

Procedure datalekkenbeleid

5.12.e

Vastgesteld in DB 2025-0128

1.1.1 Versiebeheer en distributie

Versie	Datum	Beschrijving van de wijziging	Auteur
0.1	4 nov 2024	Nieuwe versie procedure na evaluatie 2022-2024	TKNG
0.5	19 dec 2024	Definitief concept voor review PC en FG	TKNG
0.9	16 jan 2025	Definitieve versie	TKNG
1.0	20 jan 2025	Definitieve versie voor DB	TKNG
1.1	28 jan 2025	Definitief, na DB 28 januari	TKNG
		Geplande update: juli-aug	

Versie	Distributie
0.1	PC, FG
0.5	PC, FG, Directeur BSB en Hoofd BSB-Beleid, Hoofddirecteur BVS
0.9	FG (voor FG paragraaf)
1.0	DB
	Directiebestuur ter vaststelling en publicatie via intranet.

projectnummer

15 januari 2025

Inhoudsopgave

1.	Inleiding	4
2.	Datalekken, datalekregister en het Datalekken Response Team	5
2.1.	Wat is een datalek?	5
2.2.	Waarom is het belangrijk om een datalek te melden?	5
2.3.	Wat is het Datalekregister	6
2.4.	Wat is het Datalekken Response Team (DRT)	6
3.	De stappen bij een datalek	7
3.1.	Het datalek melden	7
3.2.	Overzicht krijgen (factfinding) voor risicobeoordeling	8
3.3.	Mogelijke schade/gevolgen beperken	8
3.4.	Beoordelen of er een melding aan de AP gedaan moet worden – en uitvoeren	9
3.5.	Beoordelen of betrokkenen geïnformeerd moeten worden – en uitvoeren	9
3.6.	Het registreren in het datalekregister	9
3.7.	Afsluiten datalek melding en vervolg	10
	Bijlage 1: Begrippenlijst en afkortingen	11

1. Inleiding

Het CBS verwerkt gegevens over alle burgers en bedrijven in Nederland. Een datalek kan daarom aanzienlijke gevolgen hebben voor de personen van wie de gegevens zijn gelekt. Ook voor het CBS zelf als betrouwbare overheidsorganisatie kan een datalek ernstige gevolgen hebben. Als de samenleving geen vertrouwen meer heeft in het CBS en geen gegevens meer wil afstaan, kan het CBS geen statistieken meer maken. Duidelijk beleid en een goed ingerichte datalekprocedure is daarom van groot belang. Het draagt bij aan het beter beschermen van persoonsgegevens door een snelle en adequate reactie op een datalek, het detecteren van aanwezige risico's en het leren van de datalekken die geweest zijn.

Een datalekkenregistratie en de meldplicht datalekken is daarnaast ook wettelijk verplicht. Art. 33 van de Algemene Verordening Gegevensbescherming (AVG) stelt dat iedere organisatie een datalekregister moet bijhouden. Vóór 2022 was de datalekprocedure meegenomen in de algehele Regeling beveiligingsincidenten en datalekken. Door de toenemende aandacht voor privacybescherming binnen de gehele rijksoverheid is in 2022 besloten de gehele datalekprocedure en het datalekregister te professionaliseren in een apart beleidsstuk. Het proces van melden is sindsdien eenvoudiger en laagdrempeliger geworden en er is beter overzicht door middel van een jaarlijkse CBS-brede verantwoording. In deze versie van 2025 ligt de focus op het CBS beleid hoe om te gaan met het melden, opvolgen en registreren van datalekken.

2. Datalekken, datalekregister en het Datalekken Response Team

2.1. Wat is een datalek?

De term 'datalek' komt niet voor in de wet. In de plaats daarvan heeft de Algemene verordening gegevensbescherming (AVG) het over een 'inbreuk in verband met persoonsgegevens'. De inbreuk leidt, al dan niet per ongeluk, tot **ongeoorloofde vernietiging, verlies, wijziging of verstrekking van, of toegang tot persoonsgegevens (artikel 4, punt 12, AVG)**. Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon wordt gerekend tot persoonsgegevens en elke inbreuk in verband met persoonsgegevens wordt een datalek genoemd. In deze procedure spreken we daarom voor het gemak over datalekken.

