PROTOCOL DATALEKKEN Stichting Zeldzame Bloedziekten

De AVG bepaalt dat datalekken 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 indien het waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen met zich meebrengt.

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.

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 het lekken of verloren gaan van persoonsgegevens 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
- persoonsgegevens per ongeluk gepubliceerd
- hacking, mailware of fishing
- persoonsgegevens aan verkeerde persoon verstuurd
- calamiteiten zoals brand in een datacentrum

Contactpersoon datalek

Eventuele datalekken moeten gemeld moeten aan bestuurslid van SZB Paul Peereboom paul@bloedziekten.nl 055-3551641 06-17139634

Melding

Een aangesloten patiëntenorganisatie die geen eigen beleid op dit gebied heeft, dient een datalek direct (diezelfde dag nog) te melden bij de contactpersoon datalek, zodat deze tijdig het datalek kan melden bij de Autoriteit Persoonsgegevens.

Uitvoeren van het stappenplan Datalekken

Binnen SZB draagt de contactpersoon datalek zorg voor de invoering en naleving van het hieronder opgenomen Stappenplan datalekken. Indien 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 intern melding van (mogelijke) datalek - Informeer de contactpersoon	Contactpersoon aangesloten patiëntenorganisatie
2. Beoordeel het datalek	- Onderzoek het beveiligingsincident - Onderzoek of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden - Beoordeel welke aangesloten patiëntenorganisatie binnen SZB betrokken zijn - Beoordeel of er een verwerker betrokken is bij het incident. Zo ja dan dient deze bij het proces betrokken te worden	Contactpersoon datalek
3. Bestrijdt het datalek	- Stop het datalek als het nog kan - Neem andere maatregelen om het datalek en de daaruit voortvloeiende schade te beperken - Leg de acties van de genomen maatregelen vast in het dossier	Contactpersoon datalek Contactpersoon aangesloten patiëntenorganisatie
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 stigmatisering/misbruik - 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	Contactpersoon datalek Contactpersoon aangesloten patiëntenorganisatie
5. Vaststellen Meld en Herstelaanpak	- Bepaal aanpak/informeren AP - Bepaal aanpak/informeren betrokkenen - Bepaal acties voor nazorg betrokkenen - Bepaal acties voor verbetering beveiliging	Contactpersoon datalek Contactpersoon aangesloten patiëntenorganisatie
6. Melden AP*	- Indien besloten wordt om AP te informeren dan moet dat binnen 72 uur - Melding via de website van het AP - Van tevoren kan het Meldformulier Datalekken gebruikt worden	Contactpersoon datalek Bestuur SZB

Stappenplan datalekken (vervolg)

Processtappen	Activiteit	Verantwoordelijke persoon
7. Melden betrokkenen**	- Melding via bijvoorbeeld brief - Meedelen wat er is gebeurd, welke persoonsgegevens getroffen zijn en wat de mogelijke gevolgen van het datalek zijn. - Informeren over de maatregelen die SZB neemt en die de betrokkene zelf kan nemen om schade te voorkomen	Contactpersoon datalek Secretaris SZB
8. Uitvoeren herstelwerkzaamheden	- Herstel het datalek - Verbeter de beveiliging - Lever nazorg aan de betrokkenen	Contactpersoon datalek Bestuur SZB
9. Optimaliseer het beveiligings- en het Datalek proces	- Registreer, evalueer en verbeter de beveiliging en het proces inzake melding datalekken	Contactpersoon datalek aangesloten patiëntenorganisatie Bestuur SZB

* 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 hoog risico. Dat is wellicht anders indien de adresgegevens in combinatie met de aandoening of het lidmaatschap van de patiëntenorganisatie zijn gelekt. Het lidmaatschap van de organisatie kan gezien worden als een gevoelig gegeven en de leden van de organisatie behoren wellicht tot een kwetsbare groep, die extra bescherming nodig heeft.

** 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 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.

Verwerker

Het kan gebeuren dat het datalek optreedt bij de verwerker. SZB is en blijft 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.

De verwerker moet eventuele datalekken terstond (binnen 24 uur) melden bij de Contactpersoon datalek. Die helpt bij het beoordelen of er gemeld moet worden en de afwikkeling van het datalek. Belangrijk is dat de verwerker niet buiten om SZB een datalek meldt bij de Autoriteit Persoonsgegevens.