Sinds1 januari 2016 hebben organisaties een meldplicht bij datalekken. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) onverwijld een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. En in een aantal gevallen moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

Iedereen heeft recht op eerbiediging en bescherming van zijn persoonlijke levenssfeer en een zorgvuldige omgang met zijn persoonsgegevens. De regels hiervoor zijn vastgelegd in de Wet AVG Hierin staat dat u de persoonsgegevens die verwerkt worden moet beveiligen tegen verlies en tegen onrechtmatige verwerking Een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens als het leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens Het datalek moet daarnaast ook worden gemeld aan de betrokkene indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

Bij de beslissing of u een gebeurtenis die zich heeft voorgedaan moet melden aan de Autoriteit Persoonsgegevens, en eventueel daarnaast ook aan de betrokkene, moeten er een aantal afwegingen gemaakt worden(zie het beslis schema op de laatste pagina).

Maar niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als u onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kunt uitsluiten.

U hoeft niet ieder datalek te melden aan de Autoriteit Persoonsgegevens. Volgens de wet moet u een melding doen aan de Autoriteit Persoonsgegevens als het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

Beveiligingslek;
Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. U hoeft dan geen melding te doen aan de Autoriteit Persoonsgegevens.

Beveiligingsincident;
Een is sprake van inbreuk op de beveiliging denk hierbij aan
een kwijtgeraakte USB-stick;

- een gestolen laptop;
- een inbraak door een hacker;
- een malware-besmetting;
- een calamiteit zoals een brand in een datacentrum.

Datalek;
Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident moet u bijvoorbeeld denken aan het kwijtraken van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker.

Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is over het algemeen een melding noodzakelijk. Bij persoonsgegevens van gevoelige aard moet u denken aan:

Bijzondere persoonsgegevens:
Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

• Gegevens over de financiële of economische situatie van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.

• (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.

• Gebruikersnamen, wachtwoorden en andere inloggegevens De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.

• Gegevens die kunnen worden misbruikt voor (identiteits)fraude Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn).

Melden aan de Autoriteit Persoonsgegevens;
Volgens de wet moet er melding gedaan worden aan de Autoriteit Persoonsgegevens als het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie er persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. Maar let op: als de aard van de gelekte gegevens daar aanleiding toe geeft is het mogelijk dat u een datalek moet melden waar de persoonsgegevens van slechts één persoon bij betrokken zijn.

De melding moet gedaan worden zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek. Op de *website van de Autoriteit Persoonsgegevens* is voor dit doel een *webformulier* beschikbaar. Via dit webformulier kan de melding zo nodig aangevuld of ingetrokken worden.

Als er een datalek gemeld moet worden aan de Autoriteit Persoonsgegevens, dan betekent dit niet automatisch dat dit datalek ook moet gemeld moet worden aan de betrokkene. Hiervoor wordt een aparte afweging gemaakt.

Melding aan de betrokkene:
De wet geeft aan dat er een melding gedaan moet worden aan de betrokkene als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik in hun belangen worden geschaad. Daarbij moet u bijvoorbeeld denken aan onrechtmatige publicatie, aantasting in eer en goede naam, (identiteits)fraude of discriminatie. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan kan

er in principe van uit gegaan worden dat het datalek niet alleen gemeld moet worden aan de Autoriteit Persoonsgegevens, maar ook aan de betrokkene.

De melding stelt de betrokkene in staat om alert te zijn op de mogelijke gevolgen van het datalek en om zich daar waar mogelijk tegen te wapenen door, bijvoorbeeld, een gelekt wachtwoord te vervangen. De wet schrijft voor dat de melding onverwijld gedaan moet worden. Rekening houdend met het feit dat de betrokkene naar aanleiding van de melding mogelijk maatregelen moet nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder de betrokkene daarover geïnformeerd is, hoe eerder deze in actie kan komen.

Als er passende technische beschermingsmaatregelen zijn genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kan de melding aan de betrokkene achterwege blijven. Denk bij deze beschermingsmaatregelen aan cryptografische bewerkingen zoals encryptie en hashing zoals *7-Zip*. Per geval wordt bepaalt of de maatregelen die genomen zijn voldoende bescherming bieden om de melding aan de betrokkene achterwege te kunnen laten.

Bij overtreding van de meldplicht datalekken uit de AVG kan de Autoriteit Persoonsgegevens een bestuurlijke boete opleggen. Deze bestuurlijke boete bedraagt ten hoogste het bedrag van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht. Dat is per 1 januari 2016 maximaal 820.000 euro.
Als de overtreding niet opzettelijk is gepleegd en er geen sprake is van ernstig verwijtbare nalatigheid, dan zal de Autoriteit Persoonsgegevens eerst een bindende aanwijzing opleggen voorafgaand aan eventuele oplegging van een bestuurlijke boete. Bij het opleggen van een bestuurlijke boete houdt de Autoriteit Persoonsgegevens rekening met alle omstandigheden van het geval. Een omstandigheid van het geval kan bestaan uit het feit dat de gegevens waarover het gaat niet door derden zijn ingezien.

Beslis schema:

Er is een zwakke plek in de beveiliging geconstateerd

Er heeft zich een beveiligingsincident plaatsgevonden (een dreiging of tekortkoming)

Zijn bij het beveiligingsincident persoonsgegevens verloren gegaan, of is onrechtmatige verwerking redelijkerwijs niet uit te sluiten?

Gaat het om persoonsgegevens van gevoelige aard, of is er om een andere reden sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens?

Waren niet alle gelekte gegevens (goed) versleuteld, of heeft het datalek om andere redenen waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene?