Vanaf mei 2018 wordt GDPR gehandhaafd met torenhoge boetes

GDPR heeft grote gevolgen voor industrie

De General Data Protection Regulation (GDPR) is een EU-wet die in april 2016 werd aangenomen en waarin is vastgelegd dat de data van alle individuen in de Europese Unie moet zijn beschermd. Hoewel deze wet nu inmiddels een jaar van kracht is, wordt er vanaf mei 2018 actief gehandhaafd en dit kan grote consequenties hebben voor bedrijven in de (proces)industrie.

Jan de Loper

Met de enorme toename in het digitale verkeer ligt misbruik van persoonsgegevens steeds meer op de loer. De Data Protection Directive uit 1995 voldeed niet meer aan de enorme vlucht die data inmiddels genomen heeft en daarom werd in april vorig jaar de nieuwe GDPR aangenomen. En die is bepaald niet kinderachtig: de GDPR geldt niet alleen voor bedrijven die in Europa gevestigd zijn, maar ook voor bedrijven aan de andere kant van de oceaan die wel over de gegevens van EU-burgers beschikken. Evenmin kinderachtig zijn de straffen bij het overtreden van deze nieuwe wet: maximaal 4% van de bruto omzet. Dat kan dus in de miljarden lopen.

Evenmin kinderachtig zijn de straffen bij het overtreden van deze nieuwe wet...

Data

Rajesh Pillai is cyber security expert bij Wipro. Met zeventien jaar ervaring binnen en buiten Europa bij grote bedrijven in de industrie, weet hij inmiddels wat de stand van zaken is. "De GDPR zorgt wel voor de nodige onrust bij veel bedrijven", weet hij. "Ook bedrijven in de industrie hebben tegenwoordig de beschikking over veel gegevens van hun klanten. Denk aan marketing, websystemen, enorme databases, het nieuwe Internet of Things, alles draait tegenwoordig om data."

Maatregels

Over ongeveer een jaar is de GDPR is niet alleen maar een richtlijn, maar wordt er gehandhaafd op de afgesproken regels. "Dat betekent dat veel bedrijven in korte tijd een behoorlijke hoeveelheid werk moeten verzetten", vertelt Pillai. "Doe je dat niet op tijd, hangt je dus een enorme potentiële boete boven het hoofd. Daar komt nog bij dat je als bedrijf ook nog eens verplicht bent om data breaches te melden."
Los van de financiële aderlating kan een data breach ook nog een zeer nadelig na-effect hebben door imagoschade. "Als je kijkt naar de casus van Yahoo, waar jaren geleden een datalek plaatsvond en waar het pas onlangs bekend is geworden in de media, zie je een tamelijk ongewenste situatie. De EU meent dat de consument direct op de hoogte moet worden gesteld van zo'n lek, zodat ze in staat worden gesteld maatregels te treffen. Voor de consument is dat een goede ontwikkeling."

Apple en Google

Pillai is op dit moment betrokken bij de totstandkoming van GDPR compliance bij twintig grote bedrijven. "De meeste van deze bedrijven zijn er niet zeker van dat ze voor mei 2018 klaar zullen zijn, maar de 'security hygiene' zal wel fors zijn toegenomen", weet hij te vertellen. "Bij dit proces is er een belangrijke juridische component en dat zie je terug in de achtergrond van de aangewezen persoon die binnen zo'n bedrijf verantwoordelijk wordt voor de GDPR compliance. De meeste bedrijven stellen een Chief Privacy Officer, of een Data Protection Officer aan, die met zijn of haar juridische achtergrond goed onderlegd is voor deze uitdaging. De eerste stap die gezet moet worden, is het in kaart brengen van de complete historie van data binnen het bedrijf. Dat kan zo simpel zijn als een digitaal gastenboek met daarin de namen van je bezoekers, tot een grote onderneming die apps bouwt die bij consumenten op hun smartphones draaien. Vergis je niet: ook Google en Apple moeten zich aan de GDPR houden."

Miljoen

Na het in kaart brengen van het datagebruik volgt de volgende stap. Pillai: "Firewalls moeten worden opgebouwd, of herzien, detectiesystemen en controlesystemen moeten worden opgezet, enzovoorts. Je moet als bedrijf kunnen aantonen dat je al het mogelijke hebt gedaan om de data van je klanten te beschermen."
Hoewel bij het niet voldoen aan GDPR de boetes astronomisch hoog kunnen zijn, is

Vergis je niet: ook Google en Apple moeten zich aan de GDPR houden...

de investering om een bedrijf 'GDPR proof' te maken ook niet bepaald gering. Pillai: "Bij grote bedrijven en telecom ondernemingen moet je denken aan investeringen rond de veertig miljoen. Grote fabrieken zullen ongeveer de helft van dat bedrag kwijt zijn."

Kleinere bedrijven, die geen 20 miljoen hebben liggen, hoeven niet te vrezen voor hun voortbestaan. "Je ziet dat veel bedrijven samenwerken om hun GDPR compliance te realiseren", legt Pillai uit. "Daarnaast zie je dat veel aanbieders inspringen op de GDPR wetgeving. Dit soort aanbieders bieden cloud services aan die volledig voldoen aan de GDPR. Als je die service gebruikt, ben je dus GDPR compliant."

Consument

Is het tot stand komen van de GDPR het gevolg van de big data revolutie, waar we nu overigens nog maar net aan zijn begonnen? "Ik denk het niet", antwoordt Pillai. "GDPR komt in eerste instantie door bezorgdheid aan de consumentenkant over wat er met hun gegevens gebeurt. Verhalen over datalekken dragen bij aan die bezorgdheid."