Instituut Fysieke Veiligheid

Procedure meldplicht datalekken en informatie-beveiligingsincidenten

Versie: 1.01
Vastgesteld: 17 september 2018

Instituut Fysieke Veiligheid
Bestuurs- en directieondersteuning
Postbus 7010
6801 HA Arnhem
Kemperbergerweg 783, Arnhem
www.ifv.nl
info@ifv.nl
026 355 24 00

Colofon

Opdrachtgever:	Directie IFV
Contactpersoon:	Wim Papperse
Titel:	Procedure datalekken en informatiebeveiligingsincidenten
Datum:	18 Juli 2019
Status:	Vastgesteld 17 september 2018
Versie:	1.1
Auteurs:	Carla Franken, Leon Visser, Frank Cools, Omko Huizenga

Inhoud

Inleiding

Met ingang van 1 januari 2016 is de Wet bescherming persoonsgegevens (Wbp) gewijzigd. Sindsdien geldt een meldplicht voor datalekken. Per 25 mei 2018 is de Wbp vervangen door de AVG. De meldplicht blijft bestaan onder de AVG en is uitgebreid met een plicht om datalekken intern te documenteren, ook als het gaat om kleine kwesties.
Deze meldplichthoudt in dat bedrijven, overheden en andere organisaties die persoonsgegevens
verwerken datalekken, onverwijld moeten melden aan de Autoriteit Persoonsgegevens (AP), en in bepaalde gevallen ook aan de betrokkene(n). De betrokkene is degene van wie persoonsgegevens zijn gelekt.

De bedrijven, overheden en andere organisaties tot wie de meldplicht datalekken zich richt, moeten zelf een beredeneerde afweging maken of een concreet datalek dat hen ter kennis komt onder het bereik van de wettelijke meldplicht valt.

Deze procedure beschrijft hoe te handelen binnen het IFV, wanneer er sprake is van een datalek of wanneer dit vermoed wordt. De meldplicht is eveneens van toepassing op het IFV, wanneer het datalek bij een derde is ontstaan, bijvoorbeeld een verwerker van persoonsgegevens van het IFV. Deze procedure is mede gebaseerd op de beleidsregels van de AP over de meldplicht datalekken in de Wet bescherming persoonsgegevens. Per gemeld datalek behoudt de directie van het IFV de vrijheid om te beoordelen of de procedure gevolgd kan worden, dan wel afwijking van deze procedure gerechtvaardigd is.

Per juli 2018 is deze procedure aangepast op de volgende punten:

> Zowel het afhandelen van datalekken als informatiebeveiligingsincidenten zitten nu in deze procedure. De belangrijkste reden hiervoor is de grote overlap tussen beide onderwerpen: Veel incidenten die gemeld worden zijn na onderzoek geen datalek maar vereisen dikwijls een nieuwe of aangepaste maatregel. Het treffen van deze maatregelen maakt weer deel uit van het domein van informatiebeveiliging.
> De tekst is aangepast zodat voldaan wordt aan de AVG.
> Het processchema is aangepast in overleg met de projectgroep privacy. De beschrijving van het proces is hierop aangepast waarbij de originele tekst zoveel mogelijk is overgenomen.

1 Doel

Het doel van deze procedure is vast te leggen welke stappen genomen moeten worden door het IFV bij het kennis nemen van of een vermoeden van een incident dat aangemerkt kan worden als een datalek of informatiebeveiligingsincident.

Het volgende resultaat wordt hiermee nagestreefd:

> Het steeds volgen van een eenduidige procedure;
> het zorgvuldig waarborgen van de belangen van het IFV, de betrokkene danwel een ander bedrijf dat betrokken is bij het incident, zijnde een (mogelijk) datalek;
> het op zorgvuldige en systematische wijze analyseren van een incident, zijnde een (mogelijk) datalek, zodat aanwezige risicomomenten in het proces zichtbaar worden. Centraal hierbij staat het vaststellen van de onvolkomenheden in de (toepassing van) technische en organisatorische beveiligingsmaatregelen, die (mogelijk) hebben kunnen leiden tot het incident;
> het bevorderen van het nemen van passende verbetermaatregelen en het structureel borgen van deze verbetermaatregelen;
> het realiseren van een voldoende en eenduidige interne en op verzoek externe verantwoording over de afhandeling van een incident, zijnde een (mogelijk) datalek.

