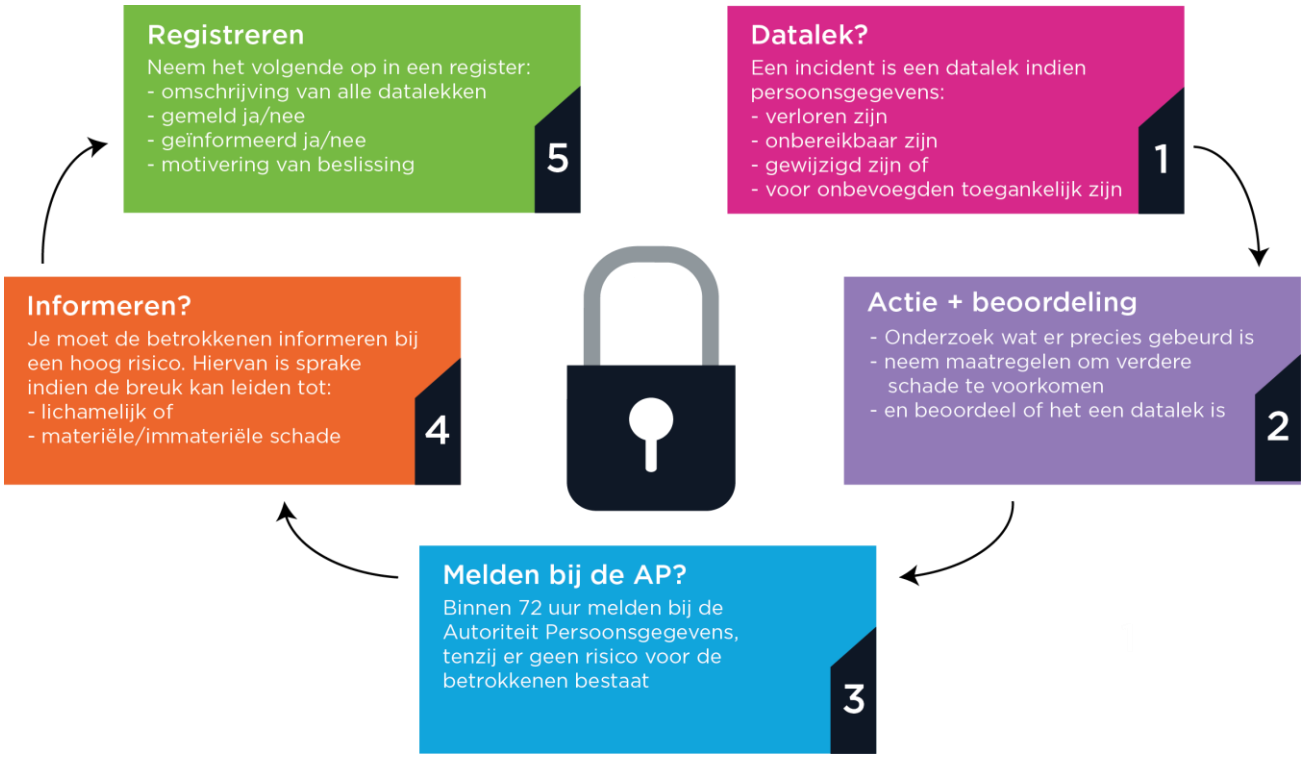
Hekkelman advocaten | notarissen

HELP! Een datalek, wat moet ik doen?

Stel je ontdekt een datalek binnen je organisatie. Hoe weet je of je dit moet melden bij de Autoriteit Persoonsgegevens (AP) en de betrokkenen moet informeren? Want niet ieder datalek hoeft gemeld te worden, maar hoe zit dat nou precies? Dit schema en de checklist helpt je bij de beoordeling.



Wat is een datalek?

In de Algemene verordening Gegevensbescherming (AVG) wordt een datalek een **inbreuk in verband met persoonsgegevens** genoemd.

Daarvan is sprake in de volgende gevallen:

- Er zijn persoonsgegevens verloren gegaan *(bijv. s een brand in het datacenter zonder back-up)*
- Er zijn persoonsgegevens onbereikbaar geworden (*er is geen toegang meer tot gegevens)*
- Persoonsgegevens zijn beschadigd *(gegevens zijn gewijzigd of niet langer volledig)*
- Onbevoegden kunnen toegang hebben (gehad) tot persoonsgegevens *(bijv. een hack of een email naar een verkeerde ontvanger)*

Tref maatregelen om het lek te dichten en de gevolgen te beperken

- Stel vast welke maatregelen zijn getroffen om het lek te dichten (corrigerende maatregelen)
- Stel vast welke maatregelen zijn getroffen ter beperking van eventuele nadelige gevolgen voor betrokkenen (preventieve maatregelen)

Beoordeel of je het datalek moet melden bij de AP

Je moet een datalek **binnen 72 uur** melden bij de Autoriteit Persoonsgegevens (AP), **tenzij** het datalek waarschijnlijk geen risico inhoudt voor de rechten en vrijheden van de getroffenen.

