

LHV-handleiding

Datalek in de huisartsenpraktijk



Kom in
actie bij een
datalek

Heeft u als huisarts te maken met een datalek in uw praktijk? Dan is het belangrijk dat u snel in actie komt. Maar hoe weet u of sprake is van een datalek? En welke acties moet u dan ondernemen? Met deze handleiding helpen we u op weg.

Vermoeden van een datalek?

Patiëntgegevens zijn gevoelige gegevens, daarom moet u een datalek waarbij patiëntgegevens betrokken zijn vrijwel altijd melden bij de Autoriteit Persoonsgegevens (hierna AP). In veel gevallen bent u ook verplicht om de patiënten te informeren van wie gegevens zijn gelekt. In de handleiding wordt uitgelegd hoe u kunt vaststellen of een bepaalde gebeurtenis een datalek is, of dit datalek moet worden gemeld aan de AP en/of aan de patiënt(en), en zo ja, wie dat zou moeten doen.

Een datalek wil zeggen dat er vanuit of binnen uw praktijk persoonsgegevens van patiënten (data) op straat zijn komen te liggen, door onbevoegden zijn ingezien of verloren zijn gegaan. De Algemene Verordening Gegevensbescherming (hierna AVG) vraagt van u om in dit soort gevallen adequaat te handelen en maatregelen te treffen.

Bij een vermoeden van een datalek moet u de volgende stappen doorlopen:

STAP
1

Beoordeel of er sprake is van een datalek

STAP
2

Beoordeel of dit datalek moet worden gemeld bij de Autoriteit Persoonsgegevens

STAP
3

Beoordeel of dit datalek moet worden gemeld aan uw patiënten

STAP
4

Neem dit datalek op in uw datalekkenregister



Bekijk [hier](#) ook het stappenplan
‘Kom in actie bij een datalek’
van de Autoriteit Persoonsgegevens.

STAP
1

Datalek, of niet?

Om een datalek te herkennen, is het van belang te weten wat een datalek precies is. Datalekken doen zich op tal van manieren voor.

Een datalek wordt in de AVG omschreven als een *‘inbreuk in verband met persoonsgegevens’*. Dit houdt een inbreuk op de beveiliging in, waarbij gegevens zijn vernietigd, verloren, gewijzigd, ongeoorloofd zijn verstrekt of dat er ongeoorloofde toegang tot die gegevens is. Een inbreuk op de beveiliging kan zich ook per ongeluk voordoen, er hoeft geen opzet in het spel te zijn.

