
  - BKR: PIA VIS-toetsen
  - Min. EZ: Inspecteur Idensys/eHerkenning
  - Min. EZ/BZK: Adviseur EU eIDAS verordening
  - SWELL: PIA sensor applicaties voor eCoaching/Wellbeing
  - Kennisnet: Impact privacy-by-design op educatieve content keten
  - ICTU: Regie op Gegevens – personal data management

Doel

“Hij is gevreesd, hij is gevaarlijk, hij is bindend, en hij komt eraan!”

Beantwoorden van twee vragen:

- Wat staat er te gebeuren met de aankomende (Uitvoeringswet) AVG?
- Hoe praktisch om te gaan met de AVG?
  - Best practices / do’s and don’ts

Voorpagina
Net binnen
Algemeen
Achtergronden
Economie
Sport
Tech
Internet
Gadgets
Games
Mobiel
Entertainment
Lifestyle
Overig
Video's
Regionaal

'Privacy in Nederland goed beschermd vergeleken met andere EU-landen'

Gepubliceerd: 05 oktober 2017 12:44
Laatste update: 05 oktober 2017 12:45

In Nederland wordt de privacy van burgers "bovengemiddeld goed" beschermd vergeleken met andere landen in de EU.

Dat is de conclusie van een onderzoek van de Universiteit Leiden in opdracht van het Ministerie van Veiligheid en Justitie. Daarbij is gekeken naar de landen Nederland, Duitsland, Zweden, het Verenigd Koninkrijk, Ierland, Frankrijk, Roemenië en Italië.

Agenda

- AVG algemeen
- Basisprincipes
- Wat is nieuw?
- Specials
- Take aways
- Vragen

AVG Algemeen

- Treedt op 25 mei 2018 in werking
- Vervangt WBP
- Harmoniseren van privacy in EU (GDPR)
- Burger/consument meer centraal
- Minder juridisch; meer over uitgangspunten, afspraken en beheersmaatregelen om naleving te garanderen
- Meer over verantwoording (dus)

Basisprincipes

- Gevoeligheid en beveiliging van de gegevens
- Limitering van het verzamelen en verwerken van gegevens
  - Beperkingen tav bijzondere gegevens
- Doelbinding en rechtmatigheid
  - Wettelijke basis, algemeen belang, toestemming van de betrokkene, vitaal belang, gerechtvaardigd belang, overeenkomst
- Gegevenskwaliteit en beschikbaarheid
- Rechten van betrokkenen en transparantie
- Verantwoording
  - Governance
  - Verantwoordelijkheden
  - Toezicht

} Ketens

Nieuwe elementen AVG

- Boetes
- Informatieverplichting
- Toestemming
- Rechten betrokkenen
- Meldplicht datalekken
- Functionaris gegevensbescherming
- Ontwerp
- Verantwoording
- Verplichtingen verwerkers
- Toezicht
- Reikwijdte
- Doorgifte aan derde landen

Boetes

- Nu: Max EUR 820.000 of 10% omzet
- AVG: Max EUR 20.000.000 of 4% omzet
  - Hangt af van type overtreding

- *Boete vs Meldplicht vs Reputatie vs Pakkans*

Informatieverplichting

- Meer dan huidige privacy policy
  - de periode waarvoor gegevens zullen worden opgeslagen
  - de rechten van de betrokkene
  - wat de bron is van de gegevens
  - de juridische grondslag voor de verwerking
  - of gegevens buiten de EER worden opgeslagen
  - of welk gerechtvaardigd belang is gediend met de verwerking
- *Actualiseer privacybeleid met de nieuwe informatieverplichtingen! Wees transparant!*
- *Transparantie houdt in dat het voor de betrokkene duidelijk is dat zijn persoonsgegevens verzameld, gebruikt, geraadpleegd of op een andere manier verwerkt worden, waarom en door wie.*
- *Leg dit vast - is onderdeel van de verantwoordingsplicht*

Toestemming

- Moeilijker om te verkrijgen dan bij WBP
- Duidelijk actieve handeling
- Ondubbelzinnig
  - Uitdrukkelijke toestemming voor bijzondere gegevens
- Vrije wilsuiting
- Specifiek en geïnformeerd: *betrek de gebruiker erbij!*
- Aantoonbaar en intrekbaar
- Toestemming van ouders bij kinderen (< 16 jaar)

