Procedure Beveiligingsincident en Datalek

Je verwerkt gegevens van jouw opvangkinderen en hun ouders. De regels rondom de privacy en veiligheid van deze gegevens zijn vastgelegd in de wet AVG (Algemene Verordening Gegevensbescherming). Maar wat nu als er toch per ongeluk, ondanks alle voorzorgsmaatregelen, gegevens verloren gaan? Dan spreken we van een beveiligingsincident of mogelijk zelfs een datalek. In deze procedure staat beschreven wat te doen bij een beveiligingsincident of datalek. Wat is het precies en hoe moet je handelen?

Wat is een datalek?

We spreken van een mogelijk datalek in het geval van een incident waarbij (gevoelige) persoonsgegevens verloren zijn gegaan. Als niet kan worden uitgesloten dat gevoelige gegevens mogelijk onrechtmatig worden verwerkt, dan spreken we zelfs van een ernstig datalek. Gevoelige persoonsgegevens van jouw klanten zijn in verkeerde handen terecht gekomen.

Wanneer het geen gevoelige persoonsgegevens betreft en je kunt wel uitsluiten dat het in verkeerde handen terecht is gekomen, spreken we van een beveiligingsincident.

Wat zijn Persoonsgegevens?
Persoonsgegevens zijn alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon. Bijvoorbeeld iemands naam, geboortedatum of geslacht. Gevoelige persoonsgegevens zijn gegevens die zó gevoelig zijn, dat de verwerking ervan iemands privacy ernstig kan beïnvloeden. Denk aan medische informatie, godsdienst of BSN .

Voorbeelden van een mogelijk datalek
De meest voorkomende situaties waarbij je het risico op een (ernstig) datalek loopt, zijn:
- Je bent je laptop, telefoon, usb-stick of papieren met daarop persoonsgegevens van jouw klanten verloren of deze zijn gestolen
- Je computer, met daarop persoonsgegevens van jouw klanten, is gehackt
- Bij een inbraak in je woning zijn persoonsgegevens meegenomen of mogelijk bekeken
- Persoonsgegevens van jouw klanten zijn zichtbaar geworden voor anderen, doordat je bijvoorbeeld een verkeerd emailadres, telefoonnummer of postadres hebt gebruikt

Stap 1: Beoordeel het datalek

Als je te maken hebt met een datalek, dan moet je zo snel mogelijk de ernst van de situatie bepalen. Is er sprake van een (ernstig) datalek of 'slechts' een beveiligingsincident? Het oordeel is bepalend voor je vervolgactie. Om te bepalen waar je mee te maken hebt, beantwoord je eerst onderstaande belangrijke vragen:

1. Zijn er persoonsgegevens van gevoelige aard gelekt?
   Als gastouder verwerk je mogelijk de volgende gevoelige persoonsgegevens:
   - Gegevens over de verzorging en ontwikkeling van je opvangkind(eren)
   - Gegevens over de gezondheid van je opvangkind(eren)
   - Beeldmateriaal (foto's en video's van kinderen)

2. Leiden de aard en de omvang van het datalek tot (een aanzienlijke kans op) ernstige nadelige gevolgen voor betrokkene(n)?

(Ernstig) datalek of beveiligingsincident?

- Is het antwoord op één of beide vragen 'Ja'?
  Dan is er sprake van een ernstig datalek. Je bent dan verplicht om daar melding van te maken bij de Autoriteit Persoonsgegevens. Zie stap 2, voor meer informatie
- Kun je de vragen allebei met 'Nee' beantwoorden?
  Gelukkig! Dan is er geen sprake van een ernstig datalek. Je hebt dan te maken met een beveiligingsincident. Deze moet je wel documenteren. Zie stap 2

Stap 2: Actie ondernemen

Ernstig datalek? Melden!

Een ernstig datalek meld je direct bij de Autoriteit Persoonsgegevens. Een ernstig datalek moet binnen 72 uur gemeld worden. Lukt dat niet? Dan moet je een motivering voor de vertraging opgeven.
De melding van het datalek heeft verder geen gevolgen voor jou. De link naar het datalek meldformulier van de overheid vind je hier: https://datalekken.autoriteitpersoonsgegevens.nl

Risico op een boete
Meld je een ernstig datalek niet? Dan loop je het risico op een boete.

Meld het datalek ook aan de betrokkenen
Je moet de personen die het betreft, altijd informeren. Je geeft hierbij aan:

- Wat er gebeurd is
- Met wie ze contact kunnen opnemen voor meer informatie (Naam en contactgegevens)
- Wat de verwachte gevolgen zijn van het datalek voor betrokkenen
- Wat betrokkenen nu moeten doen om de schade te beperken

Datalek of Beveiligingsincident? Documenteren!

Onder de nieuwe privacywetgeving moet je een document bijhouden waarin je datalekken en/of beveiligingsincidenten vastlegt. Het gaat dan om de incidenten, die niet gemeld hoeven te worden bij de Autoriteit Persoonsgegevens. Van een ernstig datalek, maak je officieel melding.

In het document beschrijf je het volgende:

- Wat er gebeurd is
- Wat de gevolgen van het incident zijn
- Welke maatregelen er genomen zijn om een dergelijke situatie in de toekomst te voorkomen

Stap 3: Rapportage en evaluatie

Nadat je voorgaande stappen hebt doorlopen, beschrijf je op één A4-tje wat je precies bij iedere stap hebt gedaan. Zo maak je een volledige rapportage over ernstige datalekken en beveiligingsincidenten. Berg deze rapportage(s) zorgvuldig op en zorg ervoor dat je deze altijd kunt overleggen aan de Autoriteit Persoonsgegevens.