INFORMATIE
BEVEILIGINGS
DIENST

# Meldplicht Datalekken

**Alle bedrijven en overheden die persoonsgegevens verwerken zijn al sinds 1 januari 2016 verplicht om een ernstig datalek direct te melden aan de Autoriteit Persoonsgegevens. Tot nu toe was dat een verplichting die voortvloeide uit de Meldplicht Datalekken. Vanaf 25 mei 2018 is de AVG van kracht, in deze wet is de meldplicht integraal opgenomen. Deze factsheet biedt achtergrondinformatie over de Meldplicht Datalekken onder de nieuwe wetgeving en geeft onder andere antwoord op vragen als 'Wat houdt de Meldplicht Datalekken in?', 'Wat is een datalek en wanneer moet ik melding doen?' en 'Wie is aansprakelijk?'.**

## Wat houdt de meldplicht datalekken in?

Met de Meldplicht Datalekken wil de Europese wetgever de gevolgen van een datalek voor de betrokkenen zoveel mogelijk beperken en hiermee een bijdrage leveren aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens. Indien er sprake is van een ernstig datalek, waarbij kans is op verlies of onrechtmatige verwerking van persoonsgegevens, moet de verantwoordelijke het datalek te melden aan de Autoriteit Persoonsgegevens. In een aantal gevallen moet het datalek ook gemeld worden aan de betrokkenen. Als er ten onrechte geen melding wordt gemaakt van een datalek kan dit bestraft worden met een bestuurlijk boete door de Autoriteit Persoonsgegevens. Organisaties kunnen de beleidsregels Meldplicht Datalekken van de Autoriteit Persoonsgegevens gebruiken bij het bepalen of er sprake is van een datalek dat moet worden gemeld bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

## Wat is er veranderd door de AVG?

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde.[1]

- Datalekken hoeven niet meer bij de autoriteit gemeld te worden als het onwaarschijnlijk is dat een incident nadelige gevolgen kan hebben voor de persoonlijke levenssfeer van betrokkenen.[2]
- Elk (vermoeden van een) datalek moet in een datalekkenregister worden opgenomen
- Datalekken hoeven alleen nog aan betrokkenen gemeld te worden als er sprake is van een hoog risico op een inbreuk op de persoonlijke levenssfeer, voorheen was dit bij elk risico.
- De maximale boetes bij het niet naleven van de AVG zijn een stuk hoger dan onder de oude wetgeving. Ze kunnen nu gemakkelijker opgelegd worden door de toezichthouder.
- Een datalek zal dus minder vaak meldplichtig zijn maar moet wel nog altijd door de verantwoordelijke worden opgenomen in het eigen datalekkenregister.
- De praktijk zal nog moeten uitwijzen wanneer er precies sprake is van een hoog risico, dit zal de verantwoordelijke bij ieder datalek zelf moeten inschatten. Hierbij moeten de gevoeligheid van de gegevens en de kans op nadelige gevolgen voor betrokkenen beide worden meegenomen in de afweging.

## Wat is een datalek en wanneer moet ik melding doen bij de AP?

Een datalek is een informatiebeveiligingsincident waarbij sprake is van een inbreuk op de beveiliging van persoonsgegevens door blootstelling aan verlies of onrechtmatige verwerking. Bij een datalek is dus de eerste vraag altijd of er sprake is van een beveiligingsincident, als dit niet zo is dan is er ook geen sprake van een datalek. De constatering dat de beveiliging van persoonsgegevens in een bepaald geval niet helemaal in orde is of het versturen van persoonsgegevens via mail is dus niet meteen een datalek. Er is wel sprake van een datalek als persoonsgegevens verloren raken of onrechtmatige verwerking redelijkerwijs niet kan worden uitgesloten. Onder onrechtmatige verwerking valt onder andere het aanpassen en/of veranderen van persoonsgegevens en niet geautoriseerde toegang tot deze persoonsgegevens.  Er is dus niet alleen sprake van een datalek bij een inbraak door een hacker. Ook het kwijtraken van een USB-stick, de diefstal van een laptop, het verzenden van gevoelige gegevens naar een onjuist e-mailadres of het verlies van gegevens bij een brand in het datacentrum terwijl er geen back-up beschikbaar is, zijn voorbeelden van een datalek. Volgens de wet moet een 'ernstig' datalek, zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking, worden gemeld aan de Autoriteit Persoonsgegevens.

VNG Realisatie

Een lek kan ernstig zijn indien er persoonsgegevens van gevoelige aard zijn gelekt, bijvoorbeeld: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen of gegevens die betrekking hebben op godsdienst of levensovertuiging, ras, politieke gezindheid, of gezondheid. Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie er persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. De aard en omvang van het datalek spelen hierbij dus een belangrijke rol. Een gemeente hoeft geen melding te doen aan de Autoriteit Persoonsgegevens indien daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten.

