Charco & Dique

E-paper

Meldplicht datalekken en AVG

Charco & Dique
020 416 54 03

charcoendique.nl
info@charcoendique.nl

Datalekken

Datalekken blijft een actueel onderwerp onder de Algemene Verordening Persoonsgegevens (AVG). Vooral de vraag wanneer een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens (AP) wordt vaak gesteld.

Het blijkt dat veel organisaties moeite hebben om te bepalen wanneer een datalek moet worden gemeld bij de AP. Om deze afweging makkelijker te maken voor organisaties heeft de AP een stappenplan en voorbeeldlijst ontwikkeld.
In de praktijk maakt de extra informatie het niet altijd overzichtelijker, waardoor de afweging om een datalek wel of niet te melden nog steeds lastig kan zijn. In deze e-paperleest u welke stappen u moet volgen bij het melden van een datalek. Ook worden een aantal praktijkvoorbeelden gegeven omtrent het wel/niet melden van een datalek bij de Autoriteit Persoonsgegevens.

Een datalek melden? Het stappenplan

Een datalek is een inbreuk op de beveiliging van persoonsgegevens. Er is niet alleen sprake van een datalek als er persoonsgegevens verloren zijn gegaan, maar ook als onrechtmatige verwerking van de persoonsgegevens ‘niet redelijkerwijs kan worden uitgesloten’. Ook als niet kan worden vastgesteld of dat daadwerkelijk is gebeurd en welke gegevens dan zijn geraadpleegd, moet de inbreuk worden beschouwd als een datalek.

Voor het melden van een datalek zijn er een aantal stappen die gevolgd moeten worden. De Autoriteit Persoonsgegevens heeft dit vastgelegd in een stappenplan. Wij lichten dit stappenplan verder voor u toe.

Stap 1: Zorg voor overzicht

Heeft uw organisatie te maken met een datalek? Dan is het belangrijk dat u direct in actie komt. Analyseer de situ-atie, zorg dat u weet wat er is gebeurd en welke gegevens zijn gelekt. Aandachtspunten hierbij zijn:

- Onderzoek of er persoonsgegevens verloren zijn ge-gaan of onrechtmatig gebruikt kunnen worden.
- Beoordeel wie of welke afdelingen binnen uw organi-satie hierbij betrokken zijn.
- Beoordeel of er een verwerker betrokken is bij het incident. Zo ja, dan moet deze persoon bij het proces betrokken worden.
- Onderzoek de aard van de gegevens die gelekt zijn. Gaat het bijvoorbeeld om gezondheidsgegevens, wachtwoorden, gegevens over financiële situaties?
- Onderzoek de omvang van de gelekte gegevens.
- Beoordeel welke impact het datalek kan hebben op de betrokken personen en wat mogelijke nadelige gevolgen kunnen zijn.

Deze informatie heeft u nodig voor de vervolgstappen.

Stap 2: Beperk de schade

Bepaal op basis van de situatie of u direct maatregelen kunt nemen om de datalek te beëindigen, of in ieder geval de schade te beperken. Tegelijkertijd kunt u ook een in-schatting maken van het mogelijke risico dat het datalek oplevert. Leg de acties van de genomen maatregelen ook direct vast in uw dossier.

Stap 3: Melden bij de AutoriteitPersoonsgegevens?

U heeft een datalek geconstateerd binnen uw maatregelenen u heeft de schade inmiddels beperkt. Moet u het datalek nu melden bij de Autoriteit Persoonsgegevens?
Op grond van de Algemene Verordening Gegevensbe-scherming (AVG) moet een datalek worden gemeld bij de AP als het ernstige nadelige gevolgen heeft voor de be-scherming van persoonsgegevens. Ook als een datalek leidt tot ‘een aanzienlijke kans’ op ernstige nadelige ge- volgen voor de bescherming van persoonsgegevens is eenmelding verplicht.

Indien dit het geval is, zorg dat u zo snel mogelijk, maar uiterlijk binnen 72 uur na de ontdekking het datalek meldtbij het meldloket datalekken van de AP. Wanneer bijvoor-beeld alleen de adresgegevens zijn gelekt van een kleine groep personen, dan is het onwaarschijnlijk dat er sprake is van een hoog risico.

Stap 4: Melden aan de betrokken personen?

U heeft bepaald of het datalek moet gemeld worden bij de AP. Nu moet u bepalen of het datalek gemeld moet worden aan de betrokken personen. Een datalek dient opgrond van de AVG te worden gemeld aan de betrokkenen als het datalek waarschijnlijk ongunstige gevolgen heeftvoor diens persoonlijke levenssfeer. Denk bijvoorbeeld
aan het op straat liggen van gevoelige gegevens (lidmaat-schap van een datingservice bij een getrouwde dominee), verhoogde kans op chantage, mogelijke identiteitsfraude, onrechtmatige publicatie of discriminatie.

