Datalekken: wie knabbelt daar aan mijn kluisje

nieuws
legal, profit, non-profit, ***29 november 2019***

De Algemene Verordening Gegevensbescherming (ook wel bekend als de AVG/GDPR) gaat over de bescherming van persoonsgegevens en legt daarbij allerlei verplichtingen op aan verwerkingsverantwoordelijken. Een persoon of onderneming die gegevens van klanten, leveranciers of werknemers bijhoudt en verwerkt is een verwerkingsverantwoordelijke. De AVG legt onder andere een aantal verplichtingen op voor 'inbreuken in verband met persoonsgegevens'. Dit is een hele mond vol, waardoor deze inbreuken ook beter gekend staan als datalekken.

Doordat de AVG zeer korte termijnen geeft om aan de meldingsverplichtingen, zoals hieronder beschreven, te voldoen, is het belangrijk dat de verwerkingsverantwoordelijke goed voorbereid is, mocht een datalek zich voordoen. Naast het documenteren van het incident, is de verwerkingsverantwoordelijke vaak verplicht om de gegevensbeschermingsautoriteit en/of betrokkenen op de hoogte te brengen.

Data, het lekt sneller dan je denkt

Het begrip datalek is zeer ruim, het omvat veel meer dan wat u er initieel onder zou verstaan. Het is niet enkel van toepassing wanneer het IT-systeem van de onderneming wordt gehackt en er gegevens gestolen worden. Naast deze 'ongeoorloofde toegang' is ook elke vernietiging, verlies of wijziging van persoonsgegevens een datalek. Zo dus ook als er persoonsgegevens op een laptop staan en deze laptop verloren of kapot gaat, waarbij geen back-up bestaat. Heeft de onderneming niet langer de controle over de data, omdat zij op een ongeoorloofde wijze verstrekt werd aan derden, dan is dit ook een datalek. De verplichtingen van de AVG gelden dus ook wanneer een onderneming een mail met persoonsgegevens naar een verkeerde geadresseerde stuurt.

Het moet nog opgemerkt dat datalekken niet enkel digitaal plaatsvinden. Persoonsgegevens die op papier zijn neergepend en die verloren gaan of gestolen worden, zijn eveneens datalekken. Er is wel maar sprake van een datalek indien de handelingen per ongeluk gebeurden of op een onrechtmatige wijze. Verwijdert of wijzigt een onderneming persoonsgegevens van klanten, omdat zij niet langer juist zijn, dan is dit uiteraard geen datalek. Het gaat ook enkel om datalekken, zoals beschreven door de AVG, indien er persoonsgegevens betrokken zijn bij het incident.

Preventie en documentatie van datalekken

Een eerste stap bij datalekken is de preventie ervan. Het is, overigens een verplichting onder de AVG, belangrijk dat de verwerkingsverantwoordelijke voldoende beveiligingsmaatregelen voorziet. Een onderneming mag bijvoorbeeld geen persoonsgegevens van personeelsleden of klanten zomaar op een onbeveiligde computer zetten. De AVG vertrekt vanuit een risicobeoordeling: gaat het om gevoeligere informatie, dan moet de verwerkingsverantwoordelijke voorzien in betere beveiliging.

De verwerkingsverantwoordelijke heeft het nodige gedaan, maar toch heeft er zich een datalek voorgedaan: wat nu?
Het incident moet **altijd** worden gedocumenteerd:

- Werknemers zijn vaak de eersten die een datalek opmerken en zijn dan ook de gepaste personen om dit te melden. Voorzie in een formulier of een uitgewerkte procedure zodat zij de verwerkingsverantwoordelijke zo snel mogelijk en met de juiste informatie kunnen verwittigen.
- Maakt de verwerkingsverantwoordelijke gebruik van een verwerker, voorzie dan zeker in een uitgewerkte meldingsprocedure. Een verwerker is een onderneming of persoon die de persoonsgegevens gaat verwerken in opdracht van de verwerkingsverantwoordelijke. Het is namelijk de verwerkingsverantwoordelijke die steeds moet instaan voor de documentatie- en meldingsverplichtingen bij datalekken. Het is dan ook belangrijk dat de verwerker doorgeeft wanneer zich bij hem een datalek voordoet. De manier waarop deze melding plaatsvindt (en wie de verplichtingen van de AVG zal nakomen) kunnen beide partijen nog regelen in de verwerkingsovereenkomst.
- Elke verwerkingsverantwoordelijke moet een document of digitaal bestand bijhouden waarin hij de informatie over elk datalek bewaart. Zo noteert hij de feiten van het datalek, zijnde de aard, de omvang, de betrokken persoonsgegevens, de verwerker bij wie het datalek zich voordeed, etc. De verwerkingsverantwoordelijke zal ook moeten bijhouden wat de gevolgen van het datalek zijn en welke maatregelen hij neemt om verdere datalekken te voorkomen.
- De verwerkingsverantwoordelijke neemt ook best op waarom hij, zoals hieronder verduidelijkt, niet over gaat tot het inlichten van de gegevensbeschermingsautoriteit en/of de betrokkenen.

