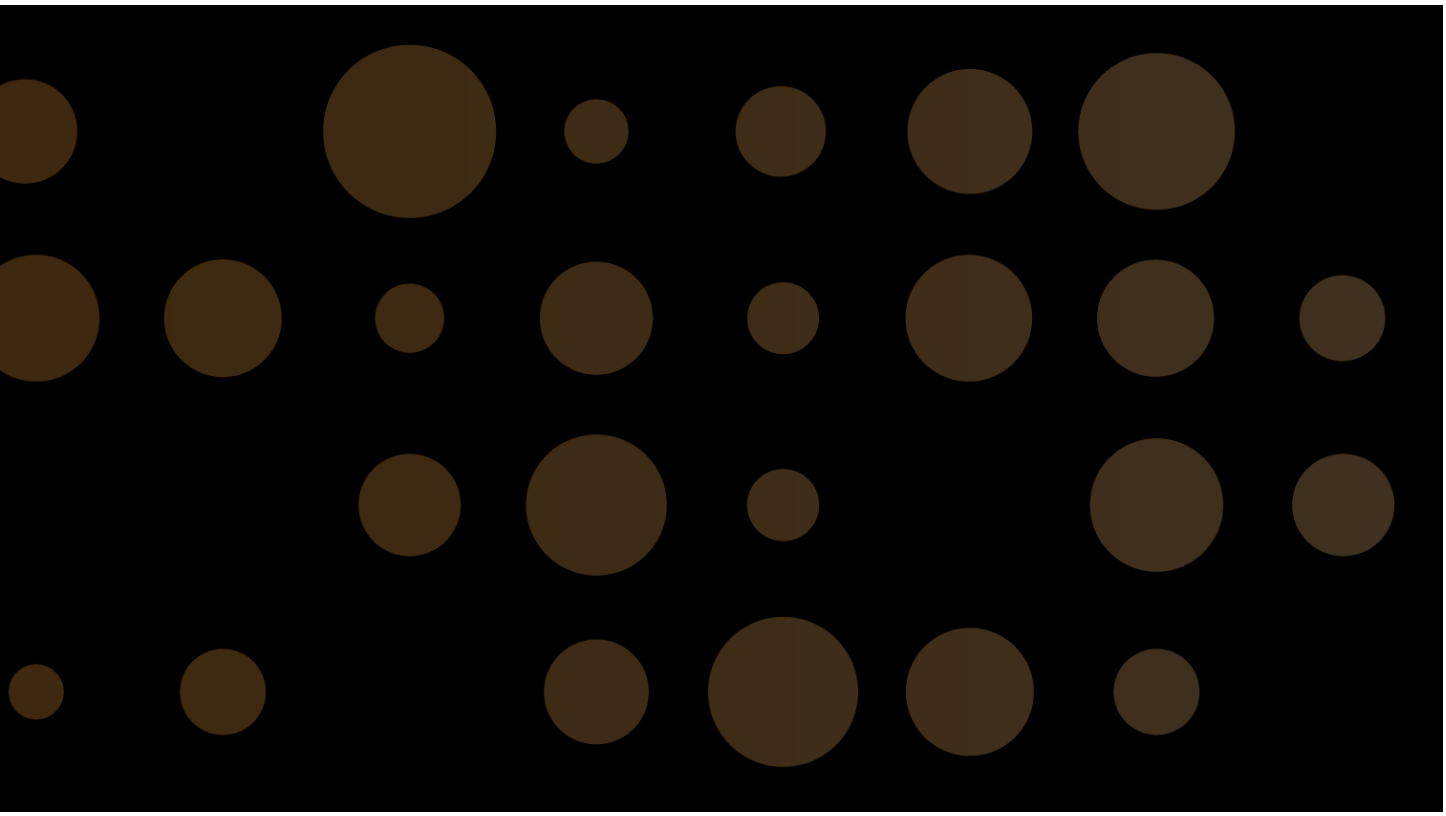
# Procedure Meldplicht Datalekken

| | |
|---|---|
| Versie | 1.1 |
| Datum | Maart 2016 |
| Auteur | Specialist Informatiebeveiliging |



Document historie

| VERSIE | WIJZIGING | DATUM | AUTEUR |
|---|---|---|---|
| 0.1 | Eerste versie | 01/12/2015 | |
| 0.2 | Toevoeging volgende stap na elke genomen stap | 04/12/2015 | |
| 0.3 | Spel- en stijlfouten | 11/12/2015 | |
| 0.4 | Aanpassingen n.a.v. review en | 22/01/2016 | |
| 0.5 | Aanpassingen n.a.v. overleg en | 03/03/2016 | |
| 1.0 | Definitieve versie | 03/303/2016 | |
| 1.1 | Toevoeging onder stap 2 | 18/03/2016 | |
| | | | |

## 1. Inleiding

Doel van deze procedure is op gecontroleerde wijze om te gaan met de gevolgen van een datalek. Aan de hand van een stappenplan wordt bepaald of er gemeld moet worden en hoe dit moet gebeuren. Deze procedure is bedoeld voor medewerkers van het inlichtingenbureau die beveiligings- en privacy incidenten behandelen.