Als criterium wordt gehanteerd ‘het risico voor de rechten en vrijheden van betrokkenen’. Indien dat risico als ‘hoog’ wordt ingeschat moet het datalek ook worden gemeld aan betrokkenen.

Stap 5: Registreer het datalek

Dit betreft de verplichting ieder datalek, maar in feite ieder data incident te registreren in een eigen incident register, ook al is het niet gemeld aan de AP of betrokkenen.

Het maakt nog eens duidelijk hoe de Autoriteit Persoonsgegevens wil omgaan met datalekken. Niet alleen de gemelde datalekken verdienen uw aandacht, maar ook (en misschien nog wel meer) de niet gemelde datalekken of data-gerelateerde incidenten. De AP zal bij eventuele bezoeken aan organisaties vragen naar het incidenten- register en alle incidenten (lek of geen lek) langs de eigen meetlat leggen.

10 tips voor het registreren van datalekken

Voor het registreren van datalekken heeft de AP 10 tips geformuleerd die handvatten kunnen bieden bij het vastleggen van een datalek.

1. Omschrijf duidelijk en volledig het incident dat zich heeft voorgedaan, wat de gevolgen zijn en welke maatregelen getroffen zijn;
2. Maak in het vastleggen van maatregelen onderscheid tussen corrigerende en preventieve maatregelen. Leg de corrigerende maatregelen ook vast in het datalekregister;
3. Het maken van één overzichtelijk (data) incidenten-register per organisatieonderdeel voorkomt versnippering van registraties;
4. Neem per incident op in welke mate de privacy officer betrokken is geweest;
5. Neem per incident op of het gemeld is bij de AP. Motiveer ook waarom een incident wel of niet gemeld is;
6. Duidelijke en tijdige communicatie over een datalek bevordert de transparantie richting bij de datalek betrokken personen. Leg deze communicatie ook vast;
7. Biedt een handleiding en trainingen aan voor de medewerkers die datalekken melden;
8. Leg bij de registratie van een datalek ook vast of er andere organisaties betrokken zijn. Denk daarbij aan medeverwerkingsverantwoordelijke, verwerkers of subverwerkers;
9. Overweeg om incidenten in het register in te delen naar aard, gevolgen en betrokkenen en mogelijke maatregelen;
10. Bespreek datalekken regelmatig met de directie en/of privacy officer. Zo kan de organisatie leren van in het verleden gemaakte fouten.

Wel of niet melden van een datalek, een aantal voorbeelden

In de praktijk blijkt dat het voor veel organisaties nog onduidelijk is wanneer een datalek gemeld moet worden. Om die meetlat te verduidelijken heeft de AP ook een 'Voorbeeldlijst wel/niet melden' ontwikkeld. De voorbeeldlijst geeft, zoals de naam al aangeeft, een aantal praktijkvoorbeelden met daarbij het AP omtrent wel/niet melden. Het lijkt een praktische lijst, maar bij een aantal voorbeelden wordt het - met name door de toelichting - niet duidelijker. Een aantal voorbeelden wordt hieronder toegelicht.

Voorbeeld 1: Wat is leidend bij eendatalek: risico of gevolg?

Bij het relatief simpele voorbeeld van een online dienst waar persoonsgegevens worden 'geëxtraheerd' lijken risico en gevolg door elkaar te worden gehaald.

Het criterium voor wel of niet melden aan de AP en betrokkenen is: het risico voor de rechten en vrijheden van betrokkenen. Wanneer dit risico als "hoog" wordt ingeschat moet het datalek ook worden gemeld aan betrokkenen. In de toelichting bij het voorbeeld geeft de AP echter het advies:

- Te melden bij de AP als er waarschijnlijk gevolgen zijn;
- Te melden aan betrokkenen als 'die waarschijnlijke gevolgen voor personen zeer ernstig zijn'.

Waar het voorbeeld scheef lijkt te gaan is in datalek situaties waar het risico heel erg klein is, maar als een datalek plaatsvindt de gevolgen heel ernstig zijn. Kiest u dan als bedrijf voor het zeer kleine risico (niet melden) of voor de zeer grote impact (wel melden). Bij die afweging moet risico en impact zo veel mogelijk zoveel mogelijk worden gescheiden. Bijvoorbeeld:

- Een onderneming is op twee momenten twee bestanden met een tussenpoos van zes maanden kwijtgeraakt.
- Er zijn geen aanwijzingen dat beide incidenten met elkaar te maken hebben.
- Los van elkaar is de informatie op bestanden niet herleidbaar tot betrokken personen.
- Gecombineerd bevatten de bestanden wel herleidbare informatie die schadelijk kan zijn voor de betrokkenen (Bestand 1: gebruikersnamen van een dating site met chathistorie; Bestand 2: gebruikersnamen met gekoppelde email adressen)

Het risico dat de gelekte bestanden bij elkaar gebracht worden lijkt heel erg klein, maar als het gebeurt is de herleidbaarheid relatief groot. Charco & Dique adviseert op basis van de impact om deze incidenten te melden bij de AP.