## Wanneer moet ik melding doen bij de betrokkenen?

Een datalek moet aan de betrokkene worden gemeld als bij een inbreuk het risico groot is dat die inbreuk ongunstige gevolgen zal hebben voor diens privéleven. Ongunstige gevolgen voor de betrokkene zijn: aantasting in eer en goede naam, identiteitsfraude of discriminatie. Als de gemeente passende technische beschermingsmaatregelen heeft genomen, waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn gemaakt, is de melding aan de betrokkene niet nodig.
De melding aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste:

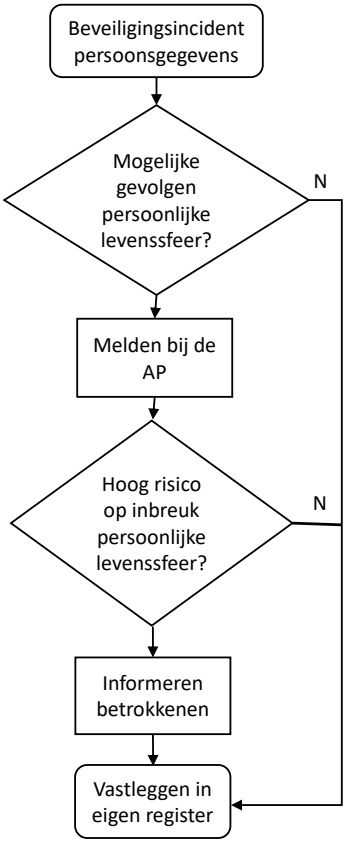
- de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

De beoordeling of een datalek gemeld moet worden aan de Autoriteit Persoonsgegevens en/of de getroffen personen, ligt te allen tijde bij de gemeente. Om te bepalen of een incident gemeld moet worden heeft de Autoriteit Persoonsgegevens beleidsregels[3] opgesteld en de werkgroep 29 van de Europese toezichthouders guidelines[4] gepubliceerd over de meldplicht in de AVG. Als de gemeente het datalek niet heeft gemeld kan de Autoriteit Persoonsgegevens verlangen dat de gemeente alsnog een melding doet. Het niet-melden kan worden bestraft met een bestuurlijke boete.

## Hoe meld ik een datalek?

De Autoriteit Persoonsgegevens stelt een webformulier beschikbaar dat gebruikt moet worden voor het melden van datalekken.[5] De Autoriteit Persoonsgegevens houdt een register bij van de ontvangen datalekmeldingen. Dit register is niet openbaar. Als er door de Autoriteit Persoonsgegevens een boete opgelegd wordt naar aanleiding van het datalek, wordt dit besluit wel openbaar gemaakt. Een datalek wordt ook openbaar gemaakt op het moment dat betrokkenen geïnformeerd moeten worden over het datalek. Bij de melding aan de betrokkene moet in ieder geval worden aangegeven wat de aard van de inbreuk is en de instanties waar de betrokkene meer informatie, over de inbreuk, kan krijgen. Verder moet aangegeven worden wat de betrokkene zelf kan doen om de negatieve gevolgen van het datalek te beperken. Bijvoorbeeld het veranderen van gebruikersnamen en wachtwoorden wanneer deze door de inbreuk mogelijk gecompromitteerd zijn.

**Stroomschema Meldplicht Datalekken**




## Wat moet ik melden?

Een melding aan het Autoriteit Persoonsgegevens omvat:

- De melder van het datalek.
- Degene met wie de Autoriteit Persoonsgegevens contact op kan nemen voor nadere informatie over de melding.
- Een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.
- Het tijdstip van de inbreuk.
- De aard van de inbreuk.
- Het type persoonsgegevens waarover het gaat.
- De gevolgen die de inbreuk kunnen hebben voor de persoonlijke levenssfeer van de betrokkenen.
- De technische en organisatorische maatregelen die de gemeente heeft getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen.
- Of de gemeente het datalek gemeld heeft aan de betrokkenen en zo niet, of de gemeente van plan is dit te gaan doen:
- Zo ja, de inhoud van de melding aan de betrokkenen.
- Zo nee, de reden waarom de gemeente afziet van het melden van het datalek aan de betrokkenen.
- Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

## Advies IBD met betrekking tot de meldplicht datalekken

Om goed voorbereid te zijn op de Meldplicht Datalekken heeft de IBD een aantal concrete adviezen. Deze adviezen hangen nauw samen met de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

