Protocol Melding Datalek

Inleiding

Indien er sprake is van een *ernstig* datalek zijn organisaties verplicht deze te melden bij de Autoriteit Persoonsgegevens (AP) via het meldloket Datalekken Autoriteit Persoonsgegevens. Niet ieder datalek moet worden gemeld bij de Autoriteit Persoonsgegevens of de betrokkenen. Afhankelijk van de impact of de verwachtte impact, wordt bepaald of een melding nodig is.

Er wordt gesproken van een datalek indien er sprake is van 'toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie'[1].

Persoonsgegevens zijn volgens artikel 4 lid 1 AVG 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Dit houdt in dat het kan gaan om ieder gegeven waarmee een individu van anderen kan worden onderscheiden. Het kan gaan om een naam, adres, BSN of een (of een combinatie van) element(en) die kenmerkend zijn voor een specifiek persoon.

A-Creation heeft om zorgvuldig te kunnen omgaan met persoonsgegevens en deze te kunnen waarborgen een procedure opgenomen in de bedrijfsvoering met betrekking tot het handelen en afhandelen bij een datalek alsmede het melden van ernstige datalekken bij betrokkene en de Autoriteit Persoonsgegevens. Zoals opgenomen in het Privacystatement van A-Creation is er een persoon aangesteld binnen A-Creation die verantwoording draagt voor zaken met betrekking tot persoonsgegevens. Binnen A-Creation is deze persoon ook verantwoordelijk voor het afhandelen van datalekken. In dit protocol wordt deze persoon omschreven als '*privacyverantwoordelijke*'.

Voorbereiden op een datalek

Om het risico op een datalek te verkleinen en om geen tijd te verliezen bij een datalek is het belangrijk om te weten wat de stromen van persoonsgegevens zijn binnen A-Creation. Medewerkers die in dienst zijn en treden bij A-Creation zijn gewezen op de meldplicht datalekken en het omgaan met persoonsgegevens als onderdeel van het inwerktraject. Zorg dat medewerkers bewust zijn van de meldplicht en wie de verantwoordelijke binnen A-Creation is.

Via verwerkersovereenkomsten is duidelijk met wie er persoonsgegevens worden gedeeld en wie er moet melden bij een datalek. De *privacyverantwoordelijke* heeft hier goed zicht op.

Stappenplan melden datalek

Stap 1 - het melden van datalekken aan de privacyverantwoordelijke

Medewerkers worden op de hoogte gebracht van de meldplicht datalekken en de wijze waarop een datalek direct gemeld dient te worden (zie voorbereiden op een datalek). Nieuwe medewerkers worden bij indiensttreding op de hoogte gebracht van het bestaan van de meldplicht datalekken en de wijze waarop een datalek direct gemeld dient te worden.

Stap 2 - Ondernemen actie

Indien het een doorlopend incident is dient er direct gekeken te worden of er actie ondernomen kan worden om het datalek te stoppen of te dichten. Indien dit mogelijk is dient deze actie direct of zo spoedig als mogelijk is ondernomen te worden om (verdere) schade te beperken.

[1] Definitie zoals gegeven door de Autoriteit Persoonsgegevens.

Bij directe actie kan gedacht worden aan het blokkeren van accounts, het uitzetten van servers of het verwijderen van gevoelige informatie.

Stap 3 - Documentatie en analyse

De *privacyverantwoordelijke* documenteert na de melding de volgende aspecten:

- Wat is er gebeurd;
- Waar is het gebeurd;
- Wanneer is het gebeurd;
- Zijn er derden bij betrokken of specifieke apparatuur;
- Welke actie is er ondernomen;
- Welke persoonsgegevens, hoeveel en welke personen zijn betrokken alsmede de aard van de persoonsgegevens (algemeen of bijzonder);
- Hoe zijn de gegevens verkregen? Is de verantwoordelijke A-Creation zelf?;
- Is er sprake van uitsluitbaarheid? Dit betekent dat de mogelijkheid dat de persoonsgegevens onrechtmatig zijn verwerkt tot een minimum beperkt zijn. Voorbeeld hiervan is een diefstal van een laptop die voorzien is van goede encryptie.