Aanleiding voor deze procedure is de meldplicht datalekken die per 01/01/2016 van kracht is. Het doel is beperking van de schade voor betrokkenen ten gevolge van 'datalekken' waarbij kans is op verlies of onrechtmatige verwerking van persoonsgegevens. De wet wordt opgenomen in de Wet bescherming persoonsgegevens (Wbp) als een nieuw artikel 34a.

De meldplicht geldt voor iedere verantwoordelijke voor de verwerking van persoonsgegevens (niet: de bewerker!), zowel in de private als publieke sector. De wet verplicht, op een enkele uitzondering na, de verantwoordelijke tot melding van een datalek aan de Autoriteit Persoonsgegevens (AP) en in bepaalde gevallen ook aan de betrokkenen. Dit laatste is afhankelijk van de ernst van de zaak en de gevolgen voor de betrokkenen.

Bij 'niet tijdige' melding kan de AP:

- een (bindende) aanwijzing geven om alsnog te melden;
- een bestuurlijke boete opleggen tot maximaal 820.000 euro per overtreding.

## 2. Wat is een datalek?

Een datalek is de inbreuk op de beveiliging van persoonsgegevens. Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke levende persoon. Persoonsgegevens kunnen direct of indirect identificeerbaar zijn.

Een datalek betreft alle beveiligingsincidenten waardoor de bescherming van persoonsgegevens op enig moment is doorbroken waardoor de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking van persoonsgegevens. Het is daarbij niet van belang of de verantwoordelijke passende technische of organisatorische beschermingsmaatregelen had getroffen of niet.

Een datalek is:

- een kwijtgeraakte USB-stick waar zich persoonsgegevens op bevinden;
- een gestolen werklaptop;
- een vastgestelde inbraak door een hacker;
- verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden;
- een besmetting met ransomware als er geen bruikbare back-up teruggezet kan worden
- het verstrekken van een wachtwoord aan een derde
- papieren met persoonsgegevens belanden op straat
- een kwetsbaarheid in een applicatie waardoor persoonsgegevens gelekt worden

## 3. Werkwijze

In de praktijk komt een datalek aanvankelijk binnen als een beveiligingsincident. Deze wordt behandeld volgens de procedure incidentenafhandeling en vastgelegd in Topdesk. Als het vermoeden bestaat dat het gaat om een datalek, wordt vervolgens het stappenplan uit hoofdstuk 4 gevolgd. De uitkomst van de verschillende stappen worden hierbij ook vastgelegd in Topdesk.

## 4. Wie moet melden?

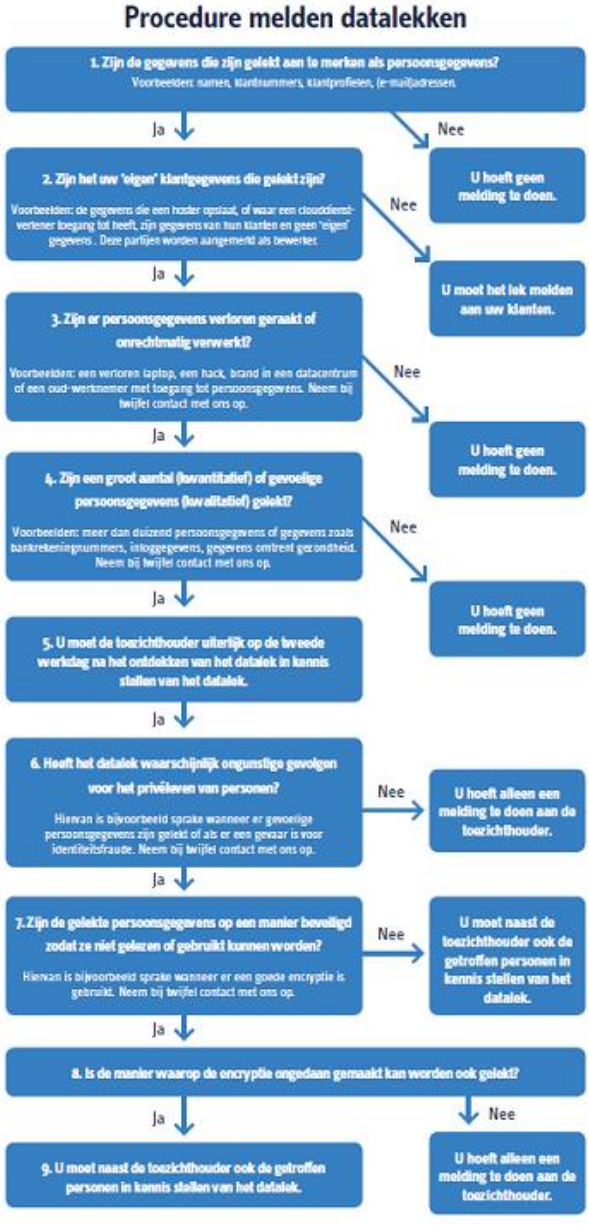
Hieronder volgt een lijst van functionarissen die een eventuele daadwerkelijke melding aan de AP moeten doen. Voordat er wordt gemeld, wordt altijd eerst de directeur en/of de betrokken afdelingsmanager in kennis gesteld.

