Procedure

melden van datalek

hub noord-brabant

Inhoud

De Algemene Verordening Gegevensbescherming (AVG) verplicht organisaties melding te maken van datalekken bij de Autoriteit Persoonsgegevens (AP). Deze procedure voorziet in een gestructureerde wijze voor het melden van datalekken in het kader van de AVG. In bijlage 1 is een stroomschema opgenomen als hulpmiddel om te beoordelen of een datalek gemeld moet worden aan de Autoriteit Persoonsgegevens dan wel aan de betrokkene.

1. Wanneer is er sprake van een datalek?

Als zich een beveiligingsincident heeft voorgedaan kan er sprake zijn van een datalek. Bij een beveiligingsincident moet bijvoorbeeld worden gedacht aan het kwijtraken van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker. Niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kan worden uitgesloten.

2. Wat te doen bij (een vermoeden van) een datalek?

Bij constatering van een (vermoedelijk) datalek moet dat direct worden gemeld bij de directeur Bedrijfsvoering of in het programma 4Me van Actacom via de tegel AVG-Incident.

De melding bevat tenminste de volgende gegevens:

- de aard van het datalek (wat is er gebeurd?);
- de oorzaak waardoor dit incident heeft plaatsgevonden (verlies, diefstal, hack, etc.);
- beschrijving van de gelekte (persoons)gegevens (aard van de gegevens, hoeveelheid, etc.);
- eventuele maatregelen die genomen zijn/worden genomen om het datalek te dichten;
- een inschatting van het risico dat de betrokkenen kunnen lopen;
- en contactgegevens van de melder.

3. Wanneer melden aan de Autoriteit Persoonsgegevens?

Niet ieder datalek behoeft te worden gemeld aan de Autoriteit Persoonsgegevens (AP). Volgens de AVG moet melding worden gedaan als het datalek (een aanzienlijke kans op) ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. 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 worden gedacht aan:

a) *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.
b) *Gegevens over de financiële of economische situatie van de betrokkene.* Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
c) *(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene.* Bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
d) *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.
e) *Gegevens die kunnen worden misbruikt voor (identiteits)fraude.* Onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (BSN).

Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie 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 een datalek moet worden gemeld waar de persoonsgegevens van slechts één persoon bij betrokken zijn.

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

Aan de hand van het stroomschema, zoals opgenomen in de bijlage, onderzoekt de directeur bedrijfsvoering of er sprake is van een “meldplichtig datalek”.

Indien het datalek meldplichtig is, dan meldt zij het datalek onverwijld (doch uiterlijk op de tweede werkdag na het ontstaan van het incident) bij het Meldloket datalekken Autoriteit Persoonsgegevens (AP): https://datalekken.autoriteitpersoonsgegevens.nl. Na afsluiting van de melding kan deze niet meer worden geraadpleegd. De directeur bedrijfsvoering maakt bij melding een print van de ontvangstbevestiging en bewaart deze bij de melding in 4Me.

De directeur bedrijfsvoering onderhoudt contact met de AP over de gedane melding. Eventuele aanwijzingen van de AP worden vastgelegd en opgevolgd.

4. Informeren van betrokkenen

Als het datalek bij de AP moet worden gemeld, dan betekent dit niet automatisch dat het datalek ook moet worden gemeld aan betrokkene(n). Daarvoor moet een aparte afweging worden gemaakt. De AVG geeft aan dat een melding aan betrokkene(n) moet worden gedaan als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

Als persoonsgegevens **van gevoelige aard** zijn gelekt, dan moet ervan worden uitgegaan dat het datalek niet alleen moet worden gemeld aan de AP, maar ook aan betrokkene(n). De melding stelt de betrokkene(n) 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 AVG schrijft voor dat de melding *onverwijld* moet worden gedaan. Daarbij moet rekening worden gehouden 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 wordt geïnformeerd, hoe eerder deze in actie kan komen.

Binnen Hub Noord-Brabant hebben wij ervoor gekozen de betrokkenen altijd te informeren. Immers, betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik in hun belangen worden geschaad. Daarbij moet bijvoorbeeld worden gedacht aan onrechtmatige publicatie, aantasting in eer en goede naam, (identiteits)fraude of discriminatie.

De directeur bedrijfsvoering stelt vast – waar nodig in overleg met de melder – of het datalek een *"Aanmerkelijk risico op verlies of onrechtmatige verwerking waaraan nadelige gevolgen voor de persoonsgegevens en de persoonlijke levenssfeer van de betrokkenen zijn verbonden"* tot gevolg heeft. Als daarvan sprake is, word(t)en de betrokkene(n) per direct over het datalek geïnformeerd. Let wel: De melding aan betrokkene(n) is niet nodig indien de persoonsgegevens versleuteld[1] of onbegrijpelijk zijn gemaakt, waardoor deze niet te lezen zijn door anderen. Dit moet van geval tot geval worden beoordeeld, omdat de effectiviteit van versleuteling mede afhangt van het moment waarop de gegevens zijn versleuteld.

De melding aan betrokkene(n) kan via e-mail en/of telefonisch. De kennisgeving bevat in ieder geval de volgende informatie:

- de aard van de inbreuk in verband met persoonsgegevens;
- op welke wijze meer informatie over de inbreuk kan worden verkregen;
- aanbevelingen om mogelijke negatieve gevolgen van de inbreuk voor betrokkenen te beperken.

De directeur bedrijfsvoering informeert de Voorzitter College van Bestuur en, afhankelijk van de aard van de inbreuk, overige relevante partijen over het datalek en de melding aan het AP.

5. Verantwoording

De directeur bedrijfsvoering houdt jaarlijks een overzicht bij van de datalekken. Hierbij is (aanvullend) aandacht voor de volgende aspecten:

- is er sprake van het niet nakomen of een tekortkoming in de beveiligingsprocedures?;
- is de organisatie verwijtbaar?;
- wat zijn de gevolgen van de datalekken? en

[1] Binnen HUB wordt gebruik gemaakt van het programma Zivver om versleutelde mails te sturen.

- welke herstelmaatregelen zijn genomen?

Na afloop van een kalenderjaar analyseert de directeur bedrijfsvoering de in dat jaar ontvangen meldingen. De rapportage is onderdeel van het jaarverslag.

Minimaal jaarlijks evalueert en beoordeelt het bestuur met het management of de procedure en de uitvoering nog met elkaar in overeenstemming zijn. Indien deze niet met elkaar overeenkomen wordt beoordeeld of de procedure geactualiseerd moet worden, of dat medewerkers (opnieuw) geïnstrueerd moeten worden over de juiste toepassing van de procedure.