Privacy Expertise Centrum

← hier het logo van jouw organisatie

Template - Richtlijnen omgaan met datalekken

Kaders voor een gestructureerde aanpak

Colofon

Deze standaard verwoordt de richtlijnen van [Organisatie] voor de manier waarop we omgaan met datalekken. Je kunt dit document gebruiken in samenhang met GB.01, Datalekken van het Toetsingskader Privacy. De richtlijnen vloeien voort uit het privacybeleid/-reglementen en hangt samen met het informatieveiligheidsbeleid, de procedure voor incidentmanagement en het integrale crisisplan van de organisatie.

Bestemd voor

Dit document is bestemd voor medewerkers van [Organisatie] en voor leidinggevenden en privacy- en securityprofessionals in het bijzonder.

Samenstelling en beheer

Dit template is gebaseerd op de initiële versie waarvan het beheer via de MBO Raad in samenwerking met ICTRecht is overgedragen aan het Privacy Expertise Centrum van SURF. Het is onderdeel van de beheercyclus.

Licentie

Dit document is verstrekt onder de creative commons-licentie CC 4.0 nc-by-sa (niet-commercieel/naamsvermelding). SURF aanvaardt geen aansprakelijkheid voor enig gebruik/toepassing van dit document.

.

Versiebeheer

Versie	Door	Datum	Toelichting/wijziging
1.0	SURF o.b.v. MBO Raad	14-08-2024	Initieel document
1.1	SURF	17-05-2025	Sjabloon (SURF-template)
1.2	SURF	10-08-2026	Richtlijn (standaard) en procedure uit elkaar getrokken voor passende invulling beleidspiramide

Inhoudsopgave

1 Inleiding

Dit document beschrijft de richtlijnen voor de interne aanpak van de organisatie van beveiligingsincidenten waarbij persoonsgegevens (kunnen) zijn betrokken. Hierbij wordt rekening gehouden met de bevoegdheden zoals die in overkoepelend beleid is uitgewerkt.

1.1 Doelstelling

Het doel van deze richtlijn is het gestructureerd omgaan met en afhandelen van (mogelijke) datalekken. Met die aanpak kan de impact/schade van een datalek voor de betrokken personen en het risico op schade voor de organisatie zelf worden beperkt.

1.2 Reikwijdte/scope

Dit document is richtlijn voor de behandeling van datalekken binnen de organisatie door de privacyprofessionals binnen de organisatie. De inhoudelijke concrete werkwijze voor de interne afhandeling, is uitgewerkt in het datalekprotocol (inclusief de voorwaarden voor het datalekregister).

In dit document beschrijven we de kaders voor de behandeling van het datalek, inclusief:

- Wat is een datalek?
- Wie behandelt een datalek?
- Hoe behandelen we een datalek? Het gaat hier om de interne aanpak rondom de behandeling: het inhoudelijke onderzoek en de benodigde acties.
- De randvoorwaarden aan de afhandeling. Het gaat hier om het tijdig melden aan de AP, passende, heldere communicatie met de betrokkenen, correcte registratie (datalekregister) en evaluatie om herhaling te voorkomen.

2 Wat is een datalek?

De formele definitie volgens artikel 4, lid 12 AVG is “*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*.”

Een datalek is daarmee een inbreuk op de beveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) van persoonsgegevens. Het is dus altijd een securityincident. Dat betekent dat het securityteam en het privacyteam moeten samenwerken bij de afhandeling.

Noot: Een onrechtmatige verwerking is een verwerking die niet voldoet aan de regels van de AVG, zonder dat er sprake van een securityincident hoeft te zijn. Een onrechtmatige verwerking kan een datalek zijn, maar is dat niet per definitie. Ook fouten in de beveiliging zijn niet per definitie een datalek.

BIV - informatiebeveiliging

Een datalek ontstaat door een probleem met Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) voor de bescherming van gegevens, zoals dit centraal staat binnen het vakgebied informatiebeveiliging:

- **Inbreuk op de beschikbaarheid**

Er is onbedoeld geen toegang tot persoonsgegevens, terwijl dat wel nodig is. Denk aan de onbedoelde vernietiging van persoonsgegevens (bijvoorbeeld bij gijzelingssoftware).

- **Inbreuk op de integriteit**

De juistheid van de persoonsgegevens is in het geding, bijvoorbeeld door een onbevoegde of onbedoelde wijziging van deze persoonsgegevens (zoals het aanpassen van examencijfers)

- **Inbreuk op de vertrouwelijkheid**

Er is sprake van onbevoegde inzage in persoonsgegevens of een onbedoelde openbaring van of toegang tot persoonsgegevens (bijvoorbeeld door het versturen van die persoonsgegevens naar een verkeerde ontvanger).

Een datalek kan ook een combinatie van deze soorten inbreuken omvatten.

