# Meldcode Datalekken en Privacy Schendingen

4 april 2023 - versie 3.1

Dit is een meldcode voor gesignaleerde datalekken en schendingen van de privacy. Sinds 25 mei 2018 geldt de meldplicht datalekken uit de Algemene Verordening Gegevensbescherming (AVG). Sinds 1 januari 2016 dienen (mogelijke) datalekken en schendingen van de privacy gemeld te worden bij de Autoriteit Persoonsgegevens.

**Referentie:**

- Beleidsregels Meldplicht Datalekken.pdf, en
- https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

**Het bevoegd gezag van:**

zorgENZOO
Euroweg 5a
9351EM Leek

**Overwegende dat**

- ZorgEnzoo verantwoordelijk is voor een goede kwaliteit van de dienstverlening aan zijn cliënten en dat deze verantwoordelijkheid ook aan de orde is in geval van privacy van haar cliënten,
- Dat de privacy van de cliënten te allen tijde gewaarborgd dient te worden,
- ZorgEnzoo zich aan de bepalingen dient te houden die de Wet Bescherming Persoonsgegevens met zich mee brengt,
- Dat de Meldplicht Datalekken deel uit maakt van de Wet Bescherming Persoonsgegevens,
- Dat onder een Datalek wordt verstaan het verkrijgen van toegang of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Het gaat hierbij op een inbreuk op de beveiliging van persoonsgegevens zoals bedoeld in Artikel 13 van de Wet Bescherming Persoonsgegevens,
- Dat zorgEnzoo voor delen van haar processen gebruik maakt van externe partijen en dat deze partijen daartoe soms dienen te beschikken over privacygevoelige gegevens van cliënten van zorgEnzoo.

**In aanmerking nemende de**

- Algemene verordening gegevensbescherming
- Het privacyreglement van zorgEnzoo.

ZorgEnzoo stelt de hierna volgende Meldcode Datalekken en Privacy Schendingen vast, en maakt gebruik van een stappenplan om (potentiële) Datalekken en/of Privacy Schendingen in kaart te brengen en te melden.

# Stappenplan bij (het vermoeden van) een datalek of schending van de privacy

## Stap 1: **Is er sprake van een potentieel 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 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). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

Bij een datalek kan het gaan om eigen gegevens die onbedoeld bij derden terecht komen, maar ook om gegevens die bij zorgEnzoo aan worden gebracht. Het versturen van een email met cliëntgegevens naar een verkeerd adres is een voorbeeld van een datalek.

## Onderstaande stappen worden uitgevoerd onder regie van de directeur.

## Stap 2: **Waarschuw indien mogelijk direct de partij die onterecht de beschikking over cliënt gegevens heeft gekregen dan wel deze met zorgEnzoo heeft gedeeld.**

Indien deze actie als resultaat heeft dat er met zekerheid kan worden uitgesloten dat het datalek heeft geleid tot onrechtmatige verwerking is er geen sprake meer van een datalek.

## Stap 3: **Doe onderzoek naar het datalek.**

Het is toegestaan om enige tijd onderzoek te doen naar het datalek. Dit dient in principe niet langer dan 72 uur te duren. Uit het onderzoek kan blijken dat er geen melding gedaan hoeft te worden.

Daar waar het gaat het om persoonsgegevens van gevoelige aard, of is er om een andere reden sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte Persoonsgegevens, dient er gemeld te worden bij de Autoriteit Persoonsgegevens.

Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident moet u bijvoorbeeld denken aan het kwijtraken van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker.

Maar niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als u onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kunt uit sluiten.

Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. U hoeft dan geen melding te doen aan de Autoriteit Persoonsgegevens.

## Stap 4: **Doe een melding bij de Autoriteit Persoonsgegevens.**

Indien vastgesteld is dat er een melding gedaan dient te worden, dient deze binnen 72 uur na ontdekking digitaal gedaan te worden. Indien de melding later plaats heeft zal moeten worden gemotiveerd waarom dit het geval is. De melding moet digitaal gedaan worden op: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage

## Stap 5: **Stel vast of de betrokkene op de hoogte gesteld dienen te worden van het datalek.**

Indien een datalek is opgetreden is er niet automatisch de noodzaak om ook de betrokkene op de hoogte te stellen. Dit is alleen noodzakelijk indien het datalek grote gevolgen voor de persoonlijke levenssfeer van de betrokkene kan hebben.

## Stap 6: **Stel de betrokkene op de hoogte van het datalek.**

Indien noodzakelijk dient een persoonlijke melding aan de betrokkene plaats te vinden over de aard van het datalek, instanties waar hij of zij meer informatie kan verkrijgen en de maatregelen die de betrokkene kan nemen om de negatieve gevolgen te beperken. Ook wordt weergegeven welke maatregelen reeds door zorgENZOO zijn genomen om de gevolgen te beperken.