De AVG

Joomla gebruikersgroep HCC-Gouda

4 juni 2018

Adrie Spruit

Disclaimer: de auteur van deze presentatie is niet juridisch geschoold. Met deze presentatie probeert de auteur een indruk - en niet meer dan dat - te geven van wat de AVG inhoudt. Raadpleeg zodra er belangen op het spel staan een in de AVG gespecialiseerde jurist.

Inhoud

- Wat is de AVG?
- Wat is de achtergrond van de AVG?
- Doel en reikwijdte van de AVG?
- Wat zijn persoonsgegevens?
- Hoe beschermt de AVG de persoonsgegevens van burgers?
- Wat zijn de rechten van burgers?
- Welke maatregelen moeten rechtspersonen nemen?
- Voor welke terreinen gelden uitzonderingen?
- Hoe zal de wet in de praktijk gaan werken?
- Iets over de acceptatie van de wet.
- Controle en handhaving.

Wat is de AVG

- AVG staat voor Algemene Verordening Gegevensbescherming.
- De AVG is een nieuwe wet voor de bescherming van **persoons**-gegevens. (https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf)
- De AVG is een Europese verordening met de betekenis van een Europese wet met zogenoemde directe werking. Hij is in Nederland als Europees land van kracht geworden zonder dat eerst een omzetting naar Nederlandse wetgeving nodig is.
- De AVG biedt nog wel ruimte voor het maken van bepaalde keuzes wat betreft de uitvoering van de wet.
- In Nederland zitten die keuzes nu in de 'Uitvoeringswet Algemene verordening gegevensbescherming' oftewel de Uitvoeringswet AVG. (https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/uavg.pdf)
- De **Uitvoeringswet AVG** is op 15 mei 2018 aangenomen door de Eerste Kamer, op 16 mei 2018 gepubliceerd en is op 25 mei 2018 van kracht geworden, dat laatste tezamen met de **AVG**.
- De AVG en de Uitvoeringswet AVG vervangen de oude Wbp oftewel de Wet bescherming persoonsgegevens, die nu dus is vervallen.
- Ter relativering: veel zat al min of meer in de Wbp. In die zin is de AVG een uitbreiding van wetgeving die al bestond.

Wat is de achtergrond van de AVG?

- De oorsprong van de AVG ligt in Europa oftewel bij de EU.
- Er was een Europese databeschermingsrichtlijn uit 1995 (Richtlijn 95/46/EG).
- Die is destijds voor de Nederlandse situatie vertaald naar de Wbp, de Wet bescherming persoonsgegevens.
- De oude Europese databeschermingsrichtlijn sloot niet meer aan bij de nieuwe digitale werkelijkheid, zo stelde men vast in 2012.
- Vanaf dat moment is men gaan werken aan een nieuwe Europese wet/verordening voor de bescherming van persoonsgegevens.
- Dat werd de General Data Protection Regulation oftewel afgekort de **GDPR**. De AVG is daarvan de Nederlandstalige versie.
- In april 2016 is de GDPR als Europese verordening vastgesteld door het **Europese Parlement** en de **Raad van de Europese Unie**.
- De **Europese Commissie** voert de wet uit en/of coördineert op Europees niveau de uitvoering van de wet.
- De invoeringsdatum van de GDPR en daarmee van ook de AVG werd toen al, in april 2016, bepaald op 25 mei 2018.

Doel en reikwijdte van de AVG (1)

- …… Het centrale doel van de AVG/GDPR is het beschermen van de **persoonsgegevens** van ……
- …… alle burgers (ingezetenen) van de Europese Unie (EU) ……
- …… tegen ongewenst gebruik door 'verwerkingsverantwoordelijken' (die verantwoordelijk zijn voor het verwerker van persoonsgegevens) ……
- …… naast die rol is er de rol van verwerker ……
- …… verwerkingsverantwoordelijken en verwerkers kunnen een natuurlijke persoon zijn of een rechtspersoon (juridisch persoon) zijn (organisaties zoals een bedrijf, een overheidsorganisatie, een ziekenhuis, een stichting, een vereniging). Wat zal het vaakst voorkomen? ……
- …… daarbij gaat het om verwerkingsverantwoordelijken en verwerkers, vaak organisaties, **waar ook ter wereld** als ze iets doen met de persoonsgegevens van **Europese burgers**.

Waar ……. staan in de tekst, laat ik de toehoorders meedenken over 'wat het goede antwoord' is …….

Doel en reikwijdte van de AVG (2)

- De AVG beschermt niet alleen, maar regelt - binnen de beschermende regels - ook het vrije verkeer van persoonsgegevens in de EU.
- Ook is de AVG gericht op het harmoniseren van de regels voor persoonsgegevens in de EU ……
- …… dus niet in elk land weer andere regels voor bedrijven en andere organisaties die in meerdere Europese landen actief zijn.

Wat zijn persoonsgegevens?