Mogelijke gevolgen van een datalek

Een datalek kan vervelende gevolgen hebben voor betrokkene(n). Je bent daarom als verwerkingsverantwoordelijke verplicht een datalek te melden aan de AP, behalve als het onwaarschijnlijk is dat het datalek tot een risico voor de rechten en vrijheden van betrokkene(n) leidt. Wanneer een datalek waarschijnlijk een hoog risico inhoudt voor betrokkene(n), moet ook een melding aan betrokkene(n) worden gedaan.

Voorbeelden van negatieve gevolgen voor betrokkene(n) zijn:

- Het verlies van controle over hun persoonsgegevens;
- Het niet uit kunnen oefenen van rechten (recht op inzage, verwijdering of rectificatie);
- Discriminatie, identiteitsdiefstal of -fraude;
- Financiële verliezen door herstelkosten;
- Angst, spanning, verdriet.

3 Wie behandelt een datalek?

De Kerngroep Datalekken handelt als uitvoeringsteam datalekken af. Dit gebeurt in samenwerking met (de kerngroep van) het securityteam volgens de procedures rondom incidentmanagement. Omdat er bij een datalek altijd sprake is van een securityincident, lopen er twee sporen die om verschillende expertise vragen en die afstemming vereist.

De Kerngroep werkt ***reactief*** aan het correct afhandelen van datalekken en werkt niet ***preventief*** aan de verhoging van de informatiebeveiliging of het beveiligingsbewustzijn.

De leden van de Kerngroep Datalekken zijn bevoegd om alle informatie op te vragen en in te zien die mogelijk samenhangen met het geconstateerde datalek. De Kerngroep Datalekken mag (nood)maatregelen afdwingen en nemen om het datalek te stoppen en/of schade als gevolg van een datalek te beperken.

Een melding van een securityincident gaat normaal gesproken naar het securityteam (het kan ook andersom). Dat team betrekt de Kerngroep Datalekken als er (mogelijk) persoonsgegevens bij het incident zijn betrokken. Waar mogelijk handelt de kerngroep de melding van een (mogelijk) datalek zelfstandig af en werkt daarbij samen met het securityteam dat het beveiligingsincident afhandelt. De Privacy Officer verzorgt de coördinatie en afhandeling van een datalek.

Samenstelling Kerngroep Datalekken

De volgende disciplines/functionarissen zijn vast vertegenwoordigd in de kerngroep:

- de ICT-manager
- de Privacy Officer
- de Functionaris Gegevensbescherming (FG)
- andere medewerkers die ter zake kennis heeft, zoals de (Information) Security Officer
- op ad hoc-basis kan de kerngroep besluiten collega's uit andere disciplines te laten deelnemen (zoals communicatie, HR, etc.).

Van eventuele overleggen wordt een verslag opgemaakt met een actie- en besluitenlijst.

Opschaling

Als er sprake is van een (mogelijk) datalek met (potentieel) ernstige gevolgen of grote impact (financieel, imago, of anders), schaalt de kerngroep in overleg met het securityteam op naar het crisismanagementteam. Bij opschaling blijft de Privacy Officer en/of de FG vanuit de Kerngroep Datalekken betrokken bij de afhandeling van het datalek, volgens het integraal crisisplan.

4 Hoe behandelen we een datalek?

We volgen vier vaste stappen voor de behandeling van een datalek:

1. Inhoudelijk onderzoek:
    a. Vaststellen of het daadwerkelijk om een datalek gaat.
    b. Wat is er gebeurd, omvang en mogelijke impact.
    c. Bepalen of de meldplicht datalekken van toepassing is.
    d. Welke acties zijn nodig.
2. Behandeling en melden:
    a. Benodigde acties uitzetten om de situatie op te lossen en de schade te beperken, inclusief eventueel melden en communicatie.
3. Registratie
4. Afhandeling en afronding van het datalek.

De Privacy Officer coördineert de behandeling van datalekken vanuit de kerngroep en zorgt voor bijvoorbeeld – in afstemming met de kerngroep – het inhoudelijke onderzoek, het vastleggen van de afhandeling (documenteren), coördinatie van communicatie intern/extern en het voorstellen van verbeteringsmaatregelen. De FG adviseert en verzorgt eventuele communicatie en correspondentie met de AP.

4.1 Inhoudelijk onderzoek

Het inhoudelijk onderzoek richt zich op het verzamelen van informatie die nodig is om te bepalen welke acties nodig zijn. Het omvat:

- Inhoudelijk onderzoek:
  - vaststellen of het beveiligingsincident zich kwalificeert als een datalek in de zin van de AVG (identificeren). Gaat het om een datalek?
  - wat er is gebeurd, de aard en omvang van het datalek bepalen (zie datalekprotocol)
  - de mogelijke gevolgen van het datalek.
- Vaststellen of de meldplicht datalekken van toepassing is (classificeren).
- Eventueel besluit tot opschaling naar CMT.

