Roos Kinderpraktijk
Wilhelminastraat 5, 6372 JS Landgraaf
Telefoon: 06-23262228
E-mail: natalie@rooskinderpraktijk.nl

Beleid meldplicht datalekken (artikel 33 en 34 AVG) Roos Kinderpraktijk

Stap 1

Wanneer er een datalek geconstateerd wordt, of wanneer het vermoeden ontstaat dat er een datalek plaats heeft gevonden, wordt Mevr. N. Roos onmiddellijk op de hoogte gesteld.

Stap 2

Mevr. N. Roos onderzoekt of er daadwerkelijk sprake is van een datalek (zie. punt 1.).

Stap 3

Mevr. N. Roos onderzoekt of het datalek gemeld moet worden aan de Autoriteit Persoonsgegevens (zie punt 2.1. en 4).

Stap 4

Indien het datalek gemeld moet worden aan de Autoriteit Persoonsgegevens, doet Mevr. N. Roos deze melding binnen 72 uur na kennisneming van het datalek (zie punt 2.2 en 2.3.).

Stap 5

Mevr. N. Roos onderzoekt of het datalek aan de betrokkenen medegedeeld moet worden (zie punt 3 en 4).

Stap 6

Indien het datalek gemeld moet worden aan betrokkenen, doet Mevr. N. Roos dit zo snel mogelijk door de betrokkenen persoonlijk te informeren (zie punt 3.1).

Stap 7

Mevr. N. Roos neemt het datalek op in het register datalekken, ook als het lek niet gemeld hoeft te worden (zie punt 5).

Toelichting beleid meldplicht datalekken

1. Datalek

Wanneer er een datalek geconstateerd wordt, of wanneer het vermoeden bestaat dat er een datalek plaats heeft gevonden, wordt de mevr. N. Roos hiervan onmiddellijk op de hoogte gesteld.

De mevr. N. Roos onderzoekt of er daadwerkelijk sprake is van een datalek. Een datalek is een inbreuk op de beveiliging van persoonsgegevens binnen de organisatie, die per ongeluk of op onrechtmatige wijze leidt tot:

- vernietiging van persoonsgegevens;
- verlies van persoonsgegevens;
- wijziging van persoonsgegevens;
- ongeoorloofde verstrekking van persoonsgegevens;
- ongeoorloofde toegang tot persoonsgegevens.

Datalek of beveiligingsincident?
Er kan een verschil gemaakt worden tussen een beveiligingsincident en een datalek. Bij een beveiligingsincident is er sprake van een lek van *gegevens*. Bij een datalek is er sprake van een lek van *persoonsgegevens*. Alleen wanneer er persoonsgegevens gelekt zijn, is er sprake van een datalek. In principe zijn dus alle datalekken beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.

Het is de taak van mevr. N. Roos om datalekken op te sporen en om maatregelen te treffen om de gevolgen van het datalek te beperken en herhaling te voorkomen.

2. Melding aan de autoriteit persoonsgegevens

Indien er een datalek heeft plaatsgevonden, dan onderzoekt mevr. N. Roos of het datalek gemeld moet worden aan de Autoriteit Persoonsgegevens.

2.1. Risico voor de rechten en vrijheden van natuurlijke personen

Meteen nadat een datalek geconstateerd wordt, moet mevr. N. Roos bepalen of het waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Wanneer dit het geval is, moet het datalek gemeld worden bij de Autoriteit Persoonsgegevens. Aan de hand van verschillende factoren kan mevr. N. Roos beoordelen of het waarschijnlijk is dat het datalek een risico voor de rechten en vrijheden van natuurlijke personen inhoudt. Zie hiervoor punt 4.

Wanneer geconstateerd is dat het waarschijnlijk is dat het datalek een risico voor de rechten en vrijheden van natuurlijke personen inhoudt, meld mevr. N. Roos het datalek aan de Autoriteit Persoonsgegevens.

