Procedure datalekken

PRV-P02

Voorbeeld IT B.V.

Hoe wij een datalek herkennen, beperken, beoordelen, melden aan de Autoriteit Persoonsgegevens en de betrokkenen, en vastleggen.

© 2026 MaasISO — licentie [Licentienummer] voor [Licentiehouder] | maasiso.nl

Voorbeeld uit de AVG Toolkit · alle 20 documenten: www.maasiso.nl/toolkits/avg/

Documentinformatie

DOCUMENTTITEL	Procedure datalekken
DOCUMENTNUMMER	PRV-P02
VERSIE	1.0
DATUM	19 oktober 2026
AUTEUR	Sanne de Vries
GOEDGEKEURD DOOR	Sanne de Vries
ORGANISATIE	Voorbeeld IT B.V.
CLASSIFICATIE	Intern

Versiehistorie

Versie	Datum	Auteur	Wijzigingen
1.0	19 oktober 2026	Sanne de Vries	Initiële versie

ART. 33 AVG · ART. 34 AVG

1. Doel

Een datalek is een inbreuk op de beveiliging waarbij persoonsgegevens verloren gaan, of onbevoegd worden ingezien, gewijzigd of verstrekt. Deze procedure zorgt dat wij een datalek snel herkennen, de schade beperken, op tijd beslissen over melden en alles vastleggen.

2. Wat is een datalek

Soort inbreuk	Voorbeelden
Vertrouwelijkheid: iemand ziet gegevens die niet voor hem bedoeld zijn	Een e-mail met gegevens naar de verkeerde ontvanger; een gestolen laptop zonder versleuteling; een aanvaller in een systeem
Integriteit: gegevens zijn onbedoeld of onbevoegd gewijzigd	Een fout in een koppeling overschrijft klantgegevens
Beschikbaarheid: gegevens zijn verloren of tijdelijk niet toegankelijk	Ransomware; een gewist bestand zonder back-up

Niet elk beveiligingsincident is een datalek. Het is een datalek zodra er persoonsgegevens bij betrokken zijn.

3. Melden binnen de organisatie

Iedereen die een (mogelijk) datalek ontdekt, meldt dat direct bij de privacycoördinator:

Gegeven	Invullen
Meldadres	privacy@voorbeeldit.nl of 030 123 45 67
Buiten kantoortijd	Bel de dienstdoende beheerder; die schakelt de privacycoördinator in
Vervanger van de privacycoördinator	Mark Jansen

Bij twijfel: melden. Wie een fout meldt, wordt daar niet op afgerekend. Laat melden is erger dan een melding te veel.

© 2026 MaasISO — licentie [Licentienummer] voor [Licentiehouder] | maasiso.nl

Voorbeeld uit de AVG Toolkit · alle 20 documenten: www.maasiso.nl/toolkits/avg/

4. Stappen

De termijn van 72 uur begint op het moment dat wij redelijkerwijs zeker weten dat er een inbreuk is.

1. **Vastleggen.** De privacycoördinator noteert datum en tijd van de ontdekking en opent een formulier (T-PRV-002 Beoordeling datalek).
2. **Beperken.** Met de IT-beheerder: toegang blokkeren, wachtwoorden vervangen, de ontvanger van een verkeerde e-mail vragen die te verwijderen en dat te bevestigen.
3. **Feiten verzamelen.** Wat is er gebeurd, welke gegevens, van hoeveel mensen, sinds wanneer, wie heeft er toegang toe gehad?
4. **Beoordelen.** Het risico voor de betrokkenen inschatten met hoofdstuk 5.
5. **Beslissen en melden.** Binnen 72 uur na ontdekking, volgens hoofdstuk 6 en 7.
6. **Vastleggen.** Elke inbreuk komt in PRV-005 Register datalekken, ook als wij niet melden.
7. **Leren.** Oorzaak vaststellen en maatregelen nemen tegen herhaling.

5. Het risico beoordelen

Wij kijken naar de gevolgen voor de mensen over wie de gegevens gaan:

Vraag	Verhoogt het risico
Welke gegevens?	Bijzondere gegevens, BSN, financiële gegevens, inloggegevens, kopie van een identiteitsbewijs
Hoeveel mensen en hoeveel gegevens per persoon?	Grote aantallen; een volledig profiel van iemand
Bij wie zijn de gegevens terechtgekomen?	Een onbekende of kwaadwillende partij
Waren de gegevens beschermd?	Niet versleuteld of anderszins leesbaar
Wat kunnen de gevolgen zijn?	Identiteitsfraude, financiële schade, discriminatie, reputatieschade, verlies van vertrouwelijkheid
Zijn de betrokkenen kwetsbaar?	Kinderen, patiënten, mensen in een afhankelijke positie

Uitkomst	Betekenis	Gevolg
Risico onwaarschijnlijk	Het is niet aannemelijk dat betrokkenen er iets van merken	Niet melden; wel registreren met onderbouwing
Risico	Betrokkenen kunnen nadeel ondervinden	Melden aan de Autoriteit Persoonsgegevens
Hoog risico	Betrokkenen kunnen ernstig nadeel ondervinden	Melden aan de Autoriteit Persoonsgegevens en de betrokkenen informeren

De privacycoördinator beslist. Bij een hoog risico of bij twijfel beslist de directie.

