

BIJLAGE 17 PROCES DATALEKKEN

INHOUDSOPGAVE

1.	Inleiding	2
1.1	Relatie met andere processen	2
1.2	Leeswijzer	3
2.	Rollen en verantwoordelijkheden	3
3.	Beschrijving werkproces 'Beoordelen en melden van datalekken'	4
3.1	Melding (mogelijk) datalek	5
3.2	Bijeenroepen Meldpunt en registreren van relevante data	5
3.3	Onderzoeken melding	6
3.4	Advies melden datalek	6
3.5	Besluit melden datalek	6
3.6	Melding	7
3.7	Registratie en afronding	7
4.	Bijlage A - Gegevens die nodig zijn voor een interne melding	8

1. Inleiding

Met ingang van 1 januari 2016 is de Wet meldplicht datalekken in werking getreden. De meldplicht datalekken geldt inmiddels op grond van de Algemene Verordening Gegevensbescherming (AVG) en verplicht onder meer tot het onverwijld melden van een datalek bij de Autoriteit Persoonsgegevens. Organisaties moeten zelf een beredeneerde afweging maken of een concreet datalek dat hen ter kennis komt onder het bereik van de wettelijke meldplicht valt.

De AVG stelt strengere eisen aan registratie. Ook datalekken die niet hoeven te worden gemeld, moeten worden geregistreerd met inbegrip van feiten over het datalek, de gevolgen daarvan en de genomen corrigerende maatregelen. De Autoriteit Persoonsgegevens moet met deze documentatie kunnen controleren of aan de meldplicht is voldaan.

Van een 'datalek' is sprake bij een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens. Kortgezegd is een datalek: een inbreuk in verband met persoonsgegevens. 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 beveiligingslek) die zou *kunnen* leiden tot een beveiligingsincident. Er heeft zich daadwerkelijk een beveiligingsincident voorgedaan en preventieve maatregelen waren niet toereikend om dit te voorkomen.

Enkele voorbeelden van beveiligingsincidenten zijn besmettingen met virussen en/of malware, pogingen om ongeautoriseerd toegang te krijgen tot informatie of systemen (hacken), verlies van een usb-stick met gevoelige informatie, diefstal van data of hardware of een gecompromitteerde mailbox.

Alleen datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht bij de Autoriteit Persoonsgegevens.

Het melden van een datalek is een verplichting van de verwerkingsverantwoordelijke in de zin van de AVG. Bij bedrijfsvoeringszaken zal dit de Vereniging het Interprovinciaal Overleg (hierna: IPO) zijn.¹ Bij opdrachten die wij voor opdrachtgevers (met name provincies) uitvoeren, zijn deze opdrachtgevers meestal de verwerkingsverantwoordelijke en het IPO verwerker. Het register van verwerkingsactiviteiten van het IPO zal uitsluitel bieden over de rol van het IPO als verwerkingsverantwoordelijke of verwerker. Het IPO moet de verwerkingsverantwoordelijke zonder onredelijke vertraging informeren zodra zij kennis heeft genomen van een inbreuk in verband met persoonsgegevens. Als dat is afgesproken bijvoorbeeld in een verwerkersovereenkomst, is het mogelijk (mede) namens de verwerkingsverantwoordelijke te melden.

De besluitvorming over de melding van een datalek bij het IPO gebeurt door de Directeur van het IPO. Om de Directeur van het IPO daarbij te ondersteunen is het interne Meldpunt Datalekken (hierna: het Meldpunt) ingericht. Dit Meldpunt wordt (parttime) bemenst door IPO medewerkers (de adviseur informatiebeveiliging, de bedrijfsjurist en twee plaatsvervangers) en zo nodig een communicatiemedewerker.

