**Procedure meldplicht datalekken de HBM**

***Versiebeheer***

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Omschrijving** | **Auteur(s)** |
| 0.1 | 24 mei 2019 | Concept | Alies Monterie |
| 0.2 | 27 juni 2019 | Concept ter review | Alies Monterie |
| 0.3 | 24 maart 2023 | Herziene versie 2022-2023 | Functionaris Gegevensbescherming (FG) |

**Contactpersonen**

|  |  |  |
| --- | --- | --- |
| **Functie** | **Naam** | **Contactinformatie** |
| Functionaris Gegevensbescherming | Stan van Riemsdijk | Telefoon: 020 663 1941  [scholen@ictrecht.nl](mailto:scholen@ictrecht.nl) |

**Inhoudsopgave**

[Inleiding 3](#_Toc12364013)

[DEEL I: Wat is een datalek? 4](#_Toc12364014)

[1.1 Is er sprake van een beveiligingsincident? 4](#_Toc12364015)

[1.2 Is er sprake van een datalek? 4](#_Toc12364016)

[1.2.1 Een beveiligingsincident met persoonsgegevens 5](#_Toc12364017)

[1.2.2 Onrechtmatige verwerking? 5](#_Toc12364018)

[2 Wanneer melden aan de AP? 7](#_Toc12364019)

[2.1 Voldoende ernstig? 7](#_Toc12364020)

[2.1.1 Kwantitatief ernstig (aantal getroffen betrokkenen/gegevens) 7](#_Toc12364021)

[2.1.2 Kwalitatief ernstig (gevoeligheid van de gegevens) 7](#_Toc12364022)

[2.2 Termijn melden AP 8](#_Toc12364023)

[2.3 Waar te melden? 8](#_Toc12364024)

[3 Wanneer melden aan de betrokkenen? 9](#_Toc12364025)

[3.1 Hoog risico 9](#_Toc12364026)

[3.2 Uitzonderingen 10](#_Toc12364027)

[3.3 Termijn 11](#_Toc12364028)

[3.4 Wat te melden aan de betrokkenen? 11](#_Toc12364029)

[4 DEEL II: Intern proces melden van een beveiligingsincident/datalek 12](#_Toc12364030)

[4.1 Intern proces 12](#_Toc12364031)

[4.2 Registratieplicht (datalekregister) 12](#_Toc12364032)

# Inleiding

In Nederlandse wetgeving is sinds 1 januari 2016 een wettelijke meldplicht voor datalekken opgenomen. Deze meldplicht houdt in dat datalekken gemeld dienen te worden bij de toezichthouder (de Autoriteit Persoonsgegevens), en in sommige gevallen ook bij de betrokkenen (de personen op wie de gelekte gegevens betrekking hebben; bijvoorbeeld leerlingen of medewerkers van de HBM).

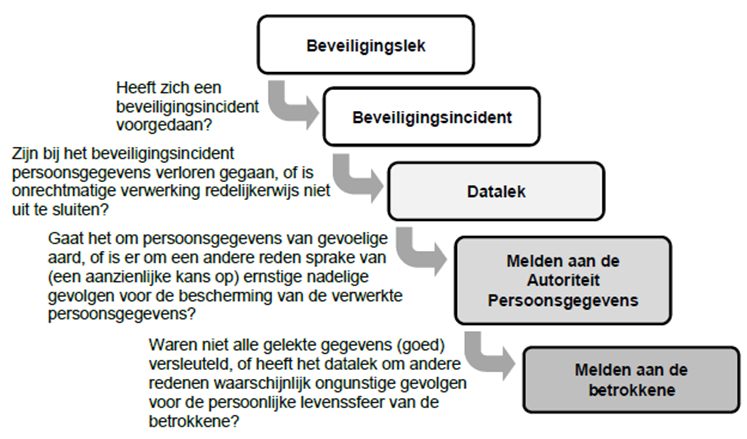
In dit datalekprotocol wordt omschreven op welke manier moet worden omgegaan met eventuele datalekken. In het plan is vastgelegd wie er intern op de hoogte gebracht moeten worden, wie verantwoordelijk is voor welke melding en hoe de melding aan de toezichthouder en eventueel ook aan de betrokkenen wordt gedaan. De beleidsregels van de toezichthouder zijn vertaald naar een praktisch en werkbaar beleid. Dit protocol heeft betrekking op alle medewerkers en externe relaties (inhuur). Tevens vallen onder het beleid alle apparaten waar vanaf geautoriseerde toegang tot netwerken en/of gegevens verkregen kan worden.