In de procedurebeschrijving zijn de te doorlopen stappen uitgewerkt.

2 Definities

AP
Autoriteit Persoonsgegevens (de nieuwe naam van het College Bescherming Persoonsgegevens met ingang van 1 januari 2016).

AVG
Algemene verordening gegevensbescherming – De privacywet die per 25 mei 2018 de WBP vervangt.

Betrokkene
Degene op wie een persoonsgegeven betrekking heeft (artikel 4, AVG).

Beveiligingslek of -incident
Een inbreuk op de beveiliging waarbij persoonsgegevens niet worden blootgesteld aan verlies of onrechtmatige verwerking; er is dan geen sprake van een datalek wel van een beveiligingslek of -incident.

Data-incident
Een incident ten aanzien van persoonsgegevens waarvan nog niet is vastgesteld of dit een datalek betreft.

Data-incidentcommissie
Een tijdelijk ingestelde onderzoekscommissie, die zorgdraagt voor een onderzoek naar een (mogelijk) datalek en over de uitkomsten rapporteert.

Datalek of Inbreuk in verband met persoonsgegevens
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 (artikel 4, AVG).

Derden
De bij het incident betrokken externe partij, anders dan betrokkene. Bijv. een verwerker van persoonsgegevens.

Genodigden
Interne betrokkenen die uitgenodigd zijn bij de bespreking(en) van het incident.

Incident
Een mogelijk beveiligingsincident, waardoor de bescherming van persoonsgegevens op enig moment is doorbroken en waardoor de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Het is daarbij niet van belang of de verantwoordelijke passende technische of organisatorische beschermingsmaatregelen heeft getroffen of niet. Ieder datalek is een incident, maar niet ieder incident is een datalek.

Persoonsgegeven
Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4, AVG).

Verantwoordelijke of verwerkingsverantwoordelijke
De partij die alleen of samen met anderen het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 4, AVG).

Verwerker
Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt (artikel 4, AVG).

