BIJLAGE: PROTOCOL DATALEKKEN

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

Aan de beatwording 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.

1.Wat is een datalek?

Er is sprake van een datalek als er 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 beveiligingsaccident. . Bij verlies zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige. Bij het lek zijn 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 USB-stick
- Diefstal van een laptop
- Inbraak door een hacker
- Persoonsgegevens per ongeluk gepubliceerd
- Hacking, mailware of fishing
- Persoonsgegevens aan een verkeerd person verstuurd
- Calamiteiten zoals brand in en datacentrum

2.contactpersoon aanwijzen

De organisatie moet een eigen contactpersoon aanwijzen aan wie eventueel dataleken gemeld moeten woorden. Dit kan bijvoorbeeld een bestuurslid of de Functionaris Gegevensbescherming zijn. (hierna: “contactpersoon”)

3. Informeren medewerkers

Medewerkers binnen de organisatie dienen zich er van bewust te zijn dat als er sprake is van een datalek, zij dit datalek direct (diezelfde dag nog) moeten melden bij de aangewezen contactpersoon, zodat deze tijdig het datalek kan melden bij de Autoriteit Persoonsgegevens. Zij dienen te zijn met het in dit protocol opgenomen stappenplan.

4.Uitvoeren van het stappenplan Datalekken

De binnen organisatie aangewezen Contactpersoon draagt zorg de invoering en naleving van het hieronder opgenomen stappenplan Datalekken. Indien er een datalek optreedt dienen de stappen in het stappenplan Datalek doorlopen te worden.

STAPPENPLAN DATALEKKKEN

Processtappen	Activiteit	Verantwoordelijk persoon
1.Er wordt een (mogelijk) datalek ontdekt	- Maak direct intern melding van (mogelijk) datalek -Informeer de verantwoordelijk contactpersoon	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 het organisatie hier betrokken zijn - Beoordeel of er een verwerker betrokken is bij het incident. Zo ja dan dient deze direct bij het proces betrokken te worden	Manager van de afdeling waar binnen het datalek heeft plaatsgebonden Manager van de afdeling die verantwoordelijk is voor de beveilingsincident (bijvoorbeeld IT) Aangewezen contactpersoon
3.Bestrijdt het datalek	-Stop het datalek als het nog kan -Neem andere maatregelen om het datalek en de daaruit voortvloeiende schade te beperkte -Leg de acties van de genomen maatregelen vast in het dossier	Manager van de afdeling waar binnen het datalek heeft plaatsgevonden Manager van de afdeling die verantwoordelijk is voor de beveilingsincident (bijvoorbeeld IT) Aangewezen contactpersoon
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 situaties of die kunnen leiden tot stigmatisering/ misbruik	Manager van de afdeling waar binnen het datalek heeft plaatsgebonden Manager van de afdeling die verantwoordelijk is voor de beveilingsincident (bijvoorbeeld IT) Aangewezen contactpersoon

	-Onderzoek de omvang van de gelekte gegevens -Beoordeel welke impact het lek kan hebben op de betrokken personen -Stel vast wat de nadelige gevolgen kunnen zijn	Functionaris Gegevensbescherming
5. Vaststellen Melden 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 van de afdeling waar binnen het datalek heeft plaatsgevonden Manager van de afdeling die verantwoordelijk is voor de beveilingsincident (bijvoorbeeld IT) Aangewezen contactpersoon Functionaris Gegevensbescherming
6.Melden AP*	-Indien besloten wordt on AP te informeren dan moet dat binnen 72 uur -Melding via de website van het AP -Van tevoren kan het Meldformulier Datalekken gebruikt worden	Aangewezen contactpersoon Functionaris Gegevensbescherming Bestuur
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 hebben -Infomeren over de maatregelen die de organisatie neemt en die betrokkene zelf kan nemen om schade te voorkomen	Aangewezen contactpersoon Functionaris Gegevensbescherming Bestuur Marketing/ communicatie
8.Uitvoeren herstelwerkzaamheden	-Herstel het datalek	Manager van de afdeling die verantwoordelijk is voor de

	-Verbeteren van de beveiliging -Lever nazorg aan de betrokkenen	beveilingsincident (bijvoorbeeld IT) Aangewezen contactpersoon

9.Optimaliseer het beveiligings- en het Datalek proces	-Registreer, evalueer en verbeter de beveiliging en het proces inzake melding datalek	Aangewezen contactpersoon Functionaris Gegevensbescherming Bestuur Manager van de afdeling die verantwoordelijk is voor de beveilingsincident (bijvoorbeeld IT)

*Melding aan de Autoriteit persoonsgegevens kan alleen achterwege blijven indien 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. Indien bijvoorbeeld uitsluitend de adresgegevens zijn gelekt van een kleine groep betrokkenen, dan is het onwaarschijnlijk dat er sprake is van een hoge risico. Dat is wellicht anders indien de adresgegevens in combinaties met het lidmaatschap van de patiënten of cliëntenorganisatie zijn gelekt. Het lidmaatschap 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 altijd de Functionaris Gegevensbescherming betrokken moeten worden.

**Indien 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 hoeveelheid van de gelekte gegevens. Als er persoonsgegevens van de gevoelige aard (bijv. gezondheidsgegevens) gelekt zijn, zal het lek in iedere geval gemeld moeten aan de betrokkenen. Bij de afweging van het risico voor de rechten en vrijheden van de betrokkenen zal altijd de Functionaris Gegevensbescherming betrokken 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 eventueel datalekken terstond(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.

Procedure melden datalek