PROTOCOL MELDEN DATALEK

1. Inleiding

In dit document wordt beschreven hoe er binnen DossierDoctors moet worden omgegaan met het aannemen, registreren en afhandelen van beveiligingsincidenten die mogelijk tot datalekken kunnen of hebben geleid. Het gaat hierbij om datalekken die betrekking hebben op het lekken van persoonsgegevens in de meest breedste zin van het woord.

Voor datalekmeldingen geldt in beginsel een meldingstermijn van **72 uur** nadat het beveiligingsincident is geconstateerd. Gezien deze korte duur is het van belang dat deze procedure wordt gevolgd, zodat er meer tijd is voor het onderzoeken en of de constatering van een datalek ook juist is. Daarnaast wordt onderzoek verricht hoe de datalek heeft kunnen gebeuren, de omvang van de datalek en of er direct maatregelen genomen moeten worden.

2. Wat is een datalek?

Bij een datalek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking. Het kan gaan om een kwijtgeraakte USB-stick of een gestolen laptop met persoonsgegevens, maar ook om een inbraak in een datasysteem, het ten onrechte verstrekken van persoonsgegevens aan derden of per ongeluk verstrekte toegang tot gegevens aan personen of instanties die daartoe geen toegang zouden mogen hebben. Het verzenden van een e-mail aan een adressenbestand waarin alle e-mailadressen voor iedereen zichtbaar zijn, is eveneens een datalek.
Een beveiligingsprobleem is in principe een beveiligingsincident dat tot een datalek leidt of kan leiden. Wanneer erbij een beveiligingsincident persoonsgegevens zijn gelekt, zijn verwijderd of verloren zijn gegaan, is sprake van een datalek zoals hierboven is gedefinieerd.

Als er sprake is van een datalek, dan zijn we verplicht dit, binnen 72 uur, te melden aan de Autoriteit Persoonsgegevens (voorheen het College bescherming persoonsgegevens) en aan de betrokkenen.
Om te zorgen voor een eenduidig beleid en om te voorkomen dat datalekken die wel gemeld hadden moeten worden, dat niet worden is met ingang van 1 april 2018 onderstaand protocol van toepassing.

3. Het protocol; hoe te handelen?

a) Onmiddellijk nadat een werknemer of derde ontdekt of ter ore komt dat er sprake kan zijn van verlies of onrechtmatige verwerking van persoonsgegevens binnen DossierDoctors, meldt deze dit per mail aan Willemien officemanager); hagenouw@dossierdoctors.nl met een cc aan de functionele mailbox contact@dossierdoctors.nl.

b) Voornoemde personen beslissen of er sprake is van een (mogelijk) datalek en of dit (mogelijke) datalek moet worden gemeld bij de Autoriteit Persoonsgegevens (AP) en/of bij de betrokkenen. Indien er sprake is van een data-lek, dan meldt de officemanager dit ‘onverwijld’ aan het Meldpunt Datalekken van de AP. Deze melding wordt gedaan via het op de website van de AP gepubliceerde meldformulier. Dit houdt in dat de officemanager, na het ontdekken van een mogelijk datalek, enige tijd mag nemen voor nader onderzoek teneinde een onnodige melding te voorkomen. De termijn voor het melden start op het moment dat de verantwoordelijke of een bewerker op de hoogte raakt van een incident dat mogelijk onder de meldplicht datalekken valt. Zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking, moet een melding worden gedaan, tenzij op dat moment inmiddels uit onderzoek is gebleken dat het incident niet onder de meldplicht datalekken valt. Het is de werknemer of derde niet toegestaan om het (mogelijke) datalek zelf aan de Autoriteit Persoonsgegevens en/of de betrokkenen te melden.

c) De officemanager stelt vervolgens in overleg met de directie vast of het data-lek een ‘aanmerkelijk risico op verlies of onrechtmatige verwerking waaraan nadelige gevolgen voor de persoonsgegevens en de persoonlijke levenssfeer van de betrokkene(n) zijn verbonden” tot gevolg heeft. Als daar sprake van is, dienen de betrokkenen geïnformeerd te worden over het data-lek.
In de kennisgeving aan de betrokkenen moet in ieder geval worden vermeld:

- de aard van de inbreuk;
- de contactgegevens waar de betrokkene meer informatie over de inbreuk kan krijgen;
- de maatregelen die zijn aanbevolen om de negatieve gevolgen van de inbreuk te beperken.

d) Het datalek moet onverwijld worden gemeld. Dit houdt in dat de officemanager, na het ontdekken van een mogelijk datalek, enige tijd mag nemen voor nader onderzoek zodat betrokkene op een behoorlijke en zorgvuldige manier kan worden geïnformeerd. De melding aan betrokkenen is niet nodig indien de persoonsgegevens versleuteld of onbegrijpelijk zijn gemaakt, waardoor deze niet te lezen zijn door anderen.

e) Indien uit het onderzoek naar voren is gekomen dat er sprake is van een datalek, worden door de directie direct maatregelen getroffen om het verder lekken van gegevens te voorkomen.

f) De officemanager houdt een overzicht bij van de datalekken, met daarin onder meer de gevolgen van de datalekken en de herstelmaatregelen die zijn genomen. Dit overzicht mag uitsluitend de voor dit doel noodzakelijke gegevens bevatten. Er moet een overzicht worden bijgehouden van alle datalekken die onder de meldplicht vallen, dus datalekken die aan de Autoriteit Persoonsgegevens moeten worden gemeld. Per datalek bevat het overzicht in ieder geval de gegevens omtrent de aard van de inbreuk en, indien dat aan de betrokkene is gemeld, de tekst van de kennisgeving.