Stappenplan datalek

Stap 1: Overzicht krijgen bij datalek

Bepaal het soort datalek:

- Inbreuk op de vertrouwelijkheid: persoonsgegevens zijn openbaar gemaakt of er is toegang geweest tot persoonsgegevens. Dit is gebeurd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd.
- Inbreuk op de integriteit: persoonsgegevens zijn gewijzigd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd.
- Inbreuk op de beschikbaarheid: de organisatie waar het datalek is (geweest) kan niet meer bij de persoonsgegevens komen. Of de gegevens zijn vernietigd. Dit is gebeurd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd.

Beantwoord deze vragen:

- Wat is de oorzaak van het datalek?
- Wanneer is het datalek ontstaan? En is het datalek nog steeds gaande?
- Hoe lang na het ontstaan van het datalek is het ontdekt? En hoe is het ontdekt?
- Wat voor soort persoonsgegevens zijn gelekt? Bijvoorbeeld naam, adres, e-mailadres, creditcardgegevens en/of bijzondere persoonsgegevens.
- Hoeveel persoonsgegevens zijn er (bij benadering) gelekt? Om hoeveel personen gaat het?
- Om wat voor groepen mensen gaat het? Bijvoorbeeld klanten, werknemers, scholieren, patiënten, inwoners etc. Gaat het om kwetsbare groepen? Bijvoorbeeld kinderen, ouderen of mensen met een beperking.
- Hoeveel onbevoegden hadden of hebben bij benadering (mogelijk) toegang tot de gelekte persoonsgegevens?
- Heeft u zicht op wie die onbevoegden zijn? En is het waarschijnlijk dat de onbevoegden kwade bedoelingen hebben met de gegevens? Of gaat het om een bekende, betrouwbare ontvanger?
- Heeft uw organisatie vooraf maatregelen getroffen waardoor de gelekte persoonsgegevens (deels) ontoegankelijk zijn voor onbevoegden? Bijvoorbeeld omdat de gegevens versleuteld zijn?

Stap 2: Beperken schadelijke gevolgen datalek

Voorbeelden van maatregelen om schade bij een datalek te beperken zijn:

- Een laptop, tablet of smartphone op afstand wissen of versleutelen.
- Een gepubliceerd bestand offline halen.
- Een verkeerde ontvanger vragen om een bevestiging dat de gegevens uit een brief of e-mail zijn vernietigd. Hoewel u op basis van zo'n bevestiging niet 100% zeker weet dat de gegevens gewist zijn, kunt u het wel meenemen in uw risico-inschatting.
- De toegang tot een medewerkersaccount of clouddienst op afstand blokkeren.

- Wanneer u verplicht bent om de slachtoffers te informeren, aangeven wat zij zelf kunnen doen om de schade te beperken.

Is er sprake van een complex datalek? Bijvoorbeeld een datalek door ransomware? En heeft u geen idee wat u moet doen? Schakel dan een expert in. Bijvoorbeeld een digitaal forensisch expert.

Stap 3: Melden datalek en informeren slachtoffers

U kunt verplicht zijn om het datalek binnen 72 uur te melden bij de AP. Ook kunt u verplicht zijn om de slachtoffers onverwijld te informeren over het datalek. U beoordeelt zelf of dit het geval is.

Beoordelen risico datalek

In de Algemene verordening gegevensbescherming (AVG) staat dat u:

- Een datalek moet melden bij de AP, tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor 'de rechten en vrijheden van betrokkenen'. Zoals de bescherming van hun persoonsgegevens en persoonlijke levenssfeer.
- De slachtoffers moet informeren als een datalek waarschijnlijk een hoog risico voor hen oplevert.

U moet dus een risico-inschatting maken om te beslissen of u een datalek wel of niet meldt bij de AP en of u de slachtoffers wel of niet informeert.

Bij het bepalen van het risico van een datalek kijkt u naar de omstandigheden van het datalek. U houdt daarbij rekening met de gevolgen voor de slachtoffers en hoe waarschijnlijk het is dat die gevolgen zich voordoen.

Soms is het risico heel duidelijk. Bijvoorbeeld wanneer medische dossiers zijn gelekt. Of als persoonsgegevens zijn gestolen door een hacker. Maar vaker is het een weging van meerdere factoren.

