

Procedure Datalekken

PRV-P02

Voorbeeldorganisatie B.V.

Procedure voor het melden en afhandelen van datalekken.

MaasISO
www.maasiso.nl

Documentinformatie

Documenttitel	Procedure Datalekken
Documentnummer	PRV-P02
Versie	1.0
Datum	9 oktober 2026
Auteur	[Naam contactpersoon]
Goedgekeurd door	[Naam contactpersoon]
Organisatie	Voorbeeldorganisatie B.V.
Classificatie	Vertrouwelijk

Versiehistorie

Versie	Datum	Auteur	Wijzigingen
1.0	9 oktober 2026	[Auteur]	Initiële versie

Doel

[Clausule Art. 33-34 AVG]

Deze procedure beschrijft de wijze waarop Voorbeeldorganisatie B.V. datalekken detecteert, beoordeelt, meldt en afhandelt. Het doel is te waarborgen dat datalekken tijdig worden geïdentificeerd, dat de Autoriteit Persoonsgegevens (AP) binnen 72 uur wordt geïnformeerd wanneer dit vereist is, en dat betrokkenen worden geïnformeerd bij een hoog risico voor hun rechten en vrijheden.

Toepassingsgebied

Deze procedure is van toepassing op alle inbreuken in verband met persoonsgegevens, waaronder:

- Onbevoegde toegang tot persoonsgegevens (vertrouwelijkheidsinbreuk)
- Onbevoegde wijziging van persoonsgegevens (integriteitsinbreuk)
- Onbeschikbaarheid of verlies van persoonsgegevens (beschikbaarheidsinbreuk)
- Diefstal of verlies van apparatuur met persoonsgegevens
- Verzending van persoonsgegevens naar de verkeerde ontvanger
- Ransomware of andere cyberaanvallen die persoonsgegevens treffen
- Onbedoelde publicatie van persoonsgegevens

Definities en afkortingen

Term	Definitie
Datalek	Een inbreuk in verband met persoonsgegevens: 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 gegevens.
AP	Autoriteit Persoonsgegevens — de Nederlandse toezichthouder voor gegevensbescherming.
Betrokkene	De natuurlijke persoon van wie de persoonsgegevens zijn getroffen door het datalek.
72- uurstermijn	De wettelijke termijn waarbinnen een meldingsplichtig datalek gemeld moet worden aan de AP.

Verantwoordelijkheden

Rol	Verantwoordelijkheid
Directie	Eindverantwoordelijkheid; besluitvorming over melding aan AP en betrokkenen; communicatie naar stakeholders.
Privacycoördinator / FG	Beoordeling van het datalek; beslissing over meldingsplicht; uitvoeren van melding aan AP; coördinatie van de respons; documentatie.
IT-verantwoordelijke	Technische analyse; beperking van de inbreuk; herstelmaatregelen; forensisch onderzoek.
Proceseigenaren	Melden van potentiële datalekken; medewerking aan onderzoek; implementeren van maatregelen.
Alle medewerkers	Onmiddellijk melden van (vermoedelijke) datalekken aan de privacycoördinator.

Werkwijze

Stap 1: Detectie en interne melding

Elke medewerker die een (vermoedelijk) datalek ontdekt, meldt dit onmiddellijk aan de privacycoördinator via:

- E-mail: [privacy@organisatie.nl]
- Telefoon: [telefoonnummer privacycoördinator]
- Incidentmeldingssysteem (indien beschikbaar)

De melding bevat minimaal: wat er is gebeurd, wanneer het is ontdekt, welke gegevens zijn getroffen en welke directe maatregelen zijn genomen.

