Privacy Expertise Centrum

← hier het logo van jouw organisatie

Template - Datalekprotocol

Procedure behandeling datalekken

Colofon

Deze procedure verwoordt hoe [Organisatie] concreet omgaat met een datalek. Je kunt dit document gebruiken in samenhang met GB.01, Datalekken van het Toetsingskader Privacy. De procedure vloeit voort uit de standaard '*Richtlijnen omgaan met datalekken. Kaders voor een gestructureerde aanpak'* en hangt samen met het informatieveiligheidsbeleid, privacybeleid/-reglementen en hangt samen met de procedure voor incidentmanagement en het integrale crisisplan van de organisatie.

Bestemd voor

Dit document is bestemd voor privacy- en securityprofessionals van [Organisatie] .

Samenstelling en beheer

Dit template is ontwikkeld via het Privacy Expertise Centrum van SURF. Het is onderdeel van de beheercyclus.

Licentie

.

Versiebeheer

Versie	Door	Datum	Toelichting/wijziging
1.0	SURF	10-08-2026	Initieel document

Inhoudsopgave

1 Inleiding

Dit document beschrijft de procedure voor de interne aanpak van de organisatie van beveiligingsincidenten waarbij persoonsgegevens (kunnen) zijn betrokken, specifiek voor de privacy- en securityprofessionals. Dit document beschrijft de concrete invulling van de 'Richtlijnen omgaan met datalekken'.

1.1 Doelstelling

Het doel van deze procedure maken we stapsgewijs concreet hoe we volgens een gestructureerd aanpak (mogelijke) datalekken afhandelen. Zo is helder wie wat moet doen op welk moment en houden we grip op de situatie. Zo kunnen we impact/schade van een datalek voor de betrokken personen en het risico op schade voor de organisatie zelf beperken.

1.2 Scope

In de richtlijnen is uitgewerkt wat een datalek is, wie het datalek behandelt en hoe we een datalek behandelen qua volgorde en randvoorwaarden. In dit document beschrijven concreet welke stappen nodig zijn voor adequate behandeling van het datalek volgens vier vaste stappen:

a. Inhoudelijk onderzoek
b. Behandeling en melden
c. Registratie
d. Afronden en evalueren

2 Inhoudelijk onderzoek

Vaststellen of er sprake is van een datalek

De Kerngroep Datalekken bepaalt of de inbreuk op de beveiliging daadwerkelijk tot een datalek heeft geleid.

Wat is er gebeurd, de omvang en impact van het datalek bepalen

Inventarisatie van wat er is gebeurd op basis waarvan de benodigde acties kunnen worden uitgezet:

- Wat is er gebeurd?
  - wie heeft het datalek of beveiligingsincident gemeld (ontdekker)?
  - wanneer het datalek is ontdekt;
  - is het een intern of een extern datalek?
  - welke gegevens het datalek omvat (type/categorie);
  - om hoeveel betrokkenen gaat het;
  - van welke groep(en) personen zijn er gegevens gelekt;
  - hoe heeft beveiligingsincident heeft plaatsgevonden
  - beschrijving wat er met de persoonsgegevens is gebeurd;
  - welke systemen er zijn betrokken/geraakt door het beveiligingsincident?
  - Wat is er al gedaan om het op te lossen?
  - Wie zijn er al geïnformeerd?
- De mogelijke gevolgen van het datalek in kaart brengen.

- Vaststellen of de meldplicht datalekken van toepassing is (classificeren).
- Beoordelen welke vervolgacties nodig zijn, inclusief communicatie.
- Eventueel besluit tot opschaling naar CMT.