Wat zijn persoonsgegevens?

De AVG definieert een persoonsgegeven als 'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon'. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is, ook als deze gegevens versleuteld of gepseudonimiseerd zijn. Denk hierbij ook aan (werk) mailadressen, IP-adressen of locatiegegevens.

Het CBS is volgens de Wet CBS verplicht de nodige technische en organisatorische voorzieningen te treffen ter beveiliging van alle gegevens (zowel persoons- als bedrijfsgegevens) tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van die gegevens. De Functionaris Gegevensbescherming (FG) houdt dan ook onafhankelijk toezicht op de verwerkingen van persoonsgegevens bij het CBS. Daarnaast heeft het CBS ervoor gekozen de FG ook toezicht te laten houden op bedrijfsgegevens bij het CBS. Om deze reden worden alle inbreuken in verband met persoons- en bedrijfsgegevens behandeld als een datalek.

Voorbeelden van mogelijke datalekken bij het CBS:

- het doorsturen van persoonsgegevens naar een verkeerde ontvanger;
- een microdatabestand in een verkeerde map zetten;
- een mailtje met cc naar de verkeerde externe personen sturen, ook als er geen inhoudelijke data in staat;
- publicatie van herleidbare personen of bedrijven;
- onjuiste rechten of onjuiste toegang tot persoonsinformatie (zowel microdata als gegevens over het personeel);
- onrechtmatigheid verwerking, bijvoorbeeld geen juiste grondslag of doelbinding of het inschakelen van een verwerker zonder verwerkersovereenkomst.

Datalekken die door andere organisaties veroorzaakt zijn moeten ook gemeld worden. Denk bijvoorbeeld aan databestanden die we via de mail krijgen in plaats van via een beveiligde uploadportal. Ook al is het geen datalek van het CBS, het CBS kan hiermee wel andere organisaties helpen en ervan leren. Bovendien kan het soms ook risico's bij het CBS aan het licht brengen, bijvoorbeeld dat onze communicatie over het aanleveren van databestanden verbeterd moet worden.

2.2. Waarom is het belangrijk om een datalek te melden?

Privacybescherming en informatiebeveiliging doen we met zijn allen. Hoe sneller een datalek bekend is, hoe sneller we dit kunnen oplossen en hoe kleiner het risico is. Alle medewerkers leveren dus een belangrijke bijdrage aan de beveiliging van het CBS door een datalek zo snel mogelijk te melden.

Sommige datalekken zijn zo klein dat dit voor (bijna) geen schade zorgt. Andere datalekken daarentegen, hebben soms grote impact op veel mensen. We zijn als CBS verplicht om de schade zoveel mogelijk te beperken zodra we op de hoogte zijn van het datalek. In sommige

gevallen moeten de betrokkenen van een datalek op de hoogte worden gesteld. Afhankelijk van de (potentiële) impact van het datalek moet een datalek soms ook binnen 72 uur gemeld worden aan de Autoriteit Persoonsgegevens (AP).

Het melden van datalekken leidt nimmer tot sancties voor medewerkers, tenzij er opzet in het spel is. Het melden van alle mogelijke datalekken is erg belangrijk voor het zelflerend vermogen van het CBS en het melden wordt dan ook gestimuleerd. Zo maken we het CBS met z'n allen veiliger.

2.3. Wat is het Datalekregister

De AVG (art. 33) stelt dat iedere organisatie een Datalekregister moet opstellen en bijhouden. Volgens de AP is het doel van het Datalekregister dat de organisatie:

- leert van eerdere datalekken en bewust is van datalekken uit het verleden;
- effectieve maatregelen neemt om de kans op nieuwe, soortgelijke datalekken te verminderen;
- met het Datalekregister aan de AP kan laten zien dat de organisatie zich houdt aan de AVG.

