Impact van de meldplicht datalekken

Vanaf 1 januari 2016 wordt het wettelijk verplicht om datalekken te melden. Zowel grootschalige inbraak als ieder kwijtraken, diefstal of onbevoegd gebruik van persoonsgegevens telt als een datalek. En dat is nog niet alles. Wie data laat lekken of persoonsgegevens verwerkt zonder zich netjes aan de wet te houden, loopt kans op boetes die kunnen oplopen tot € 810.000,- of 10% van de jaaromzet per overtreding. Wat betekent dit voor uw bedrijf? ICTRecht en Thuiswinkel.org geven in deze factsheet alle informatie. Op de laatste pagina vindt u en handige beslisboom.

1. Wat is een datalek?

De wet spreekt van een datalek wanneer persoonsgegevens verloren raken of onrechtmatig worden verwerkt.
Onder onrechtmatige verwerking valt onder andere het aanpassen en/of veranderen van persoonsgegevens en onbevoegde toegang tot, of afgifte daarvan. Kortom: een vrij brede definitie. Er is dus niet alleen sprake van een datalek als een hacker toegang tot persoonsgegevens krijgt. Ook verlies van een USB-stick in de trein, of het sturen van een mailing met adressen in het CC-veld (in plaats van het BCC-veld) telt al als datalek. En zelfs verlies van gegevens zoals bij een brand in het datacentrum terwijl er geen back up beschikbaar is, ziet de wet als een datalek.

U dient als bedrijf preventief de juiste beveiligingsmaatregelen te nemen om datalekken te voorkomen. Dit kan bijvoorbeeld door gebruik te maken van encryptietechnieken.

Lekken waarbij andere gegevens dan persoonsgegevens verloren zijn geraakt of gestolen worden, zijn geen datalekken. Als de broncode van uw nieuwe software wordt ontvreemd, of een lijst met bedrijfsnamen uit uw relatiebeheerpakket wordt gekopieerd, dan valt dat bijvoorbeeld buiten deze wet.

2. Wanneer moet u een datalek melden aan de toezichthouder?

Niet elk datalek moet worden gemeld. De wet bepaalt dat ‘ernstige’ datalekken binnen twee werkdagen bij de toezichthouder gemeld moeten worden. Een lek kan ernstig zijn als het een grote hoeveelheid data betreft (kwantitatief ernstig), maar ook als het om gevoelige gegevens gaat (kwalitatief ernstig). Een paar voorbeelden uit de tweede categorie:

- inloggegevens;
- financiële gegevens;
- kopieën van identiteitsbewijzen;
- school- of werkprestaties;
- gegevens die betrekking hebben op levensovertuiging;
- gegevens die betrekking hebben op gezondheid.

3. Wanneer moet u een datalek melden aan de getroffen personen?

Indien het datalek waarschijnlijk ongunstige gevolgen heeft voor het privéleven van de personen van wie de gegevens gelekt zijn, dient u - naast de melding aan de toezichthouder - het lek tevens binnen twee werkdagen te melden aan de personen waarvan de gegevens zijn gelekt. Dit zullen in de meeste gevallen klanten zijn. Ongunstige gevolgen zijn bijvoorbeeld:

- identiteitsfraude;
- discriminatie;
- reputatieschade;
- misbruik van inloggegevens.

Wanneer kwantitatief ernstige gegevens (zie vorige vraag) zijn gelekt, is eigenlijk altijd sprake van een ongunstig gevolg. Dit moet dus ook altijd worden gemeld aan de getroffen personen.

4. Wanneer hoeft u een datalek niet te melden?

Een datalek dat aan het criterium van vraag 2 voldoet, moet u altijd melden aan de toezichthouder. Daarbij doet het er niet toe of het datalek door een fout kwam of het gevolg was van overmacht.

