PROTOCOL MELDPLICHT DATALEKKEN
VERENIGING ZWEMBAD JEKERDAL

Een handleiding voor de correcte afhandeling van datalekken

Bedrijfsgegevens:
Waldeckpark 1
6213 AG Maastricht
KvK-nummer: 40204588

Contactgegevens:
043 325 03 97
voorzitter@jekerdal.nl

I. Inleiding

Sinds 1 januari 2016 bestaat de wettelijke verplichting om datalekken te melden. Zowel grootschalige inbreuk als ieder kwijtraken of onbevoegd gebruik van persoonsgegevens geldt als een datalek.

Op 1 mei 2018 is de Algemene Verordening Gegevensbescherming (hierna: '**AVG**') in werking getreden. Onder de AVG blijft deze meldplicht ongewijzigd. Echter, de consequenties die worden verbonden aan het lekken van data zijn aanzienlijk verhoogd met de introductie van de AVG. De AVG stelt hoge boetes die kunnen oplopen tot maximaal € 10.000.000,00 of 2% van de jaaromzet per overtreding. De Autoriteit Persoonsgegevens (hierna: '**AP**') houdt in Nederland toezicht op de naleving van de AVG door bedrijven.

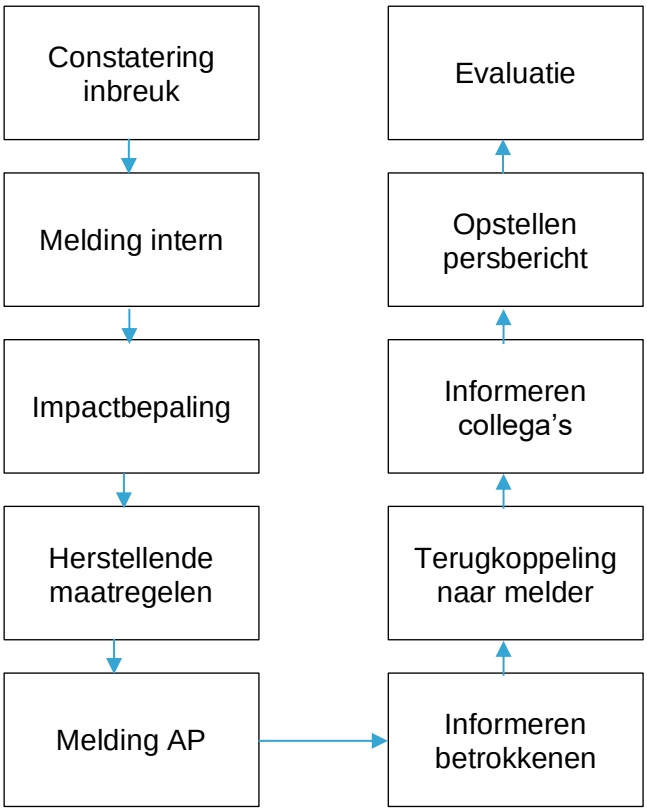
Er is sprake van een datalek wanneer persoonsgegevens verloren raken of wanneer een onrechtmatige verwerking van deze gegevens niet kan worden uitgesloten. Onder onrechtmatige verwerking kan onder meer het aanpassen en veranderen van of de onbevoegde toegang tot persoonsgegevens worden verstaan. Het gaat om een brede definitie. Er is niet alleen sprake van een datalek als een hacker toegang tot de persoonsgegevens krijgt. Ook het verlies van USB-sticks of een e-mail met de adressen in het CC-veld in plaats van in het BCC-veld kwalificeert als een datalek.

Zoals hiervoor beschreven moet het gaan om een datalek waarbij persoonsgegevens betrokken zijn. Een persoonsgegeven is informatie over een natuurlijk persoon. Een hack waarbij gegevens over bedrijven of technische informatie gestolen wordt, kan niet worden aangemerkt als een datalek.

Deze handleiding dient te worden gehanteerd door Vereniging Zwembad Jekerdal (hierna: '**Jekerdal**') indien sprake is van een datalek. Stap voor stap wordt de te volgen algemene en juridische procedure beschreven. Ook biedt deze handleiding een handvat hoe datalekken te inventariseren en betrokkenen te informeren.

II. Procedure

STAPPENPLAN



ALGEMENE PROCEDURE

Binnen 72 uur na ontdekking van het datalek moet er een melding bij de AP zijn gedaan, ongeacht feestdagen, weekenden of andere vrije dagen.