Mochten toekomstige (wettelijke) wijzigingen/veranderingen aanpassing van dit document noodzakelijk maken, dan zal de Functionaris voor de Gegevensbescherming (hierna: FG) deze aanpassing doorvoeren en het versienummer updaten.

**Deel I** van het protocol legt uit wanneer een incident gekwalificeerd kan worden als een datalek en wanneer dit gemeld moet worden aan de toezichthouder/betrokkene. **Deel II** omschrijft hoe er binnen de HBM gehandeld dient te worden in het geval van (een vermoeden van) een datalek.

# DEEL I: Wat is een datalek?

Aan de hand van het onderstaande stappenschema wordt beoordeeld of er sprake is van een datalek en of het datalek gemeld moet worden bij de Autoriteit Persoonsgegevens (hierna: AP)/ de betrokkenen.



## Is er sprake van een beveiligingsincident?

Voordat er gesproken kan worden over een datalek, moet een beveiligingsincident zich daadwerkelijk hebben voorgedaan. Alleen de dreiging van een beveiligingsincident kan nooit een datalek zijn. Uiteraard kan een concrete dreiging wel erg belangrijk zijn en dient deze zo snel mogelijk gemeld te worden bij de FG (per mail via [scholen@ictrecht.nl](mailto:scholen@ictrecht.nl) en telefonisch op 020 663 1941)

Voorbeelden van beveiligingsincidenten zijn:

* Een gestolen laptop;
* Een mailing wordt verstuurd met alle e-mailadressen in de CC in plaats van in de BCC;
* Een ransomwarebesmetting;
* Een brand bij de hostingprovider of het datacentrum.

Let op: hoewel een beveiligingsincident niet altijd een datalek hoeft te zijn (zie ook de volgende paragrafen), moet wel ieder beveiligingsincident worden geregistreerd in het datalekregister. Bij deze registratie wordt vervolgens aangegeven waarom het wel of niet tot een datalek is bestempeld door de FG en waarom.

*🡪 Kan het incident bestempeld worden als beveiligingsincident? Ga dan door naar de volgende vraag.*

## Is er sprake van een datalek?

Niet alle incidenten zijn datalekken die gemeld moeten worden bij de AP. Hoewel een ‘*datalek*’ in de Algemene Verordening Gegevensbescherming[[1]](#footnote-1) (hierna: AVG) een '*inbreuk in verband met persoonsgegevens*' wordt genoemd[[2]](#footnote-2), wordt in dit protocol (omwille van de leesbaarheid) het begrip ‘*datalek*’ gebruikt. Om te beoordelen of een beveiligingsincident heeft geleid tot een datalek, moet de volgende vraag bevestigend beantwoord worden: zijn er bij het beveiligingsincident persoonsgegevens verloren gegaan of is onrechtmatige verwerking redelijkerwijs niet uit te sluiten?

### Een beveiligingsincident met persoonsgegevens

Een beveiligingsincident kan uiteraard veel vervelende gevolgen hebben. Er kan echter alleen sprake zijn van een datalek wanneer er op een of andere manier persoonsgegevens zijn betrokken bij het beveiligingsincident. Stel dat er een USB-stick verloren raakt waarop enkel wat algemene financiële informatie van de school (behaalde omzet, winst, etc.) stond. Hoewel het natuurlijk erg vervelend is dat dergelijke gevoelige bedrijfsinformatie lekt, is het geen datalek zoals bedoeld in de AVG. Er zijn namelijk geen persoonsgegevens bij betrokken. Van belang is om een erg ruime interpretatie aan te houden van het begrip ‘persoonsgegeven’. Alle gegevens die direct of indirect (via een derde) herleidbaar zijn tot een persoon zijn persoonsgegevens. Dit moet objectief beoordeeld worden. Voorbeelden van direct herleidbare persoonsgegevens en van indirect herleidbare persoonsgegevens staan in de tabel hieronder:

|  |  |
| --- | --- |
| **Direct herleidbare persoonsgegevens** | **Indirect herleidbare persoonsgegevens** |
| Naam | Leerlingnummer |
| Adres | Postcode |
| E-mailadres[[3]](#footnote-3) | Personeelsnummer |
| Geboortedatum | IP-adres |

Het voorgaande komt er kort gezegd op neer dat alle datalekken altijd een beveiligingsincident zijn, maar dat niet alle beveiligingsincidenten ook datalekken zijn.

