

Calamiteitenplan datalekken - Bedrijf X B.V.

Datum: 01-04-2019

Versie: 4

VOORBEELD

2. Wat is een datalek?

2.1. Introductie

Niet alle datalekken moeten gemeld worden aan de toezichthouder. Een datalek dat wel gemeld dient te worden aan de toezichthouder wordt als volgt in de AVG omschreven:

Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Onder de Algemene Verordening Gegevensbescherming (AVG) wordt een datalek een 'inbreuk in verband met persoonsgegevens' genoemd. In de praktijk noemen we dit echter vaak een datalek, maar hiermee wordt hetzelfde bedoeld. Een datalek moet worden gemeld, tenzij het onwaarschijnlijk is dat deze redelijkerwijs een risico voor betrokkenen met zich meebrengt.

Om te inventariseren of iets een datalek is, zullen de volgende vragen in deze volgorde moeten worden beantwoord:

1. Is er sprake van een inbreuk op de beveiliging ('beveiligingsincident')?
2. Zijn er bij de inbreuk persoonsgegevens verloren gegaan?
3. Zijn er persoonsgegevens op onrechtmatige wijze verwerkt?
4. Leidt het verloren gaan van de persoonsgegevens, of de onrechtmatige verwerking ervan, tot een (hoog) risico voor betrokkenen?

Iedere vraag is een stap in de beslissing of er sprake is van een datalek. Deze stappen zullen hieronder worden toegelicht.

2.2. Inbreuk op de beveiliging

Van een inbreuk op beveiliging is sprake wanneer zich daadwerkelijk een incident heeft voorgedaan. Alleen een dreiging van een inbreuk op de beveiliging is daarom nog geen incident.

Voorbeelden van beveiligingsincidenten zijn:

- een kwijtgeraakte USB-stick;
- een gestolen laptop;

- een mailing wordt verstuurd met alle e-mailadressen in de CC in plaats van in de BCC
- een inbraak door een hacker;
- een malware-besmetting;
- een calamiteit zoals een brand in een datacentrum.

Een inbreuk op de beveiliging wordt vervolgens een datalek wanneer de inbreuk gevolgen heeft voor de persoonsgegevens die Bedrijf X B.V. verwerkt.

2.3. Verlies van persoonsgegevens

Indien er door de inbreuk op de beveiliging persoonsgegevens verloren zijn gegaan waar geen complete en actuele reservekopie meer van is, is dit altijd te kwalificeren als een datalek.

Voorbeeld: Wanneer een database met klantgegevens door een fout van een programmeur of een medewerker van Bedrijf X B.V. wordt vernietigd, en er geen backup van deze gegevens is, is er sprake van datalek.

Daarnaast kan ook het tijdelijk niet beschikbaar zijn van persoonsgegevens resulteren in een datalek, wanneer een betrokkene hiervan mogelijk risico's ondervindt. Denk bijvoorbeeld aan de situatie waarin medische dossiers een tijd niet beschikbaar zijn in een ziekenhuis. Hierdoor moeten mogelijk operaties worden uitgesteld, en kunnen patiënten in levensgevaar komen. Ook dan kan er worden gesproken van een datalek dat resulteert in een (hoog) risico voor de betrokkenen (in dit geval de patiënten).

2.4. Onrechtmatige verwerking

Het is echter ook mogelijk dat gegevens onrechtmatig zijn verwerkt. Dit houdt bijvoorbeeld in dat onbevoegde personen toegang hebben verkregen tot gegevens waar zij geen toegang toe mochten hebben. Andere vormen van onrechtmatige verwerking zijn het onrechtmatig wijzigen/aantasten van persoonsgegevens en het verstrekken van persoonsgegevens aan onbevoegden. Het is in dat geval aan Bedrijf X B.V. om aan te tonen dat iemand de gegevens niet heeft in kunnen zien, of er niets mee gedaan heeft.

Wanneer Bedrijf X B.V. niet uit kan sluiten dat er persoonsgegevens verloren zijn gegaan, of onrechtmatig zijn verwerkt, is er sprake van een datalek.