- Elk stukje informatie over een geïdentificeerd of identificeerbaar natuurlijk persoon is een persoonsgegeven.
- Dus informatie over een persoon waarbij duidelijk is wie de persoon is of waarbij de informatie ‘is te herleiden tot een persoon’.
- Voorbeelden zijn:
  - naam, adres, woonplaats, telefoonnummer, postcodes met huisnummers, andere locatiegegevens, BSN, e-mailadres, pasfoto, al je foto’s, videos, je surfgedrag/onlinegedrag, IP-adres, je koopgedrag, je auto, het kenteken van je auto, etc..
- Er is ook een categorie ‘gevoelige persoonsgegevens’. Die zijn extra beschermd. Voorbeelden daarvan zijn:
  - iemands ras, godsdienst, levensovertuiging, gezondheid, politieke voorkeur.
- Wat zijn geen persoonsgegevens?
  - gegevens over rechtspersonen oftewel bedrijven en andere organisaties.

Hoe beschermt de AVG de persoonsgegevens van burgers? (we gaan hier uit van verwerken door een organisatie die verwerkingsverantwoordelijke is)

- Een organisatie mag alleen persoonsgegevens verwerken als daarvoor een wettelijke grondslag aanwezig is.
- De AVG kent 6 grondslagen. Minimaal een daarvan moet van toepassing zijn. ……
- De meest in het oog springende is: er moet een aantoonbare toestemming van de betrokken persoon zijn voor gebruik voor een benoemd doel.
- De andere 5 grondslagen zijn:
  - de gegevensverwerking is noodzakelijk ter bescherming van vitale belangen;
  - de gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst;
  - de gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag;
  - de gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting;
  - de gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.

Nog een keer de grondslagen op basis waarvan je persoonsgegevens mag verzamelen en bewaren

- Het gebruik is gekoppeld aan een doel.
- Zomaar gaan verwerken voor een ander doel dan waarvoor de gegevens zijn verzameld, mag niet.
- Dat heet doelbinding.
- Ook: bewaren niet langer dan nodig voor het desbetreffende doel.

Gegevensverwerking in het kader van de uitvoering van een overeenkomst

- Wat is een overeenkomst? ……
  - …… een contract;
  - …… een koop(-overeenkomst).
- Voorbeeld:
  - als je online spullen verkoopt dan mag je de adresgegevens verwerken die nodig zijn om bestelde spullen te kunnen leveren;
  - wat mag je niet? ……
  - …… je mag ontvangen gegevens niet zonder toestemming gebruiken om bijvoorbeeld het koopgedrag van je klanten te analyseren of om gericht reclame te gaan sturen etc..

Burgers hebben rechten naar verwerkingsverant-woordelijke organisaties die onder de AVG vallen

- Burgers hebben: ……
  - recht op inzage van de eigen persoonsgegevens;
  - recht op informatie over wat er met persoonsgegevens gebeurt;
  - recht op rectificeren en aanvullen van de eigen persoonsgegevens;
  - het recht om ‘vergeten’ te worden: persoonsgegevens laten verwijderen;
  - het recht om persoonsgegevens over te dragen (met bijv. download en doorsturen);
  - recht op aanvullende menselijke afwegingen bij geautomatiseerde besluitvorming en profilering.
- Organisaties die onder de AVG vallen moeten hun organisatie zo inrichten dat ze in principe direct invulling kunnen geven aan deze rechten.

Hoe voldoe je als verwerkingsverantwoordelijke organisatie aan de AVG?

- Burgers toestemming vragen en informeren.
- Aanstellen Functionaris gegevensbescherming
- Maken en vullen van een Register van verwerkingsactiviteiten
- Beveiligen van persoonsgegevens.
- Melden datalekken.
- Verwerkingsovereenkomsten afsluiten als je persoonsgegevens **láát** verwerken.

Burgers toestemming vragen en informeren

- Burgers toestemming vragen voor het bewaren en verwerken van persoonsgegevens.
- Burgers informeren over wat je er mee doet.
- Burgers informeren over hun rechten.
- Zorgen dat je (direct = er klaar voor zijn) invulling kunt geven aan die rechten als ze erom vragen.

Functionaris gegevensbescherming

- Rechtspersonen moeten een Functionaris voor de gegevensbescherming aanstellen als ze vallen in een van de volgende categorieën:
  1. overheden en publieke organisaties (zoals ziekenhuizen);
  2. organisaties die vanuit hun kernactiviteiten op grote schaal burgers volgen en/of hun activiteiten in kaart brengen; ook cameratoezicht, personeelsvolgsystemen en monitoring van iemands gezondheid;
  3. organisaties die op grote schaal bijzondere persoonsgegevens verwerken en waarbij dit een kernactiviteit is.