### Onrechtmatige verwerking?

Wanneer duidelijk is dat er sprake is van een beveiligingsincident én wanneer duidelijk is dat hierbij persoonsgegevens betrokken zijn, moet getoetst worden of dit mogelijk een onrechtmatige verwerking van persoonsgegevens tot gevolg heeft. Alleen dan kan gesproken worden van een datalek.

Een onrechtmatige verwerking kan inhouden:

1. Een **inbreuk op de vertrouwelijkheid**: dit houdt in dat een onbevoegde persoon toegang krijgt tot bepaalde persoonsgegevens. Hiervan is tevens sprake wanneer niet is uit te sluiten dat de persoonsgegevens zijn ingezien of anderszins zijn verwerkt door daartoe onbevoegde personen. Denk hierbij aan het voorbeeld dat een leerling inlogt in het Magister-account van een leraar. Een onbevoegde persoon (de leerling in bovengenoemd voorbeeld) heeft dan inzicht in de persoonsgegevens van andere leerlingen.
2. Een **inbreuk op de integriteit**: hiervan is sprake wanneer de persoonsgegevens (mogelijk) ongeoorloofd of onopzettelijk zijn gewijzigd of aangepast. Denk hierbij aan het voorbeeld dat een leerling inlogt in het Magister-account van een leraar en zijn eigen cijfers verandert.
3. Een **inbreuk op de beschikbaarheid**: hiervan is sprake wanneer de persoonsgegevens onopzettelijk[[4]](#footnote-4) tijdelijk (*verlies van toegang*) of permanent (*vernietiging*) niet beschikbaar zijn. Denk hierbij aan het voorbeeld dat een bepaald systeem (HR Today of Magister) is gehackt en daardoor bepaalde persoonsgegevens (tijdelijk) niet beschikbaar zijn.

Uiteraard is het mogelijk dat een beveiligingsincident in meerdere categorieën van onrechtmatige verwerkingen kan vallen. Een gestolen laptop kan bijvoorbeeld prima een inbreuk op de vertrouwelijkheid zijn, én tevens een inbreuk op de beschikbaarheid van persoonsgegevens betekenen.

Let op: wanneer er twijfel bestaat of er een onrechtmatige verwerking heeft plaatsgevonden, dan wordt aangeraden om het ‘*better safe than sorry*’-principe te hanteren. Alleen wanneer de FG kan uitsluiten dat het beveiligingsincident een onrechtmatige verwerking van persoonsgegevens tot gevolg heeft, is er geen sprake van een datalek. Hieronder wat voorbeelden:

1. Per ongeluk wordt een e-mail met persoonsgegevens erin aan een verkeerd e-mailadres gestuurd. Echter, de verzender krijgt een melding dat de e-mail niet is aangekomen omdat het e-mailadres niet bestaat. Dit is dan geen datalek. Als de verzender geen foutmelding krijgt, dan valt niet uit te sluiten dat de e-mail bij een onbevoegde persoon terecht is gekomen en is er wél sprake van een datalek.
2. Iemand van de afdeling IT maakt een fout waardoor per ongeluk een database met leerlinggegevens wordt gewist. Wanneer deze database snel hersteld kan worden door middel van een recente back-up, dan kan niet gesproken worden van een datalek. Is er geen recente back-up beschikbaar? Dan is dit wel een datalek omdat de gegevens permanent onbeschikbaar zijn.
3. Een medewerker van de HBM heeft zijn wachtwoord van zijn e-mailbox op een briefje geschreven en is dit briefje kwijtgeraakt. Wanneer kan worden uitgesloten dat iemand onrechtmatig is ingelogd op de e-mailbox, bijvoorbeeld door het wachtwoord direct te resetten en in de logfiles te zien dat er in de tussentijd niet is ingelogd, dan is er geen sprake van een datalek. Indien dit niet uitgesloten kan worden, is er wel sprake van een datalek.

Mocht geoordeeld worden dat er sprake is van een datalek, dan moet deze kwalificatie uiteraard geregistreerd worden in het datalekregister. Dit betekent echter niet dat het datalek ook gemeld moet worden aan de AP en/of de betrokkenen. Hierover meer in de volgende hoofdstukken.

# Wanneer melden aan de AP?

Op het moment dat het waarschijnlijk is dat een datalek, zoals omschreven in hoofdstuk 2, zich heeft voorgedaan, dan is het aan de FG om te beoordelen of dit binnen 72 uur aan de AP gemeld moet worden.[[5]](#footnote-5)

## Voldoende ernstig?

Niet alle datalekken dienen gemeld te worden aan de AP. Alleen datalekken met een bepaalde mate van ernst moeten gemeld worden. In de AVG en de richtsnoeren van de AP wordt gesteld dat datalekken niet gemeld hoeven worden indien ‘*het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van betrokkenen*’. Kortom, wanneer een datalek waarschijnlijk een risico inhoudt voor de rechten en vrijheden van betrokkenen moet het gemeld worden bij de AP.

