Informatie over de AVG op basis van de aantekeningen van netwerkpartner Tjeerd Engel tijdens de bijeenkomst op 25 april 2018.

Wat houdt de AVG in?

De Algemene Verordening Gegevensbescherming (in het Engels *General Data Protection Regulation* of GDPR) is de nieuwe Europese privacywetgeving die op 25 mei 2018 definitief van kracht wordt. De AVG vervangt daarmee de Nederlandse Wet bescherming persoonsgegevens (Wbp) en heeft als doel persoonsgegevens beter te beschermen en die bescherming in de gehele EU gelijk te trekken.

Bedrijven/organisaties moeten (nog) duidelijk(er) maken waarom ze persoonsgegevens verzamelen, waarvoor ze die gebruiken en hoe lang de data wordt bewaard. Ook moeten ze burgers desgevraagd inzage geven in de opgeslagen data.

Wat verandert er ten opzichte van de huidige privacywetgeving?

Burgers krijgen nog meer zeggenschap over hun persoonsgegevens en wat daarmee gebeurt. Zo mogen ze hun toestemming om gegevens te verwerken niet alleen intrekken, maar ook gebruikmaken van het recht om vergeten te worden bij alle organisaties die hun gegevens hebben ontvangen via jouw bedrijf. Alle Europese privacytoezichthouders, zoals de Autoriteit Persoonsgegevens (AP), krijgen dezelfde bevoegdheden naast hun nationale bevoegdheden.

Ik lees veel over *privacy by design* en *privacy by default*. Wat betekent dat?

Privacy by design houdt in dat IT-systemen en applicaties de persoonsgegevens standaard op een hoog niveau beveiligen. Bovendien hoeven de gebruikers van de systemen geen extra handelingen te verrichten om de gegevens te beschermen.

Privacy by default betekent dat er standaard zo min mogelijk gegevens worden verwerkt. Het vereist daarnaast dat de standaardinstellingen van een product of dienst altijd zo privacyvriendelijk mogelijk zijn.

Beide punten zijn verplicht onder de AVG, dus het is van belang om de organisatie er nu al bekend mee te maken

Geldt de AVG voor elk bedrijf?

Elk bedrijf dat persoonsgegevens verwerkt, moet zich houden aan de regels die de AVG voorschrijft. Onder verwerken valt niet alleen ‘opslaan’, maar ook gebruiken, analyseren, combineren of verwijderen.

Onder persoonsgegevens vallen ‘alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon’. Naast naam- en adresgegevens betreft het dus ook bijvoorbeeld medische data, klantprofielen en klikgedrag.

Bedrijven hebben net als onder de Wpb een rechtmatige grondslag nodig om persoonsgegevens te verwerken. De betrokkene moet daarbij toestemming geven voor de verwerking van zijn persoonsgegevens of de verwerking moet noodzakelijk zijn voor de uitvoering van een overeenkomst, waarbij de betrokkene partij is.

Wat gebeurt er als ik niet (op tijd) voldoe aan de regels?

Al in mei 2016 is de AVG in Europa aangenomen, maar werd in mei 2018 daadwerkelijk van kracht. Organisaties zouden daardoor voldoende tijd gehad moeten hebben om hun bedrijfsvoering met de AVG in overeenstemming te brengen. Toch overviel het een aantal ondernemers en voor hen was deze avond zeer interessant.

De Autoriteit Persoonsgegevens gaat vanaf mei 2018 bedrijven op de vingers tikken die niet *compliant* zijn met de AVG. Deze boetes kunnen oplopen tot maximaal 4 procent van de jaaromzet of 20 miljoen euro.

Moet ik een functionaris gegevensbescherming aanstellen?

Er zijn een aantal situaties waarin je verplicht een functionaris gegevensbescherming (FG) aan te stellen. Zo zijn overheidsinstanties en publieke organisaties altijd verplicht een FG aan te stellen. Evenals organisaties waarbij het de kernactiviteit is om op grote schaal individuen te volgen of bijzondere persoonsgegevens te verwerken. Daarnaast kunnen EU-lidstaten ieder afzonderlijk situaties benoemen waarin een FG verplicht is. Voor Nederland is dat vooralsnog niet gebeurd.

De meldplicht datalekken, die ook in de AVG is opgenomen, verplicht dat elk ernstig lek binnen 72 uur na ontdekking gemeld wordt aan de AP. Betrokkenen waarvan gegevens zijn gelekt, hoeven niet geïnformeerd te worden over het datalek als aangetoond kan worden dat geen gegevens te achterhalen zijn.

Vragen die je jezelf kunt stellen

Hoewel sommige bedrijven denken dat ze niks met persoonsgegevens doen, is dat in de praktijk vaak anders. Vanaf nu wordt gehandhaafd op de AVG. Het is goed om jezelf de volgende vragen te stellen.

Worden er persoonsgegevens verwerkt? En zo ja, wat voor gegevens zijn het? Met welk doel worden ze verwerkt? Wat houdt die verwerking in? En waar worden de gegevens bewaard?

Je moet richting de Autoriteit Persoonsgegevens kunnen aantonen dat je '*in control*' bent. Breng daarom de bedreigingen in kaart, de kans dat de privacy van betrokkenen in het geding komt en wat daarvan de impact is. Zo'n risicobeoordeling vormt de leidraad voor je beleid ten aanzien van (de beveiliging van) persoonsgegevens.

Ben ik verplicht om een *Data Protection Impact Assessment* (DPIA) uit te voeren?

Als gezegd zijn organisaties van buiten de EU die gegevens van EU-burgers verwerken, verplicht om dit te doen. Bedrijven moeten ook verplicht een DPIA uitvoeren als hun gegevensverwerking

waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen van wie gegevens worden verwerkt.

Dit is het geval als een organisatie bijvoorbeeld systematisch en uitvoerig persoonlijke aspecten evalueert, op grote schaal mensen volgt of bijzondere persoonsgegevens verzamelt. Dat zijn gegevens die bijvoorbeeld iets zeggen over iemands gezondheid, ras, godsdienst of seksuele voorkeur.

Mag ik persoonsgegevens van kinderen verwerken?

Dat mag, maar je moet wel met een aantal zaken rekening houden. In het geval er toestemming nodig is om de gegevens te mogen verwerken, mag je persoonsgegevens van kinderen jonger dan 16 jaar alleen verwerken als de ouders/verzorgers daar toestemming voor hebben gegeven.

Als organisatie moet je bovendien controleren of de ouder/verzorger die toestemming daadwerkelijk heeft gegeven. Ga na in hoeverre dat mogelijk is met de systemen die je gebruikt.

Hoe zit het met mijn privacyverklaring?

De komst van de AVG betekent dat praktisch elke organisatie zijn privacyverklaring moet herzien. Deze moet onder de AVG niet alleen meer gedetailleerde informatie bevatten, maar ook in begrijpelijke taal zijn geschreven. De tekst moet toegankelijk en eenvoudig geschreven zijn en begrijpelijk zijn voor de doelgroep waarop je je richt.