2.2. Melding binnen 72 uur na kennisneming van het datalek

Wanneer er sprake is van een datalek, moet binnen 72 uur na kennisneming van het datalek een melding gedaan worden bij de Autoriteit Persoonsgegevens. Wanneer is er sprake van kennisneming van een datalek? Een verwerkingsverantwoordelijke wordt geacht kennis genomen te hebben van een datalek wanneer hij een redelijke mate van zekerheid heeft dat er een veiligheidsincident heeft plaatsgevonden waarbij persoonsgegevens betrokken zijn.

Dit is afhankelijk van de omstandigheden van de specifieke inbreuk. In sommige gevallen zal het meteen duidelijk zijn dat een datalek heeft plaatsgevonden, terwijl in andere gevallen onderzoek gedaan moet worden. De volgende stappen moeten genomen worden:

- Mevr. N. Roos stelt onverwijld onderzoek in wanneer er mogelijk een veiligheidsincident plaats heeft gevonden.
- Wanneer er daadwerkelijk een veiligheidsincident heeft plaatsgevonden, moet bepaald worden of er sprake is van een datalek. Mevr. N. Roos heeft hiervoor een korte periode van onderzoek.
- Tijdens de korte periode van onderzoek wordt mevr. N. Roos nog niet geacht kennis te hebben genomen van het datalek.
- Wanneer er kennis genomen is van het datalek, moet dit binnen 72 uur aan de Autoriteit Persoonsgegevens gemeld worden.

2.3. Welke informatie moet de melding aan de Autoriteit Persoonsgegevens bevatten?
De melding aan de Autoriteit Persoonsgegevens moet de volgende informatie bevatten:

- de aard van de inbreuk in verband met persoonsgegevens en, waar mogelijk, de categorieën en het aantal betrokkenen en persoonsgegevens;
- de naam en contactgegevens van mevr. N. Roos;
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- de maatregelen die voorgesteld of genomen zijn om de inbreuk aan te pakken.

Wanneer bovenstaande informatie niet allemaal tegelijkertijd verstrekt kan worden, is het mogelijk om deze in stappen te verstrekken. Dit kan het geval zijn wanneer er meer onderzoek nodig is.

2.4. Afhandeling van een melding door de Autoriteit Persoonsgegevens
Nadat het datalek gemeld is bij de Autoriteit Persoonsgegevens, ontvangt mevr. N. Roos een bevestiging van de melding. Als de melding aanleiding geeft tot nadere actie, dan neemt de Autoriteit Persoonsgegevens daarover contact op. In eerste instantie zal het hierbij gaan om verificatie dat de melding daadwerkelijk van mevr. N. Roos afkomstig is en om eventuele inhoudelijke vragen over de melding. Daarnaast kan de Autoriteit Persoonsgegevens op basis van de ontvangen melding actie ondernemen om adequate beveiliging van persoonsgegevens te vorderen. Wanneer blijkt dat de beveiligingsmaatregelen mogelijk niet op orde zijn, dan kan de Autoriteit Persoonsgegevens een nader onderzoek instellen naar de naleving van de beveiligingsverplichtingen uit de AVG. Daarnaast houdt de Autoriteit Persoonsgegevens een register van gemelde datalekken bij. Dit register is niet openbaar. Wanneer Roos Kinderpraktijk niet voldoet aan de meldplicht datalekken, kan de Autoriteit Persoonsgegevens een boete opleggen.

3. Melding aan betrokkenen
Wanneer een datalek waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoud, dan deelt mevr. N. Roos dit zo snel mogelijk mede aan de betrokkenen van wie de gegevens gelekt zijn. Hierbij is het belangrijkste doel om betrokkenen informatie te geven omtrent de stappen die zij kunnen nemen om zichzelf te beschermen. Hierdoor kan de betrokkene wellicht voorkomen dat het datalek ongunstige gevolgen voor hem of haar heeft. Om te bepalen of het datalek waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt, zie punt 4.

3.1. Welke informatie moet de melding aan betrokkenen bevatten?
Een melding aan betrokkenen moet de volgende informatie bevatten:

- de aard van de inbreuk;
- de naam en contactgegevens van mevr. N. Roos;
- een omschrijving van de waarschijnlijke gevolgen van het datalek;
- een omschrijving van de maatregelen die voorgesteld of genomen zijn om de inbreuk aan te pakken.