Voorbeeld: Als er per ongeluk een e-mail met persoonsgegevens aan een verkeerd e-mailadres is toegestuurd en de verzender krijgt meteen een melding dat de e-mail niet is aangekomen omdat het e-mailadres niet bestaat, dan is dit geen datalek. Als de verzender echter geen foutmelding krijgt, is niet zeker te stellen dat de e-mail niet bij een onbevoegde persoon terecht is gekomen en is dit dus wel een datalek.

3. Wanneer moet het lek gemeld worden aan de toezichthouder

3.1. Introductie

Op het moment dat er sprake is van een datalek zoals omschreven in hoofdstuk 2, dan is het aan Bedrijf X B.V. om per vastgesteld datalek te beoordelen of het datalek aan de toezichthouder gemeld moet worden. De toezichthouder stelt dat een datalek aan haar gemeld moet worden indien “er sprake is van een risico voor de rechten en vrijheden van betrokkenen”.

Hieronder wordt dit criterium nader uitgewerkt.

3.2. Kwantitatief ernstig

Een lek kan een risico teweegbrengen zijn als het een grote hoeveelheid data betreft (kwantitatief ernstig). Zo zal een lek in één van de databases van Bedrijf X B.V., waardoor NAW-gegevens van bijvoorbeeld 1.000 klanten van Bedrijf X B.V. op straat komen te liggen, kwantitatief ernstig zijn en dus gemeld moeten worden aan de toezichthouder. In de AVG is niet vastgelegd hoeveel gegevens nu maken of het datalek kwantitatief ernstig is of niet. Dit zal dus per geval moeten worden beoordeeld. Hierbij kan gekeken worden naar: Hoeveel gegevens zijn gelekt? Hoeveel mensen zijn hierbij betrokken? En, hoeveel gegevens per persoon zijn gelekt?

3.3. Kwalitatief ernstig

Daarnaast kan een lek ook ernstig zijn indien er geen grote hoeveelheden persoonsgegevens gelekt zijn, maar het wel om gevoelige persoonsgegevens gaat (kwalitatief ernstig). Een paar voorbeelden van wat gevoelige persoonsgegevens zijn:

- inloggegevens;
- financiële gegevens;
- kopieën van identiteitsbewijzen;
- strafrechtelijke gegevens;
- gegevens die betrekking hebben op werkprestaties;
- gegevens die betrekking hebben op levensovertuiging;
- gegevens die betrekking hebben op gezondheid.

De categorie ‘gevoelige persoonsgegevens’ is dus breder dan de categorie ‘bijzondere persoonsgegevens’ uit de AVG. Bijzonder persoonsgegevens zijn gegevens waaruit iemands ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie

van een persoon, gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

De aard en omvang van het datalek dienen telkens in overweging genomen te worden bij de afweging of een lek aan de toezichthouder gemeld dient te worden. Vast staat in ieder geval dat zodra er gevoelige gegevens zijn gelekt dit te allen tijde gemeld zal moeten worden aan de toezichthouder vanwege de kwalitatieve ernst hiervan, ongeacht hoeveel gegevens van hoeveel personen gelekt zijn (kwantitatieve ernst).

Voorbeeld: door een lek in de database van Bedrijf X B.V. hebben onbevoegden korte tijd inzage in de gegevens van klanten, inclusief hun achterstallige betalingen. Een dergelijk lek van gevoelige gegevens dient aan de toezichthouder gemeld te worden.

3.4. Termijn

Het datalek dient zo snel mogelijk, maar uiterlijk binnen 72 uur na ontdekking door Bedrijf X B.V., aan de Autoriteit Persoonsgegevens gemeld te worden. Deze termijn start op het moment dat Bedrijf X B.V. met redelijke zekerheid kan vaststellen dat er sprake is van een inbreuk op de beveiliging waarbij persoonsgegevens zijn betrokken.

Een melding kan achteraf worden ingetrokken of aangepast, in het geval dat binnen 72 uur nog niet bekend is wat de precieze aard of omvang van het lek is. Wanneer dit het geval is, kan dit ook gewoon bij de melding worden aangegeven.

