CALAMITEITEN DATALEKKEN ADVIES IN PRIVATE LEASE

1. Inleiding

In de huidige privacywetgeving (de Algemene Verordening Gegevensbescherming, hierna: AVG) is een meldplicht datalekken opgenomen. Deze meldplicht verplicht organisaties om datalekken te melden bij de toezichthouder (de Autoriteit Persoonsgegevens) en, in sommige gevallen, ook bij de betrokkenen (de personen op wie de gegevens die zijn gelekt betrekking hebben, bijvoorbeeld leden, abonnees en/of medewerkers). Ook onder de Algemene Verordening Gegevensbescherming (AVG), die vanaf 25 mei 2018 van toepassing zal zijn, moeten datalekken gemeld worden.

In dit calamiteitenplan wordt omschreven op welke manier Advies in Private Lease omgaat met eventuele datalekken. In het plan is vastgelegd hoe en naar wie de meldingen intern doorgezet dienen te worden, wie verantwoordelijk is voor welke melding en hoe en in welke vorm de melding aan de toezichthouder en eventueel ook aan de betrokkenen wordt gedaan.
In dit beleidsplan worden de beleidsregels van de Autoriteit Persoonsgegevens vertaald naar praktisch en werkbaar beleid voor de onderneming.

Mochten toekomstige (wettelijke) wijzigingen/veranderingen aanpassing van dit document noodzakelijk maken, dan zal de verantwoordelijke binnen de onderneming deze aanpassing doorvoeren en het versienummer updaten.

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 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), die vanaf 25 mei 2018 de Wbp zal vervangen, wordt gesproken van een ‘inbreuk in verband met persoonsgegevens’. Dit is “een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens”. Een inbreuk hoeft niet te worden gemeld wanneer 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. Kan er redelijkerwijs worden uitgesloten dat er persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt?

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 de onderneming 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 de onderneming wordt vernietigd, en er geen back-up van deze gegevens is, is er sprake van datalek.

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 de onderneming om aan te tonen dat iemand de gegevens niet heeft in kunnen zien, of er niets mee gedaan heeft.

Wanneer de onderneming niet uit kan sluiten dat er persoonsgegevens verloren zijn gegaan, of onrechtmatig zijn verwerkt, is er sprake van een datalek.

Voorbeeld: Als een medewerker van de onderneming zijn wachtwoord van zijn e-mailbox op een briefje heeft geschreven en dit briefje kwijt is geraakt, kan dit een datalek zijn als de onderneming niet uit kan sluiten dat onbevoegden toegang hebben verkregen tot de e-mailbox van de medewerker. Kan de onderneming dit echter wel uitsluiten, bijvoorbeeld door het wachtwoord direct te resetten en in de logfiles te zien dat er in de tussentijd niemand heeft ingelogd, dan is dit geen 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 de onderneming 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 de onderneming, waardoor NAW-gegevens van bijvoorbeeld 1.000 klanten van de onderneming op straat komen te liggen, kwantitatief ernstig zijn en dus gemeld moeten worden aan de toezichthouder.

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 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.
Voorbeeld: door een lek in de database van de onderneming 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, aan de Autoriteit Persoonsgegevens gemeld te worden. Deze termijn start op het moment dat de onderneming, of één van haar verwerkers, op de hoogte raakt van het datalek. Een verwerker is een partij die ten behoeve van de onderneming persoonsgegevens verwerkt. Dit kan bijvoorbeeld de host van de website of een softwareleverancier zijn.

3.5. Waar te melden?
Een datalek dient via de website van de toezichthouder te worden doorgegeven. Dit kan 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.

4. Wat te melden aan de toezichthouder?
De Autoriteit Persoonsgegevens wil specifieke informatie ontvangen indien er sprake is van een datalek dat gemeld dient te worden. Onderstaand is deze vereiste informatie uiteengezet.

