SIONSBERG

Netwerk Ziekenhuis

Protocol Meldplicht Datalekken

1. Doel

Wanneer er een datalek heeft plaatsgevonden is Sionsberg Netwerk Ziekenhuis (SNZ) verplicht dit te melden aan de Autoriteit Persoonsgegevens. Het doel van de meldplicht is om de schade voor betrokkenen als gevolg van een datalek zo minimaal mogelijk te houden. Dit protocol beschrijft welke procedure gevolgd wordt bij een melding datalek.

2. Doelgroep/Toepassingsgebied

Iedereen binnen en buiten SNZ, die een datalek ontdekt of vermoedt. Het is voor SNZ belangrijk om in voorkomende gevallen tijdig te kunnen beoordelen of er sprake is van een datalek. Meld daarom – ook bij twijfel – (mogelijke) datalekken altijd.

Melden datalek interne medewerkers

- Meld het datalek direct bij zorgmanager en/of directeur bedrijfsvoering.
- Maak direct een VIM aan.

Melden datalek externe betrokkenen

- Neem contact op met directeur bedrijfsvoering, tel.: 088 - 0708895
- Meld het datalek via mailadres: avg@sionsberg.nl

3. Wat is een datalek?

Er is sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan, waarbij persoonsgegevens verloren zijn gegaan, of wanneer niet is uit te sluiten dat de persoonsgegevens onrechtmatig verwerkt worden.
Het gaat om situaties waarbij persoonsgegevens (mogelijk) zijn:

- Vernietigd of verloren,
- Gewijzigd,
- Verstrekt of toegankelijk gemaakt.

Niet ieder datalek is zo ernstig dat dit moet worden gemeld. Melding aan de Autoriteit Persoonsgegevens is verplicht als er sprake is van of kans op ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens. Melding aan de betrokkenen is verplicht als er kans is op ongunstige gevolgen voor hun persoonlijke levenssfeer.

Voorbeelden van datalekken:
Er is sprake van een datalek als de persoonsgegevens die SNZ verwerkt, mogelijk in handen komen van derden, die geen toegang tot deze informatie zouden mogen hebben. Voorbeelden zijn:

- De server bij de IT-leverancier wordt gehackt en de informatie wordt gestolen.
- Door een IT-incident zijn de persoonsgegevens verloren gegaan en er is geen complete en actuele reservekopie van de gegevens.
- Een computer wordt gehackt of ingezien door derden.
- Er is een mailing verstuurd met de adressen in een “cc-veld”.
- Verlies of diefstal van een telefoon, USB-stick, laptop, I-pad of smartphone met daarop persoonsgegevens.
- Verlies of diefstal van een geprinte lijst met persoonsgegevens.

- Wachtwoorden om in te loggen zijn in handen van een derde gevallen, waardoor deze onbevoegd toegang heeft tot persoonsgegevens.

4. Verantwoordelijkheden en bevoegdheden

In geval van een datalek zal het ***Team Datalekken*** direct onderzoek doen naar de oorzaak, omvang en herstel en tevens zorgdragen voor de melding. Dit team bestaat uit:

Hans Mallie	Directeur Bedrijfsvoering (voorzitter Team Datalekken)	hans.mallie@sionsberg.nl tel.: 088 - 0708895
Melvin Mac Gillavry	Bestuurslid	melvin.macgillavry@sionsberg.nl
Hetty Hetebrij	Manager Kwaliteit & Veiligheid	hetty.hetebrij@sionsberg.nl
Rik Kroon	Functionaris Gegevensbescherming	tel.: 06 - 15961732