De eerste verantwoordelijkheid voor een eventuele melding ligt bij de Specialist Informatiebeveiliging. Bij afwezigheid/onbereikbaarheid ligt de verantwoordelijkheid bij de Beleidsadviseur Informatiebeveiliging en/of de Privacyfunctionaris. Bij afwezigheid/onbereikbaarheid van deze personen ligt de verantwoordelijkheid bij de directeur en/of de betrokken afdelingsmanager.

## 5. Stappenplan

Gebruik eventueel '*De meldplicht datalekken in de Wet bescherming persoonsgegeven (Wbp), beleidsregels voor toepassing van artikel 34a van de Wbp*', uitgegeven door de Autoriteit Persoonsgegevens en verkrijgbaar via de website https://autoriteitpersoonsgegevens.nl voor meer informatie.

Een overzicht van het te volgen stappenplan is hiernaast schematisch weergegeven.




**STAP 1: PERSOONSGEGEVENS**

Zijn de gegevens die zijn gelekt aan te merken als persoonsgegevens?

Een gegeven is geen persoonsgegeven, indien doeltreffende technische en organisatorische maatregelen getroffen zijn waardoor een daadwerkelijke identificatie van individuele personen redelijkerwijs wordt uitgesloten (anonimisering). Een persoon is wel identificeerbaar als zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Bevatten de gegevens bijvoorbeeld namen, (e-mail)adressen of BSN's?

**JA:** ga naar stap 2
**NEE:** je hoeft geen melding te doen

## STAP 2: VERANTWOORDELIJKE / BEWERKER?

Zijn het onze eigen gegevens die gelekt zijn?

De *verantwoordelijke* is degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 1, sub d, Wbp). Het gaat hierbij om de vraag wie uiteindelijk bepaalt welke verwerking er plaatsvindt van welke persoonsgegevens en voor welk doel. Ook is van belang wie er beslist over de middelen voor die verwerking: de vraag op welke manier de gegevensverwerking zal plaatsvinden. Deze bevoegdheden kunnen soms in verschillende handen liggen. In dat geval is er sprake van gezamenlijke verantwoordelijkheid.

**JA:** (verantwoordelijke) Ga naar stap 3.
**NEE:** (bewerker) De meldplicht datalekken richt zich alleen tot de *verantwoordelijke* voor de verwerking van persoonsgegevens (de *verantwoordelijke*). Er hoeft dus geen melding bij de AP te worden gemaakt. Als *bewerker* heb je wel je verantwoordelijkheid richting de *verantwoordelijke*, zodat deze op tijd melding kan maken. De richtlijn is dit binnen 4 uur door te geven.

Het IB levert hierbij alle informatie aan die nodig is voor de *verantwoordelijke* om aan de verplichting te voldoen. Daarnaast houdt zij de *verantwoordelijke* op de hoogte van eventuele nieuwe ontwikkelingen rond het incident, en van de maatregelen die het IB treft om aan haar eigen kant de gevolgen van het incident te beperken en herhaling te voorkomen.

DUO: meldpuntdatalekken@duo.nl
GGK? Melden aan VNG

## STAP 3: DATALEK?

In deze stap zijn er verschillende vragen om rekening mee te houden:

### Stap 3A: is er sprake van een inbreuk op de beveiliging?

Een inbreuk op de beveiliging houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Er is niet uitsluitend sprake van een dreiging, of van een tekortkoming in de beveiliging (ook wel aangeduid als een beveiligingslek) die zou kunnen leiden tot een beveiligingsincident. Er heeft zich daadwerkelijk een beveiligingsincident voorgedaan, en de preventieve maatregelen die IB eventueel heeft getroffen waren niet toereikend om dit te voorkomen.

