STICHTING MEDIC

Procedure Datalekken

In het kader van de Privacywetgeving geldt sinds 1 januari 2016 de meldplicht datalekken. Met deze meldplicht is bij wet geregeld dat organisaties direct een melding moeten doen bij de Autoriteit Persoonsgegevens (AP), zodra er sprake is van een datalek. Hierbij moet er kans zijn op ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens. In een aantal gevallen moet dit datalek ook gemeld worden aan de betrokkenen. Stichting Medic dient zich als organisatie ook te conformeren aan deze meldplicht.

In deze procedure wordt daarom beschreven wat er dient te gebeuren op het moment dat er sprake is van een (vermeend) datalek.

> *Een bewerker verwerkt persoonsgegevens ten behoeve van de verantwoordelijke, zonder dat hij aan het rechtstreekse gezag van de verantwoordelijke is onderworpen (artikel 1, sub e, Wbp). Van verwerking door een bewerker is bijvoorbeeld sprake bij het verwerken van persoonsgegevens in de cloud of bij externe hosting van een website waar persoonsgegevens worden verwerkt.*[1]

Het belang van een adequate melding is groot. Indien een melding te laat gedaan wordt of indien er sprake is van ernstige tekortkomingen aan de zijde van Stichting Medic, kan er een boete van maximaal €820.000,- of 10% van de netto jaaromzet opgelegd worden. Een melding van een (mogelijk) datalek moet binnen 72 uur gedaan worden.

> *Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens. We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden. Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.*[2]

[1] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken.pdf

[2] Website AP: https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

1. Melden mogelijk datalek

Op het moment dat u het idee of vermoeden heeft dat er een datalek is, moet u dit zo snel mogelijk melden bij het bestuur.

Wanneer is iets mogelijk een datalek?

Naar letter van de wet kan iets al heel snel een datalek zijn. Hieronder volgen enkele voorbeelden.

- Iemand heeft onbedoeld de beschikking gekregen over de inlog-gegevens van de gegevensbeheerder.
- Een brief die gestuurd is naar de verkeerde persoon en gelezen wordt door iemand anders dan de persoon waar deze voor bestemd was;
- Een ledenlijst met persoonsgegevens die verstrekt is aan iemand die hier geen inzicht in had mogen hebben;
- Een maillijst die verstrekt is aan een externe partij die dit niet had mogen ontvangen.

2. Bepalen of het daadwerkelijk een datalek is

Het bestuur bepaalt vervolgens of het gemelde issue daadwerkelijk een datalek is. Tevens moet er bepaald worden of het lek zo ernstig is dat de betrokkenen (de personen waarvan gegevens gelekt zijn) geïnformeerd dienen te worden. Indien er informatie niet duidelijk is zal er geprobeerd worden om dit duidelijker te krijgen bij de melder, dan wel bij andere mogelijk betrokkenen

3. Melding maken bij de AP

Indien er wordt bepaald dat het daadwerkelijk een datalek betreft, wordt er een melding gedaan bij de AP.

4. Betrokkenen informeren

Indien de aard van het datalek dusdanig is dat de betrokkenen dienen te worden geïnformeerd zal dit zo snel mogelijk gedaan worden. De vorm van communicatie hangt af van de hoeveelheid gegevens die gelekt is.

5. Vastleggen datalek

Een datalek dat gemeld is bij de AP wordt vastgelegd in een dossier onder verantwoording van het bestuur.