Meldcode Datalekken en Privacy Schendingen

ZvA-maatwerk B.V.
Vastgesteld door directie
Laatst geactualiseerd: **11 februari 2026**

---

1. Doel en reikwijdte

Deze meldcode beschrijft de interne procedure van ZvA-maatwerk B.V. bij:

- het signaleren van (mogelijke) datalekken
- het beoordelen van risico's
- het melden bij de bevoegde toezichthouder
- het informeren van betrokkenen
- het registreren en evalueren van incidenten

Deze meldcode is van toepassing op alle medewerkers, zzp'ers, stagiaires, vrijwilligers en ingehuurde derden die werkzaamheden verrichten voor of namens ZvA-maatwerk B.V.

---

2. Wettelijk kader

ZvA-maatwerk B.V. verwerkt persoonsgegevens conform:

- De **Algemene Verordening Gegevensbescherming (AVG)**
- De **Uitvoeringswet AVG (UAVG)**
- Richtlijnen van de Autoriteit Persoonsgegevens
- Contractuele afspraken met opdrachtgevers (Wmo, Jeugdwet, WLZ)

Op grond van artikel 33 en 34 AVG geldt een meldplicht bij datalekken die risico's opleveren voor betrokkenen.

---

3. Organisatiegegevens

Naam organisatie:
ZvA-maatwerk B.V.

Bezoekadres dagbesteding:
De Groene Ster 14 (Veld A)
8926 XE Leeuwarden

Rechtsgeldig vertegenwoordiger:
Aafke Feenstra – Directeur / Bestuurder

E-mailadres privacyzaken:
[invullen]

---

4. Definitie datalek (2026)

Een datalek is:

Een inbreuk op de beveiliging die per ongeluk of onrechtmatig leidt tot vernietiging, verlies, wijziging, ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

Een datalek kan zowel digitaal als fysiek plaatsvinden.

Voorbeelden:

- E-mail met persoonsgegevens verzonden naar verkeerd adres
- Verlies of diefstal van laptop/telefoon
- Onbevoegde inzage in cliëntdossier
- Hack of ransomware
- Onvoldoende afgeschermde cloudomgeving
- Dossier achtergelaten in openbare ruimte

---

5. Interne meldplicht

Iedere medewerker of samenwerkingspartner die een (mogelijk) datalek constateert, meldt dit **onmiddellijk** bij de directie.

Melding bevat minimaal:

- Datum en tijdstip constatering
- Omschrijving incident
- Soort persoonsgegevens
- Aantal betrokken personen (indien bekend)
- Reeds genomen maatregelen

Er geldt een interne meldplicht van **direct melden, uiterlijk binnen 24 uur** na constatering.

---

6. Stappenplan bij (vermoeden van) datalek

Stap 1 – Beoordeling: is er sprake van een datalek?

De directie beoordeelt:

- Is er sprake van een beveiligingsincident?
- Zijn persoonsgegevens daadwerkelijk verloren gegaan of onrechtmatig verwerkt?
- Is er een risico voor rechten en vrijheden van betrokkenen?

Indien geen persoonsgegevens zijn geraakt, wordt het incident geregistreerd als beveiligingsincident (geen meldplicht).

Stap 2 – Directe beheersmaatregelen

Zo spoedig mogelijk worden maatregelen genomen om:

- Verdere verspreiding te stoppen
- Toegang te blokkeren
- Apparatuur te beveiligen
- Onbevoegde ontvangers te verzoeken gegevens te verwijderen

Stap 3 – Risicoanalyse (binnen 72 uur)

ZvA-maatwerk beoordeelt:

- Gaat het om bijzondere persoonsgegevens (gezondheid, begeleiding, strafrecht)?
- Hoe gevoelig zijn de gegevens?
- Wat is de mogelijke impact voor betrokkenen?
- Is identiteitsfraude of reputatieschade mogelijk?

Uitkomst:

- Geen risico → geen melding bij AP, wel registratie
- Wel risico → melding bij AP
- Hoog risico → melding bij AP + informeren betrokkenen

Stap 4 – Melding bij Autoriteit Persoonsgegevens

Indien sprake is van een meldplichtig datalek, wordt dit binnen **72 uur na ontdekking** gemeld via het meldloket van de Autoriteit Persoonsgegevens.

Indien melding later plaatsvindt, wordt dit gemotiveerd.

Stap 5 – Informeren betrokkenen

Indien sprake is van een hoog risico voor de rechten en vrijheden van betrokkenen, worden zij **onverwijld geïnformeerd**.

De melding bevat:

- Aard van het datalek
- Mogelijke gevolgen
- Reeds genomen maatregelen
- Adviezen ter beperking van schade
- Contactgegevens voor nadere informatie

---

7. Registratieplicht (verantwoordingsplicht AVG)

Alle datalekken — ook niet-meldplichtige incidenten — worden geregistreerd in het interne:

Register Datalekken en Beveiligingsincidenten

Dit register bevat:

- Datum
- Omschrijving
- Risicobeoordeling
- Besluit melding ja/nee
- Eventuele melding betrokkenen
- Corrigerende maatregelen

Dit register wordt jaarlijks geëvalueerd.

---

8. Externe verwerkers

Met externe partijen (ICT, administratie, softwareleveranciers) zijn verwerkersovereenkomsten gesloten conform artikel 28 AVG.

Indien een datalek plaatsvindt bij een verwerker:

- Meldt deze het incident direct aan ZvA-maatwerk
- Blijft ZvA-maatwerk verwerkingsverantwoordelijke
- Voert ZvA-maatwerk de meldprocedure richting AP uit

---

9. Preventieve maatregelen

ZvA-maatwerk borgt privacy door:

- Beperkte autorisaties per medewerker
- Sterke wachtwoordvereisten en tweestap verificatie
- Versleutelde opslag
- Afsluitbare dossierkasten
- Clean desk beleid
- Periodieke bewustwording medewerkers
- Verwerkersovereenkomsten
- Interne audits op AVG

---

10. Evaluatie en herziening

Deze meldcode wordt:

- Jaarlijks geëvalueerd
- Aangepast bij wetswijzigingen
- Geactualiseerd bij organisatorische wijzigingen

De directie is eindverantwoordelijk voor naleving.

Vaststelling

Aldus vastgesteld door de directie van ZvA-maatwerk B.V.

Plaats: Leeuwarden
Datum: 11 februari 2026

Handtekening:

Naam: Aafke Feenstra
Functie: Directeur / Bestuurder