Protocol meldplicht datalekken[1]

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties die een ernstig datalek hebben, dit direct moeten melden bij de Autoriteit Persoonsgegevens. In sommige gevallen moeten zij dit tevens melden aan de mensen van wie de persoonsgegevens zijn gelekt. Maar wanneer spreekt men van een datalek en wanneer moet u dit wel, of niet melden? Om hierover duidelijkheid te verschaffen, hebben wij dit Protocol voor u opgesteld.

Wat is een datalek?

Bij een datalek is sprake van een inbreuk op de beveiliging van persoonsgegevens waarbij deze zijn blootgesteld aan verlies of onrechtmatige verwerking ervan. Denk hierbij aan een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop, een inbraak in een databestand door een hacker of het ten onrechte verstrekken van persoonsgegevens aan derden.

Meldplicht

Mocht u een datalek constateren in uw organisatie of vermoeden dat hiervan sprake is, dan kunt u aan de hand van de volgende zeven vragen bepalen of u dit moet melden bij de Autoriteit Persoonsgegevens en de betrokkenen.

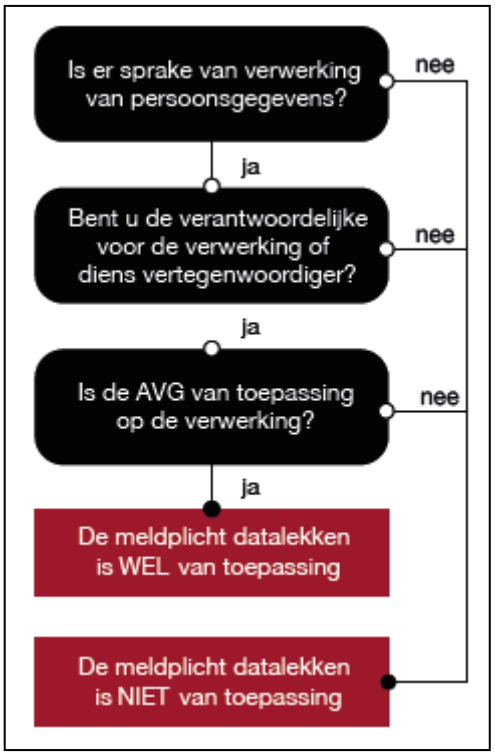
1. Is de meldplicht datalekken uit de Algemene Verordening Gegevensbescherming van toepassing?
2. Is een gebeurtenis te beschouwen als een datalek?
3. Moet het datalek worden gemeld aan de Autoriteit Persoonsgegevens?
4. Hoe en wanneer moet het datalek worden gemeld aan de Autoriteit Persoonsgegevens?
5. Moet het datalek ook worden gemeld aan de betrokkene, dat is degene van wie de persoonsgegevens zijn gelekt?
6. Hoe en wanneer moet het datalek worden gemeld aan de betrokkene?
7. Welke gegevens moeten worden vastgelegd?

Deze vragen worden in dit protocol verder toegelicht. Aan het slot van dit protocol volgen enkele algemene aanbevelingen.

[1] Op basis van modelprotocol van Edventure met kenmerk 160235/dec2017AVG

1. Is de meldplicht datalekken uit de Algemene Verordening Gegevensbescherming (AVG) van toepassing?

<u>Dat is het geval indien:</u>



- sprake is van verwerking van persoonsgegevens (elk gegeven betreffende een geïdentificeerde of identificeerbare persoon, zoals NAW-gegevens, IP- adressen en foto's). Verwerking van persoonsgegevens betreft elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, zoals het verzamelen, vastleggen, ordenen, raadplegen en verspreiden.
- u de verwerkingsverantwoordelijke – degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking vaststelt – of diens vertegenwoordiger bent. Als u bij de verwerking derden inschakelt, blijft u ter zake de meldplicht de eindverantwoordelijke.
- de AVG op de verwerking van toepassing is. Bepaalde verwerkingen vallen door hun aard of hun doelstelling buiten de reikwijdte van de AVG, bijvoorbeeld verwerkingen ten behoeve van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden. Op de verwerking van persoonsgegevens voor uitsluitend journalistieke, artistieke of literaire doeleinden is de AVG gedeeltelijk van toepassing maar de meldplicht datalekken niet. Daarnaast is van belang waar de activiteiten plaatsvinden waarvoor de persoonsgegevens worden verwerkt en waar de al dan niet geautomatiseerde middelen zich bevinden die bij de verwerking worden gebruikt (in een ander land).