Bepalen of de meldplicht datalekken van toepassing is

Risico of geen risico objectief afwegen

De volgende factoren helpen je om de afweging objectief te maken:

1. De aard van de inbreuk (gewist, gewijzigd of gelekt).
2. De aard en gevoeligheid van de persoonsgegevens en de hoeveelheid.
3. Het gemak waarmee betrokkenen kunnen worden geïdentificeerd (hoe makkelijker te herleiden, hoe hoger het risico).
4. De ernst van de gevolgen voor de betrokkenen (financiële schade, identiteitsfraude, lichamelijk letsel, psychisch leed, reputatieschade, dus fysiek, materieel en immaterieel).
5. Kenmerken van de onbevoegde ontvanger (verkeerde collega, partijen waarmee je een zakelijke relatie hebt, wettelijk beroepsgeheim).
6. Bijzondere kenmerken van de betrokkenen.
7. Bijzondere kenmerken van onze instelling.
8. Aantal betrokkenen.
9. De aard en gevoeligheid van de persoonsgegevens en de hoeveelheid (bijzondere, strafrechtelijke of gevoelige persoonsgegevens).

Gebruik de Enisa-formule om de conclusie te onderbouwen of een melding bij de AP moet worden gedaan.

Opschaling

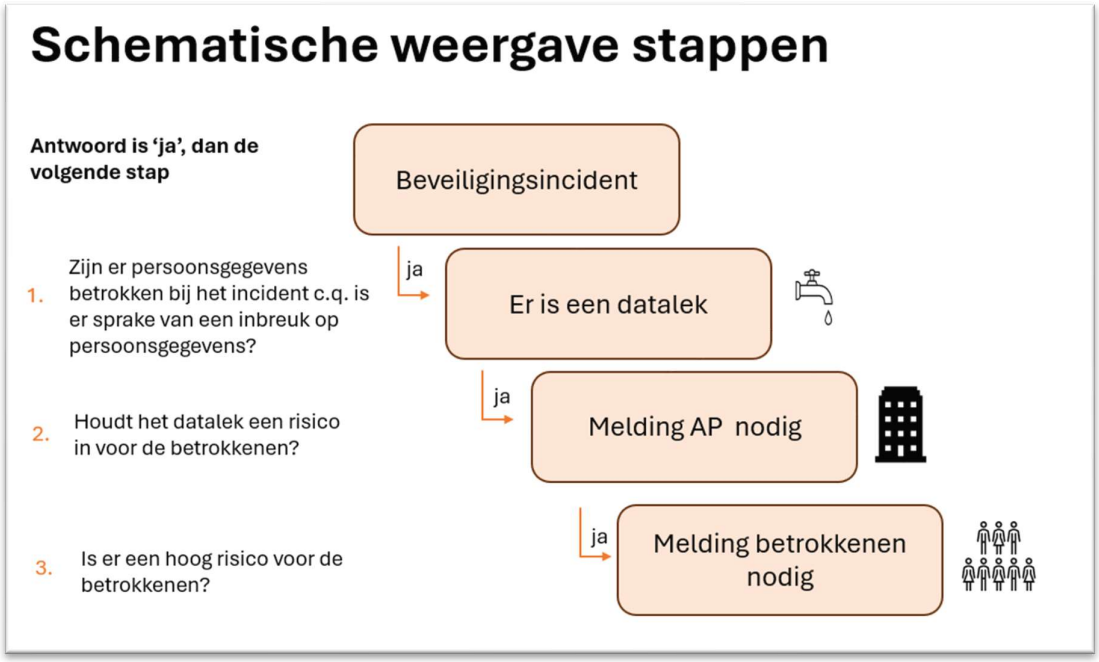
Gaat het om een (mogelijk) datalek met ernstige gevolgen of grote impact voor de betrokkenen en/of de organisatie, dan schaalt de kerngroep in overleg met het securityteam op naar het crisismanagementteam.

3 Behandeling en melden

In deze fase zet je de benodigde acties uit om de situatie op te lossen. Dit gebeurt meestal in overleg met het securityteam. Dit kan zijn van communicatie met een onjuiste ontvanger van een bestand tot het tijdelijk beperken van toegang tot een applicatie of opschaling. De behandeling omvat:

- Coördinatie met het securityteam over het nemen van (nood)maatregelen om het datalek te verhelpen en/of schade te beperken.
- Eerste registratie van het incident in het datalekregister.
- Het (laten) nemen van het besluit tot het melden van het datalek bij de AP en/of de betrokkenen (zie het 4.3, Meldplicht datalekken).
- Het daadwerkelijk melden van het datalek bij de AP en de betrokkenen.
- Afhandeling van overige (interne en externe) communicatie* rondom het datalek, zo nodig in overleg met het communicatieteam.