1.1 Relatie met andere processen

Het proces 'Beoordelen en melden datalek' is een proces dat parallel loopt aan een aantal andere processen, zoals het daadwerkelijk oplossen van het datalek. Voor het oplossen van

het lek dienen processen ingericht te worden en afspraken gemaakt te worden met de leveranciers van het IPO. Het dichten van het lek moet zo snel mogelijk gebeuren en parallel lopen aan het eventueel melden van het datalek bij de Autoriteit Persoonsgegevens.



Figuur 1 Proces beoordelen en melden datalek loopt parallel aan andere processen.

1.2 Leeswijzer

Dit document bevat in het eerstvolgende hoofdstuk een beschrijving van de rollen en verantwoordelijkheden bij datalekken. Daarna volgt een beschrijving van het werkproces 'beoordelen en melden van datalekken'. In het laatste hoofdstuk staan een aantal aandachtspunten.

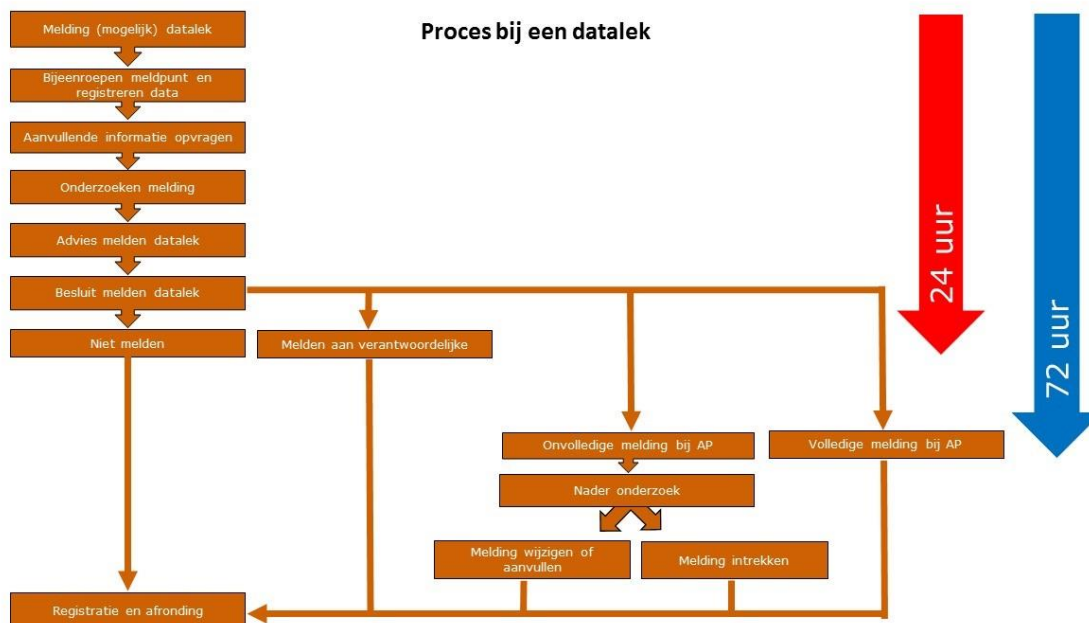
2. Rollen en verantwoordelijkheden

Rol	Verantwoordelijkheid
Adviseur informatiebeveiliging	Coördinator Meldpunt Datalekken; Risicobeheersing (informatieveiligheid); Coördinatie proces/bewaking voortgang; Bijhouden logboek; Formuleren advies van het Meldpunt aan de Directeur van het IPO; Inhoudelijke voorlichting melding; Doen van melding bij de Autoriteit Persoonsgegevens.
Bedrijfsjurist	Lid Meldpunt Datalekken; Risicobeheersing (juridisch); Formuleren advies van het Meldpunt aan de Directeur van het IPO; Juridisch voorlichting melding aan de Directeur van het IPO.
Communicatiemedewerker	Lid Meldpunt Datalekken bij mogelijke imagoschade of impact op betrokkenen; Wordt geïnformeerd bij kans op vragen van betrokkenen of de pers. Onderhoudt contacten met de pers. Adviseert over het contact met betrokkenen.
Incidentmelder	Melden incident aan het Meldpunt Datalekken bij voorkeur via het e-mailadres privacy@bij12.nl
Unitmanager / teamleider	Verantwoordelijk voor het oplossen en behandelen van het datalek / incident in zijn unit / team. Indien van toepassing: verantwoordelijk voor het melden van het datalek aan betrokkenen.
Directeur van het IPO	Besluit over melding aan de verwerkingsverantwoordelijke of de Autoriteit Persoonsgegevens op basis van het advies van het Meldpunt; Vastleggen besluit ten behoeve van logboek; Terugkoppelen besluit aan Meldpunt Datalekken; Zo nodig informeren MT van het IPO en de algemeen directeur van het IPO.
Autoriteit Persoonsgegevens	Nederlandse privacytoezichthouder waar datalekken gemeld moeten worden.