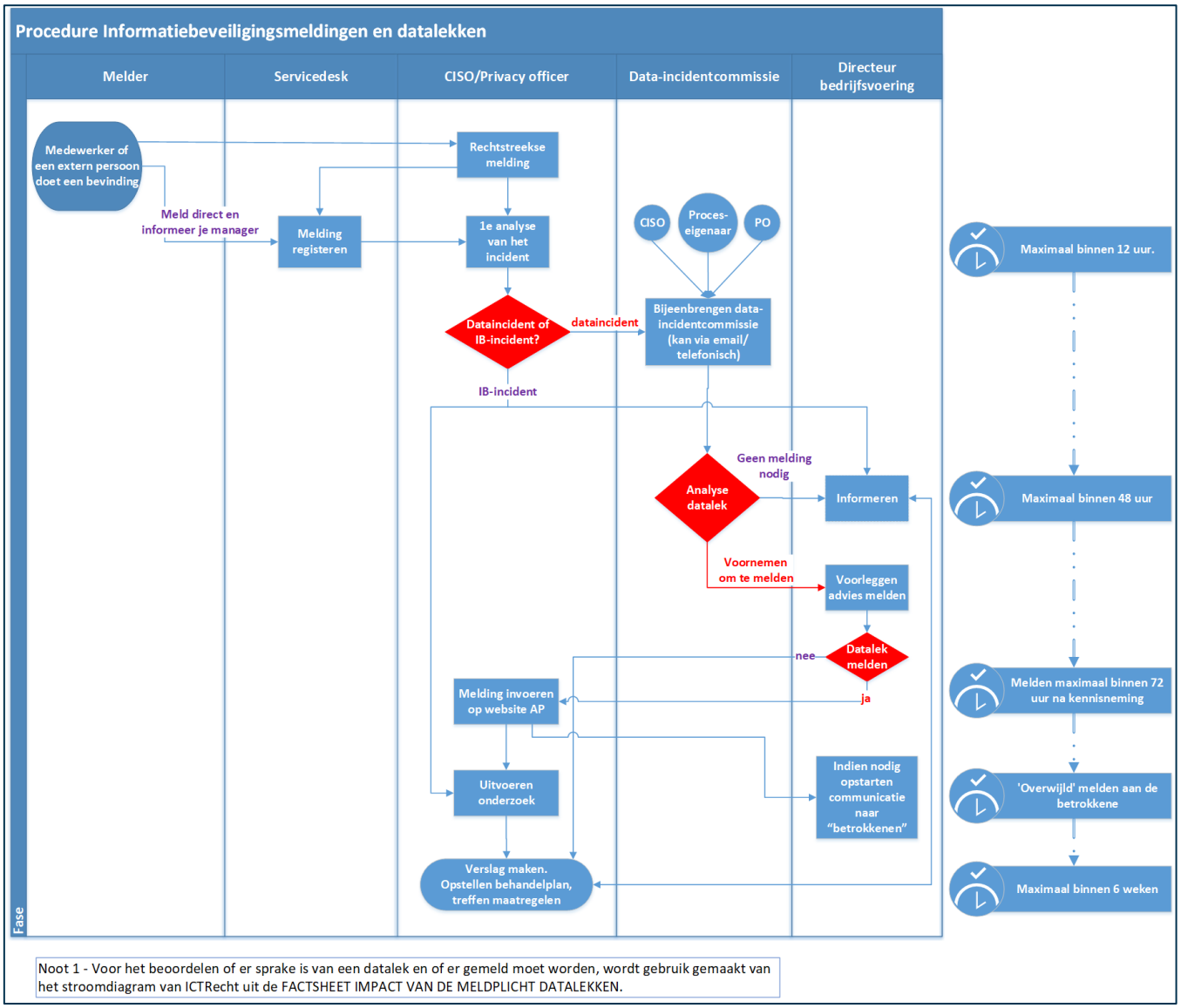
Verwerking van persoonsgegevens
Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 4, AVG).

3 Toepassingsgebied

Deze procedure wordt gehanteerd bij het melden en afhandelen van (mogelijke) datalekken en informatiebeveiligingsincidenten bij het IFV, dan wel van (mogelijke) incidenten die buiten het IFV hebben plaatsgevonden, maar waarvoor het IFV als Verwerkingsverantwoordelijke wel de eindverantwoordelijkheid draagt (bijv. bij een Verwerker).

4 Werkwijze

Voor het totaaloverzicht is een processchema opgesteld. Vervolgens wordt specifieke informatie per processtap over de te verrichten activiteiten en bijbehorende verantwoordelijkheden en bevoegdheden uitgewerkt.



4.1 Identificeren en melden van een incident

De medewerker die een incident constateert, meldt dit per omgaande bij zijn manager, de servicedesk, FG of security officer. Deze procedure wordt dan gestart.

Ook (de medewerker van) een Verwerker kan een datalek constateren en melden aan diens opdrachtgever bij het IFV.
Daarnaast is het ook mogelijk dat er meldingen komen van buiten het IFV over een datalek. Bijvoorbeeld door beveiligingsonderzoekers, media of een betrokkene van wie data gelekt is.

4.2 Registreren van een incident

Het incident wordt vastgelegd door de Servicedesk. Zij gebruikt hiervoor het gangbare incidentregistratiesysteem. Aan het incident worden kenmerken meegegeven zodat deze later terug te vinden zijn als een datalek of informatiebeveiligingsincident.
Bij een melding rechtstreeks aan de CISO of privacy officer wordt, in principe, de melding alsnog bij de Servicedesk geregistreerd.