Een datalek kan zowel bij Bedrijf X B.V. ontstaan of bij één van haar verwerkers, op de hoogte raakt van het datalek. Een verwerker is een partij die ten behoeve van Bedrijf X B.V. persoonsgegevens verwerkt. Dit kan bijvoorbeeld de host van de website of een softwareleverancier zijn. Het is de verwerkingsverantwoordelijke die uiteindelijk de melding aan de toezichthouder doet, tenzij anders afgesproken. Het is dan ook van belang voor Bedrijf X B.V. om met haar verwerkers goede schriftelijke afspraken te maken over het melden van datalekken Bedrijf X B.V..

3.5. Waar te melden?

Een datalek dient via de website van de toezichthouder te worden doorgegeven. Voor Nederland kan dit via het [meldloket](#) op de website van de Autoriteit Persoonsgegevens. Bij dit invulformulier dienen diverse gegevens ingevuld te worden. Deze worden in hoofdstuk 4 nader uiteengezet.

- Wat is de aard van het incident?
 - o Apparaat (bijvoorbeeld telefoon of laptop), gegevensdrager (bijvoorbeeld USB-stick) of papier kwijtgeraakt of gestolen
 - o Brief of postpakket kwijtgeraakt of geopend retour ontvangen
 - o Hacking, malware (bijvoorbeeld ransomware) en/of phishing
 - o Persoonsgegevens bij oud papier gezet
 - o Persoonsgegevens nog aanwezig op een afgedankt apparaat of gegevensdrager (bijvoorbeeld USB-stick)
 - o Persoonsgegevens per ongeluk gepubliceerd
 - o Persoonsgegevens van verkeerde persoon getoond in portaal
 - o Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger
 - o Overig
- Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens is geweest.

Persoonsgegevens die betrokken zijn bij het datalek

- Om welk type persoonsgegevens gaat het? (Meerdere antwoorden mogelijk)
 - o Naam
 - o Geslacht, geboortedatum en/of leeftijd
 - o Burgerservicenummer (BSN)
 - o Contactgegevens
 - o Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord)
 - o Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
 - o Paspoortkopieën of kopieën van andere legitimatiebewijzen
 - o Locatiegegevens
 - o Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen
 - o Bijzondere persoonsgegevens (bijvoorbeeld ras, etniciteit, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens, genetische gegevens en biometrische gegevens)
 - o Overige/onbekende gegevens, namelijk (vul aan)
- Geef (eventueel bij benadering) aan hoeveel gegevensrecords ('gegevensregisters') zijn getroffen door de inbreuk.

De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

- Van welke groepen mensen zijn persoonsgegevens betrokken bij het datalek?
 - o Werknemers
 - o Klanten (huidig en potentieel)
 - o Leerlingen of studenten
 - o Patiënten
 - o Minderjarigen
 - o Personen uit kwetsbare groepen
- Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
- Van minimaal en maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

Maatregelen die zijn getroffen voordat het datalek plaatsvond

- Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?
- Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk waren gemaakt, om welk deel gaat dat dan?
- Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk waren gemaakt, op welke manier is dit dan gebeurd?

Gevolgen van het datalek

- Wat zijn de gevolgen van de inbreuk?
 - o Onbevoegden hebben kennis kunnen nemen van de gegevens
 - o De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt
 - o Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt binnen de eigen organisatie
 - o Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties
 - o Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen
 - o Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen
 - o Anders, namelijk [vul aan]
- Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?
 - o Discriminatie
 - o Identiteitsdiefstal of -fraude
 - o Financiële verliezen
 - o Reputatieschade
 - o Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens
 - o Ongeoorloofde ongedaanmaking van pseudonimisering
 - o Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen
 - o Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen
- Geef een inschatting van de ernst van de mogelijke gevolgen voor betrokkenen:
 - o Verwaarloosbaar
 - o Beperkt
 - o Aanzienlijk
 - o Zeer groot

Vervolgacties naar aanleiding van het datalek

- Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?
 - o Ja

5. Wanneer moet het lek worden gemeld aan de betrokkenen?

5.1. Introductie

Het kan mogelijk zijn dat een datalek niet alleen aan de toezichthouder, maar ook aan de personen van wie de gegevens zijn gelekt (de betrokkenen) gemeld moet worden. Dit is het geval wanneer het datalek een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen.