3.2. Gevallen waarin een mededeling aan betrokkenen niet vereist is
Een melding aan de betrokkenen is niet vereist in de volgende gevallen:

- er zijn passende beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop het datalek betrekking heeft;
- er zijn achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico zich waarschijnlijk niet meer voor zal doen;
- een mededeling aan de betrokkenen zou onevenredige inspanning vergen. In dat geval komt er een openbare mededeling of soortgelijke maatregel waarbij betrokkenen worden geïnformeerd voor in de plaats.

4. Risico voor de rechten en vrijheden van natuurlijke personen
Mevr. N. Roos is niet verplicht om alle datalekken aan de Autoriteit Persoonsgegevens en de betrokkene te melden. Dit is alleen verplicht wanneer het datalek waarschijnlijk een risico (melding Autoriteit Persoonsgegevens) of een hoog risico (mededeling aan betrokkenen) inhoudt voor de rechten en vrijheden van natuurlijke personen. Van een dergelijk risico is sprake wanneer een datalek kan leiden tot fysieke, materiele of immateriële schade voor de betrokkene van wie de gegevens gelekt zijn.

Met de volgende factoren moet rekening gehouden worden om te bepalen of er sprake kan zijn van een (hoog) risico:

<u>De aard van de inbreuk</u>
De aard van het datalek kan effect hebben op het risico voor betrokkenen. Het onbedoeld onthullen van gegevens aan een derde partij heeft andere gevolgen voor betrokkenen dan de onbedoelde vernietiging van gegevens.

<u>De aard, gevoeligheid en hoeveelheid van de persoonsgegevens</u>
De aard en gevoeligheid van de gelekte gegevens spelen een belangrijke rol bij de beoordeling of er sprake is van een risico voor de rechten en vrijheden van natuurlijke personen. Gevoelige gegevens zullen eerder schade aan personen toebrengen dan niet-gevoelige gegevens. De volgende gegevens worden beschouwd als gevoelige gegevens:

- *Bijzondere persoonsgegevens*
  Bijzondere persoonsgegevens zijn persoonsgegeven omtrent godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
- *Gegevens over de financiële of economische situatie van de betrokkene*
  Onder deze gegevens vallen onder andere gegevens over (problematische) schulden, salaris- en betalingsgegevens.
- *Gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene*

Onder deze gegevens vallen onder andere gegevens over verslavingen, prestaties op school of werk of relatieproblemen.

- *Gebruikersnamen, wachtwoorden en andere inloggegevens (useradministratie)*
  De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang tot geven. Er moet rekening gehouden worden met het feit dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- *Gegevens die kunnen worden misbruikt voor (identiteits)fraude*
  Onder deze gegevens vallen onder andere biometrische gegevens, kopieën van identiteitsbewijzen en het Burgerservicenummer.

Wanneer bovenstaande gegevens gelekt zijn, kan dit een reden zijn om het datalek te melden aan de Autoriteit Persoonsgegevens. Ook moet er rekening gehouden met eventuele andere gegevens van de betrokkene die reeds openbaar zijn. In combinatie met de gelekte gegevens kan dit een risico opleveren. De hoeveelheid gelekte gegevens kan ook van belang zijn, hoewel dit geen doorslaggevende factor is: ook een kleine hoeveelheid gelekte gegevens kan een risico opleveren.

<u>Hoe eenvoudig individuen aan de hand van de gegevens geïdentificeerd kunnen worden</u>
Er moet beoordeeld worden hoe eenvoudig het is voor partijen die toegang hebben tot de gelekte gegevens om aan de hand van deze gegevens individuen te identificeren of de gelekte gegevens te linken aan andere informatie waarmee individuen geïdentificeerd kunnen worden. Wanneer individuen gemakkelijk aan de hand van de gelekte gegevens geïdentificeerd kunnen worden, geeft dit meer reden om het datalek te melden.

<u>Bijzondere kenmerken van individuen</u>
Wanneer een datalek betrekking heeft op bijzondere individuen, dan kan dit een reden zijn om het datalek te moeten melden. Het kan zo zijn dat een datalek betrekking heeft op de persoonsgegevens van kinderen of andere kwetsbare individuen, die daardoor een groter risico lopen.

