Stappenplan bij een datalek

Een datalek zit in een klein hoekje en overkomt de beste. Bij een datalek komt er in korte tijd veel op een organisatie af. Snel en adequaat handelen is dan cruciaal. In dit stappenplan ziet u wat u moet doen bij een (potentieel) datalek.

Definitie: Wat is een datalek?
De AVG kent de term 'datalek' niet en spreekt in plaats daarvan over 'een inbreuk in verband met persoonsgegevens'. Afhankelijk van de context is er sprake van een datalek als persoonsgegevens per ongeluk of onrechtmatig:

- Vernietigd zijn (bijv. brand in een datacenter)
- Verloren zijn gegaan (bijv. USB-stick met persoonsgegevens verloren)
- Toegankelijk (kunnen) zijn voor onbevoegden (bijv. hacker heeft persoonsgegevens buitgemaakt).

1 Zijn er persoongegevens betrokken?

Persoonsgegevens zijn gegevens die direct over iemand gaan, of die naar een persoon te herleiden zijn. Zoals een naam, (email)adres, bankrekeningnummer of IP adres.

nee → Er is geen datalek in de zin van de AVG. Het is wel van belang om het lek te verhelpen.

ja

2 Handel zo snel mogelijk bij een datalek

Het lek moet binnen 72 uur gemeld worden aan de Autoriteit Persoonsgegevens en/of de betrokkenen. Neem hiervoor de volgende voorbereidende stappen.

I. Leg informatie vast over
- Aard van het datalek
- Oorzaak van het lek
- Omvang van de gevolgen

II. Maak een actieteam. Bij voorkeur met mensen met uiteenlopende disciplines

III. Houd een logboek bij met alle gebeurtenissen en genomen acties van begin tot eind

3 Probeer het datalek te verhelpen

Schakel daarbij de betrokken IT-leveranciers in. Zij kunnen het datalek verhelpen en onderzoek doen naar de oorzaak.

4 Beoordeel of je het datalek moet melden bij de Autoriteit Persoonsgegevens (AP) en de betrokkenen

Het uitgangspunt is dat je een datalek meldt bij de **Autoriteit Persoonsgegevens**, tenzij het onwaarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.
De **betrokkene(n)** informeer je alleen als het datalek een hoog risico vormt voor de privacy van de betrokkene(n).

nee

ja

5 Melding aan de Autoriteit Persoonsgegevens en de betrokkenen

Deze melding **aan de AP** bevat in ieder geval de volgende informatie:
- Een beschrijving van het datalek
- Naam en contactgegevens van een contactpersoon
- Welke categorieën betrokkenen betrokken zijn bij het datalek (bijv. minderjarigen)
- Wat voor persoonsgegevens zijn gelekt
- De waarschijnlijke gevolgen van het datalek
- De voorgestelde of genomen maatregelen om het datalek te verhelpen of de gevolgen te beperken

De melding **aan de betrokkenen** doe je in beginsel rechtstreeks. Het belangrijkste doel van het melden aan de betrokkenen, is dat zij zelf voorzorgs-maatregelen kunnen nemen.

6 Bepaal een communicatiestrategie

Door betrokkenen en eventuele media goed te informeren, voorkomt u paniek en houdt u de regie in handen. Dit verkleint ook het risico op schadeclaims door betrokkenen.

7 Registreer het datalek in het interne datalek register

Iedere organisatie moet een datalekregister opstellen. Hierin staat welke datalekken er in de organisatie zijn geweest.

8 Bereid je voor op toekomstige (juridische) gevolgen

Maak per datalek een juridische analyse van de situatie en tref voorbereidingen voor een onderzoek door de Autoriteit Persoonsgegevens of een claim vanuit een betrokkene.

? Twijfelt u of er sprake is van een datalek?

Of heeft u hulp nodig bij het nemen van maatregelen, het doen van een melding aan de Autoriteit Persoonsgegevens of betrokkenen, of bij het bepalen van de juridische gevolgen? Ons Privacy en Cybersecurity Team staat klaar om Eerste Hulp Bij Datalekken te verlenen.

Sven Wakker
06 4000 88 25
wakker@dirkzwager.nl

Dafne de Boer
026 353 83 23
d.deBoer@dirkzwager.nl

dirkzwager