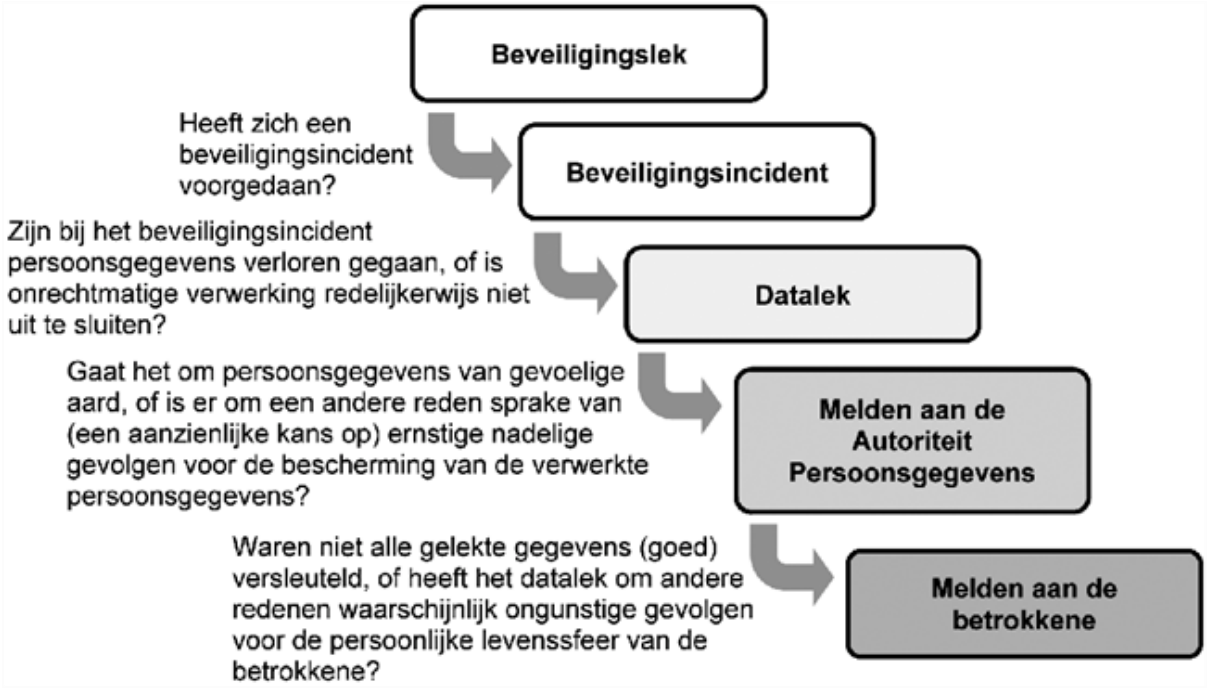
Zo nodig zullen andere functionarissen bij het onderzoek betrokken worden zoals bijvoorbeeld de zorgmanager, de afdeling ICT of de IT-leverancier.

Het team datalekken beoordeelt of het lek gemeld moet worden. Zo nodig doet het team melding bij:

- De Autoriteit Persoonsgegevens (AP)
- De Inspectie Gezondheidszorg en Jeugd (IGJ)
- Betrokkenen (patiënten, medewerkers etc.)

5. Werkwijze

Een (mogelijk) datalek kan op verschillende manieren worden aangedragen. Persoonlijk/mondeling, via telefoon, VIM of e-mail; door een medewerker of een externe betrokkene (bijvoorbeeld een verwerker). Maar ook op andere manieren kan een incident aan het licht komen, bijvoorbeeld door een klacht of een signaal uit de buitenwereld.
Na melding van een datalek, roept de directeur bedrijfsvoering/voorzitter het Team Datalekken bij elkaar om te bepalen of er inderdaad sprake is van een datalek. Hierbij wordt onderstaande beslisboom gebruikt.



Voor de behandeling van het datalek wordt onderstaand **stappenplan** gevolgd.

Stap 1: verzamelen feiten en analyse

Het Team datalekken beoordeelt of het een datalek is aan de hand van de volgende vragen:

1. Is er sprake van een inbreuk op de beveiliging?
2. Zijn bij de inbreuk persoonsgegevens verloren gegaan?
3. Kan ik redelijkerwijs uitsluiten dat er persoonsgegevens onrechtmatig zijn verwerkt?

Om te bepalen of er sprake is van een echt datalek en een voorlopige inschatting te maken van de ernst, verzamelt en analyseert het team datalekken de feiten en omstandigheden waaronder het incident plaatsvond. Vervolgens wordt door de voorzitter van het Team Datalekken vastgesteld of de melding al dan niet een datalek is.

Stap 2a: de melding is *geen* datalek

De melding wordt geregistreerd in het Datalekkenregister voor intern gebruik (t.b.v. het signaleren van trends en leerpunten). De melder krijgt een reactie terug.

Stap 2b: de melding is een datalek

Het Team Datalekken zorgt ervoor dat er zo snel mogelijk maatregelen worden genomen om verder verlies van persoonsgegevens of schade aan persoonsgegevens te voorkomen. Voorbeelden van maatregelen zijn:

a) Onmiddellijk contact opnemen met de IT-leverancier bij bijvoorbeeld een malware- of virusbesmetting om te overleggen over mogelijke aanpassingen in de systemen.

b) Het wijzigen van een wachtwoord, zodat een derde geen toegang meer heeft.
c) Het waarschuwen van betrokkenen (patiënten of medewerkers), zodat zij zelf maatregelen kunnen nemen.
d) Het resetten van alle wachtwoorden, waarbij leden een nieuw wachtwoord moeten opgeven.
e) Andere partijen die betrokken zijn bij de dienstverlening van de SNZ waarschuwen.

