Samen aanjagen van vernieuwing

Procedure datalekken

Template

Auteur(s): Naam auteur(s)

Versie: Versienummer
Datum: Kies of typ een datum
Kenmerk: Omschrijving

Documentinformatie

Dit document maakt onderdeel uit van een complete set (beleidspiramide) met formeel vastgestelde documenten op strategisch, tactisch en operationeel niveau. Dit document heeft betrekking op de laag Procedure in de beleidspiramide.

Versiebeheer

Versie	Datum	Auteur	Verwerking

Distributielijst

Versie	Datum	Ontvanger	Doel

Vaststelling

Versie	Datum	Vastgesteld door	Vastgesteld op

Samenhang met andere documenten

Naam	Bovenliggend	Gelijk niveau	Onderliggend
[INFORMATIEBEVEILIGINGSBELEID]	x		
[PRIVACYBELEID]	x		

Verwijzingen naar SURFaudit Toetsingskader Privacy

Kader	Verwijzing (tags)
SURFaudit Toetsingskader	GB.01, GB.02
…	

Creative Commons

Inhoudsopgave

Samenvatting

Hier komt een samenvatting, op zichzelf leesbaar, van de inhoud van dit document in max. 1 A4.

1 Inleiding

In deze procedure voor datalekken wordt beschreven hoe onze instelling omgaat met datalekken en is bedoeld voor alle medewerkers, inclusief de Privacy Officer ('PO') en, indien aangesteld, de Functionaris Gegevensbescherming ('FG').

Je leest in deze procedure welke stappen er gevolgd moeten worden bij een (mogelijk) datalek.

- Stap 1 t/m 3 zijn voor alle medewerkers van toepassing (incl. bijlagen).
- Stap 4 en 5 zijn specifiek voor de PO / FG van onze instelling (incl. bijlagen).

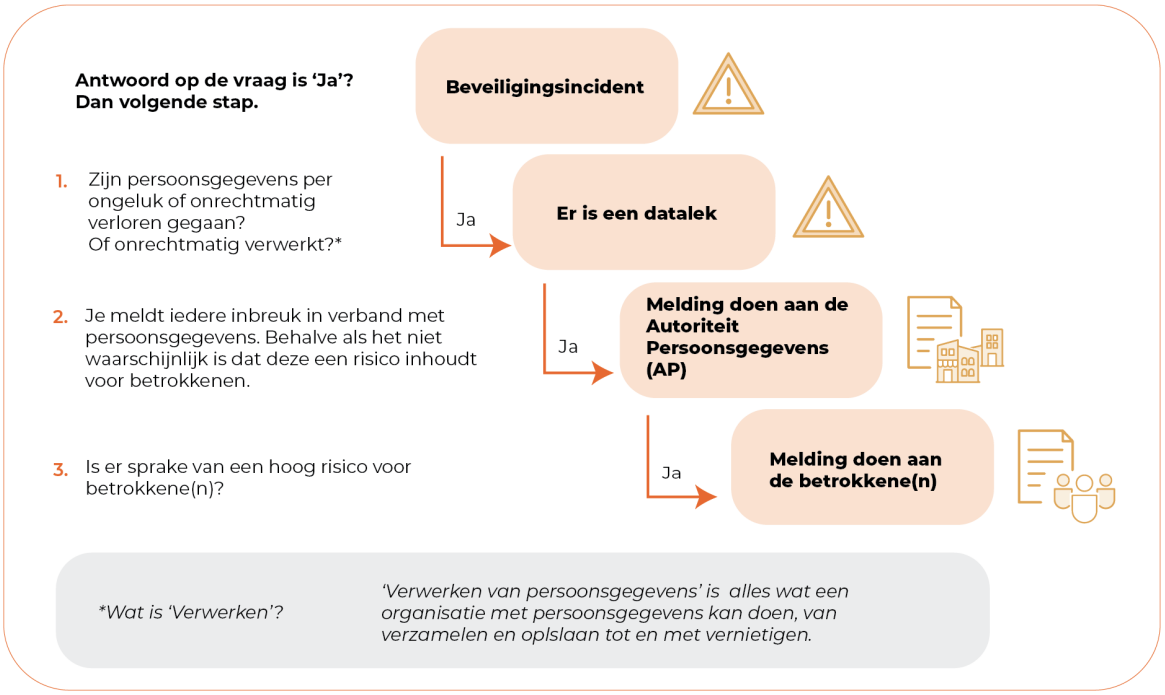
1.1 Melden?

Wie beslist of en wanneer een (mogelijk) datalek moet worden gemeld?