**JA:** (wel inbreuk) dit is een beveiligingslek. Er kan tevens sprake zijn van een datalek, ga naar stap 3B.
**NEE:** (geen inbreuk) dit is geen datalek. Je hoeft geen melding te doen.

### Stap 3B: zijn er persoonsgegevens verloren gegaan?

Verlies houdt in dat IB de persoonsgegevens niet meer heeft. Bij het beveiligingsincident zijn de persoonsgegevens vernietigd of op een andere manier verloren gegaan, en IB beschikt niet over een complete en actuele reservekopie van de gegevens.

**JA:** (wel verloren) dit is een datalek, ga naar stap 4.
**NEE:** (niet verloren) er kan toch sprake zijn van een datalek, ga naar stap 3C.

### Stap 3C: kan er uitgesloten worden dat er persoonsgegevens onrechtmatig zijn verwerkt?

Onder onrechtmatige vormen van verwerking vallen de aantasting van de persoonsgegevens, onbevoegde kennisneming, wijziging, of verstrekking daarvan. Als IB redelijkerwijs niet kunt uitsluiten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid, dan moet u de inbreuk beschouwen als een datalek.

**JA:** (kan uitgesloten worden) dit is geen datalek. Je hoeft geen melding te doen.
**NEE:** (kan niet uitgesloten worden) dit is een datalek, ga naar stap 4.

## 6. Meldplicht Autoriteit Persoonsgegevens

De meldplicht valt uiteen in de meldplicht aan de Autoriteit Persoonsgegevens en die aan de betrokkenen. In dit hoofdstuk wordt omschreven wanneer en hoe er aan de Autoriteit Persoonsgegevens moet worden gemeld.

### STAP 4: MELDING AP

In deze stap zijn twee vragen om rekening mee te houden:

### Stap 4A: zijn er persoonsgegevens van gevoelige aard gelekt?

Bij het beantwoorden van de vraag of er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens, moet er in ieder geval gekeken worden naar de aard van de getroffen gegevens. Is er sprake van bijzondere persoonsgegevens of van persoonsgegevens die anderszins van gevoelige aard zijn? Bij dit laatste moet je bijvoorbeeld denken aan gegevens over betalingsachterstanden.

Bij een aantal categorieën van persoonsgegevens, in dit kader aangeduid als persoonsgegevens van gevoelige aard, kunnen verlies of onrechtmatige verwerking onder meer leiden tot stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, financiële schade of tot (identiteits)fraude. Tot deze categorieën van persoonsgegevens moeten in ieder geval worden gerekend:

- *Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp* Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
- *Gegevens over de financiële of economische situatie van de betrokkene* Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
- *(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene* Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- *Gebruikersnamen, wachtwoorden en andere inloggegevens* De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de

inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.

- *Gegevens die kunnen worden misbruikt voor (identiteits)fraude* Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (BSN).

Ook gegevens uit DNA-databanken, gegevens waar een bijzondere, wettelijk bepaalde geheimhoudingsplicht op rust en gegevens die onder een beroepsgeheim vallen (bijvoorbeeld het medisch beroepsgeheim) in de zin van artikel 9, vierde lid, van de Wbp moeten tot de persoonsgegevens van gevoelige aard worden gerekend.

**JA:** (wel gevoelige gegevens) dit moet gemeld worden bij de AP, ga naar stap 5. Mogelijk moet dit ook gemeld worden aan de betrokkenen, ga daarna naar stap 6.
**NEE:** (geen gevoelige gegevens) ga naar stap 4B.

### Stap 4B: leiden de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?

De aard en omvang van de getroffen verwerking is mede bepalend voor de beantwoording van de vraag of er bij een datalek sprake is van (een aanzienlijke kans op) nadelige gevolgen voor de bescherming van persoonsgegevens. Een datalek bij instellingen als de Belastingdienst, de Sociale Verzekeringsbank (SVB) of bij een commerciële bank of verzekeraar kan leiden tot financieel nadeel voor de betrokkene of tot de compromittering van gegevens die beschermd worden door een geheimhoudingsplicht. Beveiligingslekken in de omvangrijke verwerkingen van persoonsgegevens waarover de overheid beschikt kunnen ook zeer grote gevolgen hebben voor de betrokkenen.

