



ACA IT-Solutions, onderdeel van Crowe

Whitepaper:

Data Privacy Management

Verantwoordelijkheid richting klant,
medewerker en wetgever.

Data Privacy Management

Als een klant, medewerker of sollicitant je vraagt of zijn/haar persoonsgegevens veilig en respectvol worden behandeld, kun je daar volmondig ja op antwoorden?



Inleiding

Automatisering en digitalisering maken het (bedrijfs)leven een stuk makkelijker. Technologische ontwikkelingen volgen elkaar in rap tempo op. De hoeveelheid data die wordt gegenereerd en rondgaat in organisaties is groter dan ooit. Dit brengt ook risico's met zich mee. Bijvoorbeeld op het vlak van security en privacy. Regelmatig komt het voor dat persoonlijke gegevens van bijvoorbeeld klanten of medewerkers op straat komen te liggen of in verkeerde handen terecht komen.

Organisaties hebben een grote maatschappelijke verantwoordelijkheid om op een veilige en respectvolle manier om te gaan met persoonsgegevens. Sinds de invoering van de Europese privacywet (AVG, Engels: GDPR) is er veel meer aandacht voor dit onderwerp.

Het managen van data en het garanderen van de privacy is een lastig vraagstuk, zo blijkt in de praktijk. Er bestaat geen blauwdruk, want elke organisatie werkt anders. Een gedegen, beleidsmatige aanpak is daarom essentieel.



Maarten de Rooij, IT Business Professional ACA IT-Solutions

De privacywet in het kort

De Algemene verordening gegevensbescherming beschrijft regels voor de verwerking van persoonsgegevens en gelden voor zowel commerciële bedrijven, overheidsinstanties als non-profit instellingen. De privacywet heeft als doel om privacygevoelige gegevens van personen te beschermen.

Basisprincipes AVG

- *Rechtmatigheid, eerlijkheid en transparantie* – Persoonlijke data dienen op een rechtmatige, eerlijke en transparante manier verwerkt te worden in relatie tot personen waar de data betrekking op hebben.
- *Integriteit en vertrouwelijkheid* – Er dient sprake te zijn van adequate beveiliging van persoonlijke data, inclusief maatregelen tegen ongeautoriseerde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.
- *Data minimalisering* – Alleen data opslaan en gebruiken die noodzakelijk is en uitsluitend beschikbaar is voor medewerkers die de data nodig hebben voor bedrijfsdoeleinden.
- *Afbakening van het doel* – Persoonlijke data mogen uitsluitend worden gebruikt voor duidelijke en rechtmatige doelen.
- *Afbakening van de opslag* – Persoonlijke data worden niet langer opgeslagen dan noodzakelijk is.



Imagoschade en boetes

De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacywet en kan hoge boetes opleggen als bedrijven of instanties de wet niet naar behoren naleven. De sancties variëren van waarschuwingen tot bindende maatregelen, tot een maximale boete van 20 miljoen euro of 4% van de jaaromzet. Waar de AP bij aanvang alleen extreme gevallen behandelde, zien we nu dat de boetehandhaving steeds sneller en grootschaliger wordt.

Daarbij wordt ook veelvuldig gehandeld naar aanleiding van klachten die worden ingediend. Hierdoor heeft ook de bevolking invloed op de werkwijze en focus van de AP. De AP kan ervoor kiezen om incidenten publiekelijk bekend te maken. Heeft jouw organisatie een privacy issue (zoals een datalek) dan dien je dit te melden bij de AP en ook de getroffen personen te worden geïnformeerd. Dit kan leiden tot enorme reputatieschade.

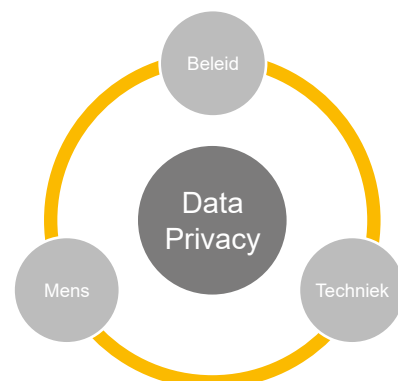
Mindset is essentieel

Data privacy is niet 'met één druk op de knop' geregeld en moet ook niet gezien worden als een losse exercitie. Een integratie in de bedrijfsprocessen en mindset is essentieel: beleid-techniek-mens. Door deze aanpak wordt de organisatie een stuk veiliger, wordt data privacy gedragen in de organisatie en wordt respectvol omgegaan met privacygevoelige persoonsgegevens.

Eerste aanspreekpunt in jouw organisatie

Het is raadzaam om binnen jouw organisatie een vast aanspreekpunt aan te stellen. Deze rol wordt vaak toebedeeld aan de Data Protection Officer (DPO), de Privacy Officer of de Functionaris Gegevensbescherming (FG).

In de praktijk blijkt het lastig om deze functie in te vullen. Bovendien is het een functie/rol die vaak niet groot genoeg is om fulltime uit te voeren. Aangezien het gaat om een complex en specialistisch vraagstuk wordt afgeraden om dit toe te bedelen aan een medewerker die dit 'erbij doet'.



Soms is het verplicht om een Functionaris Gegevensbescherming (FG) aan te stellen. Dit geldt voor:

- Overheidsinstanties en publieke organisaties (zoals zorg en onderwijs)
- Organisaties die op grote schaal individuen of diens activiteiten in kaart brengen
- Organisaties die op grote schaal bijzondere persoonsgegevens verwerken



Review & GAP Analyse

Een succesvolle implementatie van data privacy in de organisatie vereist een gedegen plan van aanpak. We zien vaak dat in 2018 “AVG compliancy” als een eenmalig project is opgepakt en daarna is stilgevallen. Ook zien we bij een analyse dat er grote risico's over het hoofd worden gezien. Daarom is een structurele aanpak van data privacy een must en kun je na implementatie tegen jouw klanten, medewerkers en sollicitanten zeggen: ja, wij stellen alles in het werk om veilig en respectvol met persoonsgegevens om te gaan.

ACA IT-Solutions kan voor jouw organisatie een Review & Gap Analyse verzorgen. Wij beoordelen de huidige situatie en analyseren welke risico's nog niet/onvoldoende zijn afgedekt. In een uitgebreide rapportage wordt deze analyse toegelicht en worden praktische verbetervoorstellen gedaan. Daarbij wordt gekeken naar de gaps op het vlak van wetgeving, ICT-beveiliging en de werkwijze van medewerkers. Op basis hiervan bepalen we in samenspraak de benodigde vervolgstappen. Onze specialisten ondersteunen je graag bij de implementatie.



Advies & ondersteuning

Bij ACA IT-Solutions, onderdeel van Crowe, draait alles om de drie-eenheid: Beleid, Techniek en Mens. Elk vraagstuk is een samenspel van deze elementen. Dat leidt tot innovatieve IT-bedrijfsoplossingen, waarbij continuïteit, beschikbaarheid en veiligheid essentieel zijn. Daarmee bereiken onze klanten een onderscheidend resultaat.

Contact

Wil je meer informatie of een afspraak maken? Neem dan contact met ons op via onderstaande contactgegevens.

Adresgegevens

ACA IT-Solutions, onderdeel van Crowe
Beukenlaan 40-50
5651 CD Eindhoven

Contactgegevens

040 - 8 800 100
info@aca-it.nl
www.aca-it.nl