De verwerkingsverantwoordelijke, namelijk 'onze instelling', beslist dit. De beslissing wordt dus door ons bestuur / directie genomen. De FG adviseert. De feitelijke melding kan worden uitgevoerd door de PO / FG of iemand anders die hiervoor is gemandateerd.

1.2 Schematisch weergave stappenplan

Schematische weergave te nemen stappen van dit calamiteitenplan datalekken.



2 Stappenplan bij (mogelijk) datalek

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

Meld dit direct bij onze PO / FG.

- Naam: [persoonlijke naam of functienaam]
- E-mailadres: [persoonlijke mailadres of gedeeld mailadres]
- Telefoonnummer: [persoonlijk telefoonnummer of gedeeld telefoonnummer]

2.1 Belangrijke punten als je een datalek vermoedt

In de Algemene verordening gegevensbescherming ('AVG') staat dat datalekken verplicht intern geregistreerd moeten worden. Daarnaast dienen datalekken, in sommige gevallen, te worden gemeld bij de Autoriteit Persoonsgegevens ('AP') en de betrokkenen. Voor deze melding bij de AP heeft onze instelling vanaf het moment van ontdekking **72 uur** de tijd. Betrokkenen dienen zo snel mogelijk te worden geïnformeerd. Deze termijn loopt ook door buiten werktijd.

Belangrijke punten als je een datalek ontdekt:	
Als medewerker is het belangrijk dat je een melding maakt van een vermoedelijk datalek bij de PO/FG.	De PO/FG zal beoordelen of daadwerkelijk sprake is van een datalek.
In sommige gevallen is het verplicht om het datalek te melden aan de toezichthouder en soms aan de betrokkene(n) (dat is de persoon op wie de gegevens die gelekt zijn betrekking hebben).	Alle datalekken moet geregistreerd worden binnen onze instelling.
In Nederland is de Autoriteit Persoonsgegevens ('AP') die toezichthouder.	

2.2 Stap 1: Is er een datalek?

Voor wie: alle medewerkers van onze instelling.

Een datalek houdt in dat er een inbreuk is op de beveiliging waarbij persoonsgegevens zijn betrokken. Een datalek kan meerdere oorzaken hebben, bijvoorbeeld wanneer persoonsgegevens onbedoeld of onrechtmatig worden gedeeld, vernietigd of (tijdelijk) niet beschikbaar zijn. Maar ook als personen toegang hebben tot de persoonsgegevens, terwijl ze geen toegang zouden moeten hebben.

- 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.

2.3 Stap 2: Wat moet je doen als (je denkt dat) er sprake is van een datalek?

Voor wie: alle medewerkers van onze instelling.

Het eerste wat je moet doen is: **direct een melding maken bij de PO / FG van onze instelling**. Ook bij de geringste vorm van twijfel! De PO / FG is bereikbaar via de contactgegevens vermeld eerder in dit hoofdstuk.

2.4 Stap 3: Inventariseren en beoordelen

Voor wie: alle medewerkers van onze instelling.

Het vermoedelijke datalek moet geïnventariseerd en beoordeeld worden, want de PO / FG moet voldoende informatie ontvangen.

2.5 Stap 4: Moet het datalek bij de AP worden gemeld?

Voor wie: de PO / FG en het bestuur van onze instelling.

Bij deze stap dient altijd de FG te worden geïnformeerd en geraadpleegd. De PO / FG dient te bepalen of het bestuur altijd, soms of achteraf wordt geïnformeerd.

Een datalek moet gemeld worden bij de AP wanneer er sprake is van een risico voor de rechten en vrijheden van betrokkenen. Bij het beoordelen hiervan wegen veel factoren mee. Een opsomming hiervan staat in Bijlage 4. Brengt een datalek inderdaad een risico voor de rechten en vrijheden van betrokkenen met zich mee? Dan moet de PO / FG het datalek melden bij de AP.

2.6 Stap 5: Moet het datalek aan betrokkene(n) worden gemeld?

Voor wie: de PO / FG en het bestuur van onze instelling.

Een datalek moet gemeld worden aan de betrokkene(n) wanneer het datalek voor hen een hoog risico inhoudt.

2.6.1 Wettelijke verplichte informatie voor aan de betrokkene(n)

In de melding aan de betrokkene(n) is het wettelijk verplicht om de onderstaande informatie op te nemen.

- De aard van de inbreuk (duidelijke, eenvoudige uitleg van het datalek).
- De waarschijnlijke gevolgen van het datalek 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 PO / FG of een ander privacy-contactpunt binnen onze instelling.

In Bijlage 5 tref je een template aan die gebruikt kan worden voor deze melding.