- *Bezint eer ge begint aan toestemming!*

Rechten betrokkenen

- Inzage (binnen 8 weken op basis van Algemene wet bestuursrecht)
- Om derden inzage te geven
- Om toestemming te geven en in te trekken
- Om persoonsgegevens te laten wissen
  - Om vergeten te worden
- Rectificatie
- Beperking van de verwerking van persoonsgegevens
- Dataportabiliteit

- *Borg de rechten van de betrokkenen in procedures, werkprocessen, online omgevingen, etc.*

Meldplicht datalekken

- Verplichte melding van inbreuken op persoonsgegevens aan toezichthouders
- Waar mogelijk binnen 72 uur nadat bewustwording datalek
  - Kennisgeving aan toezichthouders is niet vereist indien het onwaarschijnlijk is dat de inbreuk zal leiden tot een hoog risico voor de rechten en vrijheden van natuurlijke personen
- Verantwoordelijken moeten ook, zonder onnodige vertraging, datalekken aan betrokkenen melden.
  - Deze meldplicht is alleen vereist indien de inbreuk waarschijnlijk zal resulteren in een groot risico voor de rechten en vrijheden van individuen.
- Betrokkenen hoeven dus doorgaans minder snel te worden geïnformeerd over een datalek dan op dit moment

- *Maak procedures voor het geval van een datalek*

Functionaris Gegevensbescherming

- Nodig voor:
  - overheidsinstanties of publieke organen
  - degenen die krachtens een nationale wet een DPO moeten aanstellen
    - nog niet bekend of dit in NL gaat gebeuren
  - verantwoordelijken en verwerkers die als *kernactiviteit* hebben:
    - reguliere, *systematische* en *grootschalige* controle van personen (profilering - bijvoorbeeld door middel van camera's, het monitoren van e-mail van werknemers of voertuigvolgsystemen); of
    - *grootschalige* verwerking van 'bijzondere categorieën gegevens' en/of 'strafrechtelijke gegevens'. Hieronder vallen ook de nieuwe categorieën persoonsgegevens: genetische en biometrische gegevens.

- *Denk goed na over wie je aanstelt als FG*

Ontwerp

- Gegevensbescherming door ontwerp en door standaardinstellingen (privacy by design and by default)
  - *Dataminimalisatie, versleuteling, toegangscontrole, tijdige verwijdering van data, anonimisering en pseudonimisering*

- Gegevensbeschermingseffectbeoordeling (privacy impact assessment)

Verantwoording

- Meldplicht voorgenomen verwerking aan autoriteit vervalt
- Administratie van de verwerkingsprocessen door verantwoordelijke (en verwerker)
  - Alleen voor organisaties met meer dan 250 medewerkers
  - Of wanneer sprake is van een verwerking bijzondere gegevens
- Verantwoordelijke kan aantonen dat verwerkingen geschieden in overeenstemming met de vereisten die de AVG daaraan stelt

- *Haal bezem door gegevensverwerkingen – DPIA*
- *Maak een register van verwerkingsactiviteiten*

Verplichtingen verwerkers

- Meer verplichtingen dan nu het geval is
  - het documenteren van verwerkingen
  - het aanstellen van een functionaris gegevensbescherming
  - het verkrijgen van toestemming van de verantwoordelijke alvorens een sub-verwerker in te schakelen
  - het melden van een datalek aan de verantwoordelijke
  - het treffen van passende technische en organisatorische maatregelen
  - het verlenen van medewerking aan de bevoegde toezichthouder
  - het handelen in overeenstemming met de eisen voor doorgifte naar buiten de EER
  - het uitvoeren van privacy impact assessments
- Contractuele waarborgen tussen verantwoordelijke en verwerker
  - geheimhouding, vernietiging van persoonsgegevens, uitvoering van audits
- Komt een subverwerker zijn verplichtingen niet na, dan blijft de verwerker volledig aansprakelijk richting de verantwoordelijke