3. Beschrijving werkproces 'Beoordelen en melden van datalekken'

Beoordelen en melden van datalekken
Procesbeschrijving Het proces van de beoordeling en eventuele melding van een datalek bij de verwerkingsverantwoordelijke of de Autoriteit Persoonsgegevens (AP) dient 'onverwijld' te worden afgerond. Dat wil zeggen: in het geval van een (mogelijk) datalek, dient er z.s.m. na constatering van dit (mogelijke) datalek: • een besluit genomen te worden over het wel of niet melden, en zo ja; • binnen 24 uur na constatering gemeld te worden aan een verwerkingsverantwoordelijke; of • binnen 72 uur na constatering gemeld te worden aan de AP. Het Meldpunt adviseert op basis van een beredeneerde afweging of een geconstateerd datalek gemeld moet worden. Een melding kan na nader onderzoek of besluitvorming zo nodig worden aangevuld, gewijzigd of ingetrokken.
Input Interne melding van een (mogelijk) datalek, bijvoorbeeld in de vorm van een beveiligingsincident waarbij persoonsgegevens betrokken zijn. Deze melding kan gedaan worden in de vorm van bijvoorbeeld een telefoontje en/of een e-mail.
Output 1. Advies en besluit over het melden aan een verwerkingsverantwoordelijke, de Autoriteit Persoonsgegevens en zo nodig de betrokkenen. 2. Registratie datalek. 3. Melding aan de verwerkingsverantwoordelijke of de Autoriteit Persoonsgegevens. 4. Eventueel aanvulling, wijziging of intrekking van de melding. 5. Zo nodig melding aan betrokkenen.
Resultaat Conform de geldende regelgeving moet het IPO onverwijld een melding doen bij de Autoriteit Persoonsgegevens zodra zij een (potentieel) ernstig datalek heeft, waarvoor het IPO verwerkingsverantwoordelijke is. Is het IPO verwerker en is de provincie (of een andere opdrachtgever) verwerkingsverantwoordelijke, dan moet de verwerkingsverantwoordelijke in staat worden gesteld binnen 72 uur te melden bij de Autoriteit Persoonsgegevens. Het IPO kan ook (mede) namens de verwerkingsverantwoordelijke melden bij de Autoriteit Persoonsgegevens als dat is afgesproken, bijvoorbeeld in een verwerkersovereenkomst. Betrokkenen moeten door of namens de verwerkingsverantwoordelijke worden geïnformeerd over een inbreuk op hun persoonsgegevens als die grote risico's voor de rechten en vrijheden van de natuurlijke persoon met zich kan brengen, zodat hij de nodige voorzorgsmaatregelen kan treffen.
Wet- en regelgeving en kaders Algemene verordening gegevensbescherming; Uitvoeringswet Algemene verordening gegevensbescherming; Europese Guidelines meldplicht datalekken; Interprovinciale Baseline Informatieveiligheid / Baseline Informatiebeveiliging Overheid.
Informatiesystemen die het mogelijk maken om het proces uit te voeren F-schijf en Synergy (Logboek, naslagwerk) Microsoft Office (Word, Excel, Outlook, Exchange) Intranet IPO (procesbeschrijving) Helpdesksystemen van GBO provincies, PAS, etc. (incidentmelding en - afhandeling) Website Autoriteit Persoonsgegevens https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

Een overzicht van het proces bij een datalek is in *Figuur 2* weergegeven en in de hierop volgende paragrafen verder uitgewerkt.