- Zorg voor bewustwording bij medewerkers. Ook zij dienen te weten wat datalekken zijn, bij wie ze dit binnen de gemeente moeten melden en wat de gevolgen kunnen zijn van een datalek voor de gemeente.
- Stimuleer veilige methoden om data te delen. Uit analyse van gemelde datalekken blijkt dat deze vaak ontstaan door het onzorgvuldig omgaan met email.
- Zorg binnen de gemeente voor een veilige omgeving voor het melden van datalekken, beloon melders van datalekken en straf ze niet.
- Leg een register van datalekken aan en vermeld daarin ook de niet gemelde datalekken/incidenten.
- Bij een datalek dat openbaar is of dreigt te worden is goede crisiscommunicatie van groot belang. De IBD kan u hierbij helpen, aarzel niet om daar gebruik van te maken.
- Sluit een verwerkersovereenkomst af indien uw gemeente gebruikmaakt van een Clouddienstverlener. De IBD biedt een standaard verwerkersovereenkomst template met relevante artikelen over de meldplicht onder de AVG.
- Draag zorg voor encryptie van persoonsgegevens om te voorkomen dat bij een datalek de gegevens kunnen worden gelezen door een derde. Dit geldt voor persoonsgegevens in transport en in opslag.
- Richt een incidentmanagementproces in om ervoor te zorgen dat bij incidenten tijdig en doeltreffend kan worden gehandeld.
- Zorg voor passende procedures en technische maatregelen om een datalek te kunnen ontdekken. Denk hier aan de incidentprocedure, logging en monitoring/analyseren van de logging.

## Welke gegevens leg ik als gemeente zelf vast over een datalek

De gemeente moet een administratie bijhouden van alle datalekken[6], dus ook van de datalekken die niet gemeld hoeven te worden. Per datalek moeten in ieder geval de feiten en de gegevens omtrent de aard van de inbreuk worden vastgelegd. Bijvoorbeeld de oorzaak van het datalek, de soort gegevens die gelekt zijn, het moment dat het lek is ontdekt en op welke wijze het lek gedicht is. Wanneer het datalek is gemeld aan de betrokkene, dan moet ook de tekst van de kennisgeving aan de betrokkene in de administratie opgenomen worden. Voor het bewaren van de administratie kan worden uitgegaan van een minimale bewaartermijn van één jaar.

## Wie is verantwoordelijk?

Veel gemeenten laten de verwerking van hun persoonsgegevens geheel of gedeeltelijk uitvoeren door derden, een zogeheten 'verwerker'.[7] Van verwerking door een verwerker is bijvoorbeeld sprake bij het verwerken van persoonsgegevens in de cloud of bij externe hosting van een website waar persoonsgegevens worden verwerkt. Indien een gemeente persoonsgegevens laat verwerken door een verwerker, dan moet de gemeente ervoor zorgen dat de verwerker maatregelen treft, die nodig zijn zodat de gemeente aan de Meldplicht Datalekken kan voldoen. Bijvoorbeeld door de gemeente tijdig en adequaat te informeren over de datalekken waarvan de verwerker kennis krijgt. Er moeten schriftelijke afspraken worden gemaakt waarin wordt vastgelegd op welke wijze de gemeente door de verwerker op de hoogte wordt gesteld van een datalek.

Deze afspraken kunnen worden opgenomen in een verwerkersovereenkomst. Als verantwoordelijke blijft de gemeente eindverantwoordelijk voor de melding van een datalek aan de Autoriteit Persoonsgegevens.

## Wie is aansprakelijk?

De bestuurder van een gemeente is aansprakelijk voor de eventuele schade die ontstaat bij een datalek en moet hiervan melding te doen aan de Autoriteit Persoonsgegevens en eventueel bij de betrokkenen.

### Verwijzingen

1 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/voorbereiding-op-de-avg#stap-7-meldplicht-datalekken-5897

2 idem

3 https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/thematische-beleidsregels/beleidsregels-meldplicht-datalekken-2015

4 http://ec.europa.eu/newsroom/document.cfm?doc_id=47741

5 autoriteitpersoonsgegevens.nl

6 Artikel 33 lid 5 AVG

7 Zie ook: https://www.informatiebeveiligingsdienst.nl/faq/wanneer-ben-ik-een-verwerkersverantwoordelijke/ en https://www.informatiebeveiligingsdienst.nl/faq/wanneer-ben-ik-een-verwerker/

### Meer informatie

Meer informatie over onze dienstverlening vindt u in de andere factsheets van de IBD en op de website www.IBDgemeenten.nl. Hier kunnen gemeenten bovendien via de community relevante informatie met elkaar delen, vragen aan elkaar stellen en documenten uitwisselen. De helpdesk van de IBD is te bereiken tijdens kantooruren van 9:00 tot 17:00 uur op het nummer 070 204 55 11 of via het e-mailadres info@IBDgemeenten.nl. Tijdens deze kantooruren reageert de IBD binnen 30 minuten op een incidentmelding. Buiten kantooruren is de IBD op hetzelfde nummer bereikbaar voor spoedeisende meldingen en zal de IBD binnen 60 minuten reageren op een telefonische oproep.