FACTSHEET DATALEK

DIGIVAARDIG IN DE ZORG

Wat is een datalek?

Bij een datalek gaat het om ongeoorloofde of onbedoelde toegang tot persoonsgegevens. Maar ook om het ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgegevens. Ook hierdoor kunnen de betrokken personen namelijk schade leiden. De term ‘datalek’ komt niet voor in de wet. In de plaats daarvan heeft de Algemene verordening gegevensbescherming (AVG) het over een ‘inbreuk in verband met persoonsgegevens’.

Hiervan is sprake bij een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens (artikel 4, punt 12, AVG).

Categorieën datalekken

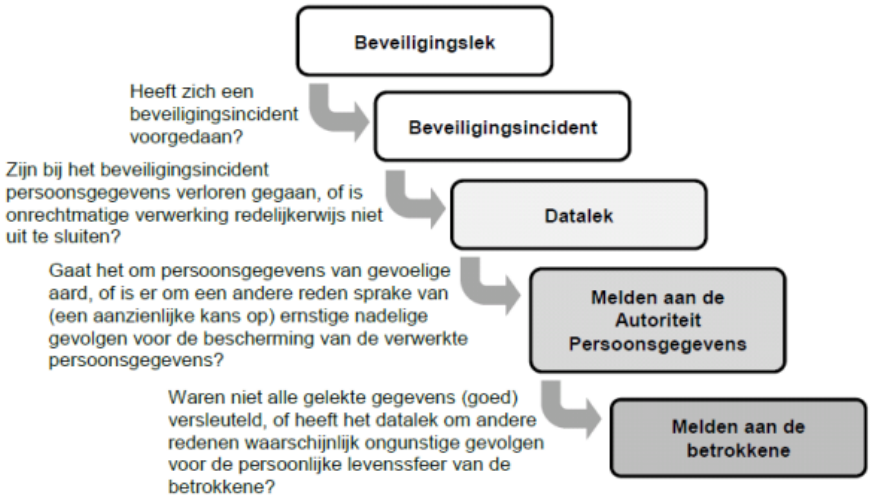
Er zijn 3 categorieën datalekken te onderscheiden:

- **Inbreuk op de vertrouwelijkheid**, wanneer er sprake is van een onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens.
- **Inbreuk op de integriteit**, wanneer er sprake is van een onbevoegde of onopzettelijke wijziging van persoonsgegevens.
- **Inbreuk op de beschikbaarheid**, wanneer er sprake is van een onbevoegd of onopzettelijk verlies van toegang tot, of vernietiging van, persoonsgegevens.

Een datalek kan, afhankelijk van de omstandigheden, in meer dan 1 van deze 3 categorieën vallen.

Voorbeelden datalekken

- het verlies van een USB-stick met niet-versleutelde persoonsgegevens;
- een cyberaanval waarbij persoonsgegevens zijn buitgemaakt;
- een besmetting met ransomware waarbij persoonsgegevens ontoegankelijk zijn gemaakt.



(Bron: Autoriteit Persoonsgegevens, Beleidsregels meldplicht datalekken, pag. 4-5).

Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Maar niet ieder beveiligingsincident is ook een datalek.
Er is sprake van een datalek als er bij het beveiligingsincident een aanmerkelijke kans bestaat dat persoonsgegevens verloren zijn gegaan, of als u onrechtmatige verwerking (kennisneming) van de persoonsgegevens niet redelijkerwijs kunt uitsluiten. We kunnen ook zeggen dat in zulke gevallen de controle over de persoonsgegevens is verloren. Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. U hoeft dan geen melding te doen aan de Autoriteit Persoonsgegevens.

Wat te doen bij een datalek?

Sinds 1 januari 2016 is er een wet van kracht die in het geval van een datalek om adequaat handelen vraagt. De eerste reactie bij een vermoeden van een datalek bestaat uit 3 stappen.