Een eenvoudige manier om te toetsen of een datalek voldoende ernstig is om te melden aan de AP, is om te kijken of het datalek kwantitatief en/of kwalitatief voldoende ernstig is. Deze begrippen worden hieronder verder uitgewerkt.

### Kwantitatief ernstig (aantal getroffen betrokkenen/gegevens)

Een datalek kan een risico inhouden voor betrokkenen indien het een grote hoeveelheid gegevens betreft. In de AVG of in de richtsnoeren van de AP is echter niet vastgelegd waar de grens precies ligt. Per datalek zal daarom een inschatting moeten worden gemaakt of het datalek voldoende (kwantitatief) ernstig is. Hierbij kan rekening worden gehouden met de volgende vragen:

* Hoeveel personen zijn getroffen door het datalek?
* Hoeveel gegevens van deze personen zijn betrokken bij het datalek?

Van kwantitatief ernstig kan niet gesproken worden wanneer een A4’tje met een paar e-mailadressen onbedoeld op straat komt te liggen. Die paar e-mailadressen zijn bijvoorbeeld niet interessant voor spammers. Dit is anders wanneer het gaat om tientallen of meer dan honderd e-mailadressen.

### Kwalitatief ernstig (gevoeligheid van de gegevens)

Hetgeen is genoemd in de paragraaf hiervoor, betekent niet dat een datalek nooit gemeld hoeft te worden indien het datalek slechts één betrokkene treft. Een datalek kan namelijk ook een risico inhouden voor de rechten en vrijheden van betrokkenen wanneer gevoelige gegevens gelekt worden.

Let op: met ‘gevoelige persoonsgegevens’ wordt niet hetzelfde bedoeld als de ‘bijzondere persoonsgegevens’ zoals opgesomd in de AVG.[[6]](#footnote-6) **Bijzondere** persoonsgegevens zijn gegevens over iemands ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, genetische of biometrische gegevens met oog op unieke identificatie, gezondheid, seksuele leven en strafrechtelijk verleden.

De categorie ‘**gevoelige** persoonsgegevens’ is wat breder en omvat bijvoorbeeld ook:

* Inloggegevens;
* Een registratie op een zwarte lijst;
* Financiële gegevens, zoals winsten uit kansspelen;
* Kopieën van identiteitsbewijzen;
* Gegevens die betrekking hebben op werkprestaties.

Stel nu dat het eerdergenoemde A4’tje met een paar e-mailadressen een koptekst heeft met “Leerlingen met gedragsproblemen”. In dat geval is het datalek misschien niet *kwantitatief* ernstig, maar de gevoeligheid van de gelekte informatie maakt het datalek ineens wel *kwalitatief* ernstig. Dit heeft tot gevolg dat dit datalek gemeld moet worden aan de AP. Hetzelfde zou gelden als er geen “Leerlingen met gedragsproblemen” had gestaan, maar het e-mailadressen betrof van kinderen van bekende Nederlanders.

Bij het nagaan of een datalek ‘kwalitatief ernstig’ is moet daarom niet alleen gekeken worden naar de soort gegevens, maar ook naar alle andere omstandigheden, zoals:

* Van wie zijn de gegevens precies gelekt?
* Aan wie zijn de gegevens gelekt?
* Hoe gemakkelijk kunnen betrokkenen geïdentificeerd worden?
* Hoe ernstig kunnen de mogelijke gevolgen zijn voor de betrokkenen?

Wanneer een datalek mogelijk kan leiden tot: discriminatie, (identiteits-)fraude, financiële schade en/of reputatieschade, dan is het datalek voldoende kwalitatief ernstig en moet het gemeld worden bij de AP.

Hieronder een kleine tabel waarin het voorgaande simpel wordt weergegeven.

|  |  |  |
| --- | --- | --- |
|  | **Wel kwantitatief ernstig** | **Niet kwantitatief ernstig** |
| **Wel kwalitatief ernstig** | MELDEN | MELDEN |
| **Niet kwalitatief ernstig** | MELDEN | NIET MELDEN |

## Termijn melden AP

Een datalek dat waarschijnlijk een risico inhoudt voor betrokkenen dient zo snel mogelijk, maar uiterlijk binnen 72 uur na ontdekking door de FG, aan de AP gemeld te worden. Deze termijn start op het moment dat de FG met een redelijke mate van zekerheid kan vaststellen dat een beveiligingsincident heeft plaatsgevonden die tot onrechtmatige verwerking of verlies van persoonsgegevens heeft geleid.

