FRANKLIN

Welke stappen moet een onderneming nemen wanneer er zich een gegevenslek voordoet?

MR FRANKLIN CHECKLIST

Ondernemingen worden steeds meer geconfronteerd met gegevenslekken. Door de digitalisering gaan we steeds meer data verwerken en delen, veelal over het internet. Die grote beschikbaarheid en deelbaarheid van data verhoogt het risico op een datalek enorm. De GDPR legt enkele verplichtingen op wanneer er zich binnen uw onderneming een datalek voordoet. Wanneer er zich een datalek voordoet bij een verwerker van u, moet hij u hiervan op de hoogte brengen en moeten door de verwerkingsverantwoordelijke dezelfde verplichtingen voldaan worden als voor een intern datalek!

ZES STAPPEN BIJ EEN GEGEVENSLEK

Stap 1: Evalueer het gegevenslek

Wanneer er zich een gegevenslek voordoet moet er vooreerst gekeken worden wat het datalek inhoudt (hoeveel mensen hebben onrechtmatig toegang tot de data, is er kwaad opzet, is de data nog toegankelijk en/of beschikbaar...) Daarnaast moet er een impact-analyse plaatsvinden waarbij gekeken wordt welke impact dit datalek heeft voor de personen van wie de gegevens gelekt worden. Zo zal het lekken van login gegevens of kredietkaart gegevens doorgaans een grotere impact hebben dan het lekken van een lijst met contactgegevens.

Wat is een gegevenslek?

Er is sprake van een gegevenslek wanneer een onbevoegd persoon toegang krijgt of kan krijgen tot persoonsgegevens. Een datalek kan veroorzaakt worden door kwaad opzet zoals een hacking of diefstal maar ook door een interne vergissing zoals een email naar de verkeerde persoon sturen of een smartphone verliezen.

Tip: De risico-analyse kan gebeuren met onze gratis online tool Dr. Breach (www.doctorbreach.eu).

dr breach

Stap 2: melding datalek aan GBA

Wanneer het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkenen, moet dit meegedeeld worden aan de Gegevensbeschermingsautoriteit (GBA) binnen de 72 uur. De termijn gaat in zodra de verwerkingsverantwoordelijke “in kennis” is van het datalek. Het is steeds de verwerkingsverantwoorelijke die de melding moet doen. Dit kan door een formulier in te vullen op de website van de GBA.

Stap 3: melden gegevenslek aan betrokkenen

De verwerkingsverantwoordelijke moet het datalek meedelen aan alle betrokkenen voor wie het datalek een hoog risico inhoudt. Dit kan het geval zijn wanneer kredietkaart gegevens betrokken zijn of login gegevens. Deze personen moeten persoonlijk op de hoogte gebracht worden zodat zij zich gepast op de gevolgen kunnen voorbereiden en eventueel maatregelen kunnen nemen om de gevolgen te beperken. Hoewel voor deze meldplicht geen uitdrukkelijke termijn is opgenomen, spreekt het voor zich dat deze melding best zo snel mogelijk gebeurt.

MR. FRANKLIN

Stap 4: Meld het datalek aan de verwerkingsverantwoordelijke

Wanneer je persoonsgegevens verwerkt als verwerker voor een verwerkingsverantwoordelijke moet je de verwerkingsverantwoordelijke zo snel mogelijk na ontdekken van het gegevenslek hiervan op de hoogte brengen.

Stap 5: Noteer het gegevenslek in het datalekkenregister

Elk gegevenslek moet opgenomen worden in een intern register van datalekken. Dit register moet minimaal de volgende informatie bevatten:

- het tijdstip van het datalek;
- een beschrijving van het datalek;
- de gevolgen van het datalek;
- de genomen maatregelen om de schade te beperken en toekomstige gelijkaardige incidenten te voorkomen;
- een risicoanalyse van het datalek
- indien het gegevenslek gemeld werd aan de GBA of de betrokkene het tijdstip. Indien niet, de reden.

Stap 6: Neem maatregelen om de schade te beperken en soortgelijke datalekken te voorkomen

Bij de vaststelling van een gegevenslek moeten er maatregelen genomen worden om de schade zoveel als mogelijk te beperken, dit zowel voor de eigen onderneming, als voor de personen die bij het gegevenslek zijn betrokken.

Indien nodig moeten er maatregelen genomen worden om het risico op een soortgelijk datalek in de toekomst te verlagen of voorkomen.

Stel een SPOC aan

Benoem binnen uw organisatie een contactpersoon (SPOC) voor datalekken.

Het doel hiervan is dat wanneer iemand binnen uw organisatie een vermoedelijk gegevenslek vaststelt, hiervan zelf geen evaluatie moet doen maar zo snel mogelijk de SPOC moet contacteren die dan de verdere verplichtingen op zich neemt.

Hoe kan Mr. Franklin u bijstaan?

Mr. Franklin kan u op verschillende manieren bijstaan indien er zich een gegevenslek heeft voorgedaan in uw organisatie:

- Bij de analyse van het datakek
- Bij de aangifte van het gegevenslek bij de GBA
- Bij de communicatie naar betrokkenen en het opstellen van persmededelingen
- Bij het opstellen van een datalekregister

Indien u preventief wenst op te treden kan Mr. Franklin u bijstaan bij de opmaak van een interne procedure gegevenslekken en bij de opleiding van uw personeelsleden, van wie algemeen aangenomen wordt dat zij doorgaans de zwakste schakel zijn binnen uw veiligheidsbeleid.

Waarom kiezen voor Mr. Franklin?

Mr. Franklin is een advocatenkantoor met bijzondere expertise op vlak van GDPR en databescherming. Onze GDPR specialisten en gecertificeerde DPO's stonden reeds meer dan 250 ondernemingen bij met heldere adviezen en een kwalitatieve en persoonlijke service tegen een duidelijke tarifering aan vaste prijzen.

Indien u interesse hebt in onze diensten kan u steeds vrijblijvend een offerte aanvragen bij Olivier Sustronck via olivier@misterfranklin.be of telefonisch op het nummer 0486 27 53 05.