Handout datalekken

De Privacywetgeving bepaalt dat er een meldplicht is bij de Autoriteit Persoonsgegevens (AP), in geval 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. 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 Scoutinggroep St. Joris Zutphen, ook een bewerker van Scouting Nederland. Een melding van een (mogelijk) datalek moet binnen 72 uur gedaan worden bij de AP.

Bewerker
Een bewerker verwerkt persoonsgegevens ten behoeve van de verantwoordelijke, zonder dat hij aan het rechtstreekse gezag van de verantwoordelijke is onderworpen. 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.

Datalek
Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van (bijzondere) 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. Bij een datalek zijn de (bijzondere) 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
- een inbraak in een databestand door een hacker.

Maar ook:

- Iemand heeft onbedoeld de beschikking gekregen over de inloggegevens 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.
- 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.

Sancties
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 Scouting Nederland, kan er een boete van maximaal €820.000,- of 10% van de netto jaaromzet opgelegd worden.

Procedure

1. Datalek melden

Leden
Binnen de vereniging kan een vermoeden van een datalek worden gemeld bij de secretaris van de vereniging, via voorzitter@st-joris.nl of (liever) telefonisch. Indien de secretaris niet bereikbaar is, kan een melding worden gedaan via bestuur@st-joris.nl. De melding komt dan automatisch binnen bij de secretaris, groepsbegeleider en de penningmeester. Een van hen zal de melding oppakken en terugkoppelen welke actie is genomen.

Bestuur / secretaris
Op het moment dat je het idee hebt dat er een datalek is, moet dit zo snel mogelijk gemeld worden aan de werkgroep privacy 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 moment van mailen naar dit e-mailadres is het moment waarop de constatering formeel plaatsvindt.**

De volgende stappen worden ondernomen door Scouting Nederland, eventueel samen met de vereniging Scouting St. Joris Zutphen

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 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.

3. Melding maken bij de AP
Indien er wordt bepaald dat het daadwerkelijk een datalek betreft, dient er een melding gemaakt te worden bij de AP. Dit wordt gedaan door het landelijk servicecentrum. De melder (vereniging) wordt hiervan op de hoogte gebracht.

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. Het informeren zal gedaan worden door het landelijk servicecentrum. De melder wordt hiervan op de hoogte gebracht.

5. Vastleggen datalek
Een datalek, dat gemeld is bij de AP dient vastgelegd te worden in een dossier, ook dit neemt het landelijk servicecentrum voor haar rekening.

Bronnen:
https://www.scouting.nl/downloads/ondersteuning/kennisnetwerk/juridische-ondersteuning/privacywet-en-bescherming-persoonsgegevens/4213-procedure-datalekken-dataverwerkers/