Whitepaper Informatie beveiliging

De nieuwe Europese privacy verordening zal op 25 mei 2018 in werking getreden. 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 *Informatiebeveiliging & ISO 27001*.

Nut en noodzaak van een informatiebeveiligingsbeleid

Bijna iedere organisatie beschikt tegenwoordig over persoonsgegevens. Een informatiebeveiligingsbeleid helpt bij het formuleren van een visie op de bescherming van deze data en stelt heldere spelregels voor de medewerkers. Het kan worden gezien als een toevoeging aan het personeelsreglement, specifiek toegesneden op de verwerking van data. Dat betekent niet dat het een lijvig document hoeft te zijn van vijfhonderd pagina's. Soms zijn twee kantjes al voldoende om duidelijkheid te geven. Het gaat hierbij vaak om ongeschreven regels die door de meeste medewerkers al trouw worden opgevolgt. De toegevoegde waarde van het opstellen van een informatiebeveiligingsbeleid is dat deze "mores" wordt geformaliseerd. Het is een goed moment om met elkaar in gesprek te gaan over de manier waarop er binnen uw organisatie wordt omgegaan met de verwerking van persoonsgegevens. Door het beleid regelmatig te reviseren is er blijvende aandacht voor het belang van informatiebeveiliging.

Een pragmatische kijk op informatiebeveiliging

Het implementeren van een informatiebeveiligingsbeleid kent een aantal aspecten. Allereerst moet er een overzicht worden gemaakt van de huidige stand van zaken. Hoe staat de organisatie er nu voor op het gebied van de regels rondom de verwerking van persoonsgegevens als ook de technische beheersmaatregelen? Door dit in kaart te brengen kan er een discussie op gang komen over de gewenste maatregelen en kan er een overzicht worden gemaakt van de *quick wins*. Vaak is er met beperkte inspanning al veel winst te behalen op het gebied van informatiebeveiliging. Zodra er een duidelijke visie is kan er een informatiebeveiligingsbeleid worden opgesteld. Het is belangrijk om hierbij zoveel mogelijk verschillende stakeholders te betrekken. Voor een successvolle implementatie van een informatiebeveiligingsbeleid is draagkracht binnen de organisatie essentieel. Nadat het informatiebeveiligingsbeleid is vastgesteld, is het daarom aan te raden om dit aan de gehele organisatie te presenteren. Om ervoor te zorgen dat de genomen beheersmaatregelen de tand des tijds doorstaan, dient het verder aanbeveling om periodiek een audit uit te voeren om te controleren of het beleid nog in overeenstemming is met de praktijk.

Wel of geen ISO 27001 certificering voor mijn organisatie?

Organisaties die namens klanten persoonsgegevens verwerken zullen vaak de vraag krijgen of ze ISO 27001 gecertificeerd zijn. Dat is de internationale standaard ten aanzien van informatiebeveiliging. In sommige gevallen wordt ISO certificering geëist als onderdeel van de contractonderhandelingen. Een ISO certificering is een kostbare aangelegenheid. Startende ondernemingen doen er verstandig aan om te kijken of het mogelijk is om te volstaan met een informatiebeveiligingsbeleid. Dat bevat grotendeels dezelfde beheersmaatregelen die verplicht zijn voor een ISO certificering, maar kan voor een fractie van de kosten worden opgesteld. Er vindt dan geen externe audit plaats van het informatiebeveiligingsbeleid. Het behalen van een ISO certificering kan echter ook zorgen voor een concurrentievoordeel. Een organisatie kan een goede sier maken naar zowel klanten als consumenten wanneer het beschikt over een extern gecertificeerd informatiebeveiligingsbeleid.

Project Privacy kan uw organisatie helpen met uw informatiebeveiligingsbeleid

Project Privacy kan uw organisatie ondersteunen bij het implementeren van een informatiebeveiligingsbeleid. Daarnaast kunnen we u ook begeleiden bij het behalen van een ISO 27001 certificering. Wij regelen dan het gehele traject, inclusief audit door een ISO certificerende instantie. Maar vaak volstaat het om de huidige praktijk onder woorden te brengen. Om die reden komen we graag langs met onze ‘checklist informatiebeveiliging’ voor een vrijblijvende intake.

Wat kunt u concreet van ons verwachten:

- Een intake informatiebeveiliging met checklist voor vaststellen van de huidige situatie
- Het schrijven van een informatiebeveiligingsbeleid die toepasbaar is op uw situatie
- Een Technical Factsheet op één A4 voor potentiële klanten
- ‘Awareness’ presentatie en training geven aan uw medewerkers
- Een overzicht van *quick wins* en een plan van aanpak voor de lange termijn
- Ondersteuning bij het implementeren van (technische) beheersmaatregelen

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 *Privacy by Design*.

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