1. Constatering inbreuk op de beveiliging van ICT-systemen door:
   a. Een medewerker/vrijwilliger:
      Direct intern melden bij het bestuur via 043 – 325 03 97 / voorzitter@jekerdal.nl.

   b. Een lid van Jekerdal die niet ook vrijwilliger is:
      Na melding van het lid bij de dienstdoende coördinator zet de dienstdoende coördinator de informatie direct door naar de voorzitter van het bestuur via 043 – 325 03 97 / voorzitter@jekerdal.nl.

   c. Een derde partij:
      Na melding van de derde partij lid zet de dienstdoende coördinator de informatie direct door naar de voorzitter van het bestuur via 043 – 325 03 97 / voorzitter@jekerdal.nl.

      NB. Buiten openingstijden wordt de telefoon doorgeschakeld naar de verantwoordelijke op dat moment.

2. Na de interne melding vindt een inventarisatie van het incident plaats aan de hand van **Bijlage 1**.

3. Onderzoek naar de omvang en technische aspecten van het datalek (**binnen 24 uur**).
   a. Welke inbreuk op de beveiligingsmaatregelen heeft plaatsgevonden en wanneer?

   b. Welk onderdeel van het ICT-systeem is betrokken en/of welke apparatuur? Eventueel: waar is de apparatuur verloren gegaan/gestolen?

   c. Welke gegevens zijn mogelijk betrokken?

   d. Wat zijn de (verwachte) consequenties van het incident?

4. Identificeren maatregelen om de beveiliging te herstellen en uitvoeren van deze maatregelen. Dit dient te gebeuren binnen 72 uur na melding. Indien dit niet haalbaar is binnen deze tijd, dient dit alsnog zo spoedig mogelijk te gebeuren. Er zal in dat laatste geval schriftelijk moeten worden vastgelegd waarom het niet mogelijk was om binnen 72 uur na de melding herstellende maatregelen te treffen.

5. Als het incident moet worden gemeld, dient er melding naar de AP te worden opgesteld (binnen 72 uur).

6. Indien nodig: informeren betrokkene (tegelijkertijd met melding AP).

7. Indien nodig: terugkoppeling naar melder (na melding AP).

8. Indien nodig: opstellen persbericht (na melding AP).

9. Evaluatie intern.

JURIDISCHE PROCEDURE

1. Constatering inbreuk op beveiligingssystemen of verlies van apparatuur of dossiers.

2. Welke gegevens waren toegankelijk?

3. Zijn deze gegevens aan te merken als persoonsgegevens?

> **NB.** Persoonsgegevens zijn alle gegevens betreffende een geïdentificeerde of identificeerbare persoon. Een persoon is identificeerbaar als zijn/haar identiteit redelijkerwijs zonder onevenredige inspanning kan worden vastgesteld.

4. Is er sprake van een datalek?

   a. Zijn de verwerkte persoonsgegevens onherstelbaar verwijderd of aangepast of is er sprake van onrechtmatige verwerking? Zo ja, dan is er sprake van een datalek.

NB. Een onrechtmatige verwerking is het onbedoeld en onbevoegd wijzigen, verstrekken of toegankelijk maken van persoonsgegevens.

b. Kan redelijkerwijs worden uitgesloten dat persoonsgegevens verloren zijn gegaan? Zo ja, dan is er geen sprake van een datalek.

5. Is Jekerdal de verantwoordelijke voor de verwerking?

a. Verantwoordelijk is degene die alleen of gezamenlijk met anderen het doel en de middelen van de verwerking van persoonsgegevens vaststelt.
b. Voor de gegevensverwerkingen die in samenwerking met een ander plaatsvinden bestaat een gedeelde verantwoordelijkheid. Jekerdal kan in dat geval contact opnemen met de andere partij.
c. Wanneer Jekerdal niet is aan te merken als verantwoordelijke, is Jekerdal verplicht degene die verantwoordelijk is op de hoogte te brengen van het datalek.

6. Moet dit lek worden gemeld aan de Autoriteit Persoonsgegevens?

Een datalek moet worden gemeld bij de AP, tenzij niet waarschijnlijk is dat de inbreuk een risico voor de betrokkenen inhoudt. Bijvoorbeeld wanneer:

- De persoonsgegevens publiekelijk beschikbaar zijn;
- De persoonsgegevens versleuteld zijn en het wachtwoord niet is gelekt;
- Het gaat om onbedoeld verlies van persoonsgegevens terwijl deze gegevens via een back-up te herstellen zijn. Een melding kan worden gedaan op de website van de AP (*www.autoriteitpersoonsgegevens.nl*).

7. Moet dit lek worden gemeld aan de betrokkenen (**Bijlage 2**)?

a. Een datalek moet worden gemeld aan de betrokkene wanneer de inbreuk waarschijnlijk een hoog risico voor de betrokkene inhoudt.