Stap 4 - Melden datalek

Bij de ontdekking van een datalek dient de vraag of A-Creation verantwoordelijk is voor het melden van het datalek beantwoord te worden:

<u>Antwoord: A-Creation is niet verantwoordelijk</u>

Indien A-Creation niet zelf de verantwoordelijke is, wordt er melding gedaan als bewerker / verwerker conform de contactgegevens in de verwerkersovereenkomst. De melding wordt binnen de termijn die gesteld is in de verwerkersovereenkomst gemaakt of, indien dit niet of niet duidelijk is opgenomen in de verwerkersovereenkomst, binnen 8 kantooruren na ontdekking van het datalek. De *privacyverantwoordelijke* moet zorg dragen voor de overige meldingen. A-Creation volgt alleen de instructies van de *privacyverantwoordelijke*.

Of;

<u>Antwoord: A-Creation is verantwoordelijk</u>

Als er sprake is van een niet uitsluitbaar datalek en A-Creation verantwoordelijk is, dan doet de *privacyverantwoordelijke* het volgende:

- Afronden onderzoek en goed vastleggen uitkomsten in een apart incidentenrapport.
- Inschatten ernst incident: een incident is ernstig als er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Een incident met gevoelige persoonsgegevens is altijd ernstig, ook met 1 persoon. Een incident zonder gevoelige persoonsgegevens is ernstig bij een voldoende omvang.
- Indien sprake is van een ernstig datalek wordt er een jurist ingeschakeld om mee te denken over de communicatie en met betrekking tot het handelen naar de Autoriteit Persoonsgegevens dan wel de betrokkenen.
- Als het datalek ernstig is, dan moet het incident via het webformulier gemeld worden bij de Autoriteit Persoonsgegevens. Dit moet indien mogelijk **binnen 72 uur na ontdekking**.
- De *privacyverantwoordelijke* schat in of het melden aan betrokkenen mogelijk is en of een melding eventueel nadelige gevolgen heeft voor de betrokken persoon. Als het mogelijk is om te

melden, dit geen nadelige gevolgen heeft voor betrokkenen en er geen sprake is van een goede encryptie, wordt het datalek gemeld aan betrokkenen.

Wat moet er gemeld worden aan de betrokkenen:
Indien de *privacyverantwoordelijke* beoordeeld heeft dat er een melding van het datalek aan betrokkenen gedaan moet worden, informeert A-Creation de betrokkenen onder andere over het volgende:

- Dat er een datalek heeft plaatsgevonden waarbij zijn of haar persoonsgegevens betrokken zijn geweest.
- Welke persoonsgegevens dit zijn.
- Wanneer het datalek heeft plaatsgevonden.
- Welke risico's het datalek met zich mee brengt.
- Welke stappen betrokkenen kunnen of dienen te nemen om eventuele schade zoveel mogelijk te beperken.
- Of het datalek gemeld is dan wel dient te worden bij de Autoriteit Persoonsgegevens.

- De *privacyverantwoordelijke* denkt na over verbeteringen die toekomstige datalekken kunnen voorkomen. Dit hoeft niet direct maar kan bijvoorbeeld elke maand gebeuren.

Stap 5 - Zes maandelijkse evaluatie

Alle documentatie met betrekking tot het datalek en de melding worden bewaard voor minimaal een jaar (wettelijke vereiste). De *privacyverantwoordelijke* agendeert tweemaal per jaar een evaluatie van (het beleid ten aanzien van) datalekken over de afgelopen periode (zes maanden). Indien er sprake is van nieuwe informatie waardoor blijkt dat er alsnog gemeld moet worden draagt de *privacyverantwoordelijke* hier zorg voor en wordt het datalek opnieuw opgenomen op de lijst ter evaluatie.