Procedure

Datalekken – verwerkingsverantwoordelijke

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 met kans op ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens. In een aantal gevallen moet dit datalek ook gemeld worden aan de betrokkenen. Scouting Nederland dient zich als organisatie ook te conformeren aan deze meldplicht. Dit geldt ook voor Scoutinggroepen, -regio's en andere organisatieonderdelen die in het kader van de wetgeving gezien worden als 'bewerker' van gegevens van de organisatie Scouting Nederland.

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

Het belang van een adequate melding is groot. Indien een melding te laat gedaan wordt of indien er sprake is van ernstige tekortkomingen, kan er een forse boete opgelegd worden. Een (mogelijk) datalek moet binnen 72 uur goed behandeld 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.[1]

---

1. Datalek melden

Op het moment dat je het idee hebt dat er een datalek is, moet dit zo snel mogelijk gemeld worden aan de afdeling Juridische zaken binnen het landelijk servicecentrum van Scouting Nederland. Hiervoor gebruik je het mailadres: **privacy@scouting.nl**. Bij twijfel of voor advies kun je ook van dit e-mailadres gebruik maken of telefonisch contact opnemen via 033-4960911.

Via deze mailbox worden direct de juiste personen die betrokken zijn bij de afhandeling van een datalek op de hoogte gesteld. Het is afhankelijk van de omstandigheden van het lek welke acties moeten volgen. Werkgroep privacy ondersteunt of neemt de leiding naar gelang die omstandigheden.

Indien mogelijk, neem zo snel mogelijk maatregelen om het lek te dichten.

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 log-in gegevens van de gegevensbeheerder van je groep voor Scouts Online;
- 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 van de groep met persoonsgegevens die verstrekt is aan iemand die hier geen inzicht in had mogen hebben;
- Een presentielijst met adresgegevens die verdwenen is uit het clubhuis;

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

- Een post-it met de naam, geboortedatum en het e-mailadres van een nieuw lid dat is blijven rondslingeren en voor onbevoegden inzichtelijk is geweest;
- Een maillijst die verstrekt is aan een externe partij die dit niet had mogen ontvangen.

2. Bepalen of het een datalek is
Er zal nu bepaald moeten worden of het gemelde issue daadwerkelijk een datalek is. Tevens moet er bepaald worden of het lek ernstig genoeg is dat er een melding bij de AP gemaakt moet worden en 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.

Er kan al snel sprake zijn van een datalek. Bijvoorbeeld als gegevens verloren raken, gestolen worden of op een andere manier mogelijk onder ogen zijn gekomen van onbevoegde personen. Het maakt voor bepalen van een datalek niet uit wat voor gegevens het gaat, op welke wijze of van hoeveel personen. Dat maakt wél uit voor de vervolgstappen.

3. Melding maken bij de AP
Indien er wordt bepaald dat het daadwerkelijk een datalek betreft, dient er mogelijk een melding gemaakt te worden bij de AP. Indien Scouting Nederland de verwerkingsverantwoordelijke is, zal de afdeling Juridische zaken de melding verzorgen. Als een groep, regio of andere organisatie verantwoordelijke is, dient deze organisatie dat zelf te doen. De werkgroep kan daarbij adviseren.

Alhoewel een datalek in principe gemeld moet worden, heeft de Autoriteit Persoonsgegevens duidelijk gemaakt wanneer een melding nodig is. Er hoeft niet bij elk datalek een melding gemaakt te worden. Uitgangspunt is wel dat je meldt, tenzij het niet nodig is. Dus bij twijfel doe je een melding.
Een melding moet gedaan worden als er aanzienlijke kans is op ernstige nadelige gevolgen voor de betrokken personen. Dus degenen waarvan de gegevens onderdeel zijn van het lek. Die kans op ernstige nadelige gevolgen is aannemelijk als er zeer vertrouwelijke informatie vrij is gekomen. Ook is het van belang om hoeveel personen het gaat. Dit vraagt dus om een inschatting door de verantwoordelijke organisatie. Deze melding moet zo snel mogelijk gedaan worden, maar in ieder geval binnen 72 uur nadat het datalek bij de organisatie bekend is geworden. Die tijd is gesteld zodat je als organisatie de tijd hebt om te onderzoeken wat er aan de hand is en verdere gevolgen te voorkomen.

4. Betrokkenen informeren
Indien de aard van het datalek dusdanig is dat de betrokkenen dienen te worden geïnformeerd moet dit zo snel mogelijk gedaan worden. De vorm van communicatie hangt af van de hoeveelheid gegevens die gelekt is. Het informeren moet gedaan worden door de verantwoordelijke organisatie. Indien Scouting Nederland dit verzorgt, wordt de melder wordt hiervan op de hoogte gebracht.

5. Vastleggen datalek
Een datalek dient vastgelegd te worden in een incidentenregister, ook als het niet gemeld is bij de AP. De verantwoordelijke organisatie houdt dat zelf bij. De afdeling juridische zaken van Scouting Nederland maakt van elke melding ook een registratie.

In een incidentenregister leg je vast:
- een korte omschrijving van het lek;
- wanneer het plaatsvond;
- wat er met de gegevens is gebeurd (zijn ze verloren gegaan, of door een onbevoegde ingezien, gekopieerd of gewijzigd?);
- van welke groep(en) personen er gegevens gelekt zijn, en om hoeveel personen het gaat;
- om welke soorten gegevens het gaat.

- de (mogelijke) gevolgen van de inbreuk (bijvoorbeeld een risico op identiteitsfraude of reputatieschade);
- de maatregelen die zijn genomen naar aanleiding van het lek. Welke actie is ondernomen om schade te voorkomen of zo veel mogelijk te beperken (bijvoorbeeld het op afstand wissen van gegevens, of het wijzigen van wachtwoorden)? Maar ook: wat heb je gedaan om te zorgen dat het niet nog een keer kan gebeuren?

Meer informatie is te vinden bij de Autoriteit Persoonsgegevens, via https://autoriteitpersoonsgegevens.nl/.