2. Is een gebeurtenis te beschouwen als een datalek?

<u>Dat is het geval indien:</u>

- sprake is van een inbreuk op de beveiliging, dat wil zeggen dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan, en
- bij de inbreuk persoonsgegevens verloren zijn gegaan of redelijkerwijs niet kan worden uitgesloten dat er persoonsgegevens onrechtmatig zijn verwerkt, waaronder moet worden begrepen de aantasting van de persoonsgegevens, onbevoegde kennisneming, wijziging of verstrekking daarvan.

3. Moet het datalek worden gemeld aan de Autoriteit Persoonsgegevens?

Een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens indien sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Dat is het geval indien één van de volgende situaties aan de orde is:

- Persoonsgegevens van gevoelige aard zijn gelekt, namelijk:
    - bijzondere persoonsgegevens zoals bedoeld in artikel 9 AVG:
        - betreffende iemands levensovertuiging of godsdienst, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging
        - strafrechtelijke persoonsgegevens en
        - persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag, of
    - persoonsgegevens die anderszins van gevoelige aard zijn, waaronder:
        - gegevens over de financiële of economische situatie van de betrokkene;
        - gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;

- gebruikersnamen, wachtwoorden en andere inloggegevens;
- gegevens die kunnen worden misbruikt voor (identiteits-)fraude;
- gegevens uit DNA-databanken, gegevens waar een bijzondere, wettelijk bepaalde geheimhoudingsplicht op rust en gegevens die onder een beroepsgeheim vallen.

- De aard en omvang van de inbreuk leiden tot (een aanzienlijke kans op) ernstige nadelige gevolgen. Hierbij is van belang:
  - gaat het om veel persoonsgegevens per persoon of om gegevens van grote groepen?
  - zijn de beslissingen die o.b.v. de verwerkte persoonsgegevens worden genomen ingrijpend?
  - worden de persoonsgegevens binnen ketens (zoals binnen de overheid) gedeeld?
  - gaat het om persoonsgegevens van kwetsbare groepen?

4. Hoe en wanneer moet het datalek worden gemeld aan de Autoriteit Persoonsgegevens?

De Autoriteit Persoonsgegevens stelt voor de melding een webformulier beschikbaar. Het datalek moet onverwijld worden gemeld. Dit houdt in dat de verwerkingsverantwoordelijke, na het ontdekken van een mogelijk datalek, enige tijd mag nemen voor nader onderzoek teneinde een onnodige melding te voorkomen. De termijn voor het melden begint te lopen op het moment dat de verwerkingsverantwoordelijke of een verwerker op de hoogte raakt van een incident dat mogelijk onder de meldplicht datalekken valt. Zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking, moet een melding worden gedaan, tenzij op dat moment inmiddels uit onderzoek is gebleken dat het incident niet onder de meldplicht datalekken valt.

5. Moet het datalek ook worden gemeld aan degene van wie de persoonsgegevens zijn gelekt?

Het datalek hoeft niet te worden gemeld aan de betrokkene indien één van de volgende situaties zich voordoet:

- u bent een financiële onderneming zoals bedoeld in de Wet op het financieel toezicht;
- er zijn passende technische beschermingsmaatregelen genomen waardoor de persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens, bijvoorbeeld door adequate encryptie (versleuteling) en hashing (het omzetten van gegevens in een unieke code);
- andere technische beschermingsmaatregelen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten, bijvoorbeeld door een tijdige en adequate remote wiping (het op afstand wissen van de gegevens die op een apparaat staan) en pseudonimisering (technische maatregelen om te voorkomen dat de persoonsgegevens worden gekoppeld aan de oorspronkelijke identiteit van de betrokkene);
- het is onwaarschijnlijk dat het datalek ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene: als persoonsgegevens van gevoelige aard zijn gelekt, moet sowieso worden gemeld;
- er zijn andere zwaarwegende redenen om de melding aan de betrokkene achterwege te laten.