Ook hier raden wij sterk aan om het principe ‘*better safe than sorry*’ toe te passen. De FG kan niet een week de tijd nemen om alles tot in de puntjes uit te zoeken. Bij een *redelijke zekerheid* moet al gemeld worden. Zelfs als er nog wat twijfel bestaat raden wij aan om te melden bij de AP. Het is namelijk altijd mogelijk om op een later moment de melding aan te vullen of zelfs in te trekken.

## Waar te melden?

Een datalek dient via [het meldloket](https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0) op de website van de AP te worden gemeld. Bij dit invulformulier dienen diverse gegevens ingevuld te worden.

Na het doen van een melding bij de toezichthouder, wordt er een bevestiging van deze melding getoond in de browser. In deze bevestiging staan de gegevens die zijn ingevoerd met daarbij een meldingsnummer. Dit meldingsnummer is nodig om de melding aan te passen of in te trekken. De melding kan hierna niet online geraadpleegd worden. **Het is daarom essentieel om een print, pdf-bestand of printscreen te maken van de bevestiging voordat je het browservenster sluit.**

# Wanneer melden aan de betrokkenen?

In bepaalde situaties moet een datalek niet alleen gemeld worden aan de AP, maar ook aan de betrokkenen. Dit is het geval wanneer het datalek een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen. Het woord ‘hoog’ maakt het verschil met hoofdstuk 3. Een melding aan de AP moet al worden gedaan wanneer het een risico inhoudt voor de rechten en vrijheden van de betrokkenen. Een melding aan de betrokkenen hoeft alleen te worden gedaan wanneer het een hoog risico betreft.

Het moge duidelijk zijn dat je aan deze stap niet toekomt wanneer blijkt dat het datalek niet gemeld hoeft te worden aan de AP. Er is dan namelijk geen sprake van een risico voor de rechten en vrijheden van de betrokkenen en al helemaal niet van een hoog risico.

Hieronder wordt een en ander nader uitgewerkt.

## Hoog risico

Aangezien de criteria voor het melden aan de AP en de betrokkenen vrijwel hetzelfde zijn (afgezien van het woord ‘hoog’), kan bij deze toets gekeken worden naar de punten die genoemd worden in de paragrafen 3.1.1 en 3.1.2. In de richtsnoeren van de AP worden meer specifiek de volgende punten genoemd om mee te nemen in de beoordeling:

* De aard van de inbreuk. Stel dat het gaat om gegevens betreffende iemand zijn gezondheid. In dit geval zal een inbreuk op de vertrouwelijkheid daarvan eerder een negatief gevolg hebben voor het privéleven van deze betrokkene, dan wanneer deze gegevens per ongeluk zijn verwijderd uit zijn medisch dossier (en met een nieuwe test weer te achterhalen zijn).
* De aard, gevoeligheid en omvang van de persoonsgegevens die gelekt zijn. Een lek van NAW-gegevens levert uiteraard minder risico op dan een lek van financiële gegevens. Tevens moet gekeken worden naar de omvang; gaat het om één persoonsgegeven of een combinatie van meerdere gegevens waardoor een vollediger beeld geschetst kan worden van de betrokkenen?
* Het gemak waarmee de betrokkenen kunnen worden geïdentificeerd. Zijn de gegevens versleuteld? Gaat het om direct herleidbare persoonsgegevens (zoals NAW-gegevens) of gaat het om indirect herleidbare persoonsgegevens (zoals een leerlingnummer). Niet-versleutelde en direct herleidbare persoonsgegevens leveren uiteraard een hoger risico op dan versleutelde en indirect herleidbare persoonsgegevens.
* De ernst van de gevolgen voor de betrokkenen. Wat betekent het datalek voor het privéleven van de betrokkenen? Wanneer alleen leerlingnummers op straat komen te liggen, dan zal dit niet snel negatieve gevolgen hebben voor de leerling zijn privéleven. Dit is uiteraard anders wanneer een kopie van een paspoort op straat komt te liggen, want dan bestaat er een kans op identiteitsfraude. Van een ‘hoog risico’ kan snel gesproken worden wanneer het datalek mogelijk leidt tot (identiteits)fraude, reputatieschade, lichamelijk letsel en/of financieel nadeel.
* De bijzondere kenmerken van de betrokkenen. Heeft het datalek betrekking op persoonsgegevens van kinderen, gehandicapten of andere kwetsbare personen? In dat geval zal er snel sprake zijn van een ‘hoog risico’.
* De bijzondere kenmerken van de verwerkingsverantwoordelijke. Een datalek bij een ziekenhuis zal uiteraard sneller een hoog risico opleveren dan een datalek bij een supermarkt. Scholen behoren in dit kader meer tot de categorie van ziekenhuizen, dan tot de categorie van supermarkten, omdat (gevoelige) persoonsgegevens van leerlingen (en vaak minderjarigen) worden verwerkt.
* Het aantal getroffen betrokkenen. Heeft het datalek betrekking op één persoon, of zijn honderden personen getroffen? Hoe meer mensen getroffen worden, hoe hoger het risico. Eén e-mailadres is uiteraard minder interessant voor fraudeurs dan honderden e-mailadressen.
* Overige algemene punten. Bij het beoordelen of een datalek een hoog risico oplevert voor de rechten en vrijheden van betrokkenen, moeten alle omstandigheden van het geval worden meegewogen. Hierbij is het belangrijk om niet alleen te kijken naar de mogelijke gevolgen, maar ook naar de waarschijnlijkheid dat deze gevolgen zullen intreden.

