Protocol Meldingsplicht Datalekken

De privacywetgeving verplicht sinds 1 januari 2016 de melding van datalekken. Met deze meldplicht is bij wet geregeld dat organisaties direct een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) als 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. VVV Westzaan dient zich als vereniging ook te houden aan deze meldplicht. Dit geldt ook voor alle (onderdelen van) organisaties die in het kader van de wetgeving gezien worden als 'bewerker'1 van gegevens van VVV Westzaan.

Het belang van een adequate melding is groot. Als een melding te laat gedaan wordt of als er sprake is van ernstige tekortkomingen van VVV Westzaan, kan er een hoge boete 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.

Voorbeelden van datalekken zijn een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.

In deze procedure wordt daarom beschreven wat er moet gebeuren op het moment dat er sprake is van een (vermeend) datalek bij een bewerker van VVV Westzaan.

1. Datalek melden

Op het moment dat iemand het idee heeft dat er een datalek is, moet dit zo snel mogelijk gemeld worden bij VVV Westzaan. Hiervoor gebruik je het mailadres: secretaris@vvvwestzaan.nl. Zorg er bij een melding voor dat je zeker weet dat de ontvanger het bericht ook direct zal lezen. Neem daarom altijd eerst (telefonisch) contact om een datalek melding aan te kondigen. Bij twijfel of voor advies kun je ook van dit e-mailadres gebruik maken of telefonisch contact opnemen. Zie de website voor contactgegevens. Na melding worden direct de juiste personen die betrokken zijn bij de afhandeling van een datalek op de hoogte gesteld. Het moment van melden per e-mail is het moment waarop de constatering formeel plaatsvindt.

2. 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 ledenadministratie; 1 Een bewerker verwerkt persoonsgegevens ten behoeve van de VVV Westzaan, zonder dat hij aan het rechtstreekse gezag van VVV Westzaan 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. • 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 briefje 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.

3. Bepalen of het een datalek is.

Er zal nu bepaald moeten worden of de melding daadwerkelijk een datalek is. Ook moet er bepaald worden of het lek ernstig genoeg is dat de betrokkenen (de personen waarvan gegevens gelekt zijn) geïnformeerd dienen te worden. Als er informatie niet duidelijk is, zal er geprobeerd worden om dit duidelijker te krijgen bij de melder.

4. Melding maken bij de AP.

Als er wordt bepaald dat het daadwerkelijk een datalek betreft, dient er een melding gemaakt te worden bij de AP. Dit wordt gedaan door het bestuur. De melder wordt hiervan op de hoogte gebracht.

5. Betrokkenen informeren.

Als 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 bestuur. De melder wordt hiervan op de hoogte gebracht.

6. Vastleggen datalek.

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

7. Belangrijke contactgegevens.

Autoriteit Persoonsgegevens: 0900 - 3282 535 / www.autoriteitpersoonsgegevens.n