Stap 2c: beoordelen of melden aan de Autoriteit Persoonsgegevens verplicht is

Het Team Datalekken beoordeelt of het datalek gemeld moet worden aan de Autoriteit Persoonsgegevens aan de hand van de volgende vragen:
1. Zijn er persoonsgegevens van gevoelige aard gelekt?
2. Leiden de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?

Vervolgens wordt door de voorzitter van het Team Datalekken vastgesteld of de melding al dan niet gemeld moet worden aan de Autoriteit Persoonsgegevens.

Stap 3: het datalek melden aan de Autoriteit Persoonsgegevens

Het Team Datalekken dient het datalek onverwijld te melden aan de Autoriteit Persoonsgegevens. Dit moet zonder onnodige vertraging en binnen 72 uur na de ontdekking gebeuren.

Als er nog niet volledig zicht is op wat er is gebeurd en om welke persoonsgegevens het gaat, wordt de melding gedaan op basis van de gegevens die op dat moment beschikbaar zijn. De melding kan naderhand aangevuld of ingetrokken worden.

De melding wordt gedaan met het formulier “Melden Datalekken bij Autoriteit Persoonsgegevens” op de website van de AP. Bij de melding moet in ieder geval worden aangegeven:
a) De aard van de inbreuk.
b) De instanties waar meer informatie over de inbreuk kan worden verkregen.
c) Een beschrijving van de geconstateerde en vermoedelijke gevolgen van de inbreuk en maatregelen die SNZ heeft getroffen om deze gevolgen te beperken.

De melding wordt geregistreerd in het datalekken voor intern gebruik (t.b.v. het signaleren van trends en leerpunten). De melder krijgt een reactie terug.

Stap 4: bepalen of het datalek gemeld moet worden aan de betrokkenen

Melding aan de AP betekent niet automatisch dat het datalek ook gemeld moet worden aan de betrokkene.

Het Team Datalekken maakt hiervoor een aparte afweging aan de hand van de volgende vragen:
1. Zijn er persoonsgegevens van gevoelige aard gelekt?
2. Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene?
3. Zouden betrokkenen kunnen worden geschaad door bijvoorbeeld onrechtmatige publicatie, aantasting in eer en goede naam, (identiteits)fraude of discriminatie?

De voorzitter van het Team Datalekken stelt vast of de melding al dan niet gemeld moet worden aan de betrokkenen.

Stap 5: melden aan de betrokkene

Het Team Datalekken beoordeelt of er een melding aan betrokkene moet worden gedaan. Hierbij worden een aantal aspecten afgewogen:

a) Bieden cryptografie of andere technische beschermingsmaatregelen voldoende bescherming?
b) Zal het datalek waarschijnlijk ongunstige gevolgen hebben voor de persoonlijke levenssfeer van betrokkene?
c) Zijn er zwaarwegende redenen om de melding aan betrokkene achterwege te laten?

In voorkomend geval stuurt SNZ een e-mail naar betrokkene(n), waarin wordt aangegeven:

a) wat er gebeurd is (de aard van de inbreuk)
b) welke maatregelen SNZ heeft getroffen
c) hoe betrokkene zelf eventuele negatieve gevolgen tegen kan gaan
d) hoe betrokkene SNZ kan bereiken voor vragen

Stap 6: registratie in het datalekkenregister

SNZ legt alle datalekken vast in een datalekkenregistratie. Hierin wordt een korte omschrijving gegeven van:

a) het incident
b) de feiten, context en analyse
c) of het wel of niet een datalek is
d) de eventuele melding aan de Autoriteit Persoonsgegevens (AP)
e) de eventuele melding aan betrokkene
f) de maatregelen

Datalekken worden aan het eind van elk jaar geëvalueerd door directie/MT. De evaluatie wordt opgenomen in de directiebeoordeling.

6. Revisie

Eindverantwoordelijke	: Hans Mallie, directeur bedrijfsvoering
Auteur	: Hetty Hetebrij, manager K&V
Datum laatste aanpassing	: 03-10-2019