Verzamel alle relevante informatie

Verzamel alle relevante informatie over het (vermeende) datalek. Wat is er gebeurd en wanneer, de aard van de inbreuk, de categorieën van persoonsgegevens en de categorieën van betrokkenen.

- *De publicatie Recommendations for a methodology of the assessment of severity of personal data breaches van ENISA kan als hulpmiddel dienen voor het opstellen van een methode om de ernst van inbreuken te beoordelen*

Beoordeel het risico aan de hand van de volgende relevante factoren:

- De aard van de inbreuk (*wat is er precies gebeurd?*)
- Aard, gevoeligheid en het aantal persoonsgegevens
    - *bijzondere persoonsgegevens*[1] *of gegevens van vertrouwelijke aard*[2]
- Gemak waarmee personen kunnen worden geïdentificeerd
- Ernst van de gevolgen voor personen
- Kwetsbaarheid van getroffen personen (*zoals kinderen of zieken)*
- Het aantal getroffen personen

➢ Is er een risico te verwachten, dan dien je dit te melden via het formulier op de website van de AP.

Beoordeel of de betrokkenen moeten worden geïnformeerd

Wanneer uit de beoordeling blijkt dat het datalek waarschijnlijk **een hoog risico** inhoudt voor de rechten en vrijheden van betrokken personen moeten betrokkenen worden geïnformeerd.

- Er is sprake van een hoog risico als de inbreuk kan leiden tot lichamelijke, materiële of immateriële schade voor de personen. *(bijv. discriminatie, identiteitsdiefstal of –fraude, financieel verlies en reputatieschade)*
- Ga na of de betrokkene zichzelf beter kan beschermen indien hij de inbreuk kent (*denk aan inloggegevens die op straat zijn beland)*

Informeren van betrokkenen is niet vereist indien is voldaan bij één van deze omstandigheden:

- de getroffen persoonsgegevens zijn adequaat onbegrijpelijk of ontoegankelijk gemaakt door verwerkingsverantwoordelijke (*bijv. door versleuteling met de nieuwste technieken*)
- er zijn achteraf maatregelen genomen waardoor het onwaarschijnlijk is geworden dat het hoge risico zal intreden (*bijv. gegevens worden op afstand gewist en het is zeker dan de gegevens niet zijn gebruikt*)
- betrokkenen informeren zou een onevenredige inspanning vergen (*bijvoorbeeld als het een groot aantal betrokkenen betreft*); in dat geval volstaat een openbare mededeling

Let op! Als je niet informeert, leg dit dan vast met een onderbouwing.

[1] Godsdienst of levensovertuiging, ras of etnische afkomst, politieke opvattingen, gezondheid, seksuele leven, lidmaatschap vakbond, strafrechtelijk verleden en genetische of biometrische gegevens met oog op unieke identificatie.

[2] Financieel of economisch, stigmatiserend, specifieke problemen, school of werkprestaties, inloggegevens, gegevens die bruikbaar zijn voor identiteitsfraude, gegevens die vallen onder beroepsgeheim.

NB: de AP kan na ontvangst van een melding de verwerkingsverantwoordelijke verplichten om betrokkenen (alsnog) te informeren, als dat nog niet is gebeurd.

Registreer alle datalekken

Het is verplicht een register bij te houden van alle datalekken. Dit overzicht kan namelijk worden opgevraagd door de AP ten behoeve van controle op de naleving van de meldplicht.

Wat moet je in het datalekkenregister opnemen?

- omschrijving van alle datalekken (ook de datalekken die niet zijn gemeld);
- alle relevante informatie omtrent het datalek;
- omschrijving van de corrigerende en preventieve maatregelen;
- motivering van beslissingen genomen naar aanleiding van het datalek, zoals:
    - het besluit om het datalek niet te melden
    - het niet tijdig melden van een datalek
    - het al dan niet informeren van betrokkenen

➢ Gebruik de tien tips voor een goede registratie uit de handreiking van de AP.

Tips voor datalek procedure

- stel een vast aanspreekpunt aan
- stel een team samen die de datalek beoordeelt en afhandelt (*bijv. IT-specialist, jurist en PR medewerker)*
- zorg voor een geautomatiseerde controle op hacks, malware e.d.
- creëer bewustwording binnen de organisatie met trainingen en do's & dont's
- zorg dat er afspraken zijn met de melding van datalekken bij verwerkers