Over de onderneming

- Naam van het bedrijf
- (Bezoek)adres
- Postcode
- Plaats
- KvK-nummer
- Sector waarbinnen Advies in Private Lease actief is

Over de contactpersoon en melder

- Naam
- Functie
- E-mailadres
- Telefoonnummer en alternatief telefoonnummer

Over het datalek

1. Wat is de aard van het incident?
    - Apparaat (bijvoorbeeld telefoon of laptop), gegevensdrager (bijvoorbeeld USB-stick) of papier kwijtgeraakt of gestolen
    - Brief of postpakket kwijtgeraakt of geopend retour ontvangen
    - Hacking, malware (bijvoorbeeld ransomware) en/of phishing
    - Persoonsgegevens bij oud papier gezet
    - Persoonsgegevens nog aanwezig op een afgedankt apparaat of gegevensdrager (bijvoorbeeld USB-stick)
    - Persoonsgegevens per ongeluk gepubliceerd
    - Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger

2. Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.

3. Vond de inbreuk plaats in een verwerking die is uitbesteed aan een andere organisatie (de verwerker)?
    - Ja, namelijk:
    - Nee:

4. Naam van de organisatie waaraan de verwerking is uitbesteed.

5. Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk? (Vul de aantallen in.)
    - Minimaal: (vul aan)
    - Maximaal: (vul aan)

6. Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

7. Is het bekend wanneer de inbreuk plaats vond?

8. Is de exacte datum bekend wanneer de inbreuk plaats vond?

9. Exacte datum waarop de inbreuk plaats vond.

10. Startdatum van de periode waarbinnen de inbreuk plaats heeft gevonden.

11. Einddatum van de periode waarbinnen de inbreuk plaats heeft gevonden.

12. Wanneer werd de breuk ontdekt?

13. Wat is de aard van de inbreuk? (Meerdere antwoorden mogelijk.)
    - Lezen (vertrouwelijkheid)
    - Kopiëren
    - Veranderen (integriteit)
    - Verwijderen of vernietigen (beschikbaarheid)
    - Diefstal
    - Nog niet bekend

14. Om welk type persoonsgegevens gaat het? (meerdere antwoorden mogelijk)

- Naam-, adres- en woonplaatsgegevens
- Telefoonnummers
- E-mailadressen of andere adressen voor elektronische communicatie
- Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of lidnummer)
- Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
- Burgerservicenummer (BSN)
- 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/onbekende gegevens, namelijk (vul aan)

15. Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? (Meerdere antwoorden mogelijk.)

- Stigmatisering of uitsluiting
- Schade aan de gezondheid
- Blootstelling aan (identiteits) fraude
- Blootstelling aan spam of phishing
- Anders, namelijk (vul aan)

16. Welke technische en organisatorische maatregelen heeft de onderneming getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

17. Heeft de onderneming het datalek gemeld aan de betrokkenen of is de onderneming van plan dat te gaan doen?

- Ja
- Nee
- Nog niet bekend

Vraag 17 tot en met 20 dienen uitsluitend beantwoord te worden indien er een melding aan de betrokkenen gedaan dient te worden:

17. Wanneer heeft de onderneming het datalek gemeld aan de betrokkenen, of wanneer gaat De onderneming dit doen?

- De onderneming heeft het datalek aan de betrokkenen gemeld op (datum)
- De onderneming zal het datalek aan de betrokkenen melden op (datum)
- Nog niet bekend

18. Wat is de inhoud van de melding aan de betrokkenen?

19. Hoe veel betrokkenen heeft de onderneming in kennis gesteld of gaat de onderneming in kennis stellen?

20. Welk communicatiemiddel of welke communicatiemiddelen gebruikt de onderneming of gaat De onderneming gebruiken bij het in kennis stellen van de betrokkenen?

21. Waarom ziet de onderneming af van het melden van het datalek aan de betrokkenen?

- De technische beschermingsmaatregelen die de onderneming heeft 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) De onderneming heeft zwaarwegende redenen om de melding aan de betrokkene achterwege te laten, namelijk: (vul aan)
  - Anders, namelijk: (vul aan)

22. Waren de persoonsgegevens op het moment van het ontdekken van het datalek versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? (Kieseen van de volgende opties en vul waar nodig aan.)

- Ja
- Nee
- Deels, namelijk: (vul aan)

23. Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? Als de onderneming gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.

24. Heeft de inbreuk betrekking op personen in andere EU-landen? (Kies een van de volgende opties.)

- Ja
- Nee
- Nog niet bekend

25. Heeft de onderneming het datalek gemeld bij toezichthouders in een of meer andere EU-landen, of gaat de onderneming dit nog doen?

