GDPR-compliant in zes stappen

Doe jij het wel veilig?

Cloud computing heeft de laatste jaren flink aan populariteit gewonnen. Opslag van data in de cloud bespaart investeringen in hardware, is enorm schaalbaar en vermindert de complexiteit van IT-beheer. Een mogelijk nadeel is de afhankelijkheid van de leverancier; problemen kun je immers niet zelf verhelpen. Ook is vaak onduidelijk waar bedrijfsdata zich precies bevindt. Nieuwe wetten dwingen je ertoe je bedrijfsprocessen met betrekking tot data nog eens goed te herzien om flinke boetes te voorkomen.

NIEUWE, STRENGERE PRIVACYWETGEVING

Elk bedrijf dat met persoonsgegevens werkt, moet rekening houden met de nieuwe Europese privacyverordening. Op 25 mei 2018 maakt de Wet bescherming persoonsgegevens (Wbp) definitief plaats voor de Algemene Verordening Gegevensbescherming (AVG of GDPR in het Engels). Vanaf dat moment geldt in de hele EU dezelfde wetgeving met betrekking tot privacy en de omgang met persoonsgegevens. Ook bedrijven buiten de EU die gegevens van Europese burgers verwerken (denk aan Google of Microsoft), moeten zich aan de AVG houden.

De verordening geeft burgers meer zeggenschap over hun data en wat daarmee gebeurt. Bedrijven moeten duidelijk maken (en vast-

leggen!) waarom ze bepaalde (persoons) gegevens nodig hebben en waarvoor die worden gebruikt. Burgers kunnen inzage vragen in opgeslagen data, toestemming intrekken, klachten indienen en gebruikmaken van het recht om vergeten te worden. Nieuw is het recht op dataportabiliteit, waarmee burgers het recht krijgen om de persoonsgegevens te ontvangen die een organisatie van ze heeft.

Overigens is de AVG sinds begin 2016 al in werking getreden, maar bedrijven hebben nog een krap jaar om aan alle regels en onderdelen in de verordening te voldoen. De nieuwe verordening is veel strenger dan de Nederlandse privacywetgeving. Nu moet nog sprake zijn van opzet of grove schuld voordat een datalek wordt gemeld bij de Autoriteit Persoonsgegevens (AP). Die bepaling verdwijnt en bedrijven die zich niet aan de regels houden, kunnen straks rekenen op forse boetes (tot 5 procent van hun wereldwijde omzet).
Om boetes en problemen te voorkomen, is het van belang tijdig voorbereidingen te treffen. Zo moeten organisaties die persoonsgegevens verwerken, documenteren welke gegevens worden verwerkt, met welk doel, waar data vandaan komt en met wie deze wordt gedeeld. Sommige organisaties zijn daarnaast verplicht om een functionaris gegevensbescherming (FG) aan te stellen. Die is verantwoordelijk voor de meldplicht en bekleedt een onafhankelijke positie binnen de organisatie. De AP biedt een stappenplan aan dat bedrijven op weg helpt om aan de AVG te voldoen.

DE AVG EN CLOUD COMPUTING

Steeds meer bedrijven maken gebruik van de cloud voor de verwerking van data, soms ter vervanging van hun eigen servers en opslag, soms door gebruik van SaaS. In veel gevallen zijn daarbij persoonsgegevens betrokken. Omdat de leverancier daar ook toegang tot heeft, bijvoorbeeld als hij beheeractiviteiten uitvoert, is het van belang afspraken te maken over beveiliging en geheimhouding. Doorgaans wordt dat vastgelegd in een bewerkersovereenkomst. Als klant moet je controleren of de cloudleverancier voldoet aan de verplichtingen, en actie ondernemen als dat niet het geval is.

Een belangrijk aandachtspunt – zeker bij het werken met clouddiensten – is doorgifte naar het buitenland. Er worden strenge eisen gesteld aan het (ver)plaatsen van persoonsgegevens op servers buiten de EU. Het moet duidelijk zijn waar de gegevens zich bevinden en of de locatie een 'passend beschermingsniveau' heeft. Voorkom problemen door te kiezen voor een cloudleverancier die enkel gebruikmaakt van servers binnen de EU.
Verder schrijft de AVG voor dat beveiligingsincidenten waarbij data is gelekt direct gemeld moeten worden bij de Autoriteit Persoonsgegevens. Na beëindiging van een cloudcontract (of faillissement van de leverancier) vindt een overdracht van gegevens plaats. Ook moet de leverancier de gegevens van zijn servers verwijderen.

ZO WORD JE COMPLIANT

Privacy Management Partners en cloudbeveiligingsbedrijf Netskope onderscheiden zes zaken waaraan organisaties die persoonsgegevens verwerken en gebruikmaken van de cloud moeten voldoen. Door deze stappen te doorlopen, word je compliant.

- Weet waar leveranciers van cloud-apps gegevens verwerken en opslaan. Houd daarbij rekening dat data kan circuleren tussen de verschillende datacenters waarvan de app gebruikmaakt.
- Neem adequate beveiligingsmaatregelen om persoonlijke data te beschermen tegen verlies, aanpassing en ongeoorloofde verwerking. Wees er zeker van dat de cloud-apps die je gebruikt voldoen aan de beveiligingsstandaarden.
- Controleer je dataverwerkingsovereenkomst met de aanbieders van de cloud-apps die je gebruikt. Zo weet je zeker dat ze voldoen aan de eisen van de nieuwe Europese privacywetgeving.
- Verzamel alleen data die je écht nodig hebt en beperk de verwerking van 'speciale' gegevens, die betrekking hebben op bijvoorbeeld ras, etniciteit, politieke voorkeur en religie. In principe hoeft alleen de data benodigd voor de functionaliteit van de cloud-app verzameld te worden.
- Sta niet toe dat clouddiensten persoonlijke data voor andere doeleinden gebruiken. Leg vast dat de klant eigenaar is van de data en dat deze niet met derden wordt gedeeld.
- Zorg dat persoonsgegevens worden gewist wanneer er niet meer gebruik wordt gemaakt van de clouddienst of -app.

Daarnaast is het goed om binnen de organisatie awareness te creëren, niet alleen over de nieuwe privacywetgeving, maar ook over het belang van informatiebeveiliging in het algemeen. Vaak is het niet het systeem dat onveilig is, maar liggen de risico's juist in het gebruik van de applicaties. Train en informeer daarom je medewerkers.

www.inspireertbeterondernemen.nl