5.2. Ongunstige gevolgen

Een datalek heeft ongunstige gevolgen wanneer het privéleven van de betrokkenen door het lek wordt geschaad. Voorbeelden van dergelijke gevolgen zijn:

- onrechtmatige publicatie;
- aantasting in eer en goede naam;
- identiteitsfraude;
- discriminatie;
- stigmatisering of uitsluiting;
- schade aan de gezondheid;
- reputatieschade.

Als het gaat om gevoelige persoonsgegevens of wanneer er heel veel gegevens zijn gelekt, dan is er vrijwel altijd sprake van een hoog risico. Er dient dan altijd een melding aan betrokkenen gedaan te worden (tenzij er sprake is van adequate beveiliging, zoals omschreven in de volgende paragraaf). Dit betekent bijvoorbeeld, dat zodra er financiële gegevens worden gelekt die niet adequaat zijn beveiligd, hiervan te allen tijde melding aan de betreffende personen zal moeten worden gedaan.

Voorbeeld: een medewerker van Bedrijf X B.V. laat sollicitatiebrieven en CV's in een auto liggen en deze auto wordt gestolen. Identiteitsfraude met behulp van deze CV's is niet uit te sluiten en dus is een melding aan de betrokkenen verplicht.

5.3. Encryptie en hashing

Een datalek hoeft niet aan de betrokkenen gemeld te worden indien de gelekte 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 algemeen gebruikte vormen van encryptie of hashing.

Wanneer het datalek niet hoeft te worden gemeld aan de betrokkenen omdat de gegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan zal wel van tijd tot tijd moeten worden beoordeeld of de gegevens nog steeds onbegrijpelijk of ontoegankelijk zijn (zie ook hoofdstuk 7). Wanneer bijvoorbeeld niet hoeft te worden gemeld (omdat de gegevens encrypted zijn), maar de gebruikte encryptie na anderhalf jaar gecompromitteerd zou raken, moeten de betrokkenen dus alsnog worden ingelicht over het datalek. Er kan ook voor worden gekozen om de betrokkenen direct na het datalek tóch proactief te informeren. Zo wordt voorkomen dat ruime tijd na het datalek betrokkenen alsnog op de hoogte moeten worden gesteld.

Let op: encryptie of hashing biedt echter geen bescherming tegen vernietiging van persoonsgegevens. In dergelijke gevallen dient er dus altijd een melding gedaan te worden aan de betrokkenen als de vernietiging ongunstige gevolgen voor hen heeft.

5.4. Termijn

Het datalek dient 'onverwijld' na ontdekking aan de betrokkenen gemeld te worden. 'Onverwijld' wil zeggen: zo spoedig als 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 betrokkene moet zorgvuldig gebeuren, maar mag niet onnodig worden vertraagd. De AVG koppelt hier geen 'harde' termijn aan, zoals bij de melding aan de toezichthouder wel het geval is.

Het is de verantwoordelijke die de melding aan betrokkenen doet, tenzij anders afgesproken.

6. Wat te melden aan de betrokkenen?

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

- Aard van de inbreuk, waarbij volstaan kan worden met een algemene omschrijving van wat er is gebeurd;
- Waar men terecht kan met vragen, denk hierbij aan het telefoonnummer van de klantenservice of een speciaal telefoonnummer/e-mailadres voor vragen;
- Aanbevolen maatregelen om negatieve gevolgen te beperken, zoals het veranderen van wachtwoorden.

Het volgende algemene formulier kan als template worden gebruikt. Uiteraard is het daarbij verstandig om in een begeleidend schrijven de betrokkene excuses aan te bieden en duidelijk te maken dat Bedrijf X B.V. het datalek inmiddels heeft gedicht en er alles aan zal doen om dergelijke gevallen in de toekomst te voorkomen.