In het Datalekregister moeten alle inbreuken vermeld worden die er in de organisatie zijn geweest. Dat zijn dus zowel de gemelde als niet-gemelde datalekken bij de AP, zowel de datalekken met gevoelige informatie als met niet gevoelige informatie. Het datalekregister wordt beheerd en ingevuld door het Datalekken Response Team van het CBS.

2.4. Wat is het Datalekken Response Team (DRT)

Wanneer er een datalek gedetecteerd wordt moet het CBS verschillende stappen zetten om het datalek zo snel mogelijk te beëindigen, risico's te analyseren en de gevolgen te beperken. De verantwoordelijkheid voor het uitvoeren van de stappen ligt bij de manager waar het datalek onder valt, in dit beleidsstuk de 'eigenaar' genoemd. De eigenaar wordt bij elke stap ondersteund en geadviseerd door het DRT.

Voor hulp, ondersteuning en advies heeft het CBS het DRT bestaande uit de Chief Privacy Officer en de Privacy Coördinatoren van het CBS. Het DRT heeft kennis en ervaring op het gebied van privacybescherming en datalekken, adviseert de eigenaar na een melding van een datalek en registreert het datalek en de opvolging in het datalekregister.

Het DRT zal indien nodig bij een datalekmelding andere experts betrekken (bijvoorbeeld de Functionaris Gegevensbescherming (FG), juristen of CCN-corporate) of direct escaleren in de lijn. Tijd is van essentieel belang bij het stopzetten en het beperken van de gevolgen van een datalek. Het DRT moet bij een melding alle medewerking krijgen vanuit de organisatie zodat er een snelle en zorgvuldige risico inschatting gemaakt kan worden. Alleen dan kan er een correct advies en ondersteuning gegeven worden over de benodigde maatregelen die getroffen moeten worden en of een melding gedaan moet worden aan de AP of aan betrokkenen.

De FG is als interne toezichthouder geen onderdeel van het DRT, maar zal gevraagd en ongevraagd advies geven. Het DRT betreft de FG altijd bij datalekken met potentieel grote gevolgen voor betrokkenen.

3. De stappen bij een datalek

Wanneer er een mogelijk datalek gedetecteerd wordt moet het CBS zeven stappen doorlopen. In elke stap heeft het DRT en de eigenaar (verantwoordelijk manager) een rol en verantwoordelijkheid.

1. **Het datalek melden**
2. **Overzicht krijgen (factfinding) voor risicobeoordeling**
 - DRT: voert een korte risicobeoordeling uit.
 - Eigenaar: zorgt voor alle informatie en beantwoordt alle vragen van het DRT.
3. **Mogelijke schade/gevolgen beperken;**
 - DRT: stelt maatregelen voor en adviseert over de werkwijze.
 - Eigenaar: verantwoordelijk voor het uitvoeren van de maatregelen.
4. **Beoordelen of er een melding aan de AP gedaan moet worden – en uitvoeren**
 - DRT: betreft de FG voor advies beoordeling melding aan AP.
 - Eigenaar: besluit wel/niet melden aan AP.
 - Eigenaar en DRT: beslissen in overleg wie de melding doet.
5. **Beoordelen of betrokkenen geïnformeerd moeten worden – en uitvoeren**
 - FG: geeft advies aan DRT.
 - DRT: beoordeelt of betrokkenen geïnformeerd moeten worden en geeft advies en ondersteuning.
 - Eigenaar: informeert de betrokkenen.
6. **Het registreren in het datalekregister**
 - DRT: registreert het datalek en alle acties gedurende het proces in het datalekregister.
7. **Afsluiten datalek melding en vervolg**
 - DRT: sluit datalek melding als alle acties opgevolgd zijn.

