Whitepaper Privacy by Design

De nieuwe Europese privacy verordening zal op 25 mei 2018 in werking treden. Hierdoor zal er veel veranderen op het gebied van gegevensbescherming. Project Privacy helpt ondernemers om hun organisatie klaar te maken voor de nieuwe regelgeving.

Vanaf 25 mei 2018 zijn organisaties verplicht om privacy te integreren als vast onderwerp binnen de bedrijfsvoering. Een organisatie moet weten welke gegevens er worden verzameld, via welke bronnen, welke systemen er worden gebruikt, hoe deze beveiligd zijn en wie er toegang heeft tot deze gegevens. Voorts wordt het verplicht om een Privacy Impact Assessment (PIA) te verrichten voorafgaand aan iedere wijziging in diensten en producten, processen en informatiesystemen. Een andere belangrijke aanpassing is dat het voor overheidsinstanties en organisaties verplicht wordt om een 'data protection officer' aan te stellen. Dit is een verplichting die momenteel niet geldt onder de Wet bescherming persoonsgegevens.
Met de komst van de Algemene Verordening Gegevensbescherming (AVG) worden ook de boetes verhoogd die de Autoriteit Persoonsgegevens aan organisaties kan opleggen. De boetes kunnen oplopen tot EUR 20 miljoen of 4% van de wereldwijde omzet. Organisaties hebben tot 25 mei 2018 de tijd hebben gekregen om hun bedrijfsvoering met de AVG in overeenstemming te brengen. Gezien de verstrekkende implicaties van de AVG is het aan te raden om tijdig te starten met de voorbereidingen.

Project Privacy kan u helpen om uw organisatie klaar te maken voor de nieuwe regelgeving. In dit whitepaper leest u meer over onze dienstverlening *Privacy by Design*.

Wat is *Privacy by Design*?

Organisaties die het principe hanteren van *Privacy by Design* houden al vroegtijdig rekening met het gebruik en de bescherming van persoonsgegevens bij het ontwikkelen van producten en diensten. Dit kan bijvoorbeeld door een een Privacy Impact Analyse (PIA) uit te voeren in de ontwerpfase van een project, of door gebruik te maken van privacy verhogende maatregelen (*Privacy Enhancing Technologies*, PET). Dat laatste betreft een samenhangend geheel van beleids- & ICT maatregelen ter bescherming van de persoonlijke levenssfeer. Een goed voorbeeld van PET is het beleid tot dataminimalisatie. Hierdoor wordt voorkomen dat persoonsgegevens onnodig worden verwerkt of opgeslagen. Door hier al tijdig aandacht aan te schenken kan een zorgvuldige en verantwoorde omgang met persoonsgegevens technisch worden afgedwongen. *Privacy by Design* verlangt van een organisatie dus een proactieve houding ten aanzien van de bescherming van persoonsgegevens.

Wat betekent de invoering van *Privacy by Design* voor mijn organisatie?

Het implementeren van *Privacy by Design* klinkt ingewikkelder dan het in de praktijk is. Veel organisaties zijn onbewust al bekwaam wat betreft de beveiliging van persoonsgegevens. Zo kan enkel de toevoeging van een extra hoofdstuk in een projectplan al afdoende zijn. Hierin wordt beschreven op welke wijze de (nieuwe) producten of diensten gebruik maken van persoonsgegevens. Door dit inzichtelijk te maken kan er bij de ontwikkeling van het product rekening worden gehouden met eventuele risico's op het gebied van privacy. De invoering van *Privacy by Design* is daarmee vooral bedoeld als geheugensteuntje voor de organisatie. Het hoeft geen ingrijpende impact te hebben op de bestaande werkprocessen. Het is echter wel van belang dat er binnen de organisatie inzicht bestaat over welke persoonsgegevens worden verwerkt. Daarvoor is het nodig om een goed overzicht te maken van alle datastromen en nogmaals kritisch te kijken naar het gebruik van persoonsgegevens. Het kan ook helpen om een richtlijn databeveiliging op te stellen dat als basis kan dienen voor de invoering van *Privacy by Design*. Het doel van *Privacy by Design* is dat er continue aandacht is voor de bescherming van persoonsgegevens.

De heilige graal van *Privacy by Design*: *Privacy by Default*

Organisaties die een stap verder durven te gaan implementeren het principe van *Privacy by Default*. Dat doen zij door ervoor te zorgen dat de standaardinstellingen bij programma's of websites privacyvriendelijk zijn. Het gaat daarbij niet alleen om opties die kunnen worden ingesteld, maar ook over privacyvriendelijke algemene voorwaarden, het opstellen van een goede en duidelijk leesbare privacyverklaring en het inrichten van de opt-in voor het versturen van een nieuwsbrief. Zo mogen de velden op een formulier niet standaard aangevinkt staan. Dit wordt gezien als de heilige graal in de bescherming van persoonsgegevens omdat gebruikers vaak de standaard instellingen accepteren zonder zich te verdiepen in de voorwaarden. Door op voorhand aan de kant van de gebruiker te gaan staan kan een organisatie zich positief onderscheiden. Des te meer omdat een goede en verantwoorde omgang met persoonsgegevens een essentieel element is van de vertrouwens-relatie tussen klant en organisatie.

Project Privacy kan uw organisatie helpen bij de invoering van *Privacy By Design*

Project Privacy kan uw organisatie ondersteunen bij het implementeren van *Privacy by Design*. Door onze sterke combinatie van juridische én technische kennis kunnen wij een goed beeld vormen van de maatregelen die nodig zijn om proactief rekening te houden met privacy en gegevensbescherming.

Wat kunt u concreet van ons verwachten:

- Het opstellen van een richtlijn datagebruik binnen uw organisatie
- Controleren van algemene voorwaarden en privacy beleid op privacyvriendelijkheid danwel het opstellen van nieuwe algemene voorwaarden of privacy beleid
- 'Awareness' trainingen geven aan uw persooneel
- Het in kaart brengen van alle datastromen en de informatie classificeren
- Een overzicht maken van alle (IT) systemen die worden gebruikt voor de verwerking van persoonsgegevens
- Helpen bij het opstellen van Privacy Impact Assesments bij nieuwe projecten

Project Privacy komt graag langs voor een vrijblijvend gesprek over de nieuwe AVG

Wilt u aan de hand van dit whitepaper meer informatie ontvangen over de impact van de AVG voor uw organisatie? Neem dan nu contact met ons op! Wij komen graag langs voor een vrijblijvend advies.

Naast onze dienstverlening ten aanzien van de data protection officer kunnen wij ook nog helpen bij andere uitdagingen op het gebied van de bescherming van persoonsgegevens.

Zo kunt u op onze website meer lezen over het belang van *Data Protection Officer* en *Informatiebeveiliging*.

Project Privacy
Strawinskylaan 2555,
Atrium Toren A, 12de verdieping
1077 ZZ Amsterdam

E: info@projectprivacy.nl
http://projectprivacy.nl

Melanie van Heffen
T: +31 (0)6 53 23 14 47
E: melanie@projectprivacy.nl

Remie Bolte
T: +31 (0)6 39 31 85 51
E: remie@projectprivacy.nl