contrast

UW BUSINESS • MAART 2020

Datalekken: tips en tricks.

Wat u moet weten.

Wanneer een onderneming in het nieuws verschijnt omwille van een schending van de GDPR is dat niet zelden te wijten aan een datalek. Naast de commerciële gevolgen en het risico op significante geldboetes, is zo'n datalek dus ook bijzonder schadelijk voor de reputatie van een onderneming.

De GDPR omvat verschillende verplichtingen in verband met datalekken. Die verplichtingen beginnen bij het nemen van beveiligingsmaatregelen om de integriteit, vertrouwelijkheid en beschikbaarheid van persoonsgegevens te waarborgen.

Men spreekt van een datalek op het ogenblik dat er zich, per ongeluk of te kwader trouw, een inbreuk voordoet op:

- de vertrouwelijkheid van persoonsgegevens: i.e. wanneer er een ongeoorloofde toegang is geweest tot de data, bijvoorbeeld door een hacker;
- de beschikbaarheid van persoonsgegevens: i.e. wanneer een onderneming niet langer controle over of toegang tot de data heeft, bijvoorbeeld omdat het IT systeem waarin de gegevens zijn opgeslagen (al dan niet tijdelijk) faalt;
- de integriteit van persoonsgegevens: i.e. wanneer de data zijn aangetast, bijvoorbeeld door een foutieve wijziging.

Wanneer een van deze inbreuken zich voordoet, hebben verwerkingsverantwoordelijken de verplichting om het datalek te documenteren in een intern register. Zij moeten het datalek binnen de 72 uur melden aan de toezichthoudende autoriteit, tenzij het onwaarschijnlijk is dat het datalek een risico inhoudt voor de betrokkenen. Als het datalek een hoog risico inhoudt voor de betrokkenen, moet het ook onverwijld aan deze betrokkenen worden gemeld. Bij wijze van voorbeeld, wanneer een bedrijfslaptop met HR gegevens die beveiligd is tegen ongeoorloofde toegang, gestolen wordt, lijkt het onwaarschijnlijk dat een melding nodig is. Wordt de laptop echter gestolen terwijl die niet beveiligd is en dus toegang tot bijvoorbeeld financiële informatie van werknemers mogelijk is, zal een melding aan de toezichthoudende autoriteit en de betrokkenen wellicht wel nodig zijn.

Ook verwerkers hebben verplichtingen wanneer er zich een datalek voordoet. Verwerkers moeten datalekken melden aan de verwerkingsverantwoordelijken van zodra zij daar kennis van hebben. Ze

moeten de verwerkingsverantwoordelijken ook bijstaan bij het vervullen van hun verplichtingen inzake datalekken.

Wat u moet doen.

Als onderneming moet u ervoor zorgen dat u een beleid uitwerkt inzake beveiliging en datalekken:

- Breng per verwerkingsactiviteit en per datasysteem in kaart welke datalekken zich kunnen voordoen. Verlies daarbij de minder voor de hand liggende situaties niet uit het oog, zoals documenten die voor afvalophaling buiten worden gezet of documenten die per post worden verstuurd maar verloren gaan of geopend terug worden gestuurd.
- Werk niet alleen een beveiligingsbeleid uit om te voorkomen dat datalekken zich voordoen, maar neem ook maatregelen om deze incidenten te kunnen detecteren en te remediëren wanneer zij zich voordoen. Dit betekent onder meer dat medewerkers moeten worden getraind op het identificeren van datalekken. Weten uw medewerkers dat het versturen van een e-mail met gegevens naar de verkeerde persoon en het verlies van een bedrijfslaptop datalekken zijn? Herbekijk het beveiligingsbeleid van tijd tot tijd (zeker wanneer er zich een datalek heeft voorgedaan), en pas het indien nodig aan.
- Werk interne procedures uit zodat snel en correct kan worden gehandeld wanneer er zich een datalek voordoet. Deze procedures moeten aangeven waar datalekken intern moeten worden gemeld, wie het datalek zal analyseren en desgevallend zal melden aan de toezichthoudende autoriteit en de betrokkenen of de verwerkingsverantwoordelijke, enz.

Zorg voor duidelijke afspraken tussen verwerkingsverantwoordelijken en verwerkers aan de ene kant, en/of gezamenlijke verwerkingsverantwoordelijken aan de andere kant. Zo kan de verwerker bijvoorbeeld beter geplaatst zijn dan de verwerkingsverantwoordelijke om een datalek te melden aan de betrokkenen. Omdat ondernemingen snel moeten schakelen wanneer er zich een datalek voordoet, moet de kwalificatie van de partijen als verwerker of (gezamenlijke) verwerkingsverantwoordelijke duidelijk zijn vóór het datalek plaatsvindt.