Melding datalek

Omschrijving	Op [DATUM] heeft er bij ons een datalek plaatsgevonden waarbij mogelijk uw gegevens betrokken zijn.
Vragen?	Voor vragen kunt u contact opnemen met [NAAM] via, [EMAIL] of [TELEFOON].
Wat kunt u doen?	Om de gevolgen van dit datalek te beperken raden wij u aan om [MAATREGELEN].

Uitgangspunt bij het doen van een dergelijke melding is dat dit op individuele basis dient te gebeuren. Als er bijvoorbeeld gegevens van klanten zijn gelekt, dan dient iedere klant hierover apart geïnformeerd te worden. Heeft een datalek een dusdanige omvang dat er een grotere groep wordt getroffen, dan kan er een e-mail rondgestuurd worden naar deze personen met het feit dat er een lek heeft plaatsgevonden. Vervolgens kan er in de e-mail een link opgenomen worden naar een pagina op de website waar meer informatie wordt verstrekt.

Een enkel bericht in de media is 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 écht 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.

7. Registratieplicht

Op het moment dat er sprake is van een datalek, ongeacht of deze wel/niet aan de toezichthouder en/of betrokkenen wordt gemeld, dient dit datalek intern te worden gedocumenteerd door Bedrijf X B.V. in de situaties waarin Bedrijf X B.V. ten aanzien van dit datalek is aan te merken als verwerkingsverantwoordelijke.

Voor het registreren van de datalekken zou door Bedrijf X B.V. een apart systeem kunnen worden ingericht, maar dit is niet vereist. Het enkel openen van een apart dossier voor het registreren van datalekken is hiertoe al voldoende.

Van datalekken die aan de toezichthouder zijn gemeld, dient door Bedrijf X B.V. de pdf van deze verzonden melding te worden bewaard evenals de eventuele melding die aan betrokkenen is gedaan. Wanneer het datalek niet aan de toezichthouder en/of betrokkenen is gemeld, dient hiervan de volgende informatie te worden geregistreerd:

- de feiten omtrent het datalek;
- de gevolgen; en
- de genomen corrigerende maatregelen.

Dit register dient voor de volgende doeleinden bewaard te worden:

- leren van het datalek;
- vragen van betrokkenen en derden beantwoorden;
- alsnog een melding aan betrokkenen doen, wanneer dit na verloop van tijd toch nodig blijkt;
- het mogelijk maken van een controle op de naleving van de meldplicht datalekken door de toezichthouder.

Voorbeeld: Een database met persoonsgegevens is voor korte tijd, door een hack, openbaar geweest. De persoonsgegevens in de database waren volgens de meest recente encryptiestandaard versleuteld en derhalve niet leesbaar voor mensen zonder de juiste autorisaties.

Na een half jaar blijkt echter dat de gebruikte encryptievorm door voortschrijdend inzicht achterhaald is. In dat geval zal er alsnog een melding aan de betrokkenen gedaan moeten worden van het datalek dat een half jaar geleden heeft plaatsgevonden.

NB: De administratie hoeft overigens niet openbaar gemaakt te worden. Deze dient enkel op verzoek van de toezichthouder aan de toezichthouder te worden verstrekt.

8. Interne procedure datalekken

8.1. Introductie

Een datalek kan bij Bedrijf X B.V. binnen de eigen organisatie ontstaan, maar ook bij een door Bedrijf X B.V. ingeschakelde derde (denk hierbij aan de leverancier van een CRM-systeem, de hoster, een ingeschakeld marketingbureau etc.). Wanneer een datalek zich voordoet, zal vastgesteld moeten worden waar het datalek zich heeft voorgedaan en hoe dit datalek uiteindelijk bij de toezichthouder en betrokkenen gemeld zal worden.

Dit zal bij Bedrijf X B.V. in eerste instantie de taak zijn van D. Atalek (Functionaris Gegevensbescherming). De contactgegevens van D. Atalek zijn opgenomen in paragraaf 8.5.

