Aanbevelingen naar privacycompliance

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming / General Data Protection Regulation (GDPR) van toepassing. De GDPR vervangt in Europa de huidige nationale wetten op het gebied van de verwerking van persoonsgegevens, zoals in Nederland de Wet bescherming persoonsgegevens.

De Europese wetgever heeft tegelijkertijd een voorstel gedaan voor aanpassing van de ePrivacy regels. Deze regels zien op elektronische communicatie (m.n. marketing via e-mail, SMS en direct messaging) en het gebruik van cookies en vergelijkbare technieken. Het streven is dat deze nieuwe ePrivacy Verordening (EPV) eveneens per 25 mei 2018 van toepassing zal zijn.

Beide verordeningen verzwaren de verplichtingen van organisaties die persoonsgegevens verwerken of laten verwerken. Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon is een persoonsgegeven. Dus niet alleen naam, adres, woonplaats en e-mailadres zijn persoonsgegevens, maar ook een ID-nummer, IP-adres, surfgedrag, gegevens over gezondheid etc.

Gezien de niet te stoppen hoeveelheid data die wordt verzameld, de technologische ontwikkelingen en de eenvoud van het delen van data, is het voor iedere organisatie van belang tijdig voor 25 mei a.s. actie te ondernemen. Organisaties die niet aan de regels voldoen riskeren boetes tot wel € 20 miljoen (of 4% van de wereldwijde jaaromzet). Los van eventuele boetes zal een onzorgvuldige aanpak van dataverwerking kunnen leiden tot reputatieschade. Denk bijvoorbeeld aan een datalek, die in mum van tijd *viral* gaat op social media.

Compliant zijn zal voor de meeste organisaties een grote uitdaging zijn gezien de aard en omvang van betrokken processen. Dit vraagt om een risico-gestuurde benadering, waarbij op planmatige wijze compliance wordt bereikt.

Hieronder is een aantal aanbevelingen opgenomen die kunnen helpen bij het bereiken van compliance:

1. Maak uw organisatie bewust van het belang van ***compliance***. Stel een privacybeleid op. Pas de *corporate values* en het personeelshandboek zo nodig aan.

2. Stel een **register** op waaruit blijkt dat uw organisatie voldoet aan de verplichtingen van de AVG.

3. Werk de **informatievoorziening** aan betrokkenen bij. Wees transparant en duidelijk.

4. Zorg voor een goed **informatiebeveiligingsbeleid**. Uitgangspunten voor systemen zijn *privacy-by-design* en *privacy-by-default*. Een goede toegangscontrole is een must. Zorg er eventueel voor dat gegevens gepseudonimiseerd en versleuteld zijn.

5. Voer waar nodig een ***privacy impact assessment*** (‘**PIA**’) uit, met name bij het gebruik van nieuwe technologieën.

6. Controleer of u een ***privacy officer*** moet aanstellen.

7. Wees u bewust van de extra verplichtingen bij het verwerken van gegevens van en door derden bij **uitbesteding**. Pas de verwerkersovereenkomsten aan.

8. Stel een **datalekmeldingsprotocol** op. Impactvolle datalekken dienen binnen 72 uur te worden gemeld.

9. Wees voorbereid op aanvullende **rechten van betrokkenen**, waaronder het recht op wissing, het recht op vergetelheid en dataportabiliteit).

Veelal is het aan te raden eerst in kaart te brengen wat de aard, de omvang, de context en de verwerkingsdoeleinden zijn van de dataverwerking binnen de organisatie. Op basis van deze nulmeting kunnen vervolgens verdere stappen worden ondernomen die moeten leiden tot een verantwoordelijke en transparante verwerking van persoonsgegevens.

Wilt u meer informatie? Neem dan contact op met **privacy-specialist Herwin Roerdink** via 020-5042003 of herwin.roerdink@vondst-law.com.

Uiteraard kunt u ook contact opnemen met de Klantenservice Federatie
070 7620746 of info@klantenservicefederatie.nl.