Protocol Meldplicht Datalekken

Woord vooraf
De privacywetgeving Algemene verordening gegevensbescherming (AVG) bepaalt dat datalekken direct, binnen 72 uur na ontdekking, gemeld moeten worden aan de Autoriteit Persoonsgegevens tenzij het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen.
Daarnaast moet het datalek ook aan de betrokkenen gemeld worden indien het waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen met zich meebrengt.

Dit protocol datalekken is bedoeld als hulpmiddel voor de beantwoording van de vraag of er sprake is van een datalek en of deze gemeld moet worden.
Aan de beantwoording van de vraag moet een zorgvuldige (belangen)afweging voorafgaan.

Definitie datalek
Onder een datalek verstaat de Autoriteit Persoonsgegevens: persoonsgegevens die gelekt of vernietigd zijn als gevolg van een beveiligingsincident.
Bij het lek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking.
Bij verlies zijn de persoonsgegevens er niet meer.
Onder onrechtmatige verwerking vallen bijvoorbeeld onbevoegde kennisneming, wijziging, aantasting of de verstrekking daarvan.

Alleen een dreiging of een tekortkoming in de beveiliging is niet voldoende; er moeten daadwerkelijk persoonsgegevens gelekt zijn.

Voorbeelden van inbreuken in verband met persoonsgegevens kunnen zijn:
- kwijtraken van een USB -stick
- diefstal van een laptop
- inbraak door een hacker
- persoonsgegevens per ongeluk gepubliceerd
- hacking, malware of fishing
- persoonsgegevens aan verkeerde persoon verstuurd
- calamiteiten zoals brand op de locatie waar de informatie is opgeslagen

Contactpersoon
Binnen onze organisatie is Bob Westerink (bob@paarse-pelikaan.nl) degene waarbij eventuele datalekken gemeld moeten worden en bij diens afwezigheid Nicole Smulders (nicole@paarse-pelikaan.nl).

Informeren medewerkers
Medewerkers van Stichting De Paarse Pelikaan dienen zich ervan bewust te zijn dat als er sprake is van een datalek, zij dit datalek direct (diezelfde dag nog) moeten melden bij de interne contactpersoon, zodat deze tijdig het datalek kan melden bij de Autoriteit Persoonsgegevens.
Zij dienen bekend te zijn met het in dit protocol opgenomen stappenplan.

Stichting De Paarse Pelikaan

Uitvoeren van het stappenplan Datalekken
Het bestuur draagt zorg voor de invoering en naleving van het hieronder opgenomen stappenplan. Indien er een datalek optreedt, dienen de volgende stappen doorlopen te worden:

Stap 1 - Interne melding
1.1 Degene die een datalek bij Stichting de Paarse Pelikaan ontdekt, meldt dit per omgaande aan de interne verantwoordelijke.
1.2 Indien mogelijk, zorgt degene die het datalek heeft ontdekt er gelijktijdig voor dat de gelekte gegevens meteen op afstand worden gewist of ontoegankelijk gemaakt.

Stap 2 - Onderzoek door de interne verantwoordelijke
De interne verantwoordelijke onderzoekt onder meer:
- of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden
- wie binnen (medewerkers) of buiten de organisatie (verwerker, is administratiekantoor) betrokken zijn bij het datalek.

Stap 3 - Bestrijding schade
De interne verantwoordelijke stopt het datalek indien mogelijk en neemt voorts de noodzakelijke maatregelen om het datalek en de gevolgen zo goed mogelijk te bestrijden.

Stap 4 - Vaststelling gevolgen
De interne verantwoordelijke onderzoekt de mogelijke gevolgen van het datalek aan de hand van de aard en de omvang van de gegevens die gelekt zijn en stelt vast wat de nadelige gevolgen van de betrokkenen kan zijn.

Stap 5 – Gegevens verzamelen
De ontdekker/melder van het datalek biedt (binnen 24 uur) alle medewerking aan de interne verantwoordelijk door zo snel en zo goed mogelijk (schriftelijk) antwoord te geven op de volgende vragen:
- wat is er gebeurd? (omschrijving van het incident)
- ging het per ongeluk of werd het veroorzaakt door kwade opzet (denk aan gehackte gegevens)?
- wanneer is het gebeurd? (datum en tijdstip)
- wanneer is het ontdekt? (datum en tijdstip)
- wat voor gegevens(registers) zijn gelekt?
- zijn de gegevens versleuteld, en zo ja hoe?
- konden de gegevens op afstand worden gewist of ontoegankelijk gemaakt, en zo ja, is dat gebeurd?
- wat zijn de mogelijke gevolgen voor de betrokkenen?
- hoeveel personen zijn hierdoor (bij benadering) getroffen?
- konden er al technische en/of organisatorische maatregelen worden getroffen naar aanleiding van het incident?

