Procedure bij het melden van gegevenslekken

1. Doel van deze procedure

Deze procedure legt vast wat er moet gebeuren bij een (vermoedelijk) gegevenslek.

- Welke stappen genomen moeten worden
- Door wie
- Wanneer

Met deze procedure streven we de volgende resultaten na:

- Het zorgvuldig waarborgen van de belangen van de betrokkene;
- Het zorgvuldig waarborgen van de belangen van vzw Pniël;
- Voldoen aan een vereiste uit GDPR;
- Het beperken van de risico's en de mogelijke schade bij een gegevenslek;
- Het bevorderen van het nemen van passende verbetermaatregelen;

Pniël heeft een centrale Data Protection Officer (DPO) aangesteld. Hij/zij is het aanspreekpunt als er een (vermoeden van) lek is.

2. Wat is een gegevenslek?

2.1 Wat is een persoonsgegeven

Een gegeven is een persoonsgegeven als het over een identificeerbare, natuurlijke persoon gaat. Deze persoon wordt betrokkene genoemd. In dit document onderscheiden we een aantal groepen betrokkenen: de bewoners, personeel en vrijwilligers, medewerkers, bezoekers en leveranciers. Het is van geen belang of het persoonsgegevens op een papieren dan wel digitale drager staat, en om welke type persoonsgegeven het gaat (contactgegevens, foto's, camerabeelden, geluidsopnames…).

2.2 Wat is een gegevenslek

We spreken van een inbreuk in verband met persoonsgegevens, of 'een gegevenslek', in het geval:

- Persoonlijke informatie beschikbaar is voor
  - Internen die deze gegevens niet nodig hebben in de uitoefening van hun taken
  - Externen
- Of, als persoonlijke informatie vernietigd, verloren of onterecht gewijzigd werd

Een gegevenslek vereist geen kwaad opzet. Bovendien is het voldoende dat een onbevoegde toegang zou kunnen hebben tot de gegevens.

2.3 Enkele voorbeelden van mogelijke datalekken

- Een medewerker van de leverancier komt in contact persoonsgegevens, hoewel hij daar geen toegang toe nodig heeft om zijn taken uit te kunnen voeren.
- Een vrijwilliger zoekt of kopieert persoonsgegevens naar een opslagmedium waar de verwerkingsverantwoordelijke geen toegang toe heeft.

- Er is een probleem met de beveiliging van een webserver waardoor persoonsgegevens beschikbaar worden op het internet.
- Een laptop met persoonsgegevens erop wordt gestolen.
- Een paswoord van een medewerker met toegang tot persoonsgegevens is gekend door anderen.
- Niet alle toegangen van een medewerker die de leverancier verlaten heeft worden verwijderd.

3. Werkwijze

3.1 Vaststelling van een gegevenslek

Eenieder die een beveiligingsincident met een mogelijk gegevenslek constateert, meldt dit incident meteen bij zijn leidinggevende.

Deze leidinggevende noteert de melding in het **'Formulier Incidentmelding'** en informeert Pniël.

3.2 Snelheid

Na kennisname van een mogelijke gegevenslek moet Pniël meteen verwittigd worden. De volledige doorlooptijd tussen de eerste melding en de eventuele melding aan de gegevensbeschermingsautoriteit mag **maximaal 72 uur** bedragen. Werk dus SNEL.

3.3 Eerste beoordeling aard/ernst incident

Hij die een vermoeden van een gegevenslek heeft, of dienst leidinggevende

- Verzamelt alle informatie die nuttig kan zijn om het incident te beoordelen
    - Vult het 'Formulier Incidentmelding' verder aan
- Maakt een eerste inschatting of er persoonsgegevens zouden kunnen gelekt zijn.
    - Zeker niets gelekt:
        - De procedure stopt hier
    - Bij twijfel of zeker wel iets gelekt:
        - Contacteer de centrale Data Protection Officer.
            - Stuur het ingevulde 'Formulier melding gegevenslek' via mail naar julie.vanhooreweghe@hict.be of bel naar +32 499 16 65 48
            - Heb je de DPO telefonisch niet kunnen bereiken, stuur een mail naar privacy@pniel.be

3.4 De Data Protection Officer (DPO) beoordeelt de risico's

De DPO

- Vraagt indien nodig extra informatie en
- Beoordeelt of er effectief een lek is
    - Nee:
        - De DPO zet de procedure stop.
    - Ja:
        - Hij beoordeelt de gevoeligheid van de gegevens en het risico dat die gegevens bij een groot aantal personen terecht komt en informeert het bestuur.
        - Hij onderzoekt of de gegevensbeschermingsautoriteit moet gecontacteerd worden en informeert het bestuur.
        - Hij onderzoekt hij of de betrokkenen moeten geïnformeerd worden en informeert het bestuur.

- Hij adviseert welke maatregelen bij dit incident kunnen genomen worden om nieuwe risico's of verdere schade te voorkomen.

3.5 Verdere acties op korte termijn

Het bestuur

- Oordeelt of een melding bij de politie nodig is, bijvoorbeeld bij hacking.
- Contacteert indien nodig de gegevensbeschermingsautoriteit, hetzij rechtstreeks, hetzij via de DPO.
- Beslist of en hoe de lokale directie moet communiceren naar de betrokkene(n).

3.6 Verdere acties na crisisinterventie

De DPO

- Stelt een rapport op over het lek en
- Onderzoekt welke maatregelen op middellange termijn nodig zijn om een herhaling te voorkomen.