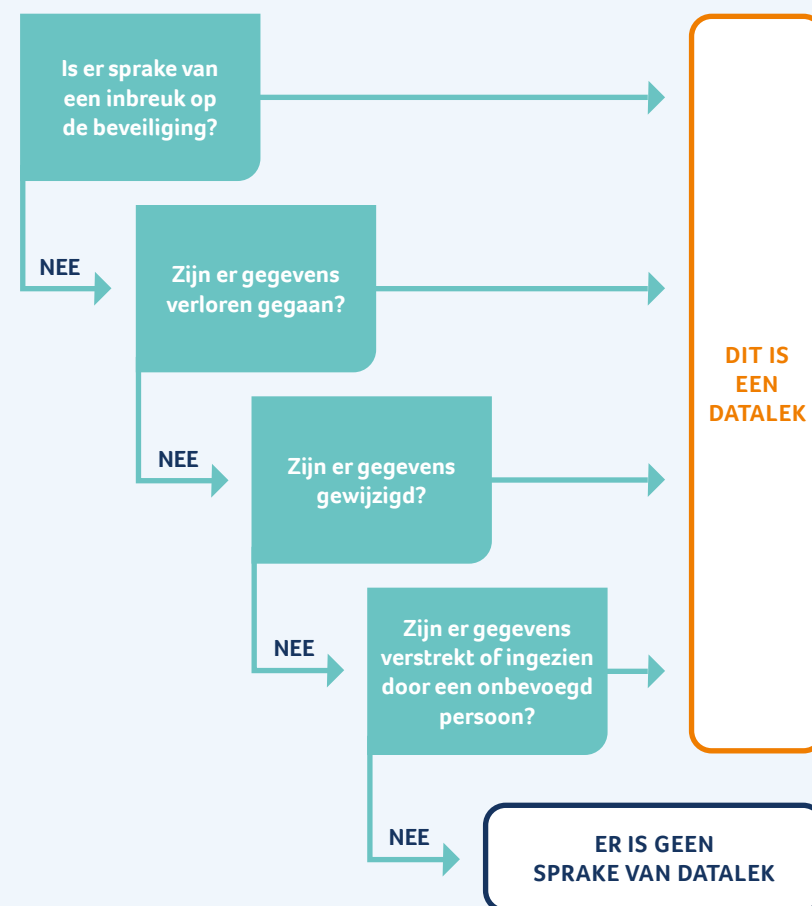
Voorbeelden

Denk hierbij aan een foutief verstuurd e-mail, het kwijtraken of verliezen of diefstal van een USB-stick of laptop met daarop persoonsgegevens, de diefstal van gegevens door een hacker, mailingen aan CC in plaats van BCC, tijdelijk niet beschikbaar zijn van gegevens vanwege een stroomstoring of een computercrash zonder back-up. Maar het kan ook zo zijn dat medische dossiers ongeoorloofd zijn ingezien door medewerkers in de praktijk. Of de schoonmaker kan in een ruimte zijn geweest waar nog een patiëntendossier open stond op het computerscherm.

De in 2019 meest gemelde oorzaak van een datalek bij de AP was het versturen van persoonsgegevens aan de verkeerde ontvanger (63%). In ruim de helft van alle meldingen ging het om gegevens van één persoon (58%). De gemelde datalekken die 5.000 of meer personen raakten, werden vaak (in 47% van de gevallen) veroorzaakt door hacking, malware en/of phishing.

Een datalek is een beveiligingsincident waarbij persoonsgegevens zijn gelekt. Bijvoorbeeld een ongeoorloofde toegang, vernietiging, verlies, wijziging of vrijkomen van persoonsgegevens, opzettelijk of onopzettelijk.

Onderstaand stroomdiagram helpt u bij het beoordelen of sprake is van een datalek of niet



STAP 2

Datalek melden bij de Autoriteit Persoonsgegevens, of niet?

Niet ieder datalek hoeft te worden gemeld bij de AP. Wanneer het onwaarschijnlijk is dat het datalek leidt tot een risico voor de rechten en vrijheden van betrokkenen, hoeft het datalek niet te worden gemeld.

Bij het inschatten van het risico moet u zich afvragen hoe waarschijnlijk het is dat een risico zich voordoet en wat de impact is als het inderdaad gebeurt. Er is een aantal **factoren** van belang bij het beoordelen van dit risico.

U moet bijvoorbeeld denken aan de hoeveelheid en de gevoeligheid van de gegevens, en hoe gemakkelijk de betrokken persoon (of personen) te identificeren is (zijn). Een andere belangrijke factor is wat er precies met de gegevens is gebeurd. Zijn deze verloren gegaan, zijn ze gewijzigd of zijn ze gelekt? Het lekken van medische gegevens aan een onbevoegde heeft namelijk andere gevolgen dan wanneer deze medische gegevens verloren zijn gegaan.

Daarnaast is het van belang dat u in uw afweging de ernst van de gevolgen voor de betrokkene(n) meeneemt, denk bijvoorbeeld aan reputatieschade. Ook kan het risico groter zijn wanneer de getroffen persoon of personen kwetsbaar is of zijn, of in het geval dat de groep van betrokken personen groot is.

De AP heeft [op haar website](#) een aantal factoren opgesomd dat een rol speelt bij het beoordelen van de risico's van een datalek.