Afgezien van de gevoelige aard van de verwerkte gegevens, die in de voorgaande paragraaf al aan de orde kwam, is voor de kans op ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens verder het volgende relevant:

- De omvang van de hierboven beschreven verwerkingen betekent dat het bij datalekken kan gaan om veel persoonsgegevens per persoon, en om gegevens van grote groepen betrokkenen. Deze beide factoren maken een gelekte dataset aantrekkelijk voor misbruik in het criminele circuit. De kans dat de gelekte dataset wordt doorverkocht, wordt daardoor ook groter, met als gevolg dat de betrokkenen langer last houden van het datalek.
- Naarmate de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpender zijn, is ook de impact van verlies of onrechtmatige verwerking groter. Bijvoorbeeld: als een organisatie financiële gegevens gebruikt om iemands kredietwaardigheid te bepalen zijn de gevolgen van verlies en onbevoegde wijziging van de gegevens ingrijpender dan bij gebruik van dezelfde gegevens voor marketingdoeleinden.
- Bij omvangrijke verwerkingen van de overheid is vaak sprake van persoonsgegevens die binnen ketens worden gedeeld. Dit betekent dat de gevolgen van verlies en onbevoegde wijziging van persoonsgegevens door de hele keten heen kunnen optreden. Voor de betrokkenen wordt het hierdoor moeilijker om de mogelijke gevolgen van een datalek te overzien en om zich daar waar mogelijk aan te onttrekken.

Als de aard en omvang van de getroffen verwerking voldoen aan het bovenstaande, dan moet IB ervan uitgaan dat er (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens aanwezig kan zijn.

**JA:** (wel ernstige gevolgen) dit moet gemeld worden bij de AP, ga naar stap 5. Mogelijk moet dit ook gemeld worden aan de betrokkenen, ga daarna naar stap 6.
**NEE:** (geen ernstige gevolgen) dit datalek hoeft niet gemeld te worden aan de AP

### STAP 5: MELDING AP

De Autoriteit Persoonsgegevens stelt een webformulier beschikbaar waarmee datalekken kunnen worden gemeld. Een overzicht van de vragen in dit webformulier zijn opgenomen in bijlage 8.

Als IB geen gebruik kan maken van het webformulier, dan kunnen volgens de AP de gevraagde gegevens per fax toegezonden worden. Je moet daarbij zorgen dat je aan kunt tonen dat je de melding tijdig heeft gedaan. Er is echter geen faxnummer te vinden op de website, wel een telefoonnummer, speciaal voor datalekken.

- Er kan melden worden gemaakt van een datalek op de website https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?1.
- Het datalek moet onverwijld gemeld worden, zo mogelijk niet later dan 72 uur na de ontdekking. Mogelijk is er na 72 uur geen volledig zicht is op het incident. De melding bij de AP kan achteraf worden bijgewerkt of zelfs ingetrokken. Als er later dan 72 uur wordt gemeld, wordt er gemotiveerd waarom.
- Je ontvangt direct een ontvangstbevestiging. Deze registeren in Topdesk.
- Bij die meldingen die aanleiding geven tot nadere actie door de Autoriteit Persoonsgegevens, zal deze contact met IB opnemen om de herkomst van de melding te verifiëren. Op termijn zal worden aangesloten op eHerkenning of andere gangbare authenticatiemiddelen.
- Melding via webformulier niet mogelijk? Bel met 0900-3282535.
- Mogelijk moet er naast een melding bij de AP, ook gemeld worden aan betrokkenen, ga door naar stap 6.

## 7. Meldplicht betrokkenen

De meldplicht valt uiteen in de meldplicht aan de Autoriteit Persoonsgegevens en die aan de betrokkenen. In dit hoofdstuk wordt omschreven wanneer en hoe er aan de betrokkenen moet worden gemeld.

### STAP 6: PRIVELEVEN

Heeft het datalek waarschijnlijk ongunstige gevolgen voor het privéleven van personen?

Het datalek moet aan de betrokkene worden gemeld als de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (artikel 34a, tweede lid, Wbp). Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik van persoonsgegevens in hun belangen worden geschaad. De schade kan van materiële of van immateriële aard zijn. Bij dit laatste moet je bijvoorbeeld denken aan onrechtmatige publicatie, aantasting in eer en goede

naam, identiteitsfraude of discriminatie. Identiteitsfraude kan overigens niet alleen leiden tot immateriële gevolgen, maar ook tot materiële gevolgen.

Het is aan IB om te beoordelen of een datalek aan de betrokkene gemeld moet worden. Indien er persoonsgegevens van gevoelige aard zijn gelekt, dan moet je er van uitgaan dat je het datalek niet alleen moet melden aan de Autoriteit Persoonsgegevens, maar ook aan de betrokkene. Verlies of onrechtmatige verwerking van dergelijke gegevens kunnen onder meer leiden tot stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, financiële schade of (identiteits)fraude.
In alle overige gevallen zult u op basis van de omstandigheden van het geval een afweging moeten maken.