Register van verwerkingsactiviteiten

- Veel verwerkingsverantwoordelijke organisaties (omvang is mede bepalend) die persoonsgegevens verwerken moeten zorgen voor een Register van verwerkingsactiviteiten.
- Daarin moet men onder andere het volgende vastleggen:
  - een beschrijving van de categorieën van persoonsgegevens;
  - een beschrijving van de categorieën van personen van wie u gegevens verwerkt. Bijvoorbeeld uitkeringsgerechtigden, klanten of patiënten;
  - de bijbehorende doelen;
  - tot wanneer de gegevens worden bewaard;
  - de categorieën van ontvangers aan wie persoonsgegevens worden verstrekt;
  - een beschrijving van de maatregelen die zijn genomen om de persoonsgegevens te beveiligen.
- Als erom wordt gevraagd, moet je het direct kunnen tonen.

Beveiliging van persoonsgegevens

- Persoonsgegevens moet je goed beveiligen.
- Elke datalek waarbij persoonsgegevens zijn betrokken, moet je melden.
- Waar? ……
- …… Bij de AP.
- Wat is een datalek? ……
- …… een datalek is een beveiligingsincident waarbij persoonsgegevens verloren zijn gegaan of niet is uit te sluiten dat deze in handen van derden zijn gevallen.

Verwerkingsovereenkomst

- Moet je voor zorgen in alle gevallen waarbij je als verwerkingsverantwoordelijke een andere partij inschakelt om persoonsgegevens voor je te verwerken.
- Het gaat daarbij om gevallen waarbij je de andere partij de opdracht geeft persoonsgegevens waarvoor je zelf verantwoordelijk bent, te verwerken. Met andere woorden: je bepaalt wat er moet gebeuren met de gegevens en hoe.
- Voorbeelden:
  - personeels- en salarisadministratie laten uitvoeren;
  - persoonsgegevens in ‘de cloud’ opslaan.
- Er is dus snel sprake van ‘laat verwerken’.
- Je blijft zelf verantwoordelijk.

Samenvatting maatregelen

Functionaris gegevens-
bescherming

Register met alle
verwerkingen

(Digitale)
beveiliging

Gegevens-
beschermingsbeleid

ook verwerkings-
overeenkomsten

ook melden
datalekken

Wat is de basis om als rechtspersoon de juiste maatregelen te kunnen treffen? ……

- …… Het op orde hebben van je bedrijfsprocessen, van je informatievoorziening en van de beveiliging van je processen en informatievoorziening,
  plus het op orde hebben van de documentatie van dat alles.
- Is dat niet op orde, dan had je al bij de start van de implementatie van het gaan voldoen aan de AVG een probleem.
- En die implementatie had op 25 mei 2018 klaar moeten zijn! ……

Uitzonderingen (en deels verfijningen)

- De meest in het oog springende uitzonderingen, zoals geregeld in de Uitvoeringswet AVG, hebben betrekking op de volgende terreinen:
  - persoonsgegevens voor journalistieke doeleinden;
  - persoonsgegevens voor wetenschappelijke doeleinden;
  - persoonsgegevens in archieven.

Hoe gaat de wet in de praktijk werken?

- Dat weten we nog niet.
- Als je in de details duikt, dan blijkt het best wel complex en omvangrijk.
- Juristen maken wetten.
- Nieuwe auto's kun je testen. Bovendien zijn auto's nooit helemaal nieuw.
- Soms blijken wetten niet te werken, bijvoorbeeld omdat de praktijk complex is, of omdat mensen het veel gedoe vinden, of omdat er onbedoeld gebruik/misbruik gaat ontstaan en/of omdat bepaalde praktijksituaties bij het ontwerpen van de wet niet zijn voorzien .

- Ook:
  - hoe gaan de machtsverhoudingen werken? Denk aan Facebook.
  - hoe belangrijk gaan de te beschermen burgers dit zelf vinden?

Wat is in de acceptatie van de AVG een meevaller geweest voor de EU? ……

- …… De discussie over wat Facebook doet/heeft gedaan/heeft toegestaan/heeft laten gebeuren met de door Facebook verzamelde gegevens van burgers.

Controleren en handhaven van de AVG

- ? ……
- …… De Autoriteit Persoonsgegevens (AP) in Den Haag (https://autoriteitpersoonsgegevens.nl/nl) controleert en handhaaft de AVG en de Uitvoeringswet AVG.
- De AP komt niet alleen op eigen initiatief in actie. Want? ……
- Men kan bij de AP klachten indienen over het niet voldoen aan de AVG en de Uitvoeringswet AVG.

Samenvatting, de kern

- Rechten van burgers (natuurlijke personen). Plichten in de praktijk vooral bij rechtspersonen (organisaties).
- Passend doel (grondslag) en doelbinding nodig voor bewaren en verwerken van persoonsgegevens.
- Er is op uitzonderingen na expliciet of impliciet toestemming nodig.
- Recht op inzien, laten verwijderen en aanpassen eigen gegevens.
- Maatregelen:
  - Functionaris gegevensbescherming.
  - Verwerkingsregister.
  - Beveiliging persoonsgegevens.
  - Melden inbraak in de gegevens.
  - Verwerkingsovereenkomsten.

Vragen?

Contact: a3@a3sinformatiebeheeradvies.nl.