Voorbeeld 2: Datalek: Persoons-gegevens naar de verkeerde klantgestuurd

De meerderheid (63%) van datalekken bestaat uit het via de post of e-mail versturen van persoonsgegevens van de ene klant naar de andere klant. De AP geeft het volgende voorbeeld:

"Een persoon belt naar het callcenter van een bank om een inbreuk in verband met persoonsgegevens te melden. De persoon heeft een maandoverzicht van iemand anders ontvangen. De verwerkingsverantwoordelijke voert een kort onderzoek uit (het onderzoek wordt binnen de 24 uur afgerond) en stelt met een redelijke mate van zekerheid vast dat er zich een inbreuk in verband met persoonsgegevens heeft voorgedaan. Hij vraagt zich af of er ergens een systeemstoring voordoet, in welk geval dit mogelijk gevolgen heeft gehad of zou kunnen hebben voor andere personen".

De expliciete vermelding dat het onderzoek binnen 24 uur wordt afgerond is bijzonder, gezien de 72 uurs termijn die geldt voor het melden van een datalek. Het advies is hier het datalek te melden aan de AP, wat bij een maandoverzicht van een bank logisch lijkt. Echter, in de toelichting valt ook te lezen dat er pas gemeld moet worden als meer personen betrokken zijn. Of 'meer' hier betekent: bij één persoon hoeft u het datalek niet te melden, maar bij twee of duizend personen wel, wordt niet duidelijk gemaakt.

Voor de melding aan betrokkenen waagt de AP zich niet aan een advies. Wel wordt een toelichting gegeven:

"De inbreuk wordt alleen meegedeeld aan de getroffen personen als er een hoog risico is en het duidelijk is dat anderen niet zijn getroffen".

Strikt genomen zegt de AP hier dat gemeld moet worden als er één persoon betrokken is. Als er sprake is van meerdere betrokkenen zou het niet gemeld hoeven te worden. Charco & Dique adviseert u in dit soort gevallen de klant wel te informeren. Iedere klant, ook al is het er maar één, die potentieel een groot risico loopt moet worden gewaarschuwd zodat actie ondernomen kan worden om de schade te voorkomen of te beperken.

Omvang groep betrokkenen

Bij het laatste voorbeeld waarbij persoonsgegevens naar de verkeerde ontvangers worden gestuurd, gaat het ook om de omvang van de groep betrokkenen. Hierbij wordt expliciet het aantal genoemd: meer dan duizend. Dat wekt de suggestie dat er een omvangscriterium moet worden gehanteerd voor melding aan de AP, los van de inhoud van het datalek. Op zich prima dat een duidelijke instructie wordt gegeven, ook al is het omvangscriterium niet echt gebaseerd op de AVG. Het lijkt logisch dat de AP in ieder geval over grote datalekken geïnformeerd wil worden, ook al is het risico voor betrokkenen niet groot.

Echter in de toelichting van het laatste voorbeeld, wordthet omvangscriterium weer minder duidelijk gemaakt.

Mogelijk dient de inbreuk niet te worden gemeld/mee-gedeeld als geen gevoelige gegevens zijn onthuld en als slechts een klein aantal e-mailadressen is onthuld.

Een ‘klein aantal’ is een relatief begrip. Charco & Dique adviseert om de omvang van het datalek minder zwaar mee te wegen dan de risico’s voor de klant.

Conclusie

Het wel of niet melden van een datalek blijft een lastige afweging. Het stappenplan en de voorbeeldlijst van de Autoriteit Persoonsgegevens geeft op een aantal punten meer houvast, maar zorgt tegelijkertijd ook voor meer on-duidelijkheid. Het zou helpen als er meer concrete criteria zouden worden geformuleerd, echter is het de vraag of dat zal gebeuren. Uiteindelijk wordt er een beroep gedaan op uw professional judgement en - misschien nog wel belangrijker - op een juiste waardering van het belang van uw klanten.

Hoe kan Charco & Dique u helpen?

Wilt u advies bij de afweging van het wel of niet melden van uw datalek? Neem dan contact met ons op. Onze specialisten denken graag met u mee.

Neem contact op →

Charco & Dique
020 416 54 03

charcoendique.nl
info@charcoendique.nl