<u>De ernst van de consequenties voor individuen</u>
Een datalek kan, mede afhankelijk van de aard van de gegevens, zeer ernstige gevolgen voor individuen hebben. Dit is zeker het geval wanneer het datalek kan leiden tot identiteitsfraude, fysieke schade of reputatieschade. Ook de bijzondere kenmerken van individuen kunnen hierbij een rol spelen. Wanneer de verwerkingsverantwoordelijk weet dat de gelekte gegevens in handen zijn van mensen die onbekende of mogelijk kwade intenties hebben, bestaat er een groter risico voor de betrokkenen. Ook wanneer betrokkenen lange-termijn effecten kunnen ondervinden van een datalek, is er sprake van een groter risico.

<u>Het aantal betrokkenen van wie persoonsgegevens zijn gelekt</u>
Een datalek kan invloed hebben op slechts één of op honderden (of nog meer) personen. Normaal gesproken is het zo dat hoe hoger het aantal betrokkenen van wie persoonsgegevens gelekt zijn, hoe groter de gevolgen van het datalek zijn. Hierbij moet echter wel rekening gehouden worden met het feit dat een datalek dat betrekking heeft op slechts één persoon ook grote gevolgen kan hebben, afhankelijk van de aard van de persoonsgegevens die gelekt zijn.

<u>Algemene punten</u>

Om het risico te kunnen bepalen, moet zowel de ernst van de potentiele gevolgen voor betrokkenen als de waarschijnlijkheid dat deze gevolgen zullen intreden meegenomen worden. Wanneer de gevolgen van een datalek ernstiger zijn of wanneer de waarschijnlijkheid dat deze gevolgen intreden groter is, wordt het risico hoger. Bij twijfel is het verstandig om altijd een melding te doen.

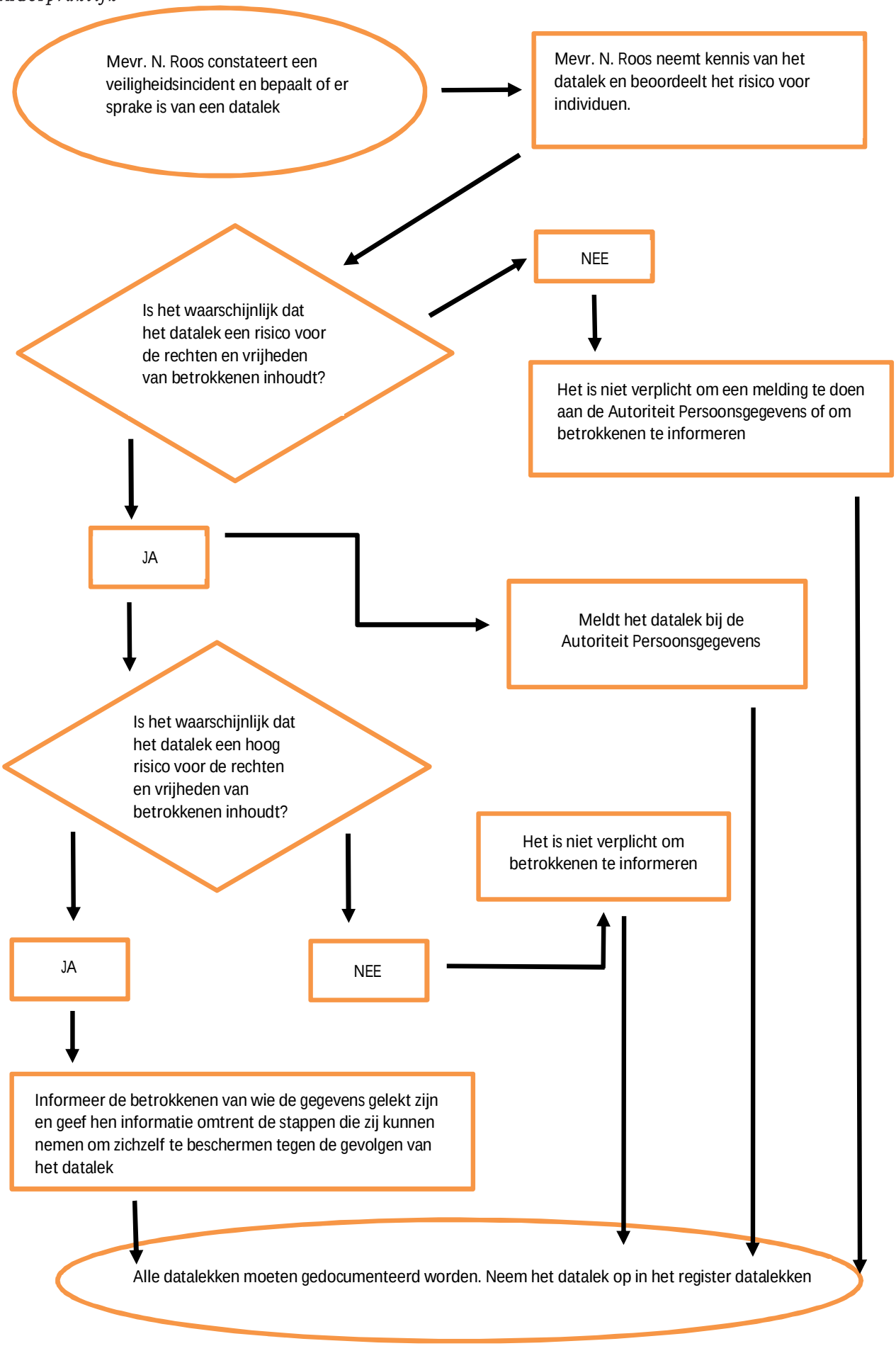
5. Documentatie van datalekken
Roos Kinderpraktijk is verplicht om een register van datalekken bij te houden. Alle datalekken moeten gedocumenteerd worden, dus ook de datalekken die niet gemeld hoeven te worden. In dit register moet per datalek de volgende informatie opgenomen worden:

