Leidraad Datalekken OV Driehuis e.o.

Van een datalek is sprake bij een inbreuk op de beveiliging van persoonsgegevens die leidt tot enige ongeoorloofde verwerking hiervan.

Een inbreuk op de beveiliging houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Er is niet uitsluitend sprake van een dreiging, of van een tekortkoming in de beveiliging (ook wel aangeduid als beveiligingslek) die zou kunnen leiden tot een beveiligingsincident. Er heeft zich daadwerkelijk een beveiligingsincident voorgedaan en de preventieve maatregelen die OV Driehuis e.o. heeft getroffen waren niet toereikend om dit te voorkomen.
Voorbeelden van een datalek zijn:

- Een hack;
- Ransomware;
- Verkeerd geadresseerde e-mails;
- Verlies inloggegevens die toegang geven tot persoonsgegevens;
- Verlies of diefstal van een usb-stick, computer of andere gegevensdrager met daarop persoonsgegevens.

Melding bij de Autoriteit Persoonsgegevens
Een datalek moet zonder vertraging worden gemeld aan de Autoriteit Persoonsgegevens. De melding kan bij het meldloket op de website van de Autoriteit worden gedaan: https://datalekken.autoriteitpersoonsgegevens.nl

Een melding kan achterwege blijven indien het niet waarschijnlijk is dat de inbreuk redelijkerwijs een risico voor betrokkenen met zich meebrengt. Het datalek moet echter wel altijd worden gedocumenteerd.
Als streeftijd voor de melding geldt een termijn van uiterlijk 72 uur nadat het datalek daadwerkelijk ter kennis is genomen door OV Driehuis e.o.
Indien een verwerker/opdrachtnemer van OV Driehuis e.o. een datalek ontdekt, dan dient deze partij OV Driehuis e.o. onverwijld, zonder onredelijke vertraging hierover te informeren, zodat OV Driehuis e.o. melding bij de Autoriteit kan doen.

Mededeling aan de betrokkene
Indien er waarschijnlijk sprake is van een hoog risico op negatieve gevolgen voor de betrokkene (de persoon van wie de persoonsgegevens zijn gelekt) dient het datalek ook aan de betrokkene te worden medegedeeld. Negatieve gevolgen zijn bijvoorbeeld:

- Verlies van controle door betrokkene over de persoonsgegevens;
- Het niet kunnen uitoefenen van de rechten (zoals wissing of rectificatie);
- Identiteitsdiefstal of –fraude;
- Financiële verliezen;
- Ongedaanmaking van pseudonomisering;
- Reputatieschade.

De mededeling aan de betrokkene dient in duidelijk en eenvoudige taal een omschrijving te omvatten van de aard van de inbreuk in verband met persoonsgegevens, alsmede de volgende informatie:

- De aard van de inbreuk in verband met de persoonsgegevens, onder vermelding van het persoonsgegevensregister (indien aanwezig) en indien mogelijk de categorieën van betrokkenen, en bij benadering het aantal betrokkenen;
- De naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt binnen OV Driehuis e.o. waar meer informatie kan worden verkregen;
- De waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens.

Mededeling aan de betrokkene is niet vereist indien:

- OV Driehuis e.o. passende technische en organisatorische maatregelen heeft getroffen waardoor misbruik is uit te sluiten. Denk hierbij aan encryptie of versleuteling;
- OV Driehuis e.o. direct na het datalek maatregelen heeft getroffen waardoor het risico voor de betrokkene zich waarschijnlijk niet meer zal voordoen;
- Het doen van de mededeling een onevenredige inspanning zou vergen, bijvoorbeeld omdat het om een zeer grote groep betrokkenen gaat.

Alle datalekken (ook welke niet aan de Autoriteit Persoonsgegevens worden gemeld) dienen te worden gedocumenteerd. Daarbij dienen in ieder geval de volgende zaken te worden geregistreerd:

- De feiten omtrent de inbreuk in verband met de persoonsgegevens;
- De gevolgen van de inbreuk;
- De genomen corrigerende maatregelen.

Samenvattend:

- Altijd: intern documenteren van het datalek;
- Melding doen bij de Autoriteit Persoonsgegevens, tenzij er redelijkerwijs geen risico bestaat voor de betrokkene(n);
- Mededeling doen aan de betrokkene bij hoog risico op negatieve gevolgen voor de betrokkene.