PROTOCOL DATALEKKEN

Achtergrond

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra er sprake is van een ernstig datalek. De meldplicht datalekken blijft onder de AVG (Algemene Verordening gegevensbescherming, per 25 mei 2018 van toepassing) grotendeels hetzelfde. De AVG stelt echter strengere eisen aan de registratie van de datalekken die zich in de organisatie hebben voorgedaan. Van belang is dat we *alle* datalekken moeten documenteren. Met deze documentatie moet de AP namelijk kunnen controleren, mocht het nodig zijn, of wij aan de meldplicht hebben voldaan.

Wanneer is er sprake van een datalek?

Bij een datalek gaat het om 'toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie'. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook de onrechtmatige verwerking van gegevens. We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens). We hoeven niet alle datalekken te melden, alleen als dit leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens (of als er een aanzienlijke kans bestaat dat dit gebeurt).

Melding Autoriteit persoonsgegevens

Is er sprake van een datalek, dan dienen wij binnen 72 uur een melding te doen bij de Autoriteit persoonsgegevens. Dat kan via deze link:
www.datalekken.autoriteitpersoonsgegevens.nl/actionpage?
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 beantwoording van deze vraag moet een zorgvuldige (belangen)afweging voorafgaan. Per situatie kan dit anders zijn. Hierbij is de aard en de omvang van de persoonsgegevens die gelekt zijn van belang.

Contactpersoon

Datalekken dienen direct (dag van ontdekking) gemeld te worden aan Piet Koremans 06-44422838

Informeren medewerkers

Alle 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) moeten melden bij de Contactpersoon, zodat deze tijdig (indien nodig) het datalek kan melden bij de Autoriteit Persoonsgegevens.

STAPPENPLAN DATALEKKEN

Processtappen	**Activiteit**	**Verantwoordelijke persoon**
1. Er wordt een (mogelijk) datalek ontdekt	- Maak direct intern melding van (mogelijke) datalek - Informeer de verantwoordelijke 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 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	Aangewezen contactpersoon
3. Bestrijdt het datalek	- Stop het datalek als het nog kan - Neem maatregelen om het datalek en de daaruit voortvloeiende schade te beperken - Leg de acties van de genomen maatregelen vast in een dossier	Aangewezen contactpersoon
4.Vaststellen impact datalek	- Onderzoek het datalek en de gevolgen daarvan - Onderzoek de aard van de gegevens die gelekt zijn, of die kunnen leiden tot stigmatisering/misbruik - Onderzoek de omvang van de gelekte gegevens - Beoordeel welke impact het lek kan hebben op betrokken personen - Stel vast wat de nadelige gevolgen kunnen zijn	Aangewezen contactpersoon

5. Vaststellen Meld en Herstelaanpak	- Bepaal aanpak/informeren AP - Bepaal aanpak/informeren betrokkenen - Bepaal acties voor nazorg betrokkenen en organisatie - Bepaal acties voor verbetering beveiliging	Aangewezen contactpersoon
6. Melden AP	- Indien besloten wordt om AP te informeren dan moet dat binnen 72 uur - Melding via de website van het AP - Meldformulier Datalekken kan gebruikt worden	Aangewezen contactpersoon
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	Aangewezen contactpersoon
8. Uitvoeren herstelwerkzaamheden	- Herstel het datalek - Verbeteren van de beveiliging - Lever nazorg aan de betrokkenen	Aangewezen contactpersoon
9. Optimaliseer het beveiligings- en het Datalek proces	- Registreer, evalueer en verbeter de beveiliging en het proces inzake melding datalekken	Aangewezen contactpersoon

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.