**JA:** (wel gevolgen voor privéleven) ga naar stap 7.
**NEE:** (geen gevolgen voor privéleven) er hoeft alleen aan de AP en niet aan de betrokkenen gemeld te worden.

## STAP 7: GOED BEVEILIGD?

Zijn de gelekte persoonsgegevens op een manier beveiligd zodat ze niet gelezen of gebruikt kunnen worden?

Als door de cryptografische bewerkingen die IB heeft toegepast de gelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kunt je de melding aan de betrokkene achterwege laten. Dit is een strenge norm, die je van geval tot geval toe moet passen op basis van de actuele stand van de techniek. Als je twijfelt over de adequaatheid van de technische beschermingsmaatregelen die je heeft getroffen, dan moet je het datalek melden aan de betrokkene.

De Europese verordening 611/2013 geeft een nadere invulling aan adequate versleuteling. Volgens deze verordening mag u gegevens als onbegrijpelijk beschouwen als ze:

- op veilige wijze zijn versleuteld met een standaardalgoritme, de sleutel voor decryptie door geen enkele inbreuk gevaar heeft gelopen en de sleutel voor decryptie zodanig werd gegenereerd dat personen zonder geautoriseerde toegang de sleutel met de beschikbare technologische middelen niet kunnen vinden; of
- zijn vervangen door een met een cryptografisch versleutelde hashfunctie berekende hashwaarde, de sleutel die hiervoor werd gebruikt door geen enkele inbreuk gevaar heeft gelopen en deze voor datahashing gebruikte sleutel zodanig is gegenereerd dat personen zonder geautoriseerde toegang de sleutel niet kunnen vinden met de beschikbare technologische middelen.

Naast encryptie vermeldt de Nederlandse wetsgeschiedenis nog een andere technische beschermingsmaatregel waarmee persoonsgegevens kunnen worden beschermd tegen onbevoegde kennisname: het op afstand wissen van de gegevens die op een apparaat staan (*remote wiping*).

Een *remote wipe* heeft echter uitsluitend kans van slagen als er aan een aantal randvoorwaarden wordt voldaan. De eerste randvoorwaarde is dat de *remote wipe* tijdig in gang wordt gezet, zodat een eventuele aanvaller nog geen kans heeft gehad om kennis te nemen van de gegevens. Verder moet op dat moment het apparaat waar het om gaat nog intact zijn en werken, zodat het in staat is om de *remote wipe* uit te voeren en de gegevens te wissen. Ook moet de toepassing die voor

het wissen van de gegevens wordt gebruikt correct werken, zodat
alle gegevens waar het om gaat daadwerkelijk worden verwijderd en er ook geen sporen achterblijven waaruit de oorspronkelijke gegevens kunnen worden gereconstrueerd.

Ook als de gelekte gegevens gepseudonimiseerd zijn zult je op basis van de specifieke omstandigheden van het geval vast moeten stellen of er aan de norm uit het zesde lid van artikel 34a Wbp wordt voldaan. Pseudonimisering wil zeggen dat je technische maatregelen hebt genomen om te voorkomen dat de persoonsgegevens worden gekoppeld aan de oorspronkelijke identiteit van de betrokkene.

**JA:** (wel goed beveiligd) ga door naar stap 8.
**NEE:** (niet goed beveiligd) Er moet naast aan de AP ook aan betrokkenen worden gemeld, ga door naar stap 9.

## STAP 8:

Is de manier waarop de encryptie ongedaan gemaakt kan worden bekend gemaakt?

Aandachtspunten bij de beoordeling zijn:

- Het algoritme zelf, of de wijze waarop dit is toegepast, kunnen kwetsbaarheden vertonen waardoor de encryptie of de hashing niet de bescherming biedt die je daarvan verwacht.
- Encryptie is omkeerbaar. Een onbevoegde die over de juiste sleutel beschikt, of deze zonder al te veel moeite kan vinden, kan de gelekte gegevens ontsleutelen.
- Hashing is herhaalbaar. Als er bij hashing geen salt is toegepast, of als een onbevoegde over de gebruikte salt beschikt of deze zonder al te veel moeite kan vinden, kan hij de gebruikte hashingmethode toepassen op een lijst met veelgebruikte waarden en daardoor bijvoorbeeld gestolen wachtwoorden achterhalen.

**NEE:** Er moet alleen aan de AP gemeld worden en niet aan de betrokkenen gemeld worden.
**JA:** Er moet naast aan de AP ook aan betrokkenen worden gemeld, ga naar stap 9.

