Datalekprotocol

# 1. Inleiding

Bij een datalek is er sprake van een inbreuk op de beveiliging, die leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of ongeoorloofde toegang tot persoonsgegevens.

Datalekken kunnen ontstaan door o.a.:

**•** moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, malware besmetting)

**•** technisch falen (ICT-storingen)

**•** menselijk falen (te eenvoudige wachtwoorden/het verstrekken van username/wachtwoord aan

collega’s en externen)

**•** calamiteit (brand datacentrum, wateroverlast)

**•** verloren USB stick of laptop

**•** verzenden van e-mail met e-mailadressen van alle geadresseerden

**•** onrechtmatige verwerking van gegevens

Dit document beschrijft de wijze waarop <*naam bedrijf>* omgaat datalekken en de melding en registratie daarvan.

# 2. Stappenplan melden datalekken

Ingeval van een incident wordt aan de hand van het onderstaande stappenplan beoordeeld of er sprake is van een datalek dat gemeld moet worden aan de Autoriteit Persoonsgegevens en eventueel aan de betrokkene.

**STAP 1: PERSOONSGEGEVENS**

Zijn de gegevens die bij het incident betrokken zijn aan te merken als persoonsgegevens?

**JA:** Er is mogelijk sprake van een datalek

* *GA NAAR STAP 2*

**NEE:** Er is geen sprake van een datalek.

**STAP 2: DATALEK**

Om vast te stellen of sprake is van een datalek moeten de volgende vragen worden beantwoord:

**Stap 2A: Is er sprake van een inbreuk op de beveiliging?**

Een inbreuk op de beveiliging houdt in dat er daadwerkelijk een beveiligingsincident heeft

plaatsgevonden. Er is niet uitsluitend sprake van een dreiging, of van een tekortkoming in de

beveiliging die zou kunnen leiden tot een beveiligingsincident. Er heeft zich daadwerkelijk een beveiligingsincident voorgedaan, en de preventieve maatregelen die <*naam bedrijf>* eventueel heeft getroffen waren niet toereikend om dit te voorkomen.

**JA:** dit is een inbreuk op de beveiliging. Er kan tevens sprake zijn van een datalek

* *GA NAAR STAP 2B*

**NEE:** dit is geen datalek. Er hoeft geen melding te worden gedaan.

**Stap 2B: Zijn er persoonsgegevens verloren gegaan?**

Zijn bij het beveiligingsincident zijn de persoonsgegevens vernietigd of op een andere manier verloren gegaan en beschikt *<naam bedrijf>* niet over een complete en actuele reservekopie van de gegevens?

**JA:** dit is een datalek

* *GA NAAR STAP 3*

**NEE:** er kan toch sprake zijn van een datalek

* *GA NAAR STAP 2C*

**Stap 2C: Zijn de persoonsgegevens onrechtmatig verwerkt?**

Onder onrechtmatige vormen van verwerking vallen de aantasting van de persoonsgegevens,

onbevoegde kennisneming, wijziging, of verstrekking daarvan. Als *<naam bedrijf>* redelijkerwijs niet kan uitsluiten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid, dan

moet de inbreuk worden beschouwd als een datalek.

**JA:** dit is een datalek

* *GA NAAR STAP 3*

**NEE:** dit is geen datalek. Er hoeft geen melding te worden gedaan.

**STAP 3: MELDEN DATALEK**

**Stap 3A: Is het waarschijnlijk dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen?**

Een datalek kan resulteren in lichamelijke, materiële of immateriële schade voor natuurlijke personen, zoals verlies van controle over hun persoonsgegevens, beperking van hun rechten, discriminatie, identiteitsdiefstal, of –fraude, financiële verliezen, ongeoorloofde ongedaanmaking van pseudonomisering, reputatieschade, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens of enig ander aanzienlijk economisch of maatschappelijk nadeel.

**JA:** het datalek moet worden gemeld bij de Autoriteit Persoonsgegevens.

* *GA NAAR STAP 3B*

**NEE:** er hoeft niet te worden gemeld bij de Autoriteit Persoonsgegevens

* *GA NAAR STAP 4*

**Stap 3B: Melding aan de Autoriteit Persoonsgegevens**

* Het datalek moet zonder onredelijke vertraging gemeld bij de Autoriteit Persoonsgegevens worden, zo mogelijk niet later dan 72 uur nadat <*naam bedrijf>* er kennis van heeft genomen.
* De melding kan achteraf worden bijgewerkt of zelfs ingetrokken. Als er later dan 72 uur wordt gemeld, moet gemotiveerd worden waarom.
* Meldingen kunnen digitaal gedaan worden bij het meldloket van de Autoriteit Persoonsgegevens: [http://datalekken.autoriteitpersoonsgegevens.nl](http://datalekken.autoriteitpersoonsgegevens.nl/)
* De melding moet ten minste de volgende de volgende info bevatten:
	1. de aard van het datalek, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
	2. de contactgegevens van de functionaris bij <*naam bedrijf>* waar meer informatie kan worden verkregen;
	3. de waarschijnlijke gevolgen van het datalek;
	4. de maatregelen die *<naam bedrijf>* heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.
* Mogelijk moet er naast een melding bij de AP, ook gemeld worden aan betrokkenen:
* *Ga door naar stap 3C.*

**Stap 3C: Is het waarschijnlijk dat het datalek een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen?**

Het zal van de aard van de gegevens en de omstandigheden afhangen of ook de betrokkene op de hoogte moet worden gesteld van het datalek. Hoog risico kan bijv. het geval als bij een cyberattack usernames en wachtwoorden zijn gelekt, of als het gaat om gevoelige persoonsgegevens. *<naam bedrijf>* verwerkt voornamelijk gegevens van zakelijke relaties, zoals de persoonsgegevens van contactpersonen die bij opdrachtgevers werkzaam zijn. De verwachting is dat de risico’s voor de betrokkenen in geval van een datalek niet hoog zullen zijn en dat in de meeste gevallen dus geen melding aan betrokkenen noodzakelijk zal zijn. Uiteraard zal dit in de specifieke situatie *door <naam bedrijf>* moeten worden beoordeeld.

**JA:** het datalek moet worden medegedeeld aan de betrokkene,

* *GA NAAR STAP 3D*

**NEE:** het datalek hoeft niet te worden medegedeeld aan de betrokkene,

* *GA NAAR STAP 4*

**Stap 3D: Mededeling aan betrokkene(n)**

* Als het datalek waarschijnlijk een hoog risico inhoudt voor de betrokkene(n) moet het onverwijld worden medegedeeld aan hem/hen worden medegedeeld.
* De mededeling aan betrokkene(n) bevat een omschrijving van het datalek in duidelijke en eenvoudige taal en de volgende informatie:
1. de contactgegevens van de functionaris bij *<naam bedrijf>* waar meer informatie kan worden verkregen;
2. de waarschijnlijke gevolgen van het datalek;
3. de maatregelen die *<naam bedrijf>* heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.
* *GA NAAR STAP 4*

**Stap 4: REGISTRATIE DATALEKKEN**

Alle datalekken van persoonsgegevens moeten intern worden geregistreerd en gedocumenteerd, dus ook datalekken die niet hoeven te worden gemeld. <*naam bedrijf>* houdt een overzicht bij waarin de wordt geregistreerd:

* Wat er precies is gebeurd;
* Welke gevolgen dit had voor de betrokken personen;
* Welke maatregelen er zijn genomen om de gevolgen te stoppen of in te perken;
* Welke maatregelen er zijn genomen om dit te voorkomen in de toekomst.