In schematische weergave:



Tijdig (voorlopig) melden
Als het datalek moet worden gemeld bij de AP gebeurt dit uiterlijk binnen 72 uur nadat we op de hoogte zijn van het datalek. Soms is nog niet duidelijk of het echt om een datalek gaat of dat het datalek een risico inhoudt voor de betrokkenen. In dat geval doen we binnen die 72 uur een voorlopige melding. Achteraf kun je deze sluiten of aanvullen.

De daadwerkelijke melding aan de AP verzorgt de FG. Als er melding bij de AP wordt gedaan, overweeg dan ook of de betrokkenen kunnen en/of moeten worden geïnformeerd. Het privacyteam coördineert de communicatie richting stakeholders en betrokkenen, eventueel in overleg met de afdeling die verantwoordelijk is voor communicatie.

Wettelijke verplichte informatie voor aan de betrokkene(n)
In de melding aan de betrokkene(n) is het wettelijk verplicht om de volgende informatie op te nemen (zie bijlage 1 voor een tekstvoorbeeld):

- De aard van de inbreuk (duidelijke, eenvoudige uitleg van de inbreuk).
- De waarschijnlijke gevolgen van de inbreuk voor de betrokkene(n).
- De getroffen en voorgestelde maatregelen die onze instelling heeft genomen om de gevolgen voor de betrokkene(n) te beperken.
- De acties die de betrokkene(n) zelf kan ondernemen om de gevolgen voor zichzelf te beperken, denk aan het wijzigen van een wachtwoord.
- De naam- en contactgegevens van de FG of van een ander contactpunt binnen onze organisatie waar meer informatie kan worden verkregen.

4 Registratie

Alle informatie over een datalek worden geregistreerd in het datalekregister. Die registratie omvat ten minste:

- datum van het datalek, wanneer vond het plaats;
- een korte omschrijving van het lek;
- beschrijving van wat er met de gegevens is gebeurd (ingezien, gekopieerd of gewijzigd door een onbevoegde, onbedoeld vernietigd);
- beschrijving van de groep(en) personen (en aantal) van wie de gegevens zijn ;
- beschrijving van de soort(en) persoonsgegevens;
- beschrijving van de mogelijke gevolgen zijn (zoals identiteitsfraude);
- welke maatregelen zijn genomen om schade te voorkomen of te beperken (zoals wissen op afstand, veranderen van wachtwoorden);
- of en waarom een eventueel datalek al dan niet bij de AP wordt gemeld;
- wat is gecommuniceerd en naar wie;
- welke maatregelen er worden genomen om herhaling te voorkomen (bijvoorbeeld encryptie of back-ups).

Aandachtspunten voor een goede registratie

De AP heeft een lijst gepubliceerd met aandachtspunten voor een goede registratie van datalekken.

- Omschrijf incidenten, gevolgen en corrigerende maatregelen duidelijk en volledig.
- Maak een duidelijk onderscheid tussen corrigerende en preventieve maatregelen.
- Maak één overzichtelijke registratie die altijd tot op hetzelfde inhoudelijke detailniveau wordt gevuld.
- Neem per incident op of de FG is geraadpleegd (als een FF is aangesteld).
- Neem per incident op of het datalek is gemeld bij de AP en betrokkene(n). Motiveer daarbij waarom dat wel / niet is gebeurd.
- Als er een melding is gedaan aan betrokkene(n), bewaar het bewijs van die melding en neem dit op in de registratie.
- Instrueer de personen die verantwoordelijk zijn voor het registreren van datalekken.
- Leg vast welke andere organisaties betrokken zijn geweest bij een inbreuk (zoals verwerkers of subverwerkers).
- Overweeg datalekken in te delen naar aard, gevolgen, betrokkenen en mogelijke maatregelen.
- Bespreek de datalekregistratie regelmatig met de juiste personen binnen de organisatie.