Wanneer de privacy van de betrokkenen dat vereist, is het toegestaan om het incident slechts te registreren bij de FG of privacy officer. Denk hierbij aan incidenten die gaan over collega's of waarvan de betrokkene heeft aangegeven deze als vertrouwelijk te behandelen. De Privacy officer houdt hiervoor een apart register bij welke complementair is op de registratie van de Servicedesk.

4.3 Eerste analyse van het incident

De CISO en/of privacy officer doen samen een eerste analyse van het incident. De vraag die daarbij beantwoord wordt is:

> Is dit een data-incident, informatiebeveiligingsincident, beide of is er niets aan de hand?

Leidraad voor het antwoord op deze vraag is: betreffen het hier persoonsgegevens ja/nee. Zo ja dan is er een data-incident en wordt een data-incidentcommissie ingesteld.

Bij een informatiebeveiligingsincident wordt de directeur bedrijfsvoering op de hoogte gesteld en start het monitoren en afwikkelen van het incident.

Deze eerste analyse vindt plaats maximaal binnen 12 uur nadat het incident gemeld is. Het resultaat van de analyse wordt vastgelegd in de hiervoor geldende registratie.

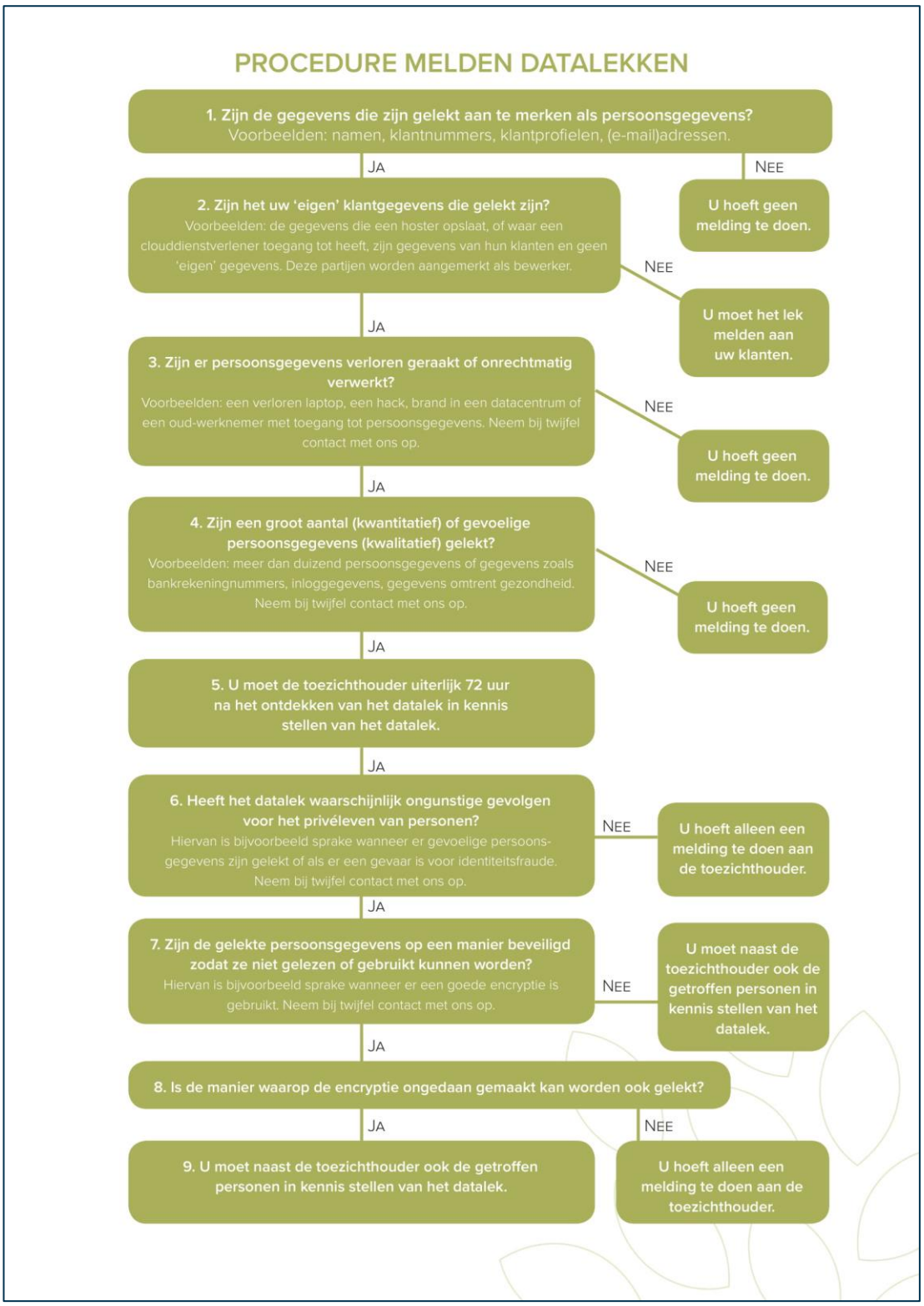
4.4 Instellen Data-incidentcommissie

Data-incidentcommissie bestaat uit ten minste drie leden en heeft tot doel om verdergaand onderzoek te verrichten. Bij de samenstelling van de Data-incidentcommissie wordt rekening gehouden met de aard van het incident. Doorgaans zal de commissie worden samengesteld uit de Privacy officer, CISO en de proceseigenaar waarop het incident betrekking heeft (doorgaans een afdelingshoofd).

> De directeur Bedrijfsvoering draagt zorg voor openstelling van alle beschikbare informatie over het datalek voor de leden van de Data-incidentcommissie.
> De directeur Bedrijfsvoering faciliteert waar nodig de Data-incidentcommissie.

4.5 Analyse datalek

De datalekkencommissie maakt een analyse of er sprake is van een daadwerkelijk datalek. Hiervoor wordt gebruik gemaakt van het stroomschema van ICT-Recht. Dit schema komt uit de "factsheet impact van de meldplicht datalekken".