Zelfs met de voornoemde richtlijnen van de AP, blijft de beoordeling of een datalek een hoog risico oplevert voor de rechten en vrijheden van betrokkenen, erg moeilijk en vrij vaag. Om datalekken objectiever te kunnen toetsen, heeft het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (ENISA) aanbevelingen opgesteld voor [een methode om de ernst van een inbreuk te beoordelen](https://www.enisa.europa.eu/publications/dbn-severity). Deze methode werkt met een puntensysteem.

Een manier om deze afweging wat makkelijker te maken is door jezelf te verplaatsen in de betrokkenen. Wat als jouw gegevens getroffen waren door het datalek?

* Is de inbreuk zo basaal dat je je schouders op zou halen en verder niets zou doen? In dat geval levert het datalek waarschijnlijk niet een hoog risico op.
* Zou je bepaalde acties/voorzorgsmaatregelen willen nemen naar aanleiding van het datalek? Denk aan: het blokkeren van je creditcard en/of ervoor zorgen dat je alert bent op mogelijke fraudeurs. Zo ja, dan wordt aangeraden om het datalek te melden.

Belangrijk om te onthouden is dat de AP vindt dat een verantwoordelijke bij twijfel gehouden is om het zekere voor het onzekere te nemen en de inbreuk moet melden aan de betrokkene(n).

## Uitzonderingen

Een datalek hoeft niet onverwijld aan de betrokkenen gemeld te worden indien:

1. *Voorafgaand* aan het datalek reeds zodanige technische en organisatorische beveiligingsmaatregelen waren genomen waardoor de persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden. Hiervan is bijvoorbeeld sprake als de persoonsgegevens voorzien zijn van een beveiliging die volgens de laatste stand van de techniek als ‘veilig’ kan worden aangemerkt. Denk hierbij bijvoorbeeld aan vormen van encryptie of hashing. Let op: encryptie of hashing biedt geen bescherming tegen *vernietiging* van persoonsgegevens. In dergelijke gevallen dient er altijd een melding te worden gedaan aan de betrokkenen, mits de vernietiging een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen.

1. *Direct na* het datalek voldoende maatregelen zijn genomen om ervoor te zorgen dat het risico voor de rechten en vrijheden van de betrokkenen zich waarschijnlijk niet meer zal voordoen. Hiervan is bijvoorbeeld sprake wanneer een gestolen laptop snel op afstand volledig gewist kon worden.
2. Het onevenredige inspanningen zou vergen om direct contact op te nemen met de betrokkenen.[[7]](#footnote-7) Hiervan is bijvoorbeeld sprake wanneer het gaat om een dataset van 50 jaar oud waarin bepaalde gegevens van 20.000 betrokkenen zijn opgenomen, maar totaal geen contactgegevens bevat. In dit geval mag niet verwacht worden dat er een enorme zoekactie wordt opgezet om de contactgegevens van ieder van deze 20.000 betrokkenen te achterhalen. Let op: dit betekent niet dat de FG volledig stil kan blijven. De FG zal in dat geval andere methoden moeten proberen om deze betrokkenen doeltreffend te informeren. Gedacht kan worden aan een publicatie in een krant of op de website.