- Ja, namelijk: (vul aan)
- Nee

26. Is de melding naar het idee van de onderneming compleet?

- Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig
- Nee, er komt later een vervolgmelding met aanvullende informatie over dit datalek

Na het doen van een melding bij de toezichthouder, wordt er een bevestiging van deze melding getoond in de browser. De ontvangstbevestiging dient door de onderneming (als pdf) te worden afgedrukt en bewaard. In deze bevestiging staat tevens het nummer van de melding vermeld, dat noodzakelijk is om een melding te wijzigen en/of in te trekken.

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. Hetzelfde geldt uiteraard indien er gegevens van medewerkers van de onderneming zijn gelekt.

5.2. Ongunstige gevolgen

Een datalek heeft ongunstige gevolgen wanneer het privéleven van de betrokkenen door het lek wordtgeschaad. 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, 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 de onderneming 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 wetgeving 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 de onderneming 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. Administratie
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 de onderneming in de situaties waarin de onderneming ten aanzien van dit datalek is aan te merken als verwerkingsverantwoordelijke.

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

Van datalekken die aan de toezichthouder zijn gemeld, dient door de onderneming 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 de onderneming binnen de eigen organisatie ontstaan, maar ook bij een door De onderneming 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 de onderneming in eerste instantie de taak zijn van de beleidsbepaler (directeur/eigenaar).

De contactgegevens van de beleidsbepaler (directeur/eigenaar) zijn opgenomen in paragraaf 8.5. Uiteraard is het daarbij van belang dat alle betrokken personen, dus zowel het personeel van de onderneming als het personeel bij de ingeschakelde derden, een datalek kunnen identificeren. Het creëren van bewustzijn binnen het personeel van de onderneming 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 de onderneming 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 de onderneming zijn. De ontdekker meldt het lek aan de beleidsbepaler (directeur/eigenaar), waarop deze in overleg zal treden met met de afdeling ICT (Alle ICT taken behartigen van de onderneming). Naar aanleiding van dit overleg zal de beleidsbepaler (directeur/eigenaar) besluiten of het datalek al dan niet wordt gemeld.

Registratie

De beleidsbepaler (directeur/eigenaar) 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

Indien de beleidsbepaler (directeur/eigenaar) het incident kwalificeert als een datalek dat gemeld moet worden, stelt zij met de afdeling ICT mondeling en/of per mail op de hoogte van de volgende informatie:

- omschrijving van het incident (intern/extern datalek);
- de bij het incident betrokken gegevens;
- de achtergrond van de kwalificatie van het incident (waarom is het wel/geen datalek dat gemeld moet
- worden);
- de (mogelijke) gevolgen;

- wie er reeds zijn geïnformeerd;
- de te nemen vervolgstappen (melding aan de toezichthouder/betrokkenen).

Vervolgens zal besloten worden door de beleidsbepaler (directeur/eigenaar) 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 de beleidsbepaler (directeur/eigenaar) zorgen voor de juiste interne administratie van het datalek (zie hoofdstuk 7).

Wanneer de onderneming 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 de onderneming plaatsvinden. Persoonsgegevens worden tenslotte met derde partijen gedeeld. Denk hierbij aan softwareleveranciers, partijen die ten behoeve van de onderneming websites leveren of ondersteunen bij de opslag van persoonsgegevens.

Wanneer er bij deze derden een datalek plaatsvindt dient dit zo spoedig mogelijk aan de onderneming gemeld te worden. Momenteel hebben deze derden een zorgplicht om een lek waarvan zij op de hoogte zijn, bij de onderneming 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 de onderneming een vast contactpersoon te hebben om deze meldingen zo snel en gestroomlijnd mogelijk te laten verlopen. Dit kan dezelfde persoon zijn die binnen de onderneming wordt aangewezen als ‘meldpunt’ bij beveiligingsincidenten en/of datalekken, namelijk de beleidsbepaler (directeur/eigenaar), of de contactpersoon van de betreffende derde partij die dit vervolgens intern zal doorgeven.

8.4. Melden aan betrokkenen

Als een datalek bij de onderneming 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 de onderneming 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 de beleidsbepaler (directeur/eigenaar).

De contactgegevens zijn:

- Naam onderneming: Advies in Private Lease
- Directeur / Eigenaar: Allard Epskamp
- Telefoonnummer: 06 20921638
- Mailadres: info@adviesinprivatelease.nl