Datalek procedure Stichting Talent Maatje Lansingerland

In dit document wordt aan de hand van een stappenplan beschreven hoe de Stichting Talent Maatje Lansingerland omgaat met een (structureel) incident betreffende het bekend zijn/worden van tot persoon herleidbare gegevens anders dan bij wie daar toe gerechtigd is. Een dergelijk incident wordt datalek genoemd.

Definitie:
Er is sprake van een datalek wanneer persoonsgegevens c.q. persoon herleidbare gegevens in handen komen van derden, die geen toegang tot de gegevens zouden mogen hebben.
Betrokkenen zijn degenen wiens persoonsgegevens het betreffen, de verwerkers daarvan, de onrechtmatige houder van deze gegevens en/of anderen die zijn betrokken bij een dergelijke inbreuk.

Alle datalekken van persoonsgegevens moeten intern worden gemeld aan en worden gedocumenteerd door de contactpersoon bescherming persoonsgegevens. Als contactpersoon is in de Stichting Talent Maatje Lansingerland vastgelegd dat dit het Dagelijks Bestuur van de Stichting is. De melding kan door iedere gebruiker en iedere medewerker of derde partij worden gedaan. De melding kan ook door een externe persoon worden gedaan bij een medewerker van de Stichting Talent Maatje Lansingerland, die er voor zorg draagt dat de vastgestelde contactpersoon van de Stichting daarvan in kennis wordt gesteld.
Alle medewerkers, vrijwilligers en leveranciers (bewerkers) van de Stichting zijn op de hoogte van de datalekprocedure.

Procedure

1. **Actie melder:**

Vaststellen of er sprake is van een datalek en zo ja, zo snel mogelijk melden bij contactpersoon bescherming persoonsgegevens. Deze melding kan schriftelijk, dan wel in persoon. In het uiterste geval kan de melding eveneens per e-mail, echter dienen de tot persoon herleidbare gegevens daarin, zoveel mogelijk te worden gemaskeerd. Wanneer het vermoeden of inschatting is dat het om een datalek met mogelijk ernstige gevolgen gaat, dit direct melden. Indien dit niet mogelijk is dan de eerstvolgende werkdag.

Toelichting:
Er is sprake van een datalek wanneer persoonsgegevens ter beschikking zijn gekomen van niet gerechtigden, verloren zijn gegaan of dat er sprake is van onrechtmatige verwerking of een beveiligingsincident.
Voorbeelden:

- Moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, malware);
- Technisch falen (fouten of bugs in software, verlate updates, storingen);
- Menselijk falen (onzorgvuldige omgang gebruikersnaam of wachtwoord, nalatigheid);

- Verloren of gestolen hardware (externe harde schijf, USB-stick, server-apparatuur of laptop);
- Verzenden van e-mail naar meerdere gebruikers met openbaring van e-mailadressen (Cc);
- Calamiteit (brand datacentrum, wateroverlast)

Noot: Controle op hacks of malware wordt zoveel mogelijk geautomatiseerd.

Stap 1:

Melden van datalek aan de Stichting Talent Maatje Lansingerland

Contactgegevens voor melding:
(contactpersonen voor bescherming persoonsgegevens)

Voorzitter Stichting Talent Maatje Lansingerland
voorzitter@shm-lansingerland.nl

Secretaris Stichting Talent Maatje Lansingerland
secretaris@shm-lansingerland.nl

Penningmeester Stichting Talent Maatje Lansingerland.
penningmeester@shm-lansingerland.nl

Voor meer informatie https://schuldhulpmaatje.nl/locatie/lansingerland/

Stap 2:

Actie contactpersoon voor bescherming persoonsgegevens

Contactpersoon voor bescherming persoonsgegevens:

- Betrokkene meldt het incident bij het algemeen bestuur van de Stichting Talent Maatje Lansingerland
- onderzoekt in eerste instantie de omvang van het incident
- meldt het incident bij de contactpersoon bescherming persoonsgegevens van de landelijke SHM organisatie, zijnde contactpersoon van de vereniging Schuld Hulp Maatje
- start vastlegging van het incident in het logboek
  (logboek maken en geef aan waar het logboek staat geregistreerd en wat er wordt geregistreerd)

Toelichting
Vragen voor onderzoek:

- Wat is precies met de gegevens gebeurd?
- Wat is de aard van de getroffen persoonsgegevens?
  - Bijzondere persoonsgegevens:
    godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap vakbond en strafrechtelijke gegevens.