6. Melden aan de Autoriteit Persoonsgegevens

Wij melden via het meldloket datalekken op de website van de Autoriteit Persoonsgegevens, uiterlijk 72 uur na de ontdekking. In de melding staat:

- wat er is gebeurd;
- de soorten betrokkenen en gegevens en bij benadering de aantallen;
- de waarschijnlijke gevolgen;
- de maatregelen die wij hebben genomen of gaan nemen;
- de contactgegevens van de privacycoördinator.

© 2026 MaasISO — licentie [Licentienummer] voor [Licentiehouder] | maasiso.nl

Voorbeeld uit de AVG Toolkit · alle 20 documenten: www.maasiso.nl/toolkits/avg/

Weten wij nog niet alles, dan doen wij een voorlopige melding en vullen die later aan. Lukt melden binnen 72 uur niet, dan melden wij zo snel mogelijk en leggen wij uit waarom het later is.

7. Betrokkenen informeren

Bij een hoog risico informeren wij de betrokkenen zonder onredelijke vertraging, in duidelijke taal:

- wat er is gebeurd en welke gegevens het betreft;
- wat de mogelijke gevolgen zijn;
- wat wij hebben gedaan;
- wat zij zelf kunnen doen, bijvoorbeeld een wachtwoord wijzigen of alert zijn op nepberichten;
- bij wie zij terechtkunnen met vragen.

Informeren is niet nodig als de gegevens voor onbevoegden onleesbaar waren, bijvoorbeeld door versleuteling, of als wij het hoge risico al hebben weggenomen. Kost het onevenredig veel moeite om iedereen persoonlijk te bereiken, dan doen wij een openbare mededeling.

8. Als wij verwerker zijn

Gaat het om gegevens die wij in opdracht van een klant verwerken, dan melden wij niet zelf aan de Autoriteit Persoonsgegevens. Wij informeren de klant zonder onredelijke vertraging, uiterlijk binnen 24 uur of de kortere termijn uit de verwerkersovereenkomst. Wij geven de klant alle informatie die hij nodig heeft om zelf te kunnen melden. De klant beslist over de melding.

Meldt een van onze verwerkers een datalek aan ons, dan start deze procedure bij stap 1. De termijn van 72 uur begint zodra de verwerker ons heeft geïnformeerd.

9. Registraties

Registratie	Waar	Bewaren
Register van alle inbreuken	PRV-005 Register datalekken	drie jaar, tenzij een wet of contract een langere termijn voorschrijft
Ingevulde formulieren, meldingen en berichten aan betrokkenen	Privacymap, submap Datalekken	drie jaar, tenzij een wet of contract een langere termijn voorschrijft

10. Verwante documenten

Document	Titel
T-PRV-002	Beoordeling datalek
PRV-005	Register datalekken
PRV-P04	Procedure verwerkers en verwerkersovereenkomsten
PRV-P05	Beveiliging van persoonsgegevens
BLD-004	Privacybeleid

© 2026 MaasISO — licentie [Licentienummer] voor [Licentiehouder] | maasiso.nl

Voorbeeld uit de AVG Toolkit · alle 20 documenten: www.maasiso.nl/toolkits/avg/

VOORBEELD UIT DE TOOLKIT

Dit is 1 van de 20 documenten uit de AVG Toolkit

U hebt een echt document uit de toolkit bekeken, ingevuld voor een voorbeeldorganisatie. In de toolkit zit de volledige set, in Word en Excel, klaar om aan te passen aan uw organisatie.

Wat zit er verder in

Algemeen	4
Beleid en organisatie	3
Registers	4
Procedures	5
Formulieren	4

Prijs

- € 195 excl. btw (€ 235,95 incl. btw), eenmalig
- 12 maanden updates bij wijzigingen in de norm of wet
- 30 dagen geld terug, zonder opgaaf van reden
- Op naam van uw organisatie geleverd, direct na betaling te downloaden

Direct bestellen

Bekijk alle documenten en voorbeeldpagina's
www.maasiso.nl/toolkits/avg/

Vragen over de inhoud? Mail info@maasiso.nl.