Uiteraard is het daarbij van belang dat alle betrokken personen, dus zowel het personeel van Bedrijf X B.V. als het personeel bij de ingeschakelde derden, een datalek kunnen identificeren. Het creëren van bewustzijn binnen het personeel van Bedrijf X B.V. is dan ook van groot belang. De ontdekker zal een incident te allen tijde moeten melden bij de hierboven genoemde persoon.

8.2. Intern datalek

Wanneer er binnen de eigen organisatie van Bedrijf X B.V. een datalek plaatsvindt, zal iedereen moeten weten hoe er gehandeld dient te worden zodat de melding van het datalek tijdig de juiste personen, en uiteindelijk de toezichthouder en betrokkenen bereikt.

Voor deze situatie dient het volgende pad te worden doorlopen. De ontdekker is degene die een (vermoedelijk) lek detecteert; dat kan iedere willekeurige medewerker van Bedrijf X B.V. zijn. De ontdekker meldt het lek aan D. Atalek (Functionaris Gegevensbescherming). D. Atalek zal vervolgens besluiten of het datalek al dan niet wordt gemeld.

Registratie

D. Atalek registreert de melding van de ontdekker. De volgende gegevens worden geregistreerd:

- Wie heeft er gemeld?
- Wat is er gemeld?
- Waar kwam de melding vandaan?
- Om welke data (gegevens) 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 is er gedaan om het incident op te lossen/in de toekomst te voorkomen?

Informeren directie

Vervolgens zal besloten worden door D. Atalek of het lek wordt gemeld aan de toezichthouder en de betrokkenen. Wanneer het datalek is gemeld aan de toezichthouder en/of de betrokkenen, dan zal D. Atalek zorgen voor de juiste interne administratie van het datalek (zie hoofdstuk 7). Wanneer Bedrijf X B.V. verwerker is en haar klant verantwoordelijke, is het van belang na te gaan welke afspraken over het melden van datalekken aan de klant er zijn gemaakt in een verwerkersovereenkomst.

8.3. Extern datalek

Een datalek kan ook buiten de organisatie van Bedrijf X B.V. plaatsvinden. Persoonsgegevens worden tenslotte met derde partijen gedeeld. Denk hierbij aan softwareleveranciers, partijen die ten behoeve van Bedrijf X B.V. websites leveren of ondersteunen bij de opslag van persoonsgegevens. Wanneer er bij deze derden een datalek plaatsvindt dient dit zo spoedig mogelijk aan Bedrijf X B.V. gemeld te worden. Momenteel hebben deze derden een zorgplicht om een lek waarvan zij op de hoogte zijn, bij Bedrijf X B.V. te melden. Onder de AVG wordt deze plicht ook expliciet benoemd.

In (sub)verwerkersovereenkomsten met deze derden dienen hier afspraken over vastgelegd te worden. Per externe partij dient Bedrijf X B.V. een vast contactpersoon te hebben om deze meldingen zo snel en gestroomlijnd mogelijk te laten verlopen. Dit kan dezelfde persoon zijn die binnen Bedrijf X B.V. wordt aangewezen als 'meldpunt' bij beveiligingsincidenten en/of datalekken, namelijk D. Atalek, of de contactpersoon van de betreffende derde partij die dit vervolgens intern zal doorgeven.

8.4. Melden aan betrokkenen

Als een datalek bij Bedrijf X B.V. bekend is, zal bepaald moeten worden op welke manier de melding, indien vereist, aan de betrokkenen (bijvoorbeeld leden) wordt gedaan. Dit calamiteitenplan kan daarbij als handleiding gebruikt worden. Wanneer de klant verantwoordelijke is en Bedrijf X B.V. verwerker, zal de klant zelf de melding aan betrokkenen moeten doen, tenzij anders afgesproken.

8.5. Contactgegevens

De volgende contactgegevens zijn van belang indien een datalek zich heeft voorgedaan. Neem altijd direct contact op met D. Atalek.

De contactgegevens zijn:

Functionaris Gegevensbescherming: D. Atalek, tel: 0201234567