Figuur 1 Procedure analyse datalekken - afkomstig van ICTRecht

> Bij de beoordeling spelen o.a. een rol:
  - Is er sprake van verlies van persoonsgegevens? Dit houdt in dat het IFV deze gegevens niet meer heeft, omdat deze zijn vernietigd of op een andere wijze verloren zijn gegaan;
  - Is er sprake van onrechtmatige verwerking van persoonsgegevens? Hieronder vallen de onbedoelde of onwettige vernietiging, verlies of wijziging van verwerkte

persoonsgegevens, of een niet geautoriseerde toegang tot verwerkte persoonsgegevens of verstrekking daarvan;
- Is er sprake van een enkele tekortkoming of kwetsbaarheid in de beveiliging?
- Kan redelijkerwijs worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid?
- Zijn er persoonsgegevens van gevoelige aard gelekt? Denk hierbij aan:
    - bijzondere persoonsgegevens conform artikel 9 AVG;
    - gegevens over de financiële of economische situatie van de betrokkene;
    - gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
    - gebruikersnamen, wachtwoorden en andere inloggegevens;
    - gegevens die kunnen worden gebruikt voor (identiteits)fraude;
- Leiden de aard en de omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen? Betrek hierbij factoren als:
    - de omvang van de verwerking; gaat het om veel persoonsgegevens per persoon, en om gegevens van grote groepen betrokkenen;
    - de impact van verlies of onrechtmatige verwerking;
    - het delen van de persoonsgegevens binnen (zorg)ketens; dit betekent dat de gevolgen van verlies en onbevoegde wijziging van persoonsgegevens door de hele keten kunnen optreden;
    - betrokkenheid van kwetsbare groepen; denk aan verstandelijk gehandicapten;

> In geval geoordeeld wordt dat sprake is van een (mogelijk) datalek, wordt tevens het communicatietraject richting betrokkene(n) en, indien van toepassing, de verwerker besproken;

> In geval het incident niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens, is er geen sprake van een datalek maar van een beveiligingslek. Melding aan de AP is dan niet aan de orde. Wel wordt het beveiligingslek onderzocht om herhaling te voorkomen.