Figuur 2 Overzicht van het proces bij een datalek.

3.1 **Melding (mogelijk) datalek**

Door: incidentmelder

Een interne melding van een beveiligingsincident vormt de input voor dit proces. Deze interne melding kan per e-mail, telefonisch of mondeling gedaan worden bij de leden van het Meldpunt. Bij voorkeur wordt een e-mail gestuurd naar privacy@bij12.nl. Zowel interne medewerkers als externe partijen (bijvoorbeeld leveranciers) kunnen deze melding doen.

Informatie die het Meldpunt nodig heeft van de melder (voorwaarden waaraan de melding moet voldoen):

- onderwerp bijvoorbeeld: "mogelijk datalek";
- naam, hoedanigheid en mobiel telefoonnummer indiener van de melding;
- datum en tijdstip ontdekking van de inbreuk op de beveiliging;
- beschrijving van het incident;
- indien mogelijk, een eerste inschatting van de impact van het incident;
- beschrijving van de persoonsgegevens die mogelijk zijn betrokken bij het incident.

3.2 **Bijeenroepen Meldpunt en registreren van relevante data**

Door: de adviseur informatiebeveiliging

Als er een melding van een incident is binnengekomen, is de eerste stap om de medewerkers van het Meldpunt bijeen te roepen. Het Meldpunt bestaat uit twee medewerkers: de adviseur informatiebeveiliging en de bedrijfsjurist. Zij analyseren de melding (juridische toets, risicobeheersing, informatieveiligheid). De adviseur informatiebeveiliging is verantwoordelijk voor het registreren van relevante data rondom het datalek. Ook wordt contact gezocht met de indiener van de melding om hem/haar op de hoogte te stellen.

Vanaf het moment dat er een melding van een datalek wordt gedaan bij het Meldpunt (input) wordt het logboek bij gehouden. De adviseur informatiebeveiliging is verantwoordelijk voor het bijhouden van dit logboek.

Ophalen van aanvullende informatie

Door: lid Meldpunt (de adviseur informatiebeveiliging)

Wanneer er nog onvoldoende informatie over de melding/het (potentiële) datalek beschikbaar is, kan het Meldpunt, indien nodig direct, aanvullende informatie ophalen. Dit kan bijvoorbeeld worden opgehaald bij de indiener van de melding, bij leveranciers (bijvoorbeeld 'logging' gegevens) of bij andere relevante stakeholders. Wanneer het ophalen van informatie moeilijkheden oplevert, kan er worden geëscaleerd via het MT IPO om zo wel de benodigde informatie te ontvangen.

3.3 Onderzoeken melding

Door: leden Meldpunt (de adviseur informatiebeveiliging en de bedrijfsjurist)

Na alle relevante informatie te hebben verzameld, onderzoekt het Meldpunt de melding. Daarbij hanteert het de Europese Guidelines Meldplicht datalekken. Hierbij wordt ook beoordeeld of het IPO of een opdrachtgever verwerkingsverantwoordelijke is.

3.4 Advies melden datalek

Door: leden Meldpunt (de adviseur informatiebeveiliging en de bedrijfsjurist)

Op basis van bovenstaand onderzoek bepaalt het Meldpunt of het incident gekwalificeerd moet worden als een datalek en of dit datalek geregistreerd en gemeld moet worden bij de verwerkingsverantwoordelijke of de Autoriteit Persoonsgegevens. Het Meldpunt brengt hierover een advies uit aan de Directeur van het IPO.