- *Loop de huidige bewerkersovereenkomsten na!*

Specials

- BSN
- Kinderen
- Profilering
- Biometrische gegevens
- Inzagerecht
- Gegevenswissing
- Dataportabiliteit
- DPIA
- Verwerkersovereenkomst

BSN

- Is BSN nu een bijzonder persoonsgegeven of niet?
  - Onder de AVG is het BSN géén bijzonder persoonsgegeven meer
  - Desondanks geldt voor gebruik BSN een wettelijke bevoegdheid óf in lijn zijn met doeleinden van de wet
- Organisaties die BSN mogen verwerken:
  - Overheid, gemeenten, zorg, onderwijs, pensioenen
  - Wet algemene bepalingen BSN, Wet Aanvullende Bepalingen Verwerking Persoonsgegevens in de Zorg, of Wet GDI

- *Ook het vervormen of versleutelen van een BSN blijft een onrechtmatige verwerking zonder grondslag uit de wet*
- *BSN mag niet naar het buitenland*

Gegevensverwerking van kinderen

- Toestemming ouders / wettelijk vertegenwoordiger nodig
- Alleen nodig als:
  - er geen andere grondslag van toepassing is,
  - het gaat om een dienst van de informatiemaatschappij, en
  - het kind jonger is dan 16 jaar
- In dat geval:
  - Toestemming vragen aan de ouders of wettelijke vertegenwoordiger
  - Nagaan of de ouders daadwerkelijk toestemming hebben verleend
  - Moet alle verstrekte informatie in voor kinderen begrijpelijk en gemakkelijke taal zijn omschreven
  - Moet het verlenen van toestemming ook makkelijk geweigerd of ingetrokken kunnen worden

Profilering

- Houd rekening met
  - Datakwaliteit
  - Transparantie
  - Menselijkheid
- Ruwe data weggooien
- Profilering kan leiden tot nieuwe bijzondere gegevens
  - Sensor data rondom activiteit vs medische gegevens

- *Waak voor her-identificatie!*

Biometrische gegevens

- Biometrische gegevens = bijzondere gegevens
- Gezicht, vingerafdruk, iris, netvlies, stem, …
- Voor het identificeren van personen en voor zover dit doel noodzakelijk en proportioneel is voor behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde
- Uitzondering Uitvoeringswet AVG
- Zonder de uitzondering is een van de weinige opties voor rechtmatig gebruik van biometrie de uitdrukkelijke toestemming
  - Problematisch gelet op de werkgever-werknemer verhouding
  - Toestemming is in die gevallen bijna nooit ‘vrij’ te geven

- *Ga niet zelf aan de slag met biometrische authenticatie*

Inzagerecht

- Alleen eigen, persoonlijke gegevens
- Wat in te zien:
  - doeleinden van verwerking
  - categorie persoonsgegevens
  - (categorie) van ontvangers
  - bewaartermijnen
  - dat de verzoeker het recht heeft gegevens te rectificeren of wissen en de verwerking te beperken of bezwaar te maken
  - dat de verzoeker het recht heeft een klacht in te dienen bij de toezichthouder
  - wanneer u de gegevens van een andere partij heeft verkregen, alle beschikbare informatie over deze bron
  - wanneer de gegevens buiten de grenzen van EU/EER zijn gegaan, welke passende waarborgen zijn genomen
- Inzage weigeren kan wanneer:
  - Het geen persoonsgegevens betreffen
  - Het afbreuk doet aan de rechten en vrijheden van anderen

- *Aandachtspunt: Identificatie van de verzoeker*

Gegevenswissing

- De persoonsgegevens zijn niet langer nodig voor doeleinden waarvoor zij zijn verzameld of verwerkt
- De verwerking was gebaseerd op toestemming maar is ingetrokken en er is geen andere rechtsgrond voor de verwerking
- Er is door de klant bezwaar gemaakt tegen de verwerking en de concrete afweging tussen het gerechtvaardigde belang is minder dan de belangen, rechten en vrijheden van de klant
- De persoonsgegevens worden onrechtmatig verwerkt. Dit is de restcategorie voor situaties waarin organisaties niet voldoen aan de AVG.
- Er geldt voor de organisatie een wettelijke verplichting om gegevens te wissen die voortvloeit uit Europees of Nederlands recht
- De persoonsgegevens zijn verzameld in het kader van het aanbieden van een app of website-account aan een kind, waarvoor het kind vanaf 16 (of sommige landen 13) jaar toestemming heeft gegeven. Deze situatie is met name beschreven om te waarborgen dat kinderen die zich op hun jonge leeftijd nog niet goed bewust waren van de consequenties, de mogelijkheid krijgen die gegevens van internet te laten verwijderen