2.7 Stap 6: Registreer het datalek in het datalekregister

Voor wie: PO / FG van onze instelling

Als de PO / FG heeft vastgesteld dat er sprake is van een datalek, dan met dit datalek geregistreerd worden in het datalekregister.

Alle datalekken moeten worden geregistreerd, ook datalekken die niet aan de AP zijn gemeld. In Bijlage 6 kun je meer lezen over welke vorm een melding in het datalekregister moet hebben.

Bijlage 1 Checklist

Wat moet je doen als (je denkt dat) er sprake is van een datalek?	
☐	De ontdekker van het vermoedelijke datalek zorgt ervoor dat de in **Bijlage 3** genoemde informatie zo snel als mogelijk wordt doorgegeven aan de PO / FG.

Inventariseren en beoordelen	
☐	De ontdekker vult **Bijlage 3** in en stuurt deze naar de PO / FG. Het kan zijn dat de informatie / vragen in deze bijlage niet afdoende zijn. Als dit zo is dan zal treedt de PO / FG met de ontdekker van het incident in contact en/of met andere personen of afdelingen die meer informatie kunnen verstrekken.
☐	De PO / FG beoordeelt of er sprake is van een datalek.

Moet het datalek bij de AP worden gemeld?	
☐	De PO / FG vult **Bijlage 4** in, zodat de afweging gemaakt kan worden.
☐	De PO / FG overweegt of het bestuur / directie op de hoogte gebracht moet worden.
☐	De PO / FG gaat in overleg met het bestuur / directie. Deze beslist op basis van het advies en bevindingen van de PO /FG of er een melding gemaakt wordt (of niet).
☐	De PO / FG meldt het datalek via het formulier op de website van de AP.
☐	Binnen 72 na ontdekking van het datalek maakt de PO / FG hier melding van.

Moet het datalek aan betrokkene(n) worden gemeld?	
☐	De PO / FG beoordeelt aan de hand van **Bijlage 4** of er een hoog risico bestaat.
☐	Het datalek heeft een hoog risico en moet worden gemeld aan de betrokkene(n).
☐	De PO / FG beoordeelt of de afdeling communicatie getrokken moet worden bij de melding. Voor de melding kan gebruik gemaakt worden van de template in **Bijlage 5**.
☐	Het datalek is gemeld aan de betrokkene(n).

Registreer het datalek in het datalekregister	
☐	De PO / FG heeft vastgesteld dat er een datalek is.
☐	De PO / FG heeft het datalek geregistreerd in het datalekregister.

Bijlage 2 Achtergrondinformatie

2.1 Wat is een datalek?

We spreken van een 'datalek' als er een inbreuk op de beveiliging heeft plaatsgevonden. Het gaat er hierbij om dat deze inbreuk ertoe leidt dat persoonsgegevens onbedoeld of onrechtmatig …

- … worden vernietigd
- … (tijdelijk) verloren gaan (niet beschikbaar zijn)
- … worden gewijzigd
- … worden verstrekt of ingezien

Zodra aan personen persoonsgegevens worden verstrekt die deze niet hadden moeten krijgen, dan die persoonsgegevens onbedoeld verstrekt of ingezien. Het kan ook zijn dat een persoon toegang heeft gekregen terwijl die geen toegang had mogen hebben tot de persoonsgegevens.

Let op: het is de verantwoordelijkheid van de verwerkingsverantwoordelijke om een datalek te melden bij de AP en eventueel bij betrokkene(n). Het is aan de PO / FG om te beoordelen of onze instelling verwerkingsverantwoordelijke of verwerker is.

- Onze instelling zal voor het gebruik van gegevens van studenten en medewerkers in het algemeen verwerkingsverantwoordelijke zijn.
- Treedt onze instelling slechts op als verwerker, dan moet de kennisname van een (mogelijk) datalek zo snel mogelijk naar de verwerkingsverantwoordelijke worden doorgezet. Dit is alleen het geval indien onze instelling gegevensverwerkingen verricht in opdracht van, en voor, een andere organisatie. Onze instelling zou in dat geval worden ingeschakeld door een andere organisatie om (een deel van) de gegevensverwerking uit te voeren. Deze situatie is vooralsnog niet aan de orde, laat dit en de eventuele gevolgen, dus altijd door de PO / FG beoordelen.

2.2 Soorten datalekken

We onderkennen drie soorten datalekken:

- **Inbreuk op de vertrouwelijkheid**
  Er is sprake van onbevoegde inzage in persoonsgegevens of een onbedoelde openbaring van of toegang tot persoonsgegevens.