6. Hoe en wanneer moet het datalek worden gemeld aan de betrokkene?

In de kennisgeving aan de betrokkene moet in ieder geval worden vermeld:

- de aard van de inbreuk
- de instanties waar de betrokkene meer informatie over de inbreuk kan krijgen (contactgegevens),
- de waarschijnlijke gevolgen van de inbreuk,
- de maatregelen die zijn aanbevolen om de negatieve gevolgen van de inbreuk te beperken.

Het datalek moet onverwijld worden gemeld. Dit houdt in dat de verwerkingsverantwoordelijke, na het ontdekken van een mogelijk datalek, enige tijd mag nemen voor nader onderzoek zodat betrokkene op een behoorlijke en zorgvuldige manier kan worden geïnformeerd en zodat maatregelen genomen kunnen worden om verdere lekken te voorkomen.

7. Welke gegevens moeten worden vastgelegd?

Er moet een overzicht worden bijgehouden van alle inbreuken op de beveiliging. Ook datalekken die niet aan de Autoriteit Persoonsgegevens gemeld hoeven worden, moeten wel gedocumenteerd worden. Per datalek bevat het overzicht in ieder geval de gegevens omtrent de aard van de inbreuk, waar mogelijk onder vermelding van de categorieën van betrokkenen en welke en hoeveel registers het betreft, de waarschijnlijke gevolgen van de inbreuk, de naam en contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen, de maatregelen die zijn voorgesteld of zijn genomen om de inbreuk aan te pakken en maatregelen die zijn genomen om de nadelige gevolgen van het datalek te beperken. De wet schrijft niet bij hoe lang het overzicht moet worden bewaard. Ga uit van een bewaartermijn van minimaal vijf jaar. In bepaalde gevallen kan het nodig zijn een langere bewaartermijn te hanteren.

Sancties

Bij overtreding van de meldplicht datalekken kan de Autoriteit Persoonsgegevens een bestuurlijke boete van ten hoogste € 10.000.000,- opleggen. Indien de overtreding niet opzettelijk is gepleegd en geen sprake is van ernstig verwijtbare nalatigheid, dan zal de Autoriteit Persoonsgegevens eerst een bindende aanwijzing opleggen.

Tot slot, enkele algemene aanbevelingen

- Als u de verwerking geheel of gedeeltelijk laat uitvoeren door een verwerker, moet u als verwerkingsverantwoordelijke maatregelen nemen om ervoor te zorgen dat u in staat blijft de meldplicht datalekken na te komen. Daartoe kunnen met de verwerker afspraken worden gemaakt. Deze afspraken moeten schriftelijk worden vastgelegd, of in een andere, gelijkwaardige vorm. Denk aan de volgende onderwerpen:
    - Gaat de verwerker u informeren over alle incidenten?
    - Hoe en wanneer vindt deze informatieverstrekking plaats?

- Gaat de verwerker eventueel zelf meldingen doen aan de Autoriteit Persoonsgegevens?
- Wordt u geïnformeerd over door de verwerker getroffen verbetermaatregelen?

- Het is aan te bevelen om intern een procedure te ontwikkelen die medewerkers een praktisch handvat biedt hoe te handelen bij een (vermoeden van een) datalek. In deze interne procedure kunnen de volgende onderwerpen aan bod komen:
  - Aan wie en binnen welke termijn moet een (mogelijk) datalek worden gemeld?
  - Door wie en hoe wordt onderzoek gedaan naar de aard en de ernst van het incident?
  - Wie verzorgt de eventuele melding aan de Autoriteit Persoonsgegevens en de betrokkenen?
- In het geval van een datalek kan er een vermoeden zijn van strafbaar handelen. Zo is bijvoorbeeld hacken strafbaar gesteld. Wanneer er aanwijzingen voor hacken zijn, dan is er alle aanleiding om daarvan aangifte te doen bij de politie.
  - Wie is intern waarvoor verantwoordelijk?
- In het geval van een datalek kan er een vermoeden zijn van strafbaar handelen. Zo is bijvoorbeeld hacken strafbaar gesteld. Wanneer er aanwijzingen voor hacken zijn, dan is er alle aanleiding om daarvan aangifte te doen bij de politie.