Hieronder staat per stap een uitgebreide toelichting beschreven. Hoewel de stappen in een logische volgorde beschreven zijn kan dit in de praktijk soms anders lopen, stappen worden vaak synchroon uitgevoerd of in een andere volgorde. Zo kan bijvoorbeeld een datalek al beëindigd worden voordat de risicobeoordeling rond is, of is het nodig direct een melding aan AP of betrokkenen te doen terwijl er nog aanvullende maatregelen getroffen worden. Bij een datalek melding is tijdig reageren essentieel.

3.1. Het datalek melden

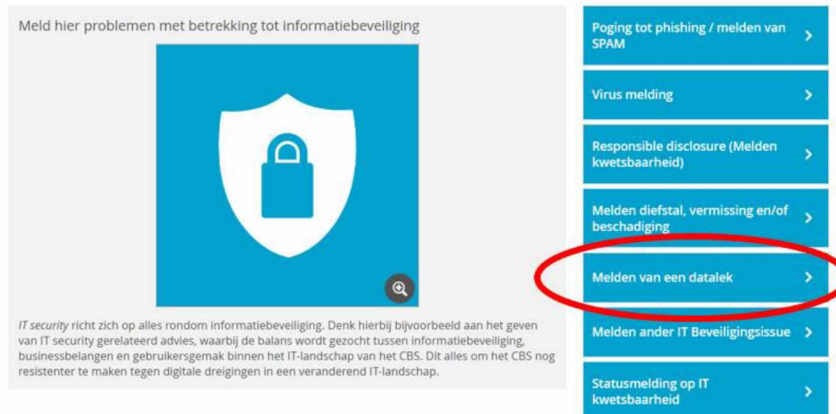
Elke medewerker kan een datalek melding doen. Wanneer je een datalek detecteert, meld je dit direct bij je leidinggevende én in TOPdesk. Je leidinggevende kan dit in de lijn opschalen indien nodig of naar een andere manager overdragen indien de verantwoordelijkheid elders ligt. De verantwoordelijk manager (vanaf nu 'eigenaar' genoemd) is uiteindelijk verantwoordelijk voor het opvolgen van de adviezen en uitvoeren van de maatregelen om het datalek te stoppen en de schade te beperken.

De melding in TOPdesk is noodzakelijk voor de registratie van het datalek en de verwerking in het datalekregister (wat wettelijk verplicht is). Door het te melden in TOPdesk komt ook het DRT in actie voor ondersteuning, hulp en advies. Zet daarom zoveel mogelijk informatie in de TOPdesk melding.

Via de link op de Privacypagina [Datalekken](#) kom je direct op de pagina om een datalek te melden. In TOPdesk zijn de meldingen over incidenten in 3 hoofdgroepen ingedeeld, IT-security, facilitair en datalekken. Soms is het onduidelijk onder welke categorie het valt, of valt een incident onder meerdere categorieën. Het maakt in zo'n geval niet uit onder welke kop je de melding zet, achter de schermen wordt de melding doorgezet naar de andere behandelaarsgroepen. Het is altijd aan te bevelen om erbij te vermelden dat je een datalek vermoedt wanneer je de melding bij een andere categorie zet. Zo weet je zeker dat het ook tijdig doorgezet wordt naar het DRT.

STARTPAGINA > STORING MELDEN > BEVEILIGING & IT SECURITY > IT SECURITY

IT security



3.2. Overzicht krijgen (factfinding) voor risicobeoordeling

Wanneer een datalek melding binnenkomt bij TOPdesk beoordeelt het DRT of een melding ook een datalek is. Zo ja, dan wordt dit opgenomen in het datalekregister. Het DRT doet een risicobeoordeling op basis van de verkregen informatie. Daarvoor is overzicht van de gebeurtenis nodig die de eigenaar aan moet leveren aan het DRT. Denk aan vragen als:

- Om wat voor soort datalek gaat het, om wat voor soort gegevens, hoeveel gegevens?
- Wat is de oorzaak van het datalek?
- Wanneer is het datalek ontstaan en bestaat het lek nog steeds?
- Hoe lang na het ontstaan van het datalek is het ontdekt en hoe is het ontdekt?
- Hoeveel onbevoegden hadden bij benadering (mogelijk) toegang en gaat het om een bekende, betrouwbare ontvanger of mogelijk iemand met kwade bedoelingen?