## STAP 9: MELDING BETROKKENEN

Er moet ook worden gemeld aan de *betrokkenen*. Dit moet 'onverwijld' gebeuren. Bij de melding aan de AP wordt een termijn afgesproken waarbinnen dit moet gebeuren. Deze termijn moet nagekomen worden. Bij melding worden minimaal de volgende gegevens verstrekt:

- de aard van de inbreuk (algemene omschrijving)
- de instanties waar de *betrokkene* meer informatie over de inbreuk kan krijgen (contactgegevens IB)
- en de maatregelen die IB de *betrokkene* aanbeveelt om te nemen om de negatieve gevolgen van de inbreuk te beperken (bijvoorbeeld wachtwoord wijzigen).

## TENSLOTTE

Alle datalekken moeten worden bijgehouden in een overzicht. Per datalek bevat het overzicht in ieder geval feiten en gegevens omtrent de aard van de inbreuk. Als het datalek is gemeld aan de *betrokkene*, dan wordt ook de tekst van de kennisgeving aan de *betrokkene* opgenomen in het overzicht. Het overzicht hoeft niet openbaar te worden gemaakt. Het overzicht moet minstens 1 jaar bewaard worden.

Er moet rekening mee worden gehouden dat een vervolgprocedure
na een datalek juridische maatregelen kan omvatten (civiel- of strafrechtelijk), en dat IB waar dat aan de orde is het bewijsmateriaal moet verzamelen, bewaren en presenteren overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

## 8. Bijlage: lijst van afkortingen en termen

| | |
|---|---|
| AP | Autoriteit Persoonsgegevens (voorheen CBP) |
| Betrokkene | de mensen van wie de persoonsgegevens zijn gelekt |
| Bewerker | verwerkt persoonsgegevens ten behoeve van de verantwoordelijke, zonder dat hij aan het rechtstreekse gezag van de verantwoordelijke is onderworpen. Dit kan ook een volgende partij in de keten zijn. |
| BSN | Burger Service Nummer |
| CBP | College ter Bescherming van Persoonsgegevens (nu AP) |
| IB | Inlichtingenbureau (in dit document niet: informatiebeveiliging) |
| Remote wipe | het op afstand wissen van de gegevens die op een apparaat staan |
| WBP | Wet bescherming Persoonsgegevens |
| Verantwoordelijke | degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt |

## 9. Bijlage: gebruikte informatiebronnen


- Autoriteit Persoonsgegevens, *De meldplicht datalekken in de Wet bescherming persoonsgegeven (Wbp), beleidsregels voor toepassing van artikel 34a van de Wbp*, 8 december 2015.
- College ter Bescherming van Persoonsgegevens, '*Meldplicht Datalekken in de Wet bescherming persoonsgegevens (Wbp) – consultatieversie*, 21 september 2015.
- Centrum voor Informatievoorziening en Privacybescherming, '*Meldplicht Datalekken*', herziende versie 0.2, november 2015.
- ICT Recht, '*Impact van de meldplicht datalekken*'

## 10.Bijlage: vragen webformulier

Dit webformulier is te vinden op https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?2. Bereid onderstaande vragen voor wanneer door uitval van systemen geen gebruik gemaakt kan worden van het webformulier. Het telefoonnummer van de Autoriteit Persoonsgegevens is 0900-3282535.

**Aard van de melding**

1. Is dit een vervolg op een eerdere melding? (Kies een van de volgende opties.)
    - Ja
    - Nee
2. Wat is het nummer van de oorspronkelijke melding? (Beantwoord deze vraag als u vraag 1 met ja hebt beantwoord.)
3. Wat is de strekking van de vervolgmelding? (Beantwoord deze vraag als u vraag 1 met ja hebt beantwoord, kies een van de volgende opties.)
    - Toevoegen of wijzigen van informatie betreffende de eerdere melding
    - Intrekking van de eerdere melding
4. Wat is de reden van intrekking? (Beantwoord deze vraag als u bij vraag 3 gekozen heeft voor optie b.)