> Tevens kan worden beoordeeld of het datalek meldingsplichtig is voor de politie in geval van vermoeden van een strafbaar feit (zie ook hierna onder 4.3).

> De Data-incidentcommissie zorg voor volledige en juiste informatie zoals opgenomen in Bijlage 1 'Formulier melding datalek'.

4.6 Advies wel of niet melden

> De directeur bedrijfsvoering wordt in alle gevallen geïnformeerd van de bevindingen van de Data-incidentcommissie.

> De Data-incidentcommissie stelt een advies op richting de directeur bedrijfsvoering of een datalek gemeld moet worden bij de AP. De directeur bedrijfsvoering maakt de afweging of er wel of niet gemeld wordt.

4.7 Melden aan de Autoriteit Persoonsgegevens

> De privacy officer verzorgt de tijdige (onmiddellijk, zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek) elektronische melding bij de AP volgens het online meldingsformulier van de AP. Dit met inachtneming van richtlijnen van de AP hierover. De Data-incidentcommissie zorgt voor volledige en juiste informatie zoals opgenomen in Bijlage 1 'Formulier melding datalek' op grond waarvan feitelijk gemeld zal worden. De privacy officer fungeert als contactpersoon voor de communicatie naar de AP. Dit geldt ook in het geval nog niet duidelijk is dat het incident een datalek is. De mogelijkheid is dan aanwezig om na vaststelling van de aard van het incident de melding aan de AP aan te vullen dan wel in te trekken.

> De algemeen directeur van het IFV is eindverantwoordelijk, de directeur Bedrijfsvoering gedelegeerd regievoerder over de interne afhandeling van het (mogelijke) datalek in al zijn facetten en over de externe afhandeling met onder meer de AP, betrokkenen en verwerker. De functionaris gegevensbescherming is toezichthouder op het proces en de privacy officer voert de taken uit.

> Het direct betrokken management zorgt ervoor dat de bij het incident betrokken medewerkers worden geïnformeerd. Het zorgt ervoor dat de betrokken medewerkers bij het incident, het mogelijke datalek, zo snel mogelijk een eigen verslag opstellen over de toedracht van het incident. Deze schriftelijke informatie wordt aan de algemeen directeur en de directeur Bedrijfsvoering verstrekt ten behoeve van de leden van de Data-incidentcommissie en het datalekken dossier.

> De AP zal na het melden van een datalek een ontvangstbevestiging sturen. Alleen indien de melding daartoe aanleiding geeft, zal de AP contact opnemen.

> Bij een datalek als gevolg van een (niet-ethische, c.q. kwaadwillende) hack (art. 138ab van het Wetboek van Strafrecht), is van belang wat de aard van de gelekte persoonsgegevens is en wat de risico’s van misbruik voor de betrokkene(n) zijn. Bij een hack ligt naast melding bij de AP, ook aangifte bij de politie voor de hand in verband met de opsporing van de daders. Aangifte loopt via een eventueel beschikbare contactfunctionaris richting politie.

4.8 Rapporteren aan de betrokkene(n)

> Indien een datalek is gemeld aan de AP, moet tevens vastgesteld worden of het datalek ook moeten worden gemeld aan de betrokkene(n). Dit ter beoordeling van en advisering door de Data-incidentcommissie.

> De beoordeling of er sprake is van een incident dat gemeld moet worden aan de betrokkenen, kan tot stand komen met behulp van het eerdergenoemde schema van ICTrecht.

