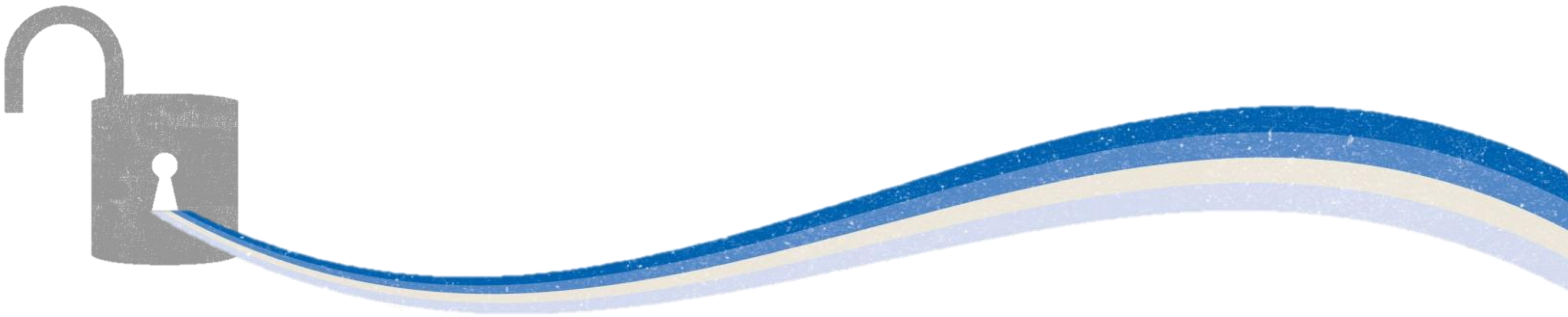
# Impact van de meldplicht datalekken



Verwerkt u persoonsgegevens niet in overeenstemming met de Wet bescherming persoonsgegevens (Wbp) of lekt u data, dan loopt u sinds 1 januari het risico op boetes die kunnen oplopen tot 820.000 euro of 10 procent van de jaaromzet per overtreding.

## 1. Wat is een datalek?

De wet spreekt van een datalek wanneer persoonsgegevens verloren raken of onrechtmatige verwerking redelijkerwijs niet kan worden uitgesloten.

Persoonsgegevens zijn gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, andere gegevens vallen niet onder de Wbp.

Onder onrechtmatige verwerking valt onder andere het aanpassen en/of veranderen van persoonsgegevens en onbevoegde toegang tot, of afgifte daarvan. Dus niet alleen het door een hacker verkrijgen van toegang tot persoonsgegevens, maar 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).

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

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

Niet elk datalek hoeft te worden gemeld. De wet bepaalt dat 'ernstige' datalekken zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking, 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 (bijvoorbeeld identiteitsfraude, reputatieschade of discriminatie), of wanneer kwalitatief ernstige gegevens (zie vorige vraag) zijn gelekt dient u - naast de melding aan de toezichthouder - het lek tevens onverwijld te melden aan de personen waarvan de gegevens zijn gelekt.

## 4. Wanneer hoeft u een datalek niet te melden?

Een datalek hoeft niet gemeld te worden wanneer de gelekte persoonsgegevens onleesbaar zijn (encryptie) of wanneer u de gegevens op afstand heeft verwijderd van bijvoorbeeld een gestolen laptop voordat een derde daar bij kon. 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. Wat zijn de boeterisico's?

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 zonder toestemming of een andere in de Wbp genoemde grondslag verwerken van persoonsgegevens
- het niet melden van een datalek terwijl dat wel moet;
- het niet op orde hebben van de beveiliging op de in de Wbp bedoelde wijze;
- export van persoonsgegevens naar landen buiten de EU zonder dat goed geregeld te hebben.

De boete kan oplopen tot 820.000 euro of 10 procent 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.

## 6. Wie moet melden als er een derde partij betrokken is bij de verwerking?

Als u persoonsgegevens laat verwerken door een derde partij (een 'bewerker', bijvoorbeeld een cloud-dienstverlener, salarisadministrateur, marketingbedrijf), blijft u zelf verantwoordelijk voor het melden van een datalek, ook als dat bij de bewerker plaatsvindt. U moet daarom in een bewerkersovereenkomst afspreken dat u door de bewerker op de hoogte wordt gesteld van een datalek. Een bewerker moet wel zelf melden als persoonsgegevens worden gelekt waarvoor hij zelf verantwoordelijk is, zoals zijn eigen klantadministratie.

## 7. Wat kunt u doen ter voorbereiding op de meldplicht?

Wilt u goed voorbereid zijn op de meldplicht datalekken? Onderneem dan de volgende acties:

- 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; instrueer uw werknemers;
- zorg dat u voldoet aan de regels inzake het inzagerecht, correctierecht en recht van verzet van degenen wiens persoonsgegevens worden verwerkt.

## Interne gedragscode?

Stelt u een interne gedragscode voor het personeel op? Doe dat dan bij voorkeur als aanvulling op de arbeidsovereenkomst en laat dit door de medewerkers ondertekenen. Denk ook aan het opnemen van een geheim-houdingsbeding in de arbeidsovereenkomst. Wanneer er een OR is ingesteld, heeft deze instemmingsrecht op de regeling over zaken die de privacy van werknemers raken, zoals de verwerking van personeelsgegevens.

**Contact**
Neem voor vragen contact op met één van de juristen van Grant Thornton.

**Tessa Viragh**
T 088 676 97 25
E tessa.viragh@nl.gt.com

**www.grantthornton.nl**