AVG en privacybeleid

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Met alle verkregen informatie en gegevens wordt vertrouwelijk omgegaan en niet ter beschikking aan derden gesteld, behoudens bij Wet Vastgestelde Uitzonderingen. Stichting Istia houdt zich aan de Wet Bescherming Persoonsgegevens.

- Alle formulieren en overeenkomsten worden opgeborgen in een afgesloten kast.
- De financiële- personele- en kind-administratie van Istia is opgeslagen in beveiligde online omgevingen waarbij met de leveranciers een verwerkersovereenkomst AVG is afgesloten.
- Alle digitale apparaten waar wij mee werken zijn beveiligd met een wachtwoord.
- Er zijn actuele virusscanners geïnstalleerd op de computers en laptops waar wij mee werken.
- Wij bewaren persoonsgegevens niet langer dan noodzakelijk voor het doel waarvoor deze zijn verstrekt, dan wel op grond van de wet is vereist.

Zie ook de 'Procedure Beveiligingsincident en Data-lek Istia'

Procedure Beveiligingsincident en Data-lek

Inleiding
Stichting Istia verwerkt gegevens van opvangkinderen en hun ouders. Sinds 25 mei 2018 zijn de regels rondom de privacy en veiligheid van deze gegevens aangescherpt in de vernieuwde wetgeving AVG. Maar wat nu als er toch per ongeluk, ondanks alle voorzorgsmaatregelen, gegevens verloren gaan? Dan spreken we van een beveiligingsincident of mogelijk zelfs een data-lek. In deze procedure staat beschreven wat te doen bij een beveiligingsincident of data-lek.
We spreken van een mogelijk data-lek in het geval van een incident waarbij (gevoelige) persoonsgegevens verloren zijn gegaan. Als niet kan worden uitgesloten dat gevoelige gegevens mogelijk onrechtmatig worden verwerkt, wordt er gesproken van een ernstig data-lek. Wanneer het geen gevoelige persoonsgegevens betreft en wanneer uitgesloten kan worden dat deze in verkeerde handen terecht zijn 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 data-lek De meest voorkomende situaties met risico op een data-lek zijn:

- Laptop, telefoon, usb-stick of papieren met daarop persoonsgegevens van ouders en opvangkinderen is verloren geraakt of deze zijn gestolen.
- De computer, met daarop de persoonsgegevens van de kinderopvang , is gehackt.
- Bij een inbraak zijn persoonsgegevens meegenomen of mogelijk bekeken.
- Persoonsgegevens zijn zichtbaar geworden voor anderen, doordat er bijvoorbeeld een verkeerd emailadres, telefoonnummer of postadres is gebruikt door medewerkers van Stichting Istia.

Is er sprake van een (ernstig) data-lek of ‘slechts’ een beveiligingsincident? Het oordeel is bepalend voor de vervolgactie.

- Zijn er persoonsgegevens van gevoelige aard gelekt?
- Leiden de aard en de omvang van het data-lek tot (een aanzienlijke kans op) ernstige nadelige gevolgen voor betrokkene(n)?

Is het antwoord op één of beide vragen ‘Ja’? Dan is er sprake van een ernstig data-lek. Je bent dan als organisatie verplicht om daar melding van te maken bij de Autoriteit Persoonsgegevens. Wanneer het antwoord op beide vragen nee is, is er geen sprake van een ernstig data-lek. Je hebt dan te maken met een beveiligingsincident.

Procedure bij een datalek

Een **ernstig data-lek** moet binnen 72 uur gemeld worden bij de Autoriteit Persoonsgegevens [1].
Bij vertraging dient er een motivering voor de vertraging opgeven te worden. Een melding van een data-lek heeft verder geen gevolgen.
Het data-lek moet ook aan de direct betrokkenen gemeld worden, wanneer het kan leiden tot fysieke, materiële of immateriële schade voor de betrokkenen. Zoals: discriminatie, (identiteits-)fraude, financiële schade en reputatieschade.

Wanneer er sprake is van **een beveiligings**incident dat hoeft dit niet gemeld bij de Autoriteit Persoonsgegevens. Onder de nieuwe privacywetgeving moet dit wel gedocumenteerd worden. Er dient in beschreven te worden wat er gebeurd is, wat de gevolgen zijn en welke maatregelen er zijn genomen om een dergelijke situatie in de toekomst te voorkomen. Deze rapportage(s) worden zorgvuldig opgeborgen en kunnen indien nodig overlegd worden aan de Autoriteit persoonsgegevens.

[1] De link van het data-lek meldformulier van de overheid: https://datalekken.autoriteitpersoonsgegevens.nl