Kennedy Van der Laan

CONTACT

Themadossier Datalekken

Achtergrond Meldplicht Datalekken

De voorganger van de AVG, de Privacyrichtlijn, bevatte geen verplichting om datalekken te melden. Ook de Wet bescherming persoonsgegevens (Wbp), die de Privacyrichtlijn in Nederland implementeerde, bevatte die verplichting aanvankelijk niet. Vooruitlopend op de invoering van de AVG is de verplichting om datalekken te melden in 2016 in de Wbp opgenomen. Met de komst van de AVG – en het vervallen van de Wbp – moeten datalekken worden gemeld op grond van art. 33 en 34 AVG.

Wat is een datalek?

In de AVG wordt de term 'datalek' niet gebruikt. Die spreekt in plaats daarvan van een 'inbreuk in verband met persoonsgegevens'. Art. 4 lid 12 AVG definieert dit als: 'een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens'. In de praktijk en ook door de Autoriteit Persoonsgegevens (AP) wordt de term 'datalek' als synoniem gebruikt voor de hiervoor omschreven 'inbreuk in verband met persoonsgegevens'.

Wat betekent dat concreet?

Een datalek is een inbreuk die plaatsvindt op de beveiliging van persoonsgegevens binnen een organisatie.
Dit kan verschillende vormen aannemen. Bekende voorbeelden van een datalek zijn cyberaanvallen op een organisatie, bijvoorbeeld met behulp van ransomware, waarbij ook vaak data van de organisatie wordt gestolen door de aanvallers, of het hacken van een e-mailaccount van een organisatie (Business Email Compromise). Maar een datalek kan ook intern in de organisatie plaatsvinden, bijvoorbeeld doordat een nieuwsbrief wordt verstuurd met alle geadresseerden in de "Aan" veld in plaats van de "BCC", of wanneer werknemers van een organisatie toegang hebben tot dossiers met persoonsgegevens waar zij dat niet nodig hebben voor hun functie.

Er is een datalek, wat nu?

De AVG kent twee meldplichten. Ten eerste een verplichting aan de verwerkingsverantwoordelijke om een melding te doen bij de toezichthouder – de AP. In bepaalde gevallen moet een verwerkingsverantwoordelijke het datalek ook melden aan de personen van wie persoonsgegevens zijn betrokken bij het datalek. Hieronder worden deze meldplichten nader beschreven.

Themadossier Datalekken

Is de organisatie waar het datalek zich heeft voorgedaan niet een verwerkingsverantwoordelijke voor de getroffen persoonsgegevens, maar een verwerker, dan moet die het datalek 'zonder onredelijke vertraging' melden aan de verwerkingsverantwoordelijke, zie art. 33 lid 2 AVG. Op de verwerker rust geen verplichting om te melden aan de toezichthouder of de betrokkenen. In de verwerkersovereenkomst tussen de verwerker en de verwerkingsverantwoordelijke worden hierover afspraken gemaakt. Dit is verplicht op basis van art. 28 lid 3 sub f AVG. Vaak wordt contractueel een termijn afgesproken waarbinnen de verwerker de verwerkingsverantwoordelijke op de hoogte moet stellen van het datalek, soms al binnen 24 uur. Verwerkers doen er goed aan deze termijn scherp voor ogen te houden!

*Voor meer informatie over de verhouding tussen verwerkingsverantwoordelijke en verwerking zie: themadossier **AVG: verantwoordingsplicht***

Meldplicht aan de Autoriteit Persoonsgegevens

Op grond van art. 33 lid 1 AVG moeten verwerkingsverantwoordelijken een datalek melden aan de toezichthouder zonder onredelijke vertraging en uiterlijk binnen 72 uur nadat de verwerkingsverantwoordelijke kennis heeft genomen van het datalek. Deze verplichting is opgenomen als een "ja, tenzij": datalekken moeten gemeld worden aan de AP, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkenen (de personen van wie persoonsgegevens zijn getroffen door het datalek).

Een verwerkingsverantwoordelijke kan op verschillende manieren op de hoogte raken van een datalek. Uiteraard kan dit door eigen ontdekking, bijvoorbeeld doordat de systemen op maandagochtend niet meer werken en een bericht van cybercriminelen (een 'ransomnote') wordt gevonden op de computers. Daarnaast kan de verwerkingsverantwoordelijke bekend worden met een datalek doordat het datalek wordt gemeld door een verwerker, of door een andere externe partij, zoals een betrokkene of een (ethische) hacker.

De melding van het datalek aan de AP moet worden gedaan via het online formulier. Soms is binnen de meldtermijn van 72 uur nog niet alle informatie bekend die moet worden verstrekt aan de toezichthouder. In dat geval kan een voorlopige melding worden gedaan met de beschikbare informatie. De voorlopige melding moet in de regel binnen 4 weken worden opgevolgd.

Themadossier Datalekken

Meldplicht aan betrokkenen

Als een datalek verplicht moet worden gemeld aan de AP op grond van art. 33 AVG, dan is het mogelijk dat ook de betrokkenen op de hoogte moeten worden gesteld van het datalek. Deze meldplicht aan betrokkenen staat beschreven in art. 34 AVG. Lid 1 van dat artikel bepaalt dat indien de inbreuk 'waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen', de verwerkingsverantwoordelijke onverwijld de betrokkene op de hoogte moet brengen van het datalek.

Wanneer er concreet sprake is van een hoog risico wordt in de AVG niet toegelicht. De Artikel 29 Werkgroep, het samenwerkingsorgaan van Europese privacy toezichthouders, thans het Europees Comité voor gegevensbescherming, heeft richtsnoeren opgesteld om een nadere invulling te geven aan de meldplicht aan de toezichthouder en de betrokkenen.

Een melding aan de betrokkene kan achterwege gelaten worden in de drie gevallen (zie art. 34 lid 3 AVG):

- De gegevens waren onbegrijpelijk voor onbevoegden (versleuteling);
- Na het datalek zijn maatregelen genomen die maken dat een hoog risico zich waarschijnlijk niet meer zal voordoen; of
- De melding aan de betrokkenen zou een onevenredige inspanning vergen. De individuele melding mag in dat geval vervangen worden door een algemene melding, bijvoorbeeld op de website van de getroffen organisatie.

Voor de melding aan de betrokkenen stelt de AVG geen concrete termijn, er staat alleen dat melding 'onverwijld' moet geschieden.

*Voor meer informatie over de rechten van betrokkenen zie themadossier **AVG: rechten van betrokkenen***

Administratieve boete

De AP kan voor niet of te laat gemelde datalekken een administratieve boete opleggen. Ook als een datalek het gevolg is van onvoldoende beveiligingsmaatregelen kan dit leiden tot een boete. Uit artikel 83 lid 4 AVG volgt dat de AP voor schending van (o.a.) de meldplicht datalekken een boete kan opleggen van ten hoogste 10 miljoen euro, of twee procent van de wereldwijde jaaromzet van een organisatie.

Verder leren

Cursus Datalekken: voorbereiden, herkennen en reageren
Cursus Bewustzijn van informatiebeveiliging