Mocht het zo zijn dat een beroep kan worden gedaan op uitzondering i. en/of op uitzondering ii., dan betekent dit niet dat het hier stopt. Informatie omtrent het datalek, alsmede de reden waarom het datalek niet is gemeld aan de betrokkenen, moet geregistreerd worden in het **datalekregister**. Als op enig moment blijkt dat de veiligheid van de persoonsgegevens toch niet meer gegarandeerd kan worden, dan moet de FG het datalek alsnog melden aan de betrokkenen.

Voorbeeld: stel dat een versleutelde USB-stick met gegevens van leerlingen verloren raakt. Volgens de huidige stand der techniek kan deze versleuteling niet gekraakt worden en daarom besluit de FG om de betrokkenen niet in te lichten. Drie jaar later is er op internet een tool te vinden waarmee de versleuteling van de verloren USB-stick gemakkelijk gekraakt kan worden. Dit heeft tot gevolg dat de FG alsnog het datalek moet melden aan de betrokkenen.

Gezien het voorgaande is het praktischer om de betrokkenen toch proactief te informeren. Zo wordt voorkomen dat de FG de betrokkenen een ruime tijd na het datalek alsnog moet informeren.

## Termijn

Het datalek dient ‘onverwijld’ na ontdekking aan de betrokkenen gemeld te worden. ‘Onverwijld’ wil zeggen: zo spoedig mogelijk, waarbij enige tijd mag worden genomen om de juiste informatie te verzamelen om een zorgvuldige melding te kunnen doen. Met andere woorden: de melding aan de betrokkenen moet zorgvuldig gebeuren, maar mag niet onnodig worden vertraagd. De AVG koppelt hier geen ‘harde’ termijn aan, zoals dat bij de melding aan de AP wél het geval is.

## Wat te melden aan de betrokkenen?

De melding aan betrokkenen dient in ieder geval behoorlijk en zorgvuldig uitgevoerd te worden, en moet ten minste de volgende informatie bevatten:

* De aard van de inbreuk, waarbij volstaan kan worden met een algemene omschrijving van wat er is gebeurd;
* De contactgegevens van de HBM en de FG, zoals een speciaal telefoonnummer of e-mailadres waar betrokkenen terecht kunnen met vragen ([scholen@ictrecht.nl](mailto:scholen@ictrecht.nl) en gegevensbescherming@iris-cvo.nl);
* De door de FG aanbevolen maatregelen om negatieve gevolgen te beperken, zoals het veranderen van wachtwoorden.

Uitgangspunt bij het doen van een dergelijke melding is dat dit op individuele basis dient te gebeuren. Een bericht in de media is in beginsel niet voldoende om betrokkenen te informeren. Als uitgangspunt geldt dat wanneer de betrokkenen individueel op de hoogte kunnen worden gesteld, de melding op individuele basis moet plaatsvinden. Pas als dat echt niet haalbaar is, vanwege de omvang van de groep of vanwege het feit dat niet meer te achterhalen is welke personen wel of niet zijn geraakt door het datalek, kan naar andere manieren van informeren worden gekeken.

# DEEL II: Intern proces melden van een beveiligingsincident/datalek

Wanneer een datalek zich voordoet, zal vastgesteld moeten worden waar het datalek zich heeft voorgedaan en hoe dit datalek uiteindelijk (eventueel) bij de toezichthouder en betrokkenen gemeld zal worden.

Van medewerkers wordt verwacht dat zij bij (een vermoeden van) een beveiligingsincident/datalek onmiddellijk per e-mail contact opnemen met de FG. Uiteraard is het daarbij van belang dat alle medewerkers een datalek kunnen identificeren. Het creëren van bewustzijn bij de medewerkers van de HBM is dan ook van groot belang. De ontdekker zal een incident te allen tijde moeten melden bij de FG.

## 

## Intern proces

Indien een beveiligingsincident en/of datalek heeft plaatsgevonden, dient dit meteen te worden gemeld aan de FG. Wanneer er bij de HBM een datalek plaatsvindt, moet iedereen weten hoe er gehandeld dient te worden, zodat de melding van het datalek tijdig de juiste personen, en uiteindelijk de toezichthouder en eventueel betrokkenen bereikt. Lees de onderstaande uitleg daarom goed door.

