PROTOCOL DATALEKKEN

De AVG bepaalt dat datalekken direct, binnen 72 uur, gemeld moeten worden aan de Autoriteit Persoonsgegevens ('AP'), tenzij het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen.
Daarnaast moet het datalek ook aan de betrokkenen gemeld worden als het waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen met zich meebrengt.

Aan de beantwoording van de vraag moet een zorgvuldige (belangen)afweging voorafgaan. Hierbij is bijvoorbeeld de aard en de omvang van de persoonsgegevens die gelekt zijn van belang. Als er bijzondere persoonsgegevens, zoals gegevens over gezondheid, gelekt zijn, dan is de melding meestal noodzakelijk.

Dit protocol datalekken is bedoeld als hulpmiddel voor de beantwoording van de vraag of er sprake is van een datalek en of deze gemeld moet worden.
Waar in dit stuk manager staat, kan zowel directeur als manager gelezen worden.

1: Wat is een datalek?
Er is sprake van een datalek als er een inbreuk in verband met persoonsgegevens heeft plaatsgevonden. Alleen een dreiging of een tekortkoming in de beveiliging is niet voldoende; er moeten daadwerkelijk persoonsgegevens gelekt zijn.

Onder een datalek verstaat de AP persoonsgegevens die gelekt of vernietigd zijn als gevolg van een beveiligingsincident. Bij het lek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking.
Bij verlies zijn de persoonsgegevens er niet meer.
Onder onrechtmatige verwerking vallen bijvoorbeeld onbevoegde kennisneming, wijziging, aantasting of de verstrekking daarvan.

Voorbeelden van inbreuken in verband met persoonsgegevens kunnen zijn:
- kwijtraken van een USB -stick
- diefstal van een laptop
- inbraak door een hacker
- persoons/cliëntgegevens per ongeluk gepubliceerd
- hacking, mailware of fishing
- persoonsgegevens aan verkeerde persoon verstuurd
- calamiteiten zoals brand in een datacentrum

2: Contactpersoon aanwijzen
De organisatie heeft een contactpersoon aangewezen aan wie eventuele datalekken gemeld moeten worden (FG = functionaris gegevensbescherming).

3: Informeren medewerkers
Medewerkers binnen de organisatie moeten er van bewust te zijn dat als er sprake is van een datalek, zij dit datalek direct (diezelfde dag nog) moeten melden bij de FG, zodat deze het datalek op tijd kan melden bij de Autoriteit Persoonsgegevens. Medewerkers moeten bekend zijn met het in dit protocol opgenomen stappenplan.

4: Uitvoeren van het stappenplan Datalekken

De FG zorgt voor de invoering en naleving van het hieronder beschreven stappenplan Datalekken. Als er een datalek optreedt, dienen de stappen in het stappenplan Datalekken doorlopen te worden.

STAPPENPLAN DATALEKKEN

Processtappen	Activiteit	Verantwoordelijke persoon
1. Er wordt een (mogelijk) datalek ontdekt	- Maak direct melding van (mogelijke) datalek via privacy@eilandzorg.com - Informeer FG, die manager informeert	Medewerker die het ontdekt
2. Beoordeel het datalek	- Onderzoek het beveiligingsincident - Onderzoek of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden - Beoordeel wie of welke afdelingen binnen de organisatie hierbij betrokken zijn - Beoordeel of er een verwerker betrokken is bij het incident. Zo ja dan dient deze bij het proces betrokken te worden	Manager FG FG FG
3. Bestrijdt het datalek	- Stop het datalek als het nog kan - Neem andere maatregelen om het datalek en de daaruit voortvloeiende schade te beperkten - Leg de acties van de genomen maatregelen vast in het dossier	Manager Manager FG
4.Vaststellen impact datalek	- Onderzoek het datalek en de gevolgen daarvan - Onderzoek de aard van de gegevens die gelekt zijn. Bijv. gezondheidsgegevens, wachtwoorden, gegevens over financiële situatie of die kunnen leiden tot vooroordelen/misbruik - Onderzoek de omvang van de gelekte gegevens - Beoordeel welke impact het lek kan hebben op de betrokken personen	Manager Manager FG FG

	- Stel vast wat de nadelige gevolgen kunnen zijn	FG
5. Vaststellen Meld en Herstelaanpak	- Bepaal aanpak/informeren AP - Bepaal aanpak/informeren betrokkenen - Bepaal acties voor nazorg betrokkenen - Bepaal acties voor belang van de organisatie - Bepaal acties voor verbetering beveiliging	Manager Manager Manager Manager FG
6. Melden AP*	- Indien besloten wordt om AP te informeren dan moet dat binnen 72 uur - Melding via het meldloket: digitale formulier van de website van het AP - Tel nr AP: 0900-3282535	FG Manager FG
7. Melden betrokkenen**	- Melding via bijvoorbeeld brief - Meedelen wat er is gebeurd, welke persoonsgegevens getroffen zijn en wat de mogelijke gevolgen van het datalek kunnen zijn - Informeren over de maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen	FG Manager Marketing/communicatie
8. Uitvoeren herstelwerkzaamheden	- Herstel het datalek - Verbeteren van de beveiliging - Lever nazorg aan de betrokkenen	ICT partner FG Marketing / communicatie
9. Optimaliseer het beveiligings- en het Datalek proces	- Registreer, evalueer en verbeter de beveiliging en het proces inzake melding datalekken	FG Manager

* Melding aan de Autoriteit persoonsgegevens kan alleen achterwege blijven, als het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Of hiervan sprake is, hangt mede af van de aard en omvang van de gelekte persoonsgegevens. Als bijvoorbeeld uitsluitend de adresgegevens zijn gelekt van een kleine groep betrokkenen, dan is het onwaarschijnlijk dat er sprake is van een hoog risico. Dat is wellicht anders als de adresgegevens in combinatie met het lidmaatschap van de patiënten of cliëntenorganisatie zijn gelekt. Het lidmaatschap van de organisatie kan gezien worden als een gevoelig gegeven en de leden van de organisatie kunnen wellicht behoren tot een kwetsbare groep, die extra bescherming nodig heeft. Bij de afweging van het risico voor de rechten en vrijheden van de betrokken zal de Functionaris Gegevensbescherming altijd betrokken moeten worden.

** Als het datalek waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen veroorzaakt, moet het datalek ook aan de betrokkenen gemeld worden. Het risico zal bijvoorbeeld moeten worden beoordeeld aan de hand van de aard en de hoeveelheid van de gelekte gegevens. Als er persoonsgegevens van gevoelige aard (bijv. gezondheidsgegevens) gelekt zijn, zal het lek in ieder geval gemeld moeten worden aan de betrokkenen. Bij de afweging van het risico voor de rechten en vrijheden van de betrokkenen zal altijd de Functionaris Gegevensbescherming betrokken moeten worden.

Verwerker

Het kan gebeuren dat het datalek optreedt bij de verwerker. De organisatie is en blijft (als verwerkingsverantwoordelijke) altijd verantwoordelijk voor het datalek bij de verwerker. In dat geval moet dus hetzelfde stappenplan worden afgewerkt. De verwerker zal bij de stappen betrokken moeten worden.

Via de verwerkersovereenkomst moet afgedwongen worden dat de verwerker eventuele datalekken direct (binnen 24 uur) meldt bij de organisatie en de organisatie helpt bij het beoordelen of er gemeld moet worden en de afwikkeling van het datalek. Belangrijk is dat de verwerker niet buiten de organisatie om een datalek meldt bij de Autoriteit Persoonsgegevens. De verwerker moet verder alle redelijke instructies van de organisatie opvolgen.