

Inbreuk in verband met persoonsgegevens: Datalekken onder de AVG

Wat is een datalek?

Een datalek heet in de AVG een “inbreuk in verband met persoonsgegevens”. De AVG geeft hiervan de volgende definitie: *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* (art. 4 sub 12 AVG).

Van een datalek is dus sprake als er:

- Persoonsgegevens zijn doorgezonden, opgeslagen of op een andere manier verwerkt (opslaan en/of doorsturen is ook verwerken) en;
- Deze gegevens vernietigd, verloren of gewijzigd zijn, ongeoorloofd zijn verstrekt of iemand daar ongeoorloofd toegang toe heeft gehad en;
- Dit het gevolg is van een inbreuk op de beveiliging van die gegevens, of dat nu per ongeluk of onrechtmatig is geweest.

Wanneer moet je een datalek melden?

De AVG kent een meldplicht aan de Autoriteit Persoonsgegevens (art. 33 AVG) en een meldplicht aan de betrokkene (art. 34 AVG). De betrokkene is degene op wie de persoonsgegevens betrekking hebben. De meldplicht geldt voor notarissen omdat zij *verwerkingsverantwoordelijke* zijn voor persoonsgegevens in de zin van de AVG.

Meldplicht aan de Autoriteit Persoonsgegevens

Ieder datalek moet worden gemeld aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

De melding moet zonder onredelijke vertraging plaatsvinden, indien mogelijk uiterlijk 72 uur nadat geconstateerd is dat er sprake is van een datalek.

De melding aan de Autoriteit Persoonsgegevens kan worden gedaan via het [Meldloket Datalekken](#) op de website van de [Autoriteit Persoonsgegevens](#). Het formulier geeft de benodigde gegevens aan.

Meldplicht aan de betrokkene

Levert het datalek een hoog risico op voor de rechten en vrijheden van personen? Dan moet het datalek ook onverwijld aan de betrokkene worden gemeld.

Een datalek hoeft niet aan de betrokkene te worden gemeld als aan één van de volgende drie voorwaarden is voldaan:

- a. Er zijn vooraf passende technische en organisatorische beschermingsmaatregelen genomen, zoals versleuteling;
- b. Er zijn achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;
- c. De melding aan de betrokkene zou onevenredige inspanning vergen. In dat geval komt een openbare mededeling of vergelijkbare maatregel in de plaats van de melding.

Een melding aan een betrokkene moet omvatten:

- Een duidelijke en eenvoudige omschrijving van het datalek;

- De naam en contactgegevens van de functionaris voor gegevensbescherming of als die er niet is: een ander contactpunt waar meer informatie kan worden verkregen;
- De waarschijnlijke gevolgen van het datalek;
- De maatregelen die zijn voorgesteld of genomen om het datalek aan te pakken en de nadelige gevolgen ervan te beperken.

Wat houdt het datalekkenregister in?

De verwerkingsverantwoordelijke moet onder de AVG alle datalekken documenteren, ook als deze niet zijn gemeld c.q. niet hoeven te worden gemeld. De documentatie moet de AP in staat stellen de naleving van de meldplicht te controleren. Door een *datalekkenregister* aan te leggen en bij te houden, kan aan deze verplichting worden voldaan.

In dit register worden geregistreerd:

- De feiten rondom het datalek;
- De gevolgen van het datalek;
- De genomen corrigerende maatregelen;
- De informatie die de Autoriteit Persoonsgegevens nodig heeft om te controleren of aan de meldplicht voor datalekken is voldaan: in ieder geval het tijdstip waarop het datalek bekend is geworden aan het notariskantoor.

De KNB stelt hiervan een voorbeeld beschikbaar op knb.nl.

Welke acties moet een notariskantoor ondernemen om aan de nieuwe regeling te voldoen?

Notarissen zijn als verwerkingsverantwoordelijken verantwoordelijk voor de naleving van de verplichtingen van de AVG en moeten deze naleving kunnen aantonen. Op het gebied van datalekken betekent dit:

- Een datalekkenregister aanleggen en bijhouden;
- Een protocol hanteren voor het omgaan met en melden van datalekken. Voor een voorbeeld van een dergelijk datalekkenprotocol verwijzen we naar voorbeeld op knb.nl. Wijs verantwoordelijkheden toe en maak dit protocol en de verantwoordelijkheden ook bekend bij de medewerkers.
- In de kantoororganisatie maatregelen treffen om datalekken te voorkomen en deze adequaat op te lossen.

Wat is het risico als je niet aan de nieuwe regeling voldoet?

De AVG geeft de Autoriteit Persoonsgegevens de bevoegdheid boetes op te leggen. Deze boetes kunnen voor de verplichtingen rondom de meldplicht en documentatie van datalekken oplopen tot 10 miljoen euro (art. 83 lid 4 AVG).

Daarnaast geeft de AVG gedupeerden een recht op vergoeding van schade die geleden is door een inbreuk op de AVG. De verwerkingsverantwoordelijke is aansprakelijk voor schade die is veroorzaakt door een verwerking die inbreuk maakt op de AVG (art. 82 AVG).

Voor het notariaat is imagoschade een groot risico, aangezien het vertrouwelijk omgaan met persoonsgegevens een belangrijke pijler is onder de beroepsuitoefening.