Factoren bij risico datalek

De volgende factoren helpen u om uw afweging objectief te maken:

- de aard van de inbreuk;
- de aard en gevoeligheid van de persoonsgegevens en de hoeveelheid;
- het gemak waarmee personen kunnen worden geïdentificeerd;
- de ernst van de gevolgen voor de slachtoffers;
- kenmerken van de onbevoegde ontvanger;
- bijzondere kenmerken van de persoon;
- bijzondere kenmerken van uw organisatie;
- aantal slachtoffers.

Zie: https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/datalek-wel-of-niet-melden

Stap 4: Registreren datalek in datalekregister

Volgens de AVG bent u verplicht een datalekregister op te stellen en bij te houden. Hierin houdt u bij welke datalekken er in uw organisatie zijn geweest. In het register moet u alle datalekken

vastleggen die zich binnen uw organisatie hebben afgespeeld. Ook de datalekken die u niet aan de AP heeft gemeld.

Het doel van het datalekregister is dat u als organisatie:

- leert van eerdere datalekken en bewust bent van datalekken die in het verleden hebben plaatsgevonden;
- effectieve maatregelen neemt om de kans op nieuwe, soortgelijke datalekken te verminderen;
- met uw datalekregister aan de AP kunt laten zien dat u zich houdt aan de meldplicht datalekken.

Vorm en inhoud datalekregister

In de wet staat niet hoe een datalekregister eruit moet zien. U mag zelf bepalen welke vorm uw register heeft, zolang de wettelijk verplichte informatie erin staat. Over elk datalek moet u in ieder geval de volgende informatie vermelden:

- de feiten over het datalek, zoals de oorzaak, wat er precies is gebeurd en om welke persoonsgegeven het gaat;
- de gevolgen van het datalek;
- de corrigerende maatregelen die u heeft genomen.

Zie voorbeeld: https://www.autoriteitpersoonsgegevens.nl/documenten/voorbeeld-datalekregister

10 tips voor professionele datalekregistratie

Wilt u een datalekregister maken voor uw organisatie? Gebruik de volgende tips om de vorm en inhoud van het register zo goed mogelijk te maken.

- Omschrijf incidenten, de gevolgen ervan en de corrigerende maatregelen die u heeft genomen duidelijk en volledig.
- Maak expliciet onderscheid tussen corrigerende en preventieve maatregelen. Leg corrigerende maatregelen altijd vast in het datalekregister. Het kan nuttig zijn deze maatregelen mee te nemen in de 'plan-do-check-act'-cyclus.
- Voorkom versnippering van registraties: maak 1 overzichtelijke registratie die elk onderdeel van uw organisatie even uitgebreid invult. Overweeg bijvoorbeeld om de registratie inzichtelijk te maken voor alle medewerkers, zodat zij het overzicht kunnen checken voordat zij zelf iets registreren.
- Heeft uw organisatie een functionaris gegevensbescherming (FG)? Neem dan per incident op of de FG betrokken is en zo ja, in welke mate. In het voorbeeld datalekregister van de AP kunt u dit bijvoorbeeld vermelden onder de kolom ‘Motivering voor wel/niet melden aan AP / betrokkenen’.
- Neem per incident op of het datalek is gemeld bij de AP en aan de slachtoffers. En motiveer waarom dat wel of niet is gebeurd.
- Wees transparant naar de slachtoffers als er een datalek is geweest. Communiceer hier duidelijk en tijdig over. Bewaar het bewijs van die communicatie en neem dit op in de registratie.

- Stel een handleiding op of verzorg een training voor de medewerkers die de datalekregistratie invullen. Deze instructie kan onderdeel uitmaken van een gedocumenteerde meldingsprocedure voor de meldplicht datalekken.
- Leg vast welke andere organisaties betrokken zijn geweest bij een datalek. Bijvoorbeeld medeverwerkingsverantwoordelijken, verwerkers of subverwerkers. Dit is handig als u nieuwe verwerkersovereenkomsten sluit met deze verwerkers.
- Overweeg om de datalekken in te delen naar aard, gevolgen, slachtoffers en mogelijke maatregelen.
- Bespreek de datalekregistratie regelmatig op het juiste niveau binnen de organisatie als onderdeel van een 'plan-do-check-act'-cyclus. Zo kunt u leren van fouten. De FG of privacycontactpersoon van uw organisatie kan bij deze besprekingen een actieve rol vervullen.