- de feiten omtrent het datalek. Dit omvat de oorzaak van het datalek, hetgeen er feitelijk gebeurd is en de persoonsgegevens die hierbij betrokken waren;
- de gevolgen van het datalek;
- de genomen corrigerende maatregelen.

Wanneer een datalek niet gemeld is, moeten de redenen hiervoor opgenomen worden in het verwerkingsregister. Hierbij moet ingegaan worden op de reden waarom mevr. N. Roos van mening is dat het datalek waarschijnlijk geen (hoog) risico inhoud voor de rechten en vrijheden van natuurlijke personen.

Uit beleidsregels van de Autoriteit Persoonsgegevens blijkt dat een datalek minimaal één jaar bewaard moet worden in het register datalekken. In sommige gevallen moeten de gegevens zelf minimaal drie jaar bewaard worden. De bewaartermijn van drie jaar is van toepassing in de volgende situaties:

- wanneer het datalek niet aan betrokkenen gemeld is omdat de technische beschermingsmaatregelen die Roos Kinderpraktijk genomen heeft voldoende bescherming bieden om de melding achterwege te laten;
- Wanneer er zwaarwegende redenen zijn om de melding aan betrokkenen achterwege te laten.


Mevr. N. Roos constateert een veiligheidsincident en bepaalt of er sprake is van een datalek
Mevr. N. Roos neemt kennis van het datalek en beoordeelt het risico voor individuen.
Is het waarschijnlijk dat het datalek een risico voor de rechten en vrijheden van betrokkenen inhoudt?
NEE
Het is niet verplicht om een melding te doen aan de Autoriteit Persoonsgegevens of om betrokkenen te informeren
JA
Meldt het datalek bij de Autoriteit Persoonsgegevens
Is het waarschijnlijk dat het datalek een hoog risico voor de rechten en vrijheden van betrokkenen inhoudt?
Het is niet verplicht om betrokkenen te informeren
JA
NEE
Informeer de betrokkenen van wie de gegevens gelekt zijn en geef hen informatie omtrent de stappen die zij kunnen nemen om zichzelf te beschermen tegen de gevolgen van het datalek
Alle datalekken moeten gedocumenteerd worden. Neem het datalek op in het register datalekken