- ❖ Persoonsgegevens van gevoelige aard:
  financieel of economisch (schulden), stigmatiserend (verslaving, naaktfoto's, specifieke problemen), inloggegevens, gegevens die bruikbaar zijn voor identiteitsfraude (kopie ID, BSN, handtekening, biometrische gegevens), gegevens die vallen onder beroepsgeheim.

- Wat is de omvang van het incident?
  - ❖ Aantal getroffen personen.
  - ❖ Hoeveelheid gegevens per getroffen persoon.
  - ❖ Worden de getroffen gegevens binnen een keten gedeeld?
- Wat is de impact op de betrokkenen (klanten/ pro spects/ personeel)?
  - ❖ Is sprake van kwetsbare groepen (kinderen, zieken, verstandelijk beperkten, bedreigde personen)?
  - ❖ Is er kans op financieel nadeel?

Wanneer het gaat om een incident met gevolgen voor de betrokkene en/of imagoschade voor de organisatie wordt het Algemeen Bestuur van de Stichting Talent Maatje Lansingerland bij elkaar geroepen en het stappenplan verder gevolgd. Tegelijkertijd wordt de contactpersoon van de landelijke vereniging SHM in kennis gesteld. Deze stelt het landelijke respons-team SHM in kennis. Bij het landelijke SHM wordt een responsteam geformeerd. Het landelijke responseteam bestaat uit:

- Contactpersoon bescherming persoonsgegevens
- Directie- of bestuurslid
- Communicatiemedewerker
- Privacy officer

Het landelijke responseteam werkt nauw samen met lokale SHM-organisatie.
Het landelijke responseteam kan wanneer nodig advies inwinnen bij een jurist. De landelijke organisatie faciliteert het inschakelen van een jurist voor haar leden.

Bij vorenstaande gaat het om: of van de inbreuk 'redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking, waaraan nadelige gevolgen voor de privacy van de betrokkenen zijn verbonden'

Stap 3:

Actie Stichting Talent Maatje Lansingerland (al dan niet in overleg met het landelijk responseteam)

Het Algemeen Bestuur van de Stichting bespreekt het incident en neemt maatregelen met betrekking tot het datalek.
Denk hierbij aan: het lek dichten, toegang tot informatie beperken en tegelijkertijd meer informatie vergaren over de indringer.

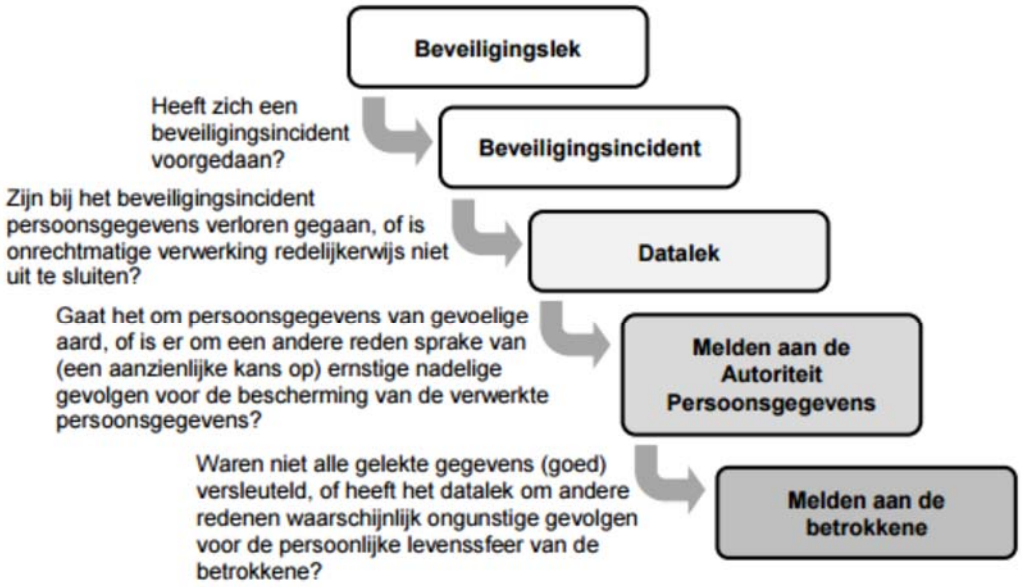
Stap 4:

Actie Stichting Talent Maatje Lansingerland (al dan niet in afstemming met het landelijk responseteam SHM)

De Stichting Talent Maatje Lansingerland bepaalt of het incident gemeld moet worden aan de Autoriteit Persoonsgegevens en betrokkene(n).
Melden bij de Autoriteit Persoonsgegevens is verplicht indien sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

De personen die zijn getroffen door het datalek dienen te worden geïnformeerd indien de inbreuk op de beveiliging waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer. Wanneer dit het geval is er altijd ook een meldplicht bij de Autoriteit Persoonsgegevens.