**Wettelijk kader voor de melding**

5. Op grond van welke wettelijke bepaling doet u deze melding?
    - artikel 34a, eerste lid, van de Wbp
    - artikel 11.3a, eerste lid, van de Tw

**Algemene informatie en contactgegevens**

6. Over welk bedrijf of welke organisatie gaat het? (Vul de onderstaande gegevens in.)
    - Naam van het bedrijf of de organisatie
    - (Bezoek)adres
    - Postcode
    - Plaats
    - KvK-nummer
7. Door wie wordt het datalek gemeld? (Vul de onderstaande gegevens in.)
    - Naam van de persoon die meldt
    - Functie van de persoon die meldt
    - E-mailadres van de persoon die meldt
    - Telefoonnummer van de persoon die meldt
    - Alternatief telefoonnummer van de persoon die meldt
8. Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding? (Vul de onderstaande gegevens in indien dit iemand anders is dan de melder van het datalek.)
    - Naam contactpersoon
    - Functie van de contactpersoon

- E-mailadres van de contactpersoon
- Telefoonnummer van de contactpersoon
- Alternatief telefoonnummer van de contactpersoon

9. In welke sector is het bedrijf of de organisatie actief?

**Gegevens over het datalek**

10. Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.
11. Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk? (Vul de aantallen in.)
    - Minimaal: (vul aan)
    - Maximaal: (vul aan)
12. Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
13. Wanneer vond de inbreuk plaats? (Kies een van de volgende opties en vul waar nodig aan.)
    - Op (datum)
    - Tussen (begindatum periode) en (einddatum periode)
    - Nog niet bekend
14. Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen.)
    - Lezen (vertrouwelijkheid)
    - Kopiëren
    - Veranderen (integriteit)
    - Verwijderen of vernietigen (beschikbaarheid)
    - Diefstal
    - Nog niet bekend
15. Om welk type persoonsgegevens gaat het? (U kunt meerder mogelijkheden aankruisen.)
    - Naam-, adres- en woonplaatsgegevens
    - Telefoonnummers
    - E-mailadressen of andere adressen voor elektronische communicatie
    - Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam / wachtwoord of klantnummer)
    - Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
    - Burgerservicenummer (BSN) of sofinummer
    - Paspoortkopieën of kopieën van andere legitimatiebewijzen
    - Geslacht, geboortedatum en/of leeftijd
    - Bijzondere persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens)
    - Overige gegevens, namelijk (vul aan)
16. Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? (U kunt meerdere mogelijkheden aankruisen.)
    - Stigmatisering of uitsluiting
    - Schade aan de gezondheid
    - Blootstelling aan (identiteits)fraude

- Blootstelling aan spam of phishing
- Anders, namelijk (vul aan)

**Vervolgacties naar aanleiding van het datalek**

17. Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

**Inlichten van betrokkenen**

18. Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen? (Kies een van de volgende opties.)
    - Ja
    - Nee
    - Nog niet bekend
19. Wanneer heeft u het datalek gemeld aan de betrokkenen, of wanneer gaat u dit doen? (Beantwoord deze vraag als u vraag 18 met ja hebt beantwoord. Kies een van de volgende opties en vul waar nodig aan.)
    - Ik heb het datalek aan de betrokkenen gemeld op (datum)
    - Ik ga het datalek aan de betrokkenen melden op (datum)
    - Nog niet bekend
20. Wat is de inhoud van de melding aan de betrokkenen? (Letterlijke weergave, beantwoord deze vraag als u vraag 18 met ja hebt beantwoord.)
21. Hoe veel betrokkenen heeft u in kennis gesteld of gaat u in kennis stellen? (Beantwoord deze vraag als u vraag 18 met ja hebt beantwoord.)
22. Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken bij het in kennis stellen van de betrokkenen? (Beantwoord deze vraag als u vraag 18 met ja hebt beantwoord.)
23. Waarom ziet u af van het melden van het datalek aan de betrokkenen? (Beantwoord deze vraag als u vraag 18 met nee hebt beantwoord. Kies een van de onderstaande opties en vul waar nodig aan.)
    - De technische beschermingsmaatregelen die ik heb getroffen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten
    - Het is onwaarschijnlijk dat het datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, want: (vul aan)
    - Ik heb zwaarwegende redenen om de melding aan de betrokkene achterwege te laten, namelijk: (vul aan)
    - Anders, namelijk: (vul aan)

**Technische beschermingsmaatregelen**

24. Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?57 (Kies een van de volgende opties en vul waar nodig aan.)
    - Ja
    - Nee

- Deels, namelijk: (vul aan)

25. Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? (Beantwoord deze vraag als u bij vraag 24 gekozen heeft voor optie a of optie c. Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.)

**Internationale aspecten**

26. Heeft de inbreuk betrekking op personen in andere EU-landen? (Kies een van de volgende opties.)
    - Ja
    - Nee
    - Nog niet bekend
27. Heeft uw bedrijf of organisatie het datalek gemeld bij toezichthouders in een of meer andere EU-landen?
    - Ja, namelijk: (vul aan)
    - Nee

**Vervolgmelding**

28. Is naar uw mening deze melding compleet? (Selecteer een van de onderstaande opties.)
    - Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig
    - Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk