Protocol melden beveiligingsincidenten en datalekken

Stichting Aandacht+
SWV VO2402
Espelerlaan 70
8302 DC Emmeloord

Bewerkt door: Audrey Eijsberg

Versie	Status	Bijgewerkt d.d. datum	Auteur	Omschrijving
1	Concept	04-06-2026	Audrey	Protocol beveiligingsincidenten en datalekken

Instemming gegeven door PMR

Versie	Status	Instemming PMR	Naam	Omschrijving
1	Concept	04-06-2026	Marijn Eva Dine	Protocol beveiligingsincidenten en datalekken

Vastgesteld door AB Aandacht+

Versie	Status	Naam	Functie
1	Definitief	A.Dijk 15-06-2026	Voorzitter DB/AB

Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacybeleid van Aandacht+.

Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het voorkomen van beveiligingsincidenten en datalekken.

Dit protocol is van toepassing op de gehele organisatie van Aandacht+, zoals vermeld in het IBP-beleid en al haar medewerkers.

Meldplicht datalekken

De meldplicht datalekken houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen, maximaal binnen 72 uur, bij de Autoriteit Persoonsgegevens (AP) zodra zij een datalek hebben. 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.

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. Of zonder dat dit wettelijk is toegestaan.

Wat is een datalek precies?

Bij een datalek gaat het om ongeoorloofde of onbedoelde toegang tot persoons-gegevens. Maar ook om het ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgegevens. Ook hierdoor kunnen de betrokken personen namelijk schade leiden.
De term ‘datalek’ komt niet voor in de wet. In de plaats daarvan heeft de Algemene verordening gegevensbescherming (AVG) het over een ‘inbreuk in verband met persoonsgegevens’.
Hiervan is sprake bij een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens (Artikel 4, punt 12, AVG).

Categorieën datalekken

Er zijn drie categorieën datalekken te onderscheiden:

- *Inbreuk op de vertrouwelijkheid*
  Wanneer er sprake is van een onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens.
- *Inbreuk op de integriteit*
  Wanneer er sprake is van een onbevoegde of onopzettelijke wijziging van persoonsgegevens.
- *Inbreuk op de beschikbaarheid*
  Wanneer er sprake is van een onbevoegd of onopzettelijk verlies van toegang tot, of vernietiging van, persoonsgegevens.

Een datalek kan, afhankelijk van de omstandigheden, in meer dan één van deze drie categorieën vallen.

Aandacht+ heeft een Privacy Officer (PO) en een Functionaris Gegevensbescherming (FG). Eventuele datalekken kunnen bij beide personen gemeld worden via privacy@aandachtplus.nl.

De binnen de organisatie aangewezen Privacy Officer (PO) draagt 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 (zie onderstaand).

Stappenplan Datalekken

Processtappen	Activiteit	Verantwoordelijke persoon
1. Er wordt een (mogelijk) datalek ontdekt	- Maak direct intern melding van (mogelijke) datalek bij PO/FG - Informeer de verantwoordelijke contactpersoon	- Medewerker die het ontdekt - PO
2. Beoordeel het datalek	- Onderzoek het beveiligingsincident - Onderzoek of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden - Beoordeel wie 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	- Directeur waar binnen het datalek heeft plaatsgebonden - Hoofd ICT - PO
3. Bestrijdt het datalek	- Stop het datalek als het nog kan - Neem andere maatregelen om het datalek en de daaruit voortvloeiende schade te beperkten - Leg de acties van de genomen maatregelen vast in het dossier	- Directeur waar binnen het datalek heeft plaatsgebonden - Hoofd ICT - PO/FG

4.Vaststellen impact datalek	- Onderzoek het datalek en de gevolgen daarvan - Onderzoek de aard van de gegevens die gelekt zijn. Bijv. gezondheids-gegevens, 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	- Directeur waar binnen het datalek heeft plaatsgebonden - Hoofd ICT - PO - FG
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	- Directeur waar binnen het datalek heeft plaatsgebonden - Hoofd ICT - PO - FG
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	- PO - FG - 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 zijn. - Informeren over de maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen	- PO - FG - Bestuur - Marketing/communicatie
8. Uitvoeren herstelwerkzaamheden	- Herstel het datalek - Verbeteren van de beveiliging - Lever nazorg aan de betrokkenen	- Hoofd ICT - PO

** 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 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 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. Bij de afweging van het risico voor de rechten en vrijheden van de betrokkenen zal altijd de Functionaris Gegevensbescherming betrokken moeten 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 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 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.

Afkortingenlijst

- PO = Privacy Officer
- FG = Functionaris Gegevensbescherming
- ICT = Informatie- en communicatietechnologie
- AP = Autoriteit Persoonsgegevens
- DB = Dagelijks Bestuur
- AB = Algemeen Bestuur
- IBP = Informatie beveiliging en Privacy
- AVG = Algemene Verordening Persoonsgegevens

Nota Bene

Het IBP-kader met toewijzing van PO, FG en andere functionarissen is nog in ontwikkeling. Dit wordt, vanwege de kleine omvang van de organisatie, in samenwerking met de schoolbesturen van de toekomstige campus gedaan (Emelwerda/Vakcollege en VariO).