1	**Beoordeel of er echt sprake is van een datalek**	Er is sprake van een datalek als door een inbreuk op de beveiliging, vertrouwelijke gegevens verloren kunnen zijn gegaan. Of als niet uitgesloten is dat deze door onbevoegden zijn verwerkt, binnen of buiten de beschermde omgeving van de praktijk of van de service provider.	Voorbeelden:[2] een USB-stick of pc op straat,[3] UZI-pas met pincode kwijt,[4] inbreuk door een hacker,[5] diefstal van dossiers,[6] fout van een medewerker.[7] Ook kan een andere (zorg)partij of gegevensbewerker melden dat uw gegevens zijn gelekt.[8]
2	**Beoordeel of u het lek moet melden bij de Autoriteit Persoonsgegevens (AP)**	Als er patiëntgegevens zijn gelekt, moet u dat binnen 72 uur na het bekend worden ervan melden bij de AP. Bij twijfel meldt u ook; u kunt een melding later altijd weer intrekken. Ten onrechte niet melden kan leiden tot hoge boete.	U meldt een datalek via het Meldloket Datalekken van de AP: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0
3	**Beoordeel of u uw patiënten moet informeren over het lek**	Als er patiëntgegevens zijn gelekt moet u uw patiënten ook onverwijld informeren. Zij moeten zo nodig maatregelen kunnen nemen om zich te beschermen tegen de gevolgen van het datalek.	U informeert uw patiënten (individueel of in combinatie met algemene voorlichting) over de aard van de inbreuk, de instanties waar de betrokkene meer informatie over de inbreuk kan krijgen, en de maatregelen die u de betrokkene aanbeveelt om te nemen om de negatieve gevolgen van de inbreuk te beperken, zoals het veranderen van gebruikersnamen en wachtwoorden. De aard van de inbreuk mag u algemeen omschrijven. U vermeldt uw contactgegevens zodat de betrokkene u kan bereiken als hij of zij vragen heeft over het datalek.

Bron: www.autoriteitpersoonsgegevens.nl

Voorkomen van een datalek

Huisartsenpraktijken kunnen en moeten hun processen aanpassen naar aanleiding van de meldplicht datalekken. Daardoor kunnen veel problemen worden voorkomen. Datalekken kunnen optreden als gevolg van tekortkomingen op het gebied van menselijk gedrag, organisatie en ICT. Organisaties kunnen verschillende maatregelen treffen om zich voor te bereiden op een datalek. De volgende maatregelen helpen de organisatie om snel en adequaat te kunnen reageren:

– **Zorg voor een goede beveiliging van de persoonsgegevens die je verwerkt.** Dit geldt zowel in de ICT-omgeving als in procedures voor omgang met persoonsgegevens binnen de organisatie. Denk hierbij aan het implementeren van de norm NEN-7510, maar ook bijvoorbeeld aan het opstellen van heldere procedures voor het verzenden, archiveren of vernietigen van documenten die privacygevoelige informatie bevatten.

– **Stel een persoon aan binnen de organisatie** die beveiligingsincidenten en potentiële datalekken beoordeelt en die zo nodig meldt bij de Autoriteit Persoonsgegevens. Zorg ervoor dat de betreffende medewerker voldoende is toegerust voor deze taak en biedt zo nodig scholing aan.

– **Zorg voor adequaat incidentenbeheer** waarbij zowel incidenten die zijn gemeld bij de AP als incidenten die niet zijn gemeld zorgvuldig worden gedocumenteerd, inclusief de afweging die tot de betreffende keuze heeft geleid.

– **Richt een procedure in voor het informeren van betrokkenen bij een datalek**. De meldplicht datalekken schrijft voor dat betrokken personen of patiënten moeten worden geïnformeerd als het aannemelijk is dat een datalek schade voor hen oplevert. Uitgangspunt is dat als er patiëntgegevens zijn gelekt, de patiënten altijd daarover moeten worden geïnformeerd.

– **Denk na over hoe om te gaan met signalen over mogelijke datalekken van buitenaf** of uit de media en leg dit eventueel vast in een communicatieplan.

– **Controleer bestaande overeenkomsten met bewerkers.** De NVZ-modelbewerkersovereenkomst kan hierbij als voorbeeld dienen. Maak aanvullende afspraken met databewerkers over wie wat doet wanneer er een datalek wordt geconstateerd.

Voorbeeld!
Follow the Money heeft zich verdiept in datalekken in de zorg en de commerciële winst hiervan. Klik op de link voor het artikel: https://www.ftm.nl/artikelen/lekkende-zorgdata

Kennisvragen:

1. De assistente stuurt een mail naar alle patiënten van de praktijk. Hoe kan hierbij een datalek ontstaan?
2. Binnen hoe veel uren moet een datalek gemeld zijn?
3. Welke instantie gaat over datalekken van persoonsgegevens?

Deze informatie is afkomstig van www.lhv.nl en bewerkt door ROER voor Digivaardig in de Zorg.
Heb je opmerkingen of vragen over dit lesmateriaal? Mail dan naar info@digivaardigindezorg.nl.

Antwoorden Kennisvragen:

1. Het is belangrijk alle mailadressen in BCC te zetten. Anders zijn alle emailadressen zichtbaar voor iedereen en dat is een datalek.
2. 72 uur
3. Bij de autoriteit persoonsgegevens: www.autoriteitpersoonsgegevens.nl