Het advies van het Meldpunt zal bestaan uit één van onderstaande opties:

1. Het incident is geen datalek: niet melden en niet registreren.
2. Het datalek niet melden maar wel registreren.
3. Het datalek melden én registreren:
 - a. melden aan de verwerkingsverantwoordelijke of de Autoriteit Persoonsgegevens;
 - b. melden aan de Autoriteit Persoonsgegevens én de verwerkingsverantwoordelijke en betrokkenen informeren;
 - c. eventueel de melding aanvullen, wijzigen of intrekken.

Wanneer er onvoldoende informatie beschikbaar is om vast te stellen of het een meldingswaardig datalek betreft of niet gewacht kan worden op besluitvorming, wordt zekerheidshalve een melding gedaan bij de Autoriteit Persoonsgegevens en wordt nader onderzoek gedaan. De melding kan later worden aangevuld, gewijzigd of ingetrokken.

Na ontdekking van een datalek moet binnen 24 uur worden gemeld aan de verwerkingsverantwoordelijke óf binnen 72 uur worden gemeld bij de Autoriteit Persoonsgegevens. Na een melding bij de Autoriteit Persoonsgegevens is er gelegenheid om aanvullend onderzoek te doen. Als dit onderzoek leidt tot een wijziging van het eerdere advies aan de Directeur van het IPO zal het Meldpunt een nieuw advies voorleggen aan de Directeur van het IPO. De Directeur van het IPO besluit naar aanleiding van het nieuwe advies over het aanvullen, wijzigen of intrekken van de melding aan de Autoriteit Persoonsgegevens en/of de melding aan betrokkenen.

3.5 Besluit melden datalek

Door: de Directeur van het IPO

De Directeur van het IPO maakt een afweging op basis van het advies van het Meldpunt om al dan niet te melden aan de verwerkingsverantwoordelijke of de Autoriteit Persoonsgegevens en eventueel betrokkenen. Het besluit wordt door de adviseur informatiebeveiliging vastgelegd in het logboek. Ook informeert het Meldpunt de indiener van de melding over dit besluit.

3.6 Melding

Door: de adviseur informatiebeveiliging

De melding aan een verwerkingsverantwoordelijke gebeurt zo mogelijk aan de Functionaris gegevensbescherming die via de website van de betreffende organisatie bekend is gemaakt.

De melding van het datalek aan de Autoriteit Persoonsgegevens gebeurt via de website van de Autoriteit Persoonsgegevens. Het betreffende formulier wordt ingevuld en verstuurd door de adviseur informatiebeveiliging (of zijn plaatsvervanger) of bij hun afwezigheid de bedrijfsjurist (of haar plaatsvervanger).

3.7 Registratie en afronding

Nadat de melding aan de verwerkingsverantwoordelijke of de Autoriteit Persoonsgegevens is gedaan, wordt er door de medewerkers van het Meldpunt een advies aan de unitmanager / teamleider geformuleerd. Het advies bevat gewenste acties, aandachtspunten en/of risico's, eventueel het informeren van de betrokkenen. De communicatiemedewerker kan hierbij adviseren.

De leden van het Meldpunt laten de indiener van de melding weten wie verantwoordelijk is voor de verdere afhandeling. De adviseur informatiebeveiliging werkt het logboek bij.

Bijlage A - Gegevens die nodig zijn voor een interne melding

Om een datalek bij het IPO Meldpunt Datalekken te melden zijn minimaal nodig:

- onderwerp bijvoorbeeld: "mogelijk datalek";
- naam, hoedanigheid en mobiel telefoonnummer indiener van de melding;
- datum en tijdstip ontdekking van de inbreuk op de beveiliging;
- beschrijving van het incident;
- indien mogelijk, een eerste inschatting van de impact van het incident;
- beschrijving van de persoonsgegevens die mogelijk zijn betrokken bij het incident.

De interne melding wordt bij voorkeur gedaan via een e-mail aan privacy@bij12.nl.