Waar melden?

Het datalek moet u melden via het [Meldloket Datalekken](#) van de Autoriteit Persoonsgegevens. Dit moet binnen 72 uur na het ontdekken van het datalek gebeuren.



Wanneer hoeft u niet te melden?

Een datalek hoeft niet gemeld te worden als er vooraf bepaalde maatregelen zijn getroffen, zoals in het geval dat de gegevens zijn versleuteld en de sleutel niet kan worden gevonden door anderen. Melden is ook niet nodig wanneer een onjuiste ontvanger betrouwbaar is, bijvoorbeeld een collega-huisarts met een beroepsgeheim.

**STAP
3**

Datalek melden aan de betrokken persoon (of personen), of niet?

Wanneer het datalek waarschijnlijk een *hoog* risico inhoudt voor de rechten en vrijheden van de betrokken personen moeten zij worden geïnformeerd.

Een dergelijk risico bestaat als het datalek kan leiden tot lichamelijke, materiële of immateriële schade voor de persoon waarop het datalek betrekking heeft, zoals discriminatie, identiteitsdiefstal of -fraude, financieel verlies en reputatieschade. Wanneer er 'gevoelige gegevens' zijn gelekt, waaronder medische gegevens, kunt u ervan uitgaan dat er sprake is van schade, en dat u het lek aan de betrokken personen zult moeten melden.

In dat geval, moet u de betrokken persoon of personen zo snel mogelijk informeren. Zij kunnen dan maatregelen treffen om zich te beschermen tegen de gevolgen van het datalek.

Wat moet u laten weten?

Het is van belang de betrokken persoon/personen te informeren over wat er is gebeurd en wat waarschijnlijk de gevolgen zijn van het datalek. Daarnaast geeft u de betrokken persoon/personen aan welke maatregelen u heeft getroffen en welke maatregelen u de betrokkene aanbeveelt zelf te nemen, om de negatieve gevolgen zoveel mogelijk te beperken. Tenslotte is het van belang de betrokken persoon/personen te informeren over de instanties waar de betrokkene informatie kan krijgen over het datalek en uw contactgegevens te vermelden voor vragen of meer informatie.

STAP 4

Datalek vastleggen in uw datalekkenregister

Elk datalek, ongeacht of u dit wel of niet aan de AP moet melden, moet u vastleggen in uw datalekkenregister. In dit register noteert u de aard van het datalek, de gevolgen daarvan en de corrigerende maatregelen.

Een voorbeeld van een datalekkenregister vindt u hier:

Voorbeelden Verwerkingsregister - LHV. Hiermee voldoet u aan het verantwoordingsbeginsel. Bovendien is de AP bevoegd deze informatie op te vragen en in te zien.

De datalekregistratie moet in ieder geval de volgende informatie bevatten:

- 1 Een omschrijving van het datalek;
- 2 Wanneer het datalek heeft plaats gevonden;
- 3 Beschrijving wat er met de persoonsgegevens is gebeurd;
- 4 Beschrijving van welke groep(en) personen er gegevens zijn gelekt;
- 5 Beschrijving van het type gegevens;
- 6 De mogelijke gevolgen van het datalek;
- 7 De maatregelen die zijn genomen om de schade te beperken en om herhaling te voorkomen.

Heeft u vragen, bijvoorbeeld over deze handleiding? Of heeft u vragen in een concrete situatie waarin u zich afvraagt of er sprake is van een datalek en of u dit moet melden aan de AP en/of aan de betrokkene(n)?

Neem dan contact op met de afdeling Juridische Zaken van de LHV [Juridisch advies - LHV](#).

Wilt u meer weten over veilige omgang met patiëntgegevens? Volg dan de cursus Informatiebeveiliging bij de LHV Academie [Organiseren van informatiebeveiliging \(op aanvraag\) – Academie \(lhv.nl\)](#)

©Landelijke Huisartsen vereniging