Toelichting
Aan de hand van de aard van de gegevens, de omvang van het incident en de impact op de betrokkenen (zie hiervoor stap 2: onderzoeken van het incident) wordt bepaald of melding noodzakelijk is. Daarbij kan onderstaand beslisschema behulpzaam zijn.



Wanneer blijkt dat het incident gemeld moet worden is dit ‘onverwijld’, binnen 72 uur na plaatsvinden of opmerken. De melding kan op een later moment eventueel nog aangevuld of ingetrokken worden.
Meldloket Autoriteit Persoonsgegevens:
https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?1

Onderstaande vragen kunnen behulpzaam zijn bij het maken van een afweging of er sprake is van ongunstige gevolgen persoonlijke levenssfeer.

- Kan betrokkene last krijgen van de inbreuk, materiële of immateriële schade lijden (aard gegevens, impact, kwetsbare groep)?
- Kan betrokkene zichzelf beter beschermen als hij de inbreuk kent?

Verder:

- Bij zwaarwegende belangen kan informatie aan betrokkenen achterwege blijven.
- De Autoriteit Persoonsgegevens kan alsnog verlangen dat betrokkenen worden geïnformeerd
- De informatie moet betrokkenen in staat stellen om de inbreuk op hun persoonlijke levenssfeer zoveel mogelijk te beperken

Informeren hoeft niet indien de getroffen persoonsgegevens onbegrijpelijk of ontoegankelijk zijn gemaakt (versleuteling of remote wissen).
Let op:

- Bij vernietiging (geen back-up) of aantasting (wijziging) van gegevens helpen deze beschermingsmaatregelen niet.
- Alle persoonsgegevens moeten zijn versleuteld op moment van de inbreuk.
- De versleuteling moet adequaat zijn (standaardalgoritme, sleutel niet gelekt en toekomstvast) - check publicaties ENISA (EU Agency for Network and
- Information Security) en NCSC (Nationaal Cyber Security Centrum).

Stap 5:

Actie Algemeen Bestuur Stichting Talent Maatje Lansingerland (al dan niet in overleg met het responsteam landelijk SHM)

Het Algemeen Bestuur bepaalt of er maatregelen nodig zijn en zet acties uit om eventuele gevolgen/schade van het incident te beperken voor betrokkene(n).

- Wat kan de Stichting doen?
- Wat kan betrokkene doen?

Het DB van de Stichting Talent Maatje Lansingerland bepaalt de wijze van afhandeling inclusief communicatie naar melder en betrokkene(n).

Het DB van de Stichting bepaalt of crisiscommunicatie opgestart moet worden, zowel intern als extern. Hiervoor is een crisiscommunicatieplan incl. kernboodschap opgesteld door de landelijke organisatie van SHM.

Stap 6:

Actie DB van de Stichting (al dan niet in overleg met responseteam landelijk vereniging SHM)

Het DB van de Stichting gaat na of er overige acties genomen moeten worden zoals:

- Of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden, zoals uit hoofde van wanprestatie (omdat een geheimhoudingsverplichting is geschonden, of in strijd met een contractuele verplichting onvoldoende beveiliging is gerealiseerd), of een onrechtmatige daad
- Of het al dan niet doen van aangifte en vaststellen of sprake is van strafrechtelijke verwijtbaarheid. Dit kan bijvoorbeeld spelen wanneer er sprake is van betrokkenheid vanuit de Stichting Talent Maatje Lansingerland zelf, een

klant, of wanneer er onvoldoende maatregelen zijn getroffen om ongeregeldheden te voorkomen
- Of naast de Autoriteit Persoonsgegevens ook andere stakeholders geïnformeerd moeten worden
- Of er individuen, klanten, leveranciers geïnformeerd moeten worden
- Of er melding gedaan moet worden bij een eventuele verzekering en bijbehorende voorwaarden.

Stap 7:

Actie DB Stichting Talent Maatje Lansingerland

Wanneer het incident onder controle is en er geen actie meer ondernomen hoeft te worden, wordt de procedure afgesloten.
Binnen 2 weken wordt het incident en de doorlopen procedure geëvalueerd door het DB van de Stichting. Het initiatief ligt bij contactpersoon bescherming persoonsgegevens.
Doel van de evaluatie is het voorkomen van soortgelijke incidenten in de toekomst en eventuele verbeteringen van de datalekprocedure.