> In opdracht van de algemeen directeur stelt de directeur Bedrijfsvoering in samenspraak met de communicatieadviseur en juridisch adviseur een kennisgeving aan betrokkene(n) op.

> De directeur Bedrijfsvoering bepaalt wat aan de betrokkene(n) wordt gemeld.

> De melding bevat in ieder geval de aard van de inbreuk, contactgegevens van het IFV waar de betrokkene(n) meer informatie over de inbreuk kan krijgen, en de maatregelen die het IFV de betrokkene(n) aanbeveelt om te nemen om de negatieve gevolgen van de inbreuk te beperken.

> De betrokkene(n) worden individueel geïnformeerd.

> Het datalek moet onverwijld gemeld worden aan de betrokkene(n). Dit houdt in dat het IFV na het ontdekken van het datalek enige tijd mag nemen voor nader onderzoek, zodat het IFV de betrokkene op een behoorlijke en zorgvuldige manier kan informeren. Wel moet hierbij rekening gehouden worden dat de betrokkene(n) naar aanleiding van de melding mogelijk maatregelen moet(en) nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder het IFV de betrokkene(n) daarover informeert, hoe eerder deze in actie kan komen.

> In de melding aan de AP is aangegeven of het IFV het datalek al aan de betrokkenen heeft gemeld en, zo niet, wanneer het IFV dat gaat doen. De termijn die het IFV in de melding aan het AP aangeeft, moet het IFV ook nakomen. Mocht deze termijn bij nader inzien niet haalbaar blijken te zijn, dan laat het IFV dit aan de AP weten door middel van een aanpassing van de melding.

4.9 Verrichten onderzoek naar incident of datalek

> Afhankelijk van de zwaarte van het incident of datalek zal de directeur Bedrijfsvoering een opdracht voor de Data-incidentcommissie formulieren. Hierover wordt de Data-incidentcommissie schriftelijk geïnformeerd, voorzien van de termijn waarbinnen de algemeen directeur de rapportage wil ontvangen. De directeur voegt bijlages toe:
  - 'Informatie voor leden van de Data-incidentcommissie' (bijlage 2)
  - 'Informatie voor te interviewen interne personen door de Data-incidentcommissie' (bijlage 3)
  - ‘Informatie voor te interviewen (medewerkers van) derden door de Data-incidentcommissie’ (bijlage 4)

> De Data-incidentcommissie stelt binnen de gestelde termijn en opdrachtverlening een (systematisch) (intern) onderzoek in naar de feitelijke toedracht van het (mogelijke) datalek.

> De Data-incidentcommissie onderzoekt verder of en zo ja hoe dergelijke incidenten in de toekomst kunnen worden voorkomen (het vermijdbaarheidsaspect).

> De bevoegdheden van de Data-incidentcommissie zijn:
  - De mogelijkheid met iedereen te spreken;
  - alle relevante documenten in te zien;
  - toegang te hebben tot alle plaatsen. Dit alles in het kader van wat de commissie nodig acht voor een zorgvuldige analyse;
  - in relatie tot de externe verwerker gelden de afspraken zoals vastgelegd in de verwerkersovereenkomst.

> De Data-incidentcommissie heeft binnen 6 weken na ontdekken van het incident het onderzoek afgerond.

> De Data-incidentcommissie kan in overleg met, of op verzoek van de algemeen directeur, besluiten om externe deskundigen te betrekken bij het onderzoek.

> De Data-incidentcommissie analyseert alle gegevens conform Bijlage 5 'Format rapportage Data-incidentcommissie'. Vervolgens stuurt de Data-incidentcommissie het conceptrapport ter verdere bespreking aan de directeur Bedrijfsvoering.

> De directeur Bedrijfsvoering plant, voordat de slotbijeenkomst plaatsvindt, een overleg met de leden van de Data-incidentcommissie ter voorbespreking van het conceptrapport.

> De Data-incidentcommissie legt het conceptrapport ter correctie op feitelijke onjuistheden voor aan de interne en externe geïnterviewden.