Op basis van de uitkomsten kunnen de benodigde acties worden uitgezet. Voor een uitgebreide instructie, zie het datalekprotocol met alle concrete stappen.

4.2 Benodigde acties/behandeling datalek

Op basis van het inhoudelijk onderzoek worden de vervolgacties uitgezet. In datalekprotocol is dit inhoudelijk uitgewerkt.

Als zich bij een door [Organisatie] ingeschakelde verwerker een datalek voordoet, worden de afspraken gevolgd die zijn vastgelegd in de verwerkersovereenkomst die met die verwerker is afgesloten.

4.3 Meldplicht datalekken

Onder de Algemene Verordening Gegevensbescherming (AVG) is de ‘Meldplicht datalekken’ van toepassing (artikel 32 en 33). Hierin is vervat in welke gevallen organisaties een datalek moeten melden. De meldplicht betekent dat sommige datalekken aan de Autoriteit Persoonsgegevens (hierna: AP) moeten worden gerapporteerd en in sommige gevallen aan de betrokkenen.

1. Melden aan de AP – verplicht, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de betrokkenen. Om dit te bepalen wordt een vaste werkwijze gevolgd, zodat de conclusie beredeneerd is.
2. Melden aan de betrokkenen – verplicht als het datalek een hoog risico oplevert voor de betrokkenen, tenzij bepaalde maatregelen dat risico wegnemen (denk hierbij aan versleuteling van gegevens als preventieve maatregel of het op afstand wissen van een verloren laptop als reactieve maatregel). Bij onze organisatie geldt dat we altijd overwegen de betrokkenen te informeren als er een melding bij de AP wordt gedaan.
   Een datalek moet altijd aan betrokken worden gemeld als persoonsgegevens van gevoelige of bijzondere aard zijn gelegd (medisch of financieel), of als het gaat om grote hoeveelheden persoonsgegevens.

De verwerkingsverantwoordelijke (onze organisatie) beslist over het al dan niet melden van datalekken. In onze organisatie neemt de [de CIO/het bestuur] de uiteindelijke beslissing. Als de meldplicht voor het datalek van toepassing is, adviseert de FG de organisatie over het al dan niet melden bij de AP en/of de betrokkenen. De (eventuele) melding zelf kan door de FG of de PO worden gedaan of iemand anders die hiervoor is gemandateerd, maar de beslissing wordt niet door hen genomen.

De beslissing om al dan niet te melden, wordt gemotiveerd en gedocumenteerd. Bij het afwijken van het advies van de FG adviseert, zorgt degene die de beslissing neemt voor een verantwoording van die beslissing.

5 Randvoorwaarden afhandeling datalek

Om een zorgvuldige afhandeling te borgen, zijn er een aantal randvoorwaarden aan de afhandeling van een datalek:

1. Tijdige melding bij de AP
2. Passende, heldere communicatie met de betrokkene
3. Correcte registratie
4. Evaluatie om herhaling te voorkomen

5.1 Tijdig melden AP

Als het besluit is om het datalek te melden, gebeurt dit uiterlijk binnen 72 uur nadat we op de hoogte zijn van het datalek.

Als een datalek een hoog risico voor de rechten en vrijheden van de medewerker inhoudt, stelt [Organisatie] de betrokkenen zo snel mogelijk op de hoogte van de inbreuk, in duidelijke en eenvoudige taal. Deze mededeling is niet vereist wanneer:

- de persoonsgegevens zijn versleuteld en niet toegankelijk zijn voor derden;
- er inmiddels maatregelen getroffen zijn die het hoge risico hebben weggenomen;
- de mededeling een onevenredige inspanning vergt. Een openbare mededeling kan dan volstaan.

5.2 Passende, heldere communicatie met de betrokkenen

Binnen onze organisatie willen we zowel aan interne als externe betrokken transparant en open communiceren over beveiligingsincidenten en datalekken. [Organisatie] communiceert zo transparant mogelijk over datalekken; afhankelijk van de aard van het datalek informeren we de betrokkenen over de situatie en de afhandeling (ook) als het datalek geen hoog risico inhoudt. Een voorwaarde is dat de betrokkene snapt welke gevolgen het datalek kan hebben en krijgt een handelingsperspectief.

5.3 Correcte registratie

[Organisatie] registreert ieder datalek, ongeacht of deze wordt gemeld bij de Autoriteit Persoonsgegevens. Daarnaast documenteert [Organisatie] de feiten over de inbreuk, de gevolgen van de inbreuk en de corrigerende maatregelen die zijn genomen. Dit gebeurt via een registratie in het datalekregister. Bij de evaluatie van het datalek wordt het datalekregister zo nodig bijgewerkt.

5.4 Evaluatie om herhaling te voorkomen

Na het afhandelen van een datalek volgt een evaluatie met rapportage.

6 Controle en evaluatie

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.