Melding van het datalek

Verwerkingsverantwoordelijken hebben onder de AVG in veel gevallen de verplichting om het datalek te melden. Zo moet hij bijna altijd de gegevensbeschermingsautoriteit inlichten. Bij een datalek waarbij veel of ‘gevoelige’ informatie over een betrokkene gelekt is, dan moet een melding evengoed gebeuren aan de betrokkenen. De enige uitzondering hierop is wanneer het datalek geen risico’s inhoudt voor de rechten en vrijheden van de personen wiens persoonsgegevens gelekt zijn. Stel dat een computerstick met persoonsgegevens van klanten wordt gestolen, maar deze is voldoende versleuteld. Een melding is dan niet aan de orde, maar

vergeet zeker niet om het incident te documenteren.

Aan de gegevensbeschermingsautoriteit

In alle overige gevallen moet de verwerkingsverantwoordelijke het datalek steeds melden aan de gegevensbeschermingsautoriteit. Deze melding moet plaatsvinden binnen de 72 uur nadat hij kennis neemt van het voorval. Deze termijn houdt niet de 'beperkte' periode in die nodig is om, voorafgaand aan de melding, het datalek te controleren. Hierbij gaat het enkel om een initieel onderzoek om er zeker van te zijn dat het inderdaad gaat om een datalek. Indien enkel naams- en adresgegevens werden gelekt, zal het vaak volstaan om enkel een melding te maken aan de gegevensbeschermingsautoriteit.

Welke informatie moet de verwerkingsverantwoordelijke dan zeker mededelen:

- de aard van het datalek, de categorieën van betrokkenen en, eventueel bij benadering, het aantal betrokkenen en de soorten persoonsgegevens;
- indien in de onderneming een aanwezig is, de naam en de contactgegevens van een Data Protection Officer of een ander contactpunt van wie de gegevensbeschermingsautoriteit meer informatie kan verkrijgen;
- de waarschijnlijke gevolgen van het datalek;
- de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om het datalek aan te pakken. Hieronder begrijpt men ook de maatregelen die de verwerkingsverantwoordelijke neemt om eventuele nadelige gevolgen van het datalek te beperken;
- hoewel dit geen wettelijke verplichting is, is het aan te raden om ook reeds mee te delen dat het datalek zich bij een verwerker heeft voorgedaan. De melding vernoemt dan ook de identiteit van de verwerker en voor welke verwerkingsactiviteiten de verwerking plaatsvond.

Aan de betrokkenen

Enkel wanneer het datalek een hoog risico inhoudt voor de betrokkenen, moet de verwerkingsverantwoordelijke hen ook informeren. Steelt een hacker gebruiksnamen, wachtwoorden en de aankoopgeschiedenis van gebruikers van een webshop, dan moeten zij hiervan een melding krijgen. Kan de verwerkingsverantwoordelijke het datalek niet rechtstreeks aan de betrokkenen melden, dan kan dit ook via een openbare melding gebeuren. De melding aan de betrokkenen moet zonder onredelijke vertraging plaatsvinden. Een onderneming kan bijvoorbeeld melding maken van een datalek via een duidelijke pop-up op haar website. Dit nadat zij de omvang van het datalek heeft kunnen vaststellen en de gevolgen hiervan heeft kunnen inschatten.

Neemt de verwerkingsverantwoordelijke na het incident maatregelen zodat er geen hoog risico meer is voor de betrokkenen, dan moet hij het datalek toch niet melden aan de betrokkenen.

Welke informatie moet de verwerkingsverantwoordelijke mededelen aan de betrokkenen?

- Een heldere communicatie staat voorop: de melding moet een omschrijving, **in duidelijke en eenvoudige taal**, van het datalek bevatten; en
- De verwerkingsverantwoordelijke geeft hierbij een korte beschrijving van de aard, omvang, mogelijke gevolgen van het datalek, welke maatregelen men heeft genomen en de contactgegevens van het aanspreekpunt.

Weet wel dat het melden van een datalek (aan de gegevensbeschermingsautoriteit) op zich geen schuldbekentenis inhoudt. Enkel indien niet voldaan is aan een correcte beveiliging of preventie kan de gegevensbeschermingsautoriteit een boete opleggen omdat een datalek heeft plaatsgevonden. De Belgische gegevensbeschermingsautoriteit krijgt jaarlijks honderden meldingen van datalekken en zij heeft op basis hiervan tot op heden nog geen enkel boete uitgeschreven. In Hongarije kreeg een hotel toch een boete van €15 000 nadat zij zelf melding had gemaakt van een datalek. Een gastenlijst was namelijk voor iedereen zichtbaar en werd door een onbevoegde gefotografeerd. Voldoet men niet aan de documentatie- of meldingsverplichtingen, dan bestaat de kans dat de gegevensbeschermingsautoriteit hiervoor een boete oplegt.

Besluit

Het mag dus duidelijk zijn dat er veel meer komt kijken bij een datalek dan u initieel zou denken. Een goede voorbereiding is essentieel. Niet enkel ter voorkoming van datalekken, maar ook met het oog op het nakomen van de verplichtingen als verwerkingsverantwoordelijke. Mocht een melding aan de betrokkenen aan de orde zijn, dan is een heldere communicatie aangewezen. Zeker om ervoor te zorgen dat de reputatie van de onderneming er niet onder komt te lijden.

Tim De Bock