Stap 2: Beoordeling en classificatie

De privacycoördinator beoordeelt het incident binnen 24 uur op de volgende aspecten:

Beoordelingsaspect	Vraag
Aard van de inbreuk	Gaat het om vertrouwelijkheid, integriteit of beschikbaarheid?
Categorieën gegevens	Welke soorten persoonsgegevens zijn getroffen? Zijn er bijzondere categorieën bij?
Categorieën betrokkenen	Welke groepen betrokkenen zijn getroffen? Zijn er kwetsbare groepen (kinderen, patiënten)?
Aantal betrokkenen	Hoeveel personen zijn (mogelijk) getroffen?
Risico voor betrokkenen	Wat zijn de mogelijke gevolgen? (identiteitsfraude, financiële schade, reputatieschade, discriminatie)
Maatregelen	Welke maatregelen zijn reeds genomen en welke aanvullende maatregelen zijn nodig?

Stap 3: Melding aan de Autoriteit Persoonsgegevens

[Clausule Art. 33 AVG]

Het datalek wordt gemeld aan de AP indien het waarschijnlijk een risico inhoudt voor de rechten en vrijheden van betrokkenen. De melding wordt gedaan binnen 72 uur na ontdekking en bevat:

- De aard van de inbreuk, inclusief categorieën en aantallen betrokkenen en gegevens
- De naam en contactgegevens van de FG of ander contactpunt
- Een beschrijving van de waarschijnlijke gevolgen van de inbreuk
- Een beschrijving van de genomen of voorgestelde maatregelen

De melding aan de AP gebeurt via het meldloket van de Autoriteit Persoonsgegevens (<https://datalekken.autoriteitpersoonsgegevens.nl>).

Stap 4: Melding aan betrokkenen

[Clausule Art. 34 AVG]

Betrokkenen worden geïnformeerd wanneer het datalek waarschijnlijk een hoog risico inhoudt voor hun rechten en vrijheden. De melding aan betrokkenen bevat:

- Een beschrijving in duidelijke en eenvoudige taal van de aard van de inbreuk
- De contactgegevens van de FG of ander contactpunt
- Een beschrijving van de waarschijnlijke gevolgen
- Een beschrijving van de genomen maatregelen en adviezen om gevolgen te beperken

Stap 5: Herstelmaatregelen

Na de directe respons worden de volgende herstelmaatregelen genomen:

- Technisch herstel: patches, wachtwoordresets, revoke van toegangsrechten
- Oorzakenanalyse: bepalen van de grondoorzaak en bijdragende factoren
- Structurele maatregelen: aanpassing van processen, systemen of trainingen om herhaling te voorkomen
- Opvolging: verificatie dat maatregelen effectief zijn geïmplementeerd

Stap 6: Evaluatie en rapportage

Na afhandeling van het datalek wordt een evaluatie uitgevoerd:

- Was de respons tijdig en adequaat?
- Zijn de maatregelen effectief om herhaling te voorkomen?
- Moeten procedures of beleid worden aangepast?
- Rapportage aan de directie met leerpunten en aanbevelingen

Registratie

Alle datalekken worden geregistreerd in het datalekkenregister, ongeacht of melding aan de AP of betrokkenen noodzakelijk was:

Registratie	Locatie	Bewaartermijn	Verantwoordelijke
Datalekkenregister	Documentbeheersysteem	Doorlopend (minimaal 3 jaar)	Privacycoördinator
Incidentrapporten	Documentbeheersysteem	5 jaar	Privacycoördinator
Meldingen aan AP	Documentbeheersysteem	10 jaar	Privacycoördinator
Communicatie aan betrokkenen	Documentbeheersysteem	5 jaar	Privacycoördinator
Evaluatierapporten	Documentbeheersysteem	3 jaar	Privacycoördinator

Verwante documenten

- BLD-004 — Privacybeleid
- PRV-001 — Verwerkingsregister
- PRV-P01 — Procedure DPIA
- PRV-P03 — Procedure Rechten Betrokkenen
- AFW-P01 — Procedure Afwijkingen en Corrigerende Maatregelen

- Informatiebeveiligingsbeleid (indien ISO 27001 actief)