Een datalek hoeft echter niet aan de getroffen personen gemeld te worden wanneer de gelekte persoonsgegevens onleesbaar zijn. Hiervan is bijvoorbeeld sprake wanneer de persoonsgegevens versleuteld zijn of wanneer u de gegevens op afstand kunt verwijderen van bijvoorbeeld een gestolen laptop. U moet er dan wel zeker van zijn dat niemand de gegevens heeft kunnen inzien. U draagt hiervoor de bewijslast.

De beoordeling of een datalek gemeld moet worden aan de toezichthouder en/of de getroffen personen, ligt te allen tijde bij u. Echter, maakt u een onjuiste inschatting dat er geen melding nodig is, dan kunt u dáár ook voor op de vingers getikt worden.

5. Hoe dient u een datalek te melden?

De toezichthouder zal een standaardformulier beschikbaar stellen voor het melden van een datalek. Bij een datalek moet dus dit formulier ingevuld worden. Dit formulier zal vervolgens opgeslagen worden in een register van de toezichthouder, dat niet openbaar is. Mocht er naar aanleiding van het lek een boete opgelegd worden, dan zal dit besluit wel openbaar zijn. Een datalek wordt vanzelfsprekend ook openbaar op het moment waarop het aan de getroffen personen wordt medegedeeld.

6. Welke informatie moet u over een datalek bewaren?

Wanneer u een datalek aan de toezichthouder meldt, dient u een overzicht hiervan in uw administratie te bewaren. Dit overzicht moet de feiten en gegevens van het lek bevatten. Denk hierbij aan de oorzaak van het lek, de soort gegevens die gelekt zijn, het moment dat het lek is ontdekt en op welke wijze het lek gedicht is. Als u het datalek ook aan de getroffen personen heeft gemeld, is het belangrijk de communicatie hierover te bewaren. Voor het bewaren van de voornoemde gegevens dient u uit te gaan van een minimale bewaartermijn van één jaar. Maak hierover ook afspraken met de bewerker, zie hiervoor vraag 8.

7. Wat zijn de gevolgen van de wet?

De wet kent vanaf 1 januari 2016 de mogelijkheid om boetes op te leggen wanneer niet voldaan wordt aan de wet. Deze boetes kunnen onder meer opgelegd worden voor:

- het niet melden van een datalek terwijl dat wel moet;
- het niet op orde hebben van de beveiliging;
- het verwerken van persoonsgegevens zonder toestemming;
- export van persoonsgegevens naar landen buiten de EU zonder dat goed geregeld te hebben.

De boete kan oplopen tot € 810.000,- of 10% van de jaaromzet. Vaak zal er eerst een waarschuwing gegeven worden, maar de toezichthouder mag besluiten direct een boete op te leggen als u opzettelijk of grof nalatig heeft gehandeld.

8. Moet een bewerker datalekken melden?

In veel gevallen wordt het verwerken van persoonsgegevens uitbesteed aan een derde partij. Deze derde partij noemt de wet een bewerker. Data kan bijvoorbeeld toegankelijk zijn voor een clouddienstverlener die updates uitvoert op software, opgeslagen staan bij een hostingprovider, of beschikbaar zijn voor het marketing bedrijf dat e-mails in opdracht van klanten verzendt.

Een bewerker hoeft een datalek niet te melden bij de toezichthouder. Wel moet de bewerker er zorg voor dragen dat haar klanten deze melding tijdig bij de toezichthouder kunnen maken. Er zullen daarom schriftelijke afspraken moeten worden gemaakt waarin wordt vastgelegd op welke wijze de klanten door de bewerker op de hoogte worden gesteld van een datalek. Deze afspraken kunnen worden opgenomen in een bewerkersovereenkomst.

Let op: bent u bewerker en zijn bij een datalek ook gegevens met betrekking tot uw eigen klantadministratie gelekt, dan zult u ook zelf een melding van het lek moeten maken. U bent daar dan immers zelf verantwoordelijk voor.