Het DRT kijkt daarnaast of er nog aanvullende vragen zijn om een duidelijk beeld te krijgen wat de risico's zijn en wat de mogelijke impact is. Het DRT schakelt indien nodig andere experts in. Deze fase moet zo snel mogelijk gebeuren om de schade te beperken.

3.3. Mogelijke schade/gevolgen beperken

De allereerste stap is dat de eigenaar het datalek zo snel mogelijk stopt. Het DRT zal dit controleren. Als het datalek nog niet gestopt is geeft het DRT advies en ondersteuning om dit datalek zo snel mogelijk te stoppen.

Als het datalek gestopt is dan moet de eigenaar maatregelen nemen om de negatieve gevolgen voor betrokkenen te beperken. Welke maatregelen dat zijn zal afhangen van de risicoanalyse uit stap 2. Het DRT kan hierbij ondersteunen en adviseren. De uitvoering ligt bij de eigenaar.

Voorbeelden van maatregelen:

- o een gepubliceerd bestand offline halen;
- o een verkeerde ontvanger vragen om een bevestiging dat de gegevens uit een brief of e-mail zijn vernietigd;
- o een inlogcode plus password aanpassen/blokken zodat een verkeerde ontvanger geen gegevens kan inzien.

3.4. Beoordelen of er een melding aan de AP gedaan moet worden – en uitvoeren

Een datalek moet wettelijk binnen 72 uur gemeld worden aan de AP, tenzij het niet waarschijnlijk is dat er een hoog risico is voor betrokkenen. Bij het inschatten van dat risico kijkt het DRT naar hoe waarschijnlijk het is dat een risico zich voordoet, en wat de impact is als het inderdaad gebeurt. Denk hierbij aan factoren als:

- de aard van de inbreuk, gevoeligheid en omvang van de persoonsgegevens;
- of er persoonsgegevens gewist, gewijzigd of gelekt zijn?
- gemak waarmee personen kunnen worden geïdentificeerd;
- ernst van gevolgen voor personen;
- bijzondere persoonskenmerken of gegevens van kwetsbare personen.

Het DRT betreft hierbij altijd de FG. De FG zal als interne toezichthouder adviseren of er een melding aan de AP gedaan moet worden. De eigenaar en het DRT overleggen samen wie de melding doet. Bij een melding aan de AP zal de eigenaar vooraf altijd de DG inlichten.

3.5. Beoordelen of betrokkenen geïnformeerd moeten worden – en uitvoeren

Een datalek brengt een hoog risico met zich mee wanneer het kan leiden tot lichamelijke, materiële of immateriële schade voor de betrokken personen. In deze gevallen moet het datalek sowieso gemeld worden aan de AP en aan de betrokkenen, tenzij er sprake is van een uitzondering op de meldplicht.

Van een hoog risico is sprake als een datalek kan leiden tot bijvoorbeeld:

- discriminatie;
- identiteitsdiefstal of –fraude;
- financiële verliezen;
- reputatieschade: bijvoorbeeld bij een datalek met gegevens over problematische schulden, verslaving of prestaties op het werk.

Ook is er sprake van een hoog risico wanneer het datalek kan leiden tot:

- het ongeoorloofd ongedaan maken van gepseudonimiseerde persoonsgegevens;
- een aanzienlijk economisch of maatschappelijk nadeel.