> De Data-incidentcommissie komt vervolgens tot een conceptrapport.

4.10 Implementeren verbetermaatregelen

> De manager in wiens domein de verbetermaatregelen liggen, is verantwoordelijk dat de vastgestelde verbetermaatregelen worden geïmplementeerd, ziet toe op de communicatie rondom en de uitvoering van de verbetermaatregelen, zorgt dat de genomen maatregelen worden geëvalueerd op bruikbaarheid en procesverbetering, en rapporteert over de voortgang aan de algemeen directeur van het IFV.

> Indien bij een verwerker verbetermaatregelen nodig zijn, is de manager die opdrachtgever is van deze verwerker daartoe verantwoordelijk.

> De CISO bewaakt de voortgang.

4.11 Slotbijeenkomst in geval van een datalek: bespreking rapport en vaststellen verbetermaatregelen

> De Privacy officer plant een slotbijeenkomst ter bespreking van het rapport van de Data-incidentcommissie.

> Voor de slotbijeenkomst worden uitgenodigd de algemeen directeur, de directeur Bedrijfsvoering, de leden van de Data-incidentcommissie, een MT-lid en/of leidinggevende, de communicatieadviseur en evt. de juridisch adviseur. De genodigden ontvangen van de directeur Bedrijfsvoering een afschrift van het conceptrapport.

> De algemeen directeur bespreekt tijdens de slotbijeenkomst het rapport en de voorgestelde SMART geformuleerde verbetermaatregelen.

> Tijdens de bijeenkomst wordt het standpunt van de algemeen directeur over het rapport van de Data-incidentcommissie vastgesteld en worden afspraken over verbeter-maatregelen vastgelegd. Tijdens de bijeenkomst wordt vastgesteld of en hoe het datalek aan de betrokkene(n) wordt gemeld.

> Na de bijeenkomst ontvangen de genodigden het definitieve rapport.

4.12 Sluiten melding en vastlegging

> De directeur Bedrijfsvoering informeert de algemeen directeur, de betrokken manager en/of leidinggevende, de bij de calamiteit betrokkenen, de communicatieadviseur en evt. de juridisch adviseur op het moment dat het datalek definitief afgehandeld is en de melding is gesloten.

> De Data-incidentcommissie wordt door de algemeen directeur van het IFV ontbonden.

> De leden van de Data-incidentcommissie vernietigen de nog in bezit zijnde documentatie.

> Het datalek dossier wordt digitaal gearchiveerd door de privacy officer voor de duur van minimaal 1 jaar. Als er redenen zijn om deze langer te bewaren wordt de directeur bedrijfsvoering hiervan op de hoogte gesteld.

Bronnen

- Algemene verordening gegevensbescherming;

Deze Procedure meldplicht datalekken is vastgesteld in de vergadering van de directie en het MT van het IFV d.d. XXXX

Handtekening algemeen directeur IFV:

L.C. Zaal

Bijlage 1 – Formulier melding datalek

1. Over welke organisatie of welk bedrijf gaat het? Vul de onderstaande gegevens in.
a. Naam van organisatie/bedrijf
b. (Bezoek)adres
c. Postcode
d. Plaats
e. KvK-nummer

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

3. Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

4. Omschrijf de groep mensen van wie persoonsgegevens betrokken zijn bij de inbreuk. Vul de aantallen in.
a. Minimaal: (vul aan)
b. Maximaal: (vul aan)

5. Wanneer vond de inbreuk plaats? Kies een van de volgende opties en vul waar nodig aan.
a. Op (datum)
b. Tussen (begindatum periode) en (einddatum periode)
c. Nog niet bekend

6. Wat is de aard van de inbreuk? U kunt meerdere mogelijkheden aangeven.
a. Lezen (vertrouwelijkheid)
b. Kopiëren
c. Veranderen (integriteit)
d. Verwijderen of vernietigen (beschikbaarheid)
e. Diefstal
f. Nog niet bekend

7. Om welk type persoonsgegