ORTHOVENTIEF
uw partner voor onderwijskwaliteit

Versiedatum: 15-3-2018

Procedure datalekken Orthoventief en CIS-Websolutions 2018

Stap 1: Is dit een datalek?

De eerste stap van de procedure datalekken is het definiëren van het begrip datalek. Er wordt gesproken over een datalek wanneer persoonsgegevens verloren raken of onrechtmatige verwerking redelijkerwijs niet kan worden uitgesloten. Onder onrechtmatige verwerking wordt verstaan het aanpassen en/of veranderen van persoonsgegevens en een onbevoegde toegang geeft tot deze gegevens. Een datalek omvat veel meer dan alleen een hacker of malware die toegang krijgt tot persoonsgegevens. Voorbeelden van een datalek zijn:

- een ransomware (cryptolocker) die data versleutelt
- het verliezen van een USB-stick
- het sturen van een mailing met adressen in het CC-veld
- verlies van gegevens als gevolg van een brand in het datacentrum terwijl er geen back-up beschikbaar is

Stap 2: Datalek melden aan de Autoriteit Persoonsgegevens (AP)?

Niet elk datalek hoeft gemeld te worden. De wet bepaalt dat alleen ‘ernstige’ datalekken na ontdekking binnen 72 uur gemeld moeten worden bij de toezichthouder. Daarbij maakt het niet uit of het datalek veroorzaakt is door een fout of overmacht. Een lek kan ernstig zijn als het een grote hoeveelheid data betreft (kwantitatief ernstig) maar ook als het om gevoelige gegevens gaat (kwalitatief ernstig). Voorbeelden van deze gevoelige gegevens zijn:

- inloggegevens
- burgerservicenummer
- financiële gegevens
- kopieën van identiteits- en rijbewijzen
- school- of werkprestaties
- medische dossiers
- gegevens die betrekking hebben op levensovertuiging

Het betreft geen datalek wanneer het gaat om andere gegevens dan persoonsgegevens.

Een aantal voorbeelden zijn:

- broncode van software
- bedrijfsnamen uit uw relatiebeheerpakket

Stap 3: Datalek melden aan betrokken personen?

Wanneer een datalek een ongunstig gevolg heeft voor de privé levens van de personen in kwestie dient u niet alleen een melding te doen aan de toezichthouder maar zult u ook melding moeten doen aan de personen waarvan de gegevens zijn gelekt. Dit zullen in de meeste gevallen klanten van u zijn.

Ongunstige gevolgen zijn bijvoorbeeld:

- identiteitsfraude
- discriminatie
- reputatieschade

Wanneer (kwalitatief ernstige) persoonsgegevens zijn gelekt dient u dit altijd te melden aan de getroffen personen. U hoeft geen melding te doen aan betrokken personen als gegevens onleesbaar zijn door versleuteling of wanneer u gegevens op afstand kunt wissen van bijvoorbeeld een gestolen laptop. Daarbij moet u wel zeker weten dat niemand deze gegevens heeft ingezien, hiervoor draagt u bewijslast. De beoordeling of een datalek gemeld moet worden aan de toezichthouder en betrokken personen ligt altijd bij u. Dit betekent ook dat u bij een verkeerde beslissing op de vingers kan worden getikt door de toezichthouder.

Stap 4: Hoe een datalek melden?

Een datalek kunt u melden bij de toezichthouder door het invullen van het volgende formulier, Meldloket datalekken (https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0) . Dit formulier zal vervolgens opgeslagen worden in een niet-openbaar register van de toezichthouder. Een datalek wordt openbaar zodra er een boete wordt opgelegd of wanneer de getroffen persoon wordt geïnformeerd.

Stap 5: Welke informatie bewaren bij een datalek?

Als u een melding gaat maken van een datalek zult u bewijs moeten hebben. Het bewijs zijn feiten zoals de oorzaak van het lek, soort gegevens die gelekt zijn, het moment dat het lek is ontdekt en op welke wijze het lek gedicht is. Mocht u contact hebben gehad met de getroffen personen over het datalek, bewaar deze communicatie in uw administratie. Voor het bewaren van de genoemde gegevens dient u uit te gaan van een minimale bewaartermijn van één jaar.

Stap 6: Moet uw bewerker (een derde partij) het datalek melden?

Wat is een bewerker? Een bewerker is volgens de wet een derde partij. Een bewerker kan uw cloud dienstverlener zijn die updates uitvoert op software, opslag van uw data verzorgt of het marketingbedrijf dat e-mails in opdracht van u verzendt. Een bewerker moet zorg dragen dat u als klant vroegtijdig een melding kan doen bij de toezichthouder. Dit houdt in dat de bewerker geen datalek hoeft te melden maar u dat moet doen. Er zullen dus schriftelijke afspraken gemaakt moeten worden waarin wordt vastgelegd op welke wijze u door de bewerker op de hoogte wilt worden vastgelegd van een datalek. Deze afspraken kunnen worden opgenomen in een bewerkersovereenkomst.

Stap 7: Voorbereiding op de meldplicht

- Breng in kaart wie uw gegevens verwerkt en of met deze partij(en) een bewerkersovereenkomst is gesloten.
- Stel met iedere partij waarmee u samenwerkt een NDA (Non Disclosure Agreement) op waarin u persoonsgegevens benoemt.
- Controleer hoe de bedrijven die voor u persoonsgegevens verwerken deze opslaan. Gebeurt dit veilig? Controleer dit uiteraard ook binnen uw eigen bedrijf.
- Als bedrijven aangeven gecertificeerd te zijn (bijvoorbeeld ISO 27001), vraag dan naar de voorwaarden van deze certificering.
- Overleg met uw verzekeraar of verzekeringstussenpersoon of u verzekerd bent tegen het lekken van persoonsgegevens (een cyberrisico verzekering).
- Hanteer intern een procedure voor de omgang met en melding van datalekken.

Melding datalek vanuit Orthoventief of CIS-websolutions

Indien zich een meldingsplichtig datalek heeft voorgedaan als gevolg van een oorzaak die valt onder de directe verantwoordelijkheid van de (sub)verwerker, dan worden in ieder geval zo spoedig mogelijk, maar uiterlijk binnen 24 uur de volgende gegevens gedeeld met de verantwoordelijke:

- De kenmerken van het incident, zoals: datum en tijdstip constatering, samenvatting incident, kenmerk en aard incident (op wat voor onderdeel van de beveiliging ziet het, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van persoonsgegevens);
- De oorzaak van het beveiligingsincident;
- De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;
- Benoemen van betrokkenen die gevolgen kunnen ondervinden van het incident, en de mate waarin;
- De omvang van de groep betrokkenen;
- Het soort gegevens dat door het incident wordt getroffen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).

Procedure datalekken

Bekijk eenvoudig of u een melding moet doen aan de toezichthouder.