Stichting ijgenwys en Anders.
Markenland 96
4871 AV Etten-Leur
076-5962598/ 06-14180025
www.ijgenwys.nl/ info@ijgenwys.nl
KVK 57386994/ AGB code 73-732659
Regiobank NL65 RBRB 082 79 76 992
Rabobank NL56 RABO 031 67 54196

PROTOCOL

DATA-LEK

Stichting ijgenwys en Anders

Markenland 96
4871 AV Etten-leur
Geldig vanaf 1 juni 2021

Inhoudsopgave

Protocol data-lek

De AVG bepaalt dat datalekken direct, binnen 72 uur, gemeld moeten worden aan de Autoriteit Persoonsgegevens (’AP’), tenzij het onwaarschijnlijk is dat het data-lek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Daarnaast moet het data-lek 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 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 data-lek en of deze gemeld moet worden.

1: Wat is een data-lek?
Er is sprake van een data-lek 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 data-lek 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
- persoonsgegevens per ongeluk gepubliceerd
- hacking, mailware of fishing
- persoonsgegevens aan verkeerde persoon verstuurd
- calamiteiten zoals brand in een datacentrum

2: Contactpersoon aanwijzen
De organisatie moet een eigen contactpersoon aanwijzen aan wie eventuele datalekken gemeld moeten worden. 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 data-lek, zij dit data-lek direct (diezelfde dag nog) moeten melden bij de aangewezen Contactpersoon, zodat deze tijdig het data-lek kan melden bij de Autoriteit Persoonsgegevens. Zij dienen bekend te zijn met het in dit protocol opgenomen stappenplan.

4: Uitvoeren van het stappenplan Datalekken
De binnen de organisatie aangewezen Contactpersoon draagt zorg voor de invoering en naleving van het hieronder opgenomen stappenplan Datalekken. Indien er een data-lek optreedt dienen de stappen in het stappenplan Datalekken doorlopen te worden.

STAPPENPLAN DATALEKKEN

Processtappen	**Activiteit**	**Verantwoordelijke persoon**
1. Er wordt een (mogelijk) data-lek ontdekt	- Maak direct intern melding van (mogelijke) data-lek - Informeer de verantwoordelijke Contactpersoon	Medewerker die het ontdekt
2. Beoordeel het data-lek	- 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 van afdeling waar binnen het data-lek heeft plaatsgebonden Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT) Aangewezen contactpersoon
3. Bestrijdt het data-lek	- Stop het data-lek als het nog kan - Neem andere maatregelen om het data-lek en de daaruit voortvloeiende schade te beperkten - Leg de acties van de genomen maatregelen vast in het dossier	Manager van afdeling waar binnen het data-lek heeft plaatsgebonden Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT) Aangewezen contactpersoon
4.Vaststellen impact data-lek	- Onderzoek het data-lek en de gevolgen daarvan - Onderzoek de aard van de gegevens die gelekt zijn. Bijv. gezondheidsgegevens, wachtwoorden, gegevens over financiële situatie of die	Manager van afdeling waar binnen het data-lek heeft plaatsgebonden Manager van de afdeling die verantwoordelijk is voor de

	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	beveiligingsincidenten (bijvoorbeeld IT) Aangewezen contactpersoon Functionaris Gegevensbescherming
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 van afdeling waar binnen het data-lek heeft plaatsgebonden Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT) Aangewezen contactpersoon Functionaris Gegevensbescherming
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	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 data-lek kunnen zijn. - Informeren over de maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen	Aangewezen contactpersoon Functionaris Gegevensbescherming Bestuur Marketing/communicatie
8. Uitvoeren herstelwerkzaamheden	- Herstel het data-lek - Verbeteren van de beveiliging - Lever nazorg aan de betrokkenen	Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT)

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

* Melding aan de Autoriteit persoonsgegevens kan alleen achterwege blijven indien het onwaarschijnlijk is dat het data-lek 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 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 altijd de Functionaris Gegevensbescherming betrokken moeten worden.

** Indien het data-lek waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen veroorzaakt, moet het data-lek 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.

5: Verwerker

Het kan gebeuren dat het data-lek optreedt bij de verwerker. De organisatie is en blijft (als verwerkingsverantwoordelijke) altijd verantwoordelijk voor het data-lek 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 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 data-lek. Belangrijk is dat de verwerker niet buiten de organisatie om een data-lek meldt bij de Autoriteit Persoonsgegevens. De verwerker moet verder alle redelijke instructies van de organisatie opvolgen.