Stap 6 - Beslissing wel of niet melden
6.1 De interne verantwoordelijke beslist zo spoedig mogelijk doch in elk geval binnen 72 uur na ontdekking van het datalek of het datalek dient te worden gemeld aan de Autoriteit Persoonsgegevens en betrokkenen. *Zie kopje 'Ter overweging' in nota bene.*

6.2 De interne verantwoordelijke overlegt met de melder van het datalek of betrokkenen op de hoogte moeten worden gesteld. Dit is zo indien het een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, tenzij inmiddels passende maatregelen zijn genomen dat het hoge risico heeft afgewend.

Stap 7 - Melding doen

7.1 De interne verantwoordelijke draagt zo nodig zorg voor de melding aan de Autoriteit Persoonsgegevens en/of de betrokkene(n) binnen 72 uur na ontdekking van het datalek.

7.2 Het is enige andere medewerker dan de interne verantwoordelijke niet toegestaan om het (mogelijke) datalek zelf aan de Autoriteit Persoonsgegevens en/of de betrokkene(n) te melden.

7.3 Als een medewerker het niet eens is met de beslissing van de interne verantwoordelijke omtrent het al dan niet melden van het datalek aan de Autoriteit Persoonsgegevens en/of de betrokkene(n), dan kan hij zijn grieven kenbaar maken aan het bestuur.

7.4 Indien daartoe verzocht, verlenen betrokkenen alle medewerking aan de verantwoordelijke om de getroffen personen conform artikel 34 AVG te kunnen informeren omtrent het datalek.

Stap 8 - Gevolgen melding

8.1 Indien het datalek negatieve gevolgen heeft voor betrokkenen, dan doet de interne verantwoordelijke er alles aan om deze gevolgen zoveel mogelijk te beperken.

8.2 Afhankelijk van de aard en de omvang van het datalek voor betrokkenen bepaalt de interne verantwoordelijke:

- op welke wijze betrokkenen worden geïnformeerd (waaronder in ieder geval de mededelingen worden gedaan welke soorten persoonsgegevens getroffen zijn, wat de mogelijke gevolgen zijn, welke maatregelen de Stichting neemt en op welke wijze betrokkenen zelf de schade kunnen voorkomen of beperken)
- welke nazorg betrokkenen krijgen
- welke acties in het belang van de organisatie noodzakelijk zijn

8.3 Indien een datalek heeft plaatsgevonden - ongeacht of deze is gemeld of niet - worden zo spoedig mogelijk adequate technische en/of organisatorische maatregelen getroffen om toekomstige gelijksoortige datalekken te voorkomen.

Stap 9 - Register

De interne verantwoordelijke houdt een register bij van alle datalekken, waarin alle gegevens rondom het datalek worden geregistreerd.

Nota bene (ter overweging)

Melding aan de Autoriteit persoonsgegevens kan alleen achterwege blijven indien het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Of hiervan sprake is hangt mede af van de aard en omvang van de gelekte persoonsgegevens. Indien bijvoorbeeld uitsluitend de adresgegevens zijn gelekt van een kleine groep betrokkenen, dan is het onwaarschijnlijk dat er sprake is van een hoog risico. Dat is wellicht anders indien de adresgegevens in combinatie met het lidmaatschap van de patiënten of cliëntenorganisatie zijn gelekt. Het lidmaatschap van de organisatie kan gezien worden als een gevoelig gegeven en de leden van de organisatie kunnen wellicht behoren tot een kwetsbare groep, die extra

bescherming nodig heeft. Bij de afweging van het risico voor de rechten en vrijheden van de betrokken zal altijd de Functionaris Gegevensbescherming betrokken moeten worden.

Indien het datalek waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen veroorzaakt, moet het datalek ook aan de betrokkenen gemeld worden. Het risico zal bijvoorbeeld moeten worden beoordeeld aan de hand van de aard en de hoeveelheid van de gelekte gegevens. Als er persoonsgegevens van gevoelige aard (bijv. gezondheidsgegevens) gelekt zijn, zal het lek in ieder geval gemeld moeten worden aan de betrokkenen. Bij de afweging van het risico voor de rechten en vrijheden van de betrokkenen zal altijd de Functionaris Gegevensbescherming betrokken moeten worden.