- **Inbreuk op de integriteit**
  De juistheid van de persoonsgegevens is in het geding, bijvoorbeeld door een onbevoegde of onbedoelde wijziging van deze persoonsgegevens.

- **Inbreuk op de beschikbaarheid**
  Er is onbedoeld geen toegang tot persoonsgegevens, terwijl dat wel nodig is. Denk aan de onbedoelde vernietiging van persoonsgegevens.

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

2.3 Mogelijke gevolgen van een datalek

Een datalek kan vervelende gevolgen hebben voor betrokkene(n). Het kan leiden tot materiële en immateriële schade. Daarom is in de AVG vastgelegd dat de verwerkingsverantwoordelijke verplicht is een datalek te melden aan de AP, behalve als het onwaarschijnlijk is dat het datalek zal leiden tot een risico voor de rechten en vrijheden van betrokkene(n). 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 verwijdering of rectificatie).
- Discriminatie, identiteitsdiefstal of -fraude.
- Financiële verliezen.
- Ongedaan maken van pseudonimisering en reputatieschade.

Bijlage 3 Inventariseren

In het geval van een datalek dient de ontdekker hiervan, dan wel de PO / FG, de onderstaande vragen te beantwoorden.

1. Wie heeft het datalek of beveiligingsincident gemeld (ontdekker)?
2. Wat is er gebeurd?
3. Wanneer heeft het beveiligingsincident plaatsgevonden?
4. Wanneer is het beveiligingsincident ontdekt?
5. Hoe heeft het beveiligingsincident plaatsgevonden?
6. Om welke gegevens gaat het?
7. Om hoeveel en welke betrokkenen gaat het?
8. Welke systemen zijn betrokken bij of geraakt door het beveiligingsincident?
9. Wat is er gedaan om het beveiligingsincident op te lossen en in de toekomst te voorkomen?

Bijlage 4 Beoordelen

Als er sprake is van een datalek en er moet beoordeeld worden of het datalek aan de AP en/of de betrokkene(n) gemeld moet worden, dan moet de PO / FG de onderstaande vragen beantwoorden.

1. Wat is er precies gebeurd (is er sprake van een intern of extern datalek)?
2. Welke gegevens zijn betrokken bij het datalek?
3. Waarom is het wel / geen datalek dat gemeld moet worden?
4. Wat zijn de (mogelijke) gevolgen van het datalek?
5. Wie zijn er al geïnformeerd?
6. Wat zijn de te nemen vervolgstappen (melding aan de AP en/of betrokkene(n))?

4.1 Wanneer melden aan betrokkenen?

Een datalek moet worden gemeld bij de AP, tenzij het **niet waarschijnlijk is** dat het datalek een risico oplevert voor 'de rechten en vrijheden van betrokkenen'. De betrokkenen moeten worden geïnformeerd als een datalek **waarschijnlijk een hoog risico** voor hen oplevert. Als beschermingsmaatregelen zijn getroffen (preventief of reactief), waardoor het risico is weggenomen, dan hoeft het datalek niet aan betrokkenen te worden gemeld. Denk hierbij aan versleuteling van gegevens als preventieve maatregel of het op afstand wissen van een verloren laptop als reactieve maatregel.

Altijd melden aan betrokkenen

Een datalek moet altijd aan betrokken worden gemeld als persoonsgegevesn van gevoelige of bijzondere aard zijn gelegd (medisch of financieel), of als het gaat om grote hoeveelheden persoonsgegevens.

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 (vuistregel: 50 of meer).
9. De aard en gevoeligheid van de persoonsgegevens en de hoeveelheid (bijzondere, strafrechtelijke of gevoelige persoonsgegevens).

Bijlage 5 Template 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 u?	Het datalek kan voor u de volgende gevolgen hebben: [OMSCHRIJVING GEVOLGEN].
Wat kunt u doen?	Om de gevolgen van dit datalek te beperken raden wij u aan om de volgende maatregelen te treffen: [MAATREGELEN].
Vragen?	Voor vragen kunt u contact opnemen met onze Privacy Officer/Functionaris Gegevensbescherming, via [e-mailadres] of [telefoonnummer].

Bijlage 6 Het datalekregister

Alle informatie rondom het datalek moet geregistreerd worden In het register. Waaronder de relevante feiten omtrent het datalek, de gevolgen daarvan en de genomen corrigerende maatregelen. Het is niet verplicht om de redenen achter het wel of niet melden aan de toezichthouder te documenteren. Het is verstandig dit toch te doen in geval het datalek niet wordt gemeld, maar het besluit wel gemotiveerd moet worden.

6.1 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 detailsniveau wordt gevuld.
- Neem per incident op of de FG is geraadpleegd (als een Fg 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.