Het DRT beoordeelt dit en betreft hierbij altijd de FG. Wanneer betrokkenen geïnformeerd moeten worden zal de FG hier altijd advies op geven. Bij externe betrokkenen zal het DRT ook het hoofd corporate communicatie betrekken voor advies. Het DRT doet een voorstel, het informeren doet de eigenaar zelf.

3.6. Het registreren in het datalekregister

Het datalekregister wordt beheerd door het DRT. Na de melding in TOPdesk en de beoordeling dat het hier om een datalek gaat, plaatst het DRT het datalek in het register. In dit register wordt alle informatie rondom risico's en acties bijgehouden totdat het datalek afgerond is en afgesloten. Alleen het DRT en de FG kunnen het datalekregister inzien. Wel maakt de CPO elk kwartaal op hoofdlijnen een rapportage over de datalekken van het afgelopen kwartaal voor de hoofddirecteuren en de DG. Indien er patronen ontstaan in de soort datalek meldingen, dan zal de CPO samen met de rest van het DRT onderzoeken of er verbetervoorstellen gedaan kunnen worden.

Zo tonen we aan dat we voldoen aan de AVG, behouden we overzicht welke datalekken we hebben gehad en kunnen we dit gebruiken voor verbetervoorstellen om toekomstige datalekken te voorkomen.

3.7. Afsluiten datalek melding en vervolg

Het DRT ondersteunt en adviseert de eigenaar bij het opvolgen van de benodigde actie. Het datalek kan alleen door het DRT worden afgesloten wanneer alle adviezen en acties opgevolgd zijn. Er zijn drie uitkomsten bij het afsluiten van een datalek melding.

1. Geen vervolgactie nodig

In dit geval is er geen vervolg, alle adviezen zijn opgevolgd en de maatregelen uitgevoerd.

2. Eigenaar heeft proces aangepast om toekomstige datalekken te voorkomen

In sommige gevallen blijkt het datalek te zijn ontstaan door een kwetsbaarheid in het proces zelf. Door de eigenaar is het proces direct aangepast. Een datalek zorgt in dit geval ervoor dat we als organisatie onszelf steeds verbeteren en continu leren.

3. Datalek is in het risicoregister gezet

Soms leidt een datalek tot het signaleren van een onderliggend risico. In dat geval is het datalek zelf wel afgerond, maar blijft er in een onderliggend proces een risico bestaan. In dat geval detecteert het DRT een risico. Het DRT geeft het advies aan de betreffende PC om dit risico in het risicoregister te zetten van de betreffende hoofddirectie en stuurt dit advies naar de PC, de verantwoordelijk manager en sluit het datalek af. De Privacy Coördinator van de betreffende hoofddirectie plaatst dit risico in het risicoregister.

Het risico staat nu in het risicoregister en het is aan de verantwoordelijk manager dit risico op te pakken volgens het reguliere risicomanagementproces.

Bijlage 1: Begrippenlijst en afkortingen

AP: Autoriteit Persoonsgegevens.

AVG: Algemene verordening gegevensbescherming; Verordening (EU) 2016/679 Van het Europees Parlement en de Raad, van 27 april 2016. In het Engels wordt dit de GDPR genoemd.

Betrokkene: degene op wie een persoonsgegeven betrekking heeft.

Bijzondere persoonsgegevens: persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging. Strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

CPO: Chief Privacy Officer.

Datalek: een 'inbreuk in verband met persoonsgegevens' dat leidt tot ongeoorloofde vernietiging, verlies, wijziging of verstrekking van, of toegang tot persoonsgegevens.

DRT: Datalekken Response Team

Eigenaar: verantwoordelijk manager waar het datalek onder valt.

FG: Functionaris Gegevensbescherming

Melding AP: de melding van een datalek aan de Autoriteit Persoonsgegevens

Persoonsgegeven: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, ook als deze gegevens versleuteld of gepseudonimiseerd zijn

PC: Privacycoördinatoren

Verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Dat is de Directeur-generaal van het CBS, decentraal gedelegeerd aan (hoofd)directeuren en teamhoofden.