NB. Van een hoog risico is sprake wanneer de verwachte nadelige gevolgen van het datalek zich met grote waarschijnlijkheid voordoen. Voorbeelden van nadelige gevolgen zijn identiteitsfraude, reputatieschade, financiële verliezen, ongewenste communicatie enzovoorts.

b. Bieden de technische beschermingsmaatregelen (zoals encryptie) die zijn genomen voldoende bescherming om de melding aan betrokkenen achterwege te kunnen laten?

I. Zijn de persoonsgegevens onherstelbaar verwijderd of aangepast? Dan heeft de encryptie geen zin gehad en moeten de betrokkenen worden ingelicht.
II. Waren alle persoonsgegevens versleuteld op het moment dat de inbreuk plaatsvond?
III. Is de versleuteling adequaat?
IV. Is het restrisico acceptabel?

Is het antwoord op II t/m IV 'ja', dan is melding aan betrokkenen niet verplicht.

c. Zijn er direct maatregelen genomen om ervoor te zorgen dat betrokkenen geen nadeel van het datalek ondervinden? Zo ja, dan is melding aan betrokkenen niet verplicht.
d. Is het informeren van alle betrokkenen een onevenredig zware inspanning (bijvoorbeeld omdat het gaat om zeer grote aantallen betrokkenen)? In dat geval is een persoonlijke mededeling per betrokkene niet nodig en kunnen betrokkenen op een andere manier worden geïnformeerd.

8. Als een datalek niet aan de AP of aan betrokkenen hoeft te worden gemeld, dan geldt wel een registratieplicht. Alle datalekken die zich hebben voorgedaan moeten op een centrale plaats worden gedocumenteerd.

BIJLAGE 1: Inventarisatie datalekken

1. Naam, bedrijf (indien van toepassing), telefoonnummer en e-mailadres melder noteren.
2. Wanneer en hoe is het datalek geconstateerd?
3. In welk systeem bevindt het lek zich?
4. Hoe werkt het lek? Is het lek reproduceerbaar?
5. Welke gegevens zijn toegankelijk geworden?
6. Welke handelingen met betrekking tot de gegevens zijn mogelijk?
7. Heeft de melder ideeën hoe het lek hersteld kan worden?
8. Gaat de melder het datalek publiek maken? Zo ja, wanneer? Indien ja, verzoek de melder om 72 uur te wachten zodat eerst maatregelen getroffen kunnen worden.

BIJLAGE 2: Informeren betrokkenen

Sommige datalekken zijn zo ernstig dat de betrokkene(n) moet(en) worden ingelicht. In deze bijlage wordt ingegaan op de vraag hoe de betrokkene(n) moet(en) worden geïnformeerd, hierna te noemen: "**de Betrokkene**" (in enkelvoud).

> **NB.** Betrokkenen zijn de personen op wie de gelekte persoonsgegevens betrekking hebben.

In de kennisgeving aan de betrokkene(n) wordt in ieder geval vermeld:

- De aard van de inbreuk: bij het beschrijven van de aard en de inhoud van de inbreuk kan met een algemene omschrijving worden volstaan. Uitwijden over de technische details is niet nodig. Er moet een aan bod komen welke gegevens zijn gelekt, wat hiervan de gevolgen voor de Betrokkene zouden kunnen zijn en welke maatregelen zijn genomen om de inbreuk aan te pakken. Belangrijk is dat de beschrijving in eenvoudige taal is.
- De vermoedelijke datum en tijdstip van het incident.
- De ernst van het datalek: informeer de Betrokkene over de gevolgen die zich mogelijk/waarschijnlijk kunnen/zullen voordoen naar aanleiding van het datalek. Denk aan identiteitsfraude, reputatieschade, financiële verliezen en ongewenste communicatie.
- De maatregelen die zijn genomen om de inbreuk aan te pakken en de nadelige gevolgen voor betrokkenen te beperken. Denk aan zaken als: Hoe is het datalek gedicht? Kan de Betrokkene een schadeclaim indienen?
- De maatregelen die de Betrokkene moet nemen om de negatieve gevolgen van de inbreuk te beperken. Denk hierbij aan het veranderen van gebruikersnamen en wachtwoorden.
- De contactgegevens: op welke manier kan de Betrokkene iemand bereiken als er nog vragen zijn.
- De instanties waar de Betrokkene meer informatie over de inbreuk kan krijgen, indien van toepassing.

Het belangrijkste is dat zoveel mogelijk betrokkenen worden bereikt, enerzijds met informatie over de nadelige gevolgen en anderzijds met informatie om de nadelige gevolgen te beperken. De mededeling is vormvrij. Het is raadzaam om de mededeling schriftelijk te doen. Dat mag ook via de e-mail.