9. Wat kunt u doen ter voorbereiding op de meldplicht?

Goed voorbereid zijn op de meldplicht datalekken? Onderneem dan de volgende acties:

- Verklein het risico op een datalek. Denk aan minimalisatie en encryptie van persoonsgegevens, voer regelmatig securitychecks uit op operating systemen, netwerken en applicaties;
- Werk volgens het Security by Design principe en zorg dat alle systemen, netwerken en applicaties up to date zijn;
- Inventariseer wie uw gegevens verwerken en of met deze partijen een bewerkersovereenkomst is gesloten;
- Update uw bewerkersovereenkomsten met een bepaling omtrent datalekken;
- Sluit met iedere partij waarmee u samenwerkt een NDA (Non Disclosure Agreement) waarin u persoonsgegevens benoemt;
- Controleer hoe de bedrijven die voor u persoonsgegevens verwerken persoonsgegevens opslaan. Gebeurt dit veilig? Controleer dit uiteraard ook binnen uw eigen bedrijf;
- Als bedrijven zeggen gecertificeerd te zijn (bijvoorbeeld ISO 27001), vraag dan naar de scope van deze certificering;
- Ga na bij 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.

10. Procedure meldplicht datalekken

Zijn er gegevens gelekt en wilt u snel en overzichtelijk zien wat de procedure voor het melden van een datalek is? Zie de volgende pagina voor de beslisboom voor het melden van datalekken.

11. Vragen?

Komt u er niet uit of een datalek gemeld moet worden, heeft u vragen over hoe u afspraken met derde partijen moet regelen of heeft u hulp nodig bij het opstellen van een interne procedure voor het melden van een datalek? Neem dan contact met ICTRecht op via 020 66 31 941 of info@ictrecht.nl en vraag naar onze privacyspecialisten.


1. Zijn de gegevens die zijn gelekt aan te merken als persoonsgegevens?
Voorbeelden: namen, klantnummers, klantprofielen, (e-mail)adressen.
Ja
Nee
U hoeft geen melding te doen.
2. Zijn het uw 'eigen' klantgegevens die gelekt zijn?
Voorbeelden: de gegevens die een hoster opslaat, of waar een clouddienstverlener toegang tot heeft, zijn gegevens van hun klanten en geen 'eigen' gegevens . Deze partijen worden aangemerkt als bewerker.
Ja
Nee
U moet het lek melden aan uw klanten.
3. Zijn er persoonsgegevens verloren geraakt of onrechtmatig verwerkt?
Voorbeelden: een verloren laptop, een hack, brand in een datacentrum of een oud-werknemer met toegang tot persoonsgegevens. Neem bij twijfel contact met ons op.
Ja
Nee
U hoeft geen melding te doen.
4. Zijn een groot aantal (kwantitatief) of gevoelige persoonsgegevens (kwalitatief) gelekt?
Voorbeelden: meer dan duizend persoonsgegevens of gegevens zoals bankrekeningnummers, inloggegevens, gegevens omtrent gezondheid. Neem bij twijfel contact met ons op.
Ja
Nee
U hoeft geen melding te doen.
5. U moet de toezichthouder uiterlijk op de tweede werkdag na het ontdekken van het datalek in kennis stellen van het datalek.
Ja
6. Heeft het datalek waarschijnlijk ongunstige gevolgen voor het privéleven van personen?
Hiervan is bijvoorbeeld sprake wanneer er gevoelige persoonsgegevens zijn gelekt of als er een gevaar is voor identiteitsfraude. Neem bij twijfel contact met ons op.
Nee
U hoeft alleen een melding te doen aan de toezichthouder.
Ja
7. Zijn de gelekte persoonsgegevens op een manier beveiligd zodat ze niet gelezen of gebruikt kunnen worden?
Hiervan is bijvoorbeeld sprake wanneer er een goede encryptie is gebruikt. Neem bij twijfel contact met ons op.
Nee
U moet naast de toezichthouder ook de getroffen personen in kennis stellen van het datalek.
Ja
8. Is de manier waarop de encryptie ongedaan gemaakt kan worden ook gelekt?
Ja
Nee
9. U moet naast de toezichthouder ook de getroffen personen in kennis stellen van het datalek.
U hoeft alleen een melding te doen aan de toezichthouder.

ICTRECHT