5 Afronding en evaluatie

Nadat een datalek is behandeld, volgt een evaluatie waarbij wordt gekeken of de genomen maatregelen ook in de toekomst herhaling helpen voorkomen. Na de evaluatie van het datalek wordt het datalekregister zo nodig bijgewerkt:

- Evalueren van het incident en de maatregelen die zijn of moeten worden genomen om herhaling in de toekomst te voorkomen.
- Bijwerken van het datalekregister inclusief de maatregelen die zijn genomen om de impact/schade te beperken en om herhaling te voorkomen.
- Eventueel bijstellen van de procedures, voorbeeldbrieven e.d. rondom de afhandeling van datalekken.
- Het privacyteam maakt een rapportage voor het management ter informatie.

6 Review

De inhoud van dit document wordt tweejaarlijks gecontroleerd en bijgesteld als dat nodig is. Hierbij zijn betrokken … De FG controleert jaarlijks steekproefsgewijs of de afgesproken regels worden nageleefd.

Bijlage 1 Template brief melding datalek aan betrokkene(n)

Melding datalek aan betrokkene(n)	
Inleidend bericht	Beste [naam],
Omschrijving + maatregelen + excuses	Op [DATUM] heeft er bij onze instelling een datalek plaatsgevonden waarbij uw gegevens betrokken zijn. [UITGEBREIDE OMSCHRIJVING + GETROFFEN MAATREGELEN]. We betreuren dat dit datalek heeft plaatsgevonden. Dit had natuurlijk niet moeten gebeuren. Wij bieden dan ook onze excuses aan.
Wat zijn de gevolgen voor je?	Het datalek kan voor u de volgende gevolgen hebben: [OMSCHRIJVING GEVOLGEN, WAT KAN ER GEBEUREN].
Wat kun je doen?	Om de gevolgen van dit datalek te beperken raden wij je aan om volgende te doen: [MAATREGELEN].
Vragen?	Voor vragen kun je contact opnemen met onze Privacy Officer of de Functionaris voor Gegevensbescherming, via [e-mailadres] of [telefoonnummer].

Bijlage 2 Hoe handel je als medewerker bij een datalek?

De informatie in deze bijlage is bedoeld als instructie voor de medewerker. De communicatie hiervan past binnen een awareness-plan. De training over datalekken kan omvatten wat een datalek is en wat je moet doen als je een datalek vermoedt.

Als je een datalek vermoedt

Is er per ongeluk iets gebeurd met persoonsgegevens dat niet de bedoeling was? Heb je het vermoeden dat er iets persoonsgegevens wordt gedaan op een manier die niet past of mag? Zijn persoonsgegevens (tijdelijk) niet beschikbaar? Of twijfel je of er sprake is van een datalek?

Direct melden
Meld dit direct bij ons meldpunt voor securityincidenten. Je mag het ook rechtstreeks aan iemand van ons privacyteam doorgeven. Daar wordt gekeken of er inderdaad sprake is van een datalek en weet men precies wat er moet gebeuren om het op te lossen. Ga dus altijd in overleg.

Een datalek houdt in dat er een inbreuk is op de beveiliging waarbij persoonsgegevens zijn betrokken. Een persoonsgegeven kan van alles zijn, denk aan: een naam, adres, e-mailadres, telefoonnummer maar ook foto's van studenten, een inschrijflijst voor een open dag of een lijst van studenten die recht hebben op extra tijd bij het maken van toetsen.

Wat is een datalek?
Een datalek is een inbreuk op de beveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) van persoonsgegevens, waardoor er iets misgaat met die persoonsgegevens. Dit kan leiden tot schade. Een datalek altijd ook een securityincident, vandaar dat je dit bij dat meldpunt kunt doorgeven.

Noot: neem eventueel informatie op over wat een datalek is in de instructie/awareness-training van medewerkers.