



PROTOCOL DATALEKKEN STICHTING DIERENAMBULANCE GOOI EN VECHTSTREEK

De Algemene Verordening Gegevensbescherming (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 betrokkenen. Daarnaast moet het datalek ook aan de betrokkenen gemeld worden indien het waarschijnlijk een groot risico voor de 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 noodzakelijk.

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 rechtmatige verwerking. Bij verlies zijn de persoonsgegevens er niet meer. Onder rechtmatige verwerking vallen bijvoorbeeld onbevoegde kennisneming, wijziging, aantasting of de verstrekking daarvan.

Voorbeelden van inbreuken in verband met persoonsgegevens kunnen zijn:

- Het kwijtraken van een USB-stick
- Diefstal of verlies van een laptop
- Inbraak door een hacker
- Persoonsgegevens die per ongeluk zijn gepubliceerd
- Hacking, malware of phishing
- Persoonsgegevens aan de verkeerde persoon gestuurd
- Calamiteiten zoals brand in een datacentrum

Contactpersoon

Voor Stichting Dierenambulance is Paul Onkenhout, manager, de contactpersoon. Hij zal ingeschakeld worden bij eventuele datalekken.



Informereren medewerkers

Medewerkers zijn zich ervan bewust dat als er sprake is van een (mogelijk) datalek, zij dit datalek direct moeten melden bij de contactpersoon, zodat deze tijdig het datalek kan melden bij de Autoriteit Persoonsgegevens. Zij zijn bekend met het in dit protocol opgenomen stappenplan. Tijdens werkoverleggen wordt dit besproken.

De binnen de stichting aangewezen contactpersoon draagt zorg voor de invoering en naleving van het hieronder stappenplan datalekken. Indien er een datalek optreedt, dienen de stappen in het stappenplan doorlopen te worden.

STAPPENPLAN DATALEKKEN

Processtappen	Activiteit	Verantwoordelijke
1. Er wordt een (mogelijk) datalek ontdekt	<ul style="list-style-type: none">- Maak direct intern een melding hierover- Informeer de contactpersoon	Degene die het ontdekt heeft
2. Beoordeel het datalek	<ul style="list-style-type: none">- Onderzoek het beveiligingsincident- Onderzoek of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden- Beoordeel wie er binnen de stichting bij betrokken zijn- Beoordeel of er een verwerker betrokken is bij het incident. Zo ja, dan dient deze bij het proces betrokken te worden	Medewerker bij wie het datalek heeft plaatsgevonden Medewerker die verantwoordelijk is voor de beveiligingsincidenten (contactpersoon)
3. Bestrijdt het datalek	<ul style="list-style-type: none">- 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	Medewerker bij wie het datalek heeft plaatsgevonden Medewerker die verantwoordelijk is voor de beveiligingsincidenten (contactpersoon)



4. Vaststellen impact datalek	<ul style="list-style-type: none">- Onderzoek het datalek en de gevolgen daarvan- Onderzoek de aard van de gegevens die gelekt zijn- 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	Medewerker bij wie het datalek heeft plaatsgevonden Medewerker die verantwoordelijk is voor de beveiligingsincidenten (contactpersoon)
5. Vaststellen meld- en herstelaanpak	<ul style="list-style-type: none">- Bepaal aanpak/informeren AP- Bepaal aanpak/informeren betrokkenen- Bepaal nazorg voor betrokkenen- Bepaal acties voor de stichting- Bepaal acties voor verbetering beveiliging	Medewerker bij wie het datalek heeft plaatsgevonden Medewerker die verantwoordelijk is voor de beveiligingsincidenten (contactpersoon)
6. Melden AP	<ul style="list-style-type: none">- Indien besloten wordt om AP te informeren, moet dat binnen 72 uur- Melding via het Meldformulier Datalekken op de website van AP	Contactpersoon
7. Melden betrokkenen	<ul style="list-style-type: none">- Melding via het rooster- Mededelen wat er is gebeurd, welke persoonsgegevens getroffen zijn en wat de mogelijke gevolgen kunnen zijn	Contactpersoon Directeur Bestuur



	<ul style="list-style-type: none">- Informeren over de maatregelen die de stichting neemt en die de betrokkene zelf kan nemen om schade voorkomen	
8. Uitvoeren herstelwerkzaamheden	<ul style="list-style-type: none">- Herstel het datalek- Verbeteren van de beveiliging- Lever nazorg aan betrokkenen	Contactpersoon
9. Optimaliseer het beveiligings- en het datalekproces	<ul style="list-style-type: none">- Registreer, evalueer en verbeter de beveiliging en proces inzake melding datalekken	Contactpersoon

Verwerker

Het kan gebeuren dat het datalek optreedt bij de verwerker. De stichting 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 terstond (binnen 24 uur) meldt bij de stichting en de stichting helpt bij het beoordelen of er gemeld moet worden en de afwikkeling van datalek. Belangrijk is dat de verwerker niet buiten de stichting om een datalek meldt bij de AP. De verwerker moet verder alle redelijke instructies van de stichting opvolgen.