Medewerkers van de HBM moeten een beveiligingsincident/datalek zo snel mogelijk melden bij de FG via:

|  |  |  |
| --- | --- | --- |
| **Functie** | **Naam** | **Contactinformatie** |
| Functionaris Gegevensbescherming | Stan van Riemsdijk | Telefoon: 020 663 1941  [scholen@ictrecht.nl](mailto:scholen@ictrecht.nl) |

Neem hierbij het contactpersoon van de betreffende school mee in de cc.

|  |
| --- |
| De medewerkers vermelden hierbij de volgende informatie:   * Omschrijving van het incident; wat voor incident heeft er plaatsgevonden? * De bij het incident betrokken persoonsgegevens; * Om welke data (gegevens) gaat het? * Welke systemen zijn betrokken bij/geraakt door het incident? * Wanneer heeft het incident plaatsgevonden?   Wat is er gedaan om het incident op te lossen/in de toekomst te voorkomen? |

De FG adviseert vervolgens of het beveiligingsincident ook een datalek is en of dit moet worden gemeld aan de AP en aan de betrokkene(n). Meldingen bij de AP worden gedaan door de FG evenals het informeren van de betrokkene(n).

In overleg met de directie wordt besloten of het datalek wordt gemeld aan de toezichthouder en de betrokkenen. Wanneer het gaat om een verwerking waarvoor de HBM verantwoordelijke is, dan zal de FG zorgen voor de juiste interne administratie van het datalek.

## Registratieplicht (datalekregister)

Op het moment dat er sprake is van een datalek, ongeacht of deze wel of niet aan de toezichthouder en/of betrokkenen wordt gemeld, dient dit datalek intern te worden gedocumenteerd door de FG. Het voorgaande geldt uiteraard voor zover de HBM ten aanzien van dit datalek is aan te merken als verwerkingsverantwoordelijke.

Voor het registreren van de datalekken zou door de FG een apart systeem kunnen worden ingericht, maar dit is niet vereist. Het enkele creëren van een apart datalekregister (bijvoorbeeld in Excel) voor het registeren van datalekken, is hiertoe al voldoende.

Van datalekken die aan de AP zijn gemeld, dient door de FG de print of pdf van deze verzonden melding te worden bewaard, evenals de eventuele melding die aan betrokkenen is gedaan. De vindplaats van deze print/pdf kan vervolgens worden opgenomen in het datalekregister. Wanneer het datalek niet aan de AP en/of betrokkenen is gemeld, dient hiervan de volgende informatie te worden geregistreerd in het datalekregister:

|  |
| --- |
| Wie heeft er gemeld? |
| Wat is er gemeld? |
| Om welke persoonsgegevens gaat het? |
| Hoe heeft het incident plaatsgevonden (welke drager is bijvoorbeeld verloren)? |
| Welke systemen zijn betrokken/geraakt door het incident? |
| Wanneer heeft het incident plaatsgevonden? |
| Wat zijn de gevolgen van het datalek? |
| Welke corrigerende maatregelen zijn er genomen? |
| Heeft de FG het datalek gemeld aan de AP? Waarom wel/niet? Meldingsnummer? |
| Heeft de FG het datalek gemeld aan de betrokkenen? Waarom wel/niet? |

De voornoemde informatie moet bewaard worden teneinde:

* Te leren van het datalek;
* Vragen van betrokkenen en derden te kunnen beantwoorden;
* Alsnog een melding aan betrokkenen te kunnen doen wanneer dit na verloop van tijd nodig blijkt;
* Een efficiënte controle op de naleving van de meldplicht datalekken door de AP mogelijk te maken.

Het datalekregister hoeft overigens niet openbaar gemaakt te worden. Deze dient enkel op verzoek van de AP aan de AP te worden verstrekt.

1. Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG. [↑](#footnote-ref-1)
2. Artikel 4 onder 12 AVG. [↑](#footnote-ref-2)
3. Als het e-mailadres geen voor- en/of achternaam bevat, dan is het géén direct herleidbaar persoonsgegeven. [↑](#footnote-ref-3)
4. Opzettelijke niet beschikbaarheid, zoals gepland systeemonderhoud, is geen onrechtmatige verwerking en daarom ook geen datalek. [↑](#footnote-ref-4)
5. Artikel 33 AVG. [↑](#footnote-ref-5)
6. Artikel 9 lid 1 AVG. Onder meer gegevens betreffende iemand zijn: ras, etnische herkomst, politieke opvatting, religieuze of filosofische opvattingen, lidmaatschap van een vakbond, genetische informatie, gezondheid, seksuele geaardheid, criminele veroordelingen of overtredingen. [↑](#footnote-ref-6)
7. Zie ook de WP29-richtsnoeren inzake transparantie, waarin het probleem van onevenredige inspanningen aan de orde komt, die beschikbaar zijn op: <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850>. [↑](#footnote-ref-7)