

Juni 2025

Protocol: Omgaan met Datalekken

Doel

Het protocol beschrijft hoe medewerkers en leidinggevenden handelen bij (vermoedens van) datalekken of schendingen van het privacybeleid. Doel is schade te beperken, transparantie te waarborgen en te voldoen aan wettelijke verplichtingen.

Stap 1. Signalering en interne melding

- **Wie:** Iedere medewerker is verplicht een (mogelijk) datalek onmiddellijk te melden.
- **Waar:** Melding bij de Functionaris Gegevensbescherming (FG)
- **Wat melden:** Aard van het lek, soort gegevens, getroffen personen, wijze van ontdekking.

Stap 2. Eerste beoordeling en containment

- **Door wie:** Functionaris Gegevensbescherming.
- **Analyse:**
 - o Wat is gelekt (bijv. naam, BSN, medische gegevens)?
 - o Hoe ernstig is het (gevoeligheid, omvang)?
 - o Wie zijn getroffen (cliënten, medewerkers, derden)?
- **Actie:** Directe maatregelen om verdere verspreiding te voorkomen.

Stap 3. Melding aan de Autoriteit Persoonsgegevens (AP)

- **Wanneer:** Als er risico is voor de rechten en vrijheden van betrokkenen.
- **Termijn:** Binnen 72 uur via autoriteitpersoonsgegevens.nl.
- **Inhoud melding:** Aard van het lek, omvang, categorieën betrokkenen, maatregelen.

Stap 4. Informeren van betrokkenen

- **Wanneer:** Bij kans op ernstige gevolgen (bijv. identiteitsfraude).
- **Hoe:** Snel, duidelijk en in begrijpelijke taal.
- **Wat:** Wat is gebeurd, gevolgen, wat kunnen zij doen, welke ondersteuning bieden wij.

Stap 5. Onderzoek

- **Doel:** Oorzaak achterhalen en impact volledig in kaart brengen.
- **Resultaat:** Rapportage met feiten, getroffen gegevens, genomen acties en aanbevelingen.
- **Opslag:** In het interne datalek-archief.

Stap 6. Herstel en preventie

- **Maatregelen:** Technische of organisatorische ingrepen om gevolgen te beperken.
- **Verbetering:** Implementatie van aanbevelingen ter voorkoming van herhaling.

Stap 7. Evaluatie en bijstelling

- **Evaluatie:** Betrokkenen bespreken proces en leerpunten.
- **Update:** Aanpassing van beleid of procedures indien nodig.

Stap 8. Documentatie

- **Archivering:** Volledige en veilige opslag van alle stukken in het interne datalek-archief.
- **Bewijsvoering:** Beschikbaar voor interne controle of toezicht door de AP.

