Werkproces datalekken

Onderdeel van het IBP beleid van Curio.

Toelichting

Doel
De correcte afhandeling van de stappen die genomen moeten worden bij een (vermoedelijk) datalek.

Uitgangspunten

- Wanneer een medewerker (het vermoeden van) een datalek heeft, wordt dit direct gemeld. Dit ben je wettelijk verplicht.
- Bij vragen / onduidelijkheden, of bij grote datalekken (>5 getroffenen) neemt de medewerker telefonisch contact op met de Security Officer, Joris Weel (telefoonnummer via portal). Bij geen gehoor de voicemail inspreken, zodat er z.s.m. kan worden teruggebeld.

Procesbeschrijving:

Stap 1: De medewerker vult **direct** het meldformulier in: www.curio.nl/datalek

Stap 2: Security officer en/of coördinator IBP registreren het (vermoedelijke) datalek.
Geen datalek? Dan melden we dit aan je terug en is er geen verdere actie noodzakelijk.

Wel datalek?
Stap 3: Functionaris Gegevensbescherming beoordeelt het datalek en of er vervolgonderzoek noodzakelijk is.

- Risico voor de rechten en vrijheden van betrokkenen? We melden het bij de autoriteit persoonsgegevens.
- Hoog risico voor de rechten en vrijheden van de betrokkenen? We melden het ook bij de betrokkenen.

Vervolg:
We melden de wijze van afhandelen altijd aan je terug.
De functionaris die het datalek heeft geregistreerd voegt het volgende toe aan de registratie:

- Wat zijn de “lessons learned”.
- Zijn er aanvullende beheersmaatregelen nodig om dit in de toekomst te voorkomen?
- Eventueel wordt er een commissie in het leven geroepen om het datalek te evalueren. Dit zal voornamelijk zijn bij grote datalekken of datalekken met een grote impact voor de betrokkenen en/of organisatie.