Dataportabiliteit

- Overdracht van gegevens naar andere verantwoordelijke
- Voorwaarden:
  - Alleen persoonsgegevens over de betrokkene
  - Verstrekt door de betrokkene
    - Niet afgeleide gegevens (profilering)
  - Geautomatiseerd
    - Papieren bestanden vallen erbuiten
    - Gestructureerd, in een machineleesbaar formaat inclusief metagegevens
  - Alleen voor gegevens
    - noodzakelijk ter uitvoering van een overeenkomst
    - Waarvoor toestemming is gegeven
  - Geen afbreuk aan de rechten en vrijheden van derden

DPIA - Data Protection Impact Assessment

- Privacy risico analyse
- Wanneer nodig:
  - Profilering
  - Geautomatiseerde beslissingen
  - Stelselmatige en grootschalige monitoring
  - Bijzondere gegevens
  - Grootschalige gegevensverwerkingen
  - Gekoppelde databases
  - Kwetsbare personen
  - Nieuwe technologieën (IoT)
  - Buiten de EU
  - Blokkering van recht, dienst of contract

- *Voer een DPIA tijdig uit om een goed beeld te krijgen van de risico's*
- *Toon aan dat er wat met de uitkomsten van de DPIA is gedaan*

Verwerkersovereenkomst

- Tussen verantwoordelijke en verwerker
- Legt het volgende vast:
  - Algemene beschrijving systeem/gegevens en risico's
  - Soort verwerking – instructies
  - Geheimhoudingsplicht
  - Beveiliging om de risico's te mitigeren
  - Sub-verwerkers
  - Privacyrechten gebruiker (inzage, etc.)
  - Andere verplichtingen (meldplicht, DPIA)
  - Verwijderen gegevens
  - Audit

- *Steek in op een win-win voor beide partijen; niet wie de zwartepiet krijgt*

Take aways

- AVG dwingt om privacy goed te regelen
  - Boetes
  - Overweeg integratie met ISMS
- Voldoen aan AVG is niet triviaal
  - Nadenken over veel aspecten en situaties
  - Juiste keuzes maken
  - Zo concreet en inhoudelijk mogelijk
- Belangrijk de gebruiker centraal te stellen
  - Informatieplicht – transparantie, rechten gebruiker
- Borgen van verantwoording essentieel
  - Verantwoordingsplicht – FG, DPIA, verwerkersovereenkomsten
  - Documentatieplicht – Register verwerkingen, procesbeschrijvingen

Vragen

BACKUP SLIDES

Juridische reikwijdte

- De reikwijdte van de AVG is breder
- Verantwoordelijken en verwerkers die zijn gevestigd buiten de EU moeten voldoen aan AVG indien de verwerking van persoonsgegevens betrekking heeft op:
  - het aanbieden van goederen of diensten aan particulieren in de EU; of
  - het monitoren van gedrag van individuen in de EU

Toezicht

- Er is een toezichthouder
- ‘one-stop-shop’: dat organisaties met vestigingen in meerdere lidstaten worden onderworpen aan het toezicht van één toezichthouder
- Oprichting van een zogeheten Europees Comité voor Gegevensbescherming
  - Geschillenbeslechting en juridische opinies
- *Bepaal de toezichthouder*

Doorgifte aan derde landen

- Geen overdracht van persoonsgegevens aan een land buiten de Europese Economische Ruimte (EER),
  - tenzij er sprake is van een ‘passend beschermingsniveau’ of er een vrijstelling van toepassing is.
- De verantwoordelijkheid voor de naleving van deze regel rust op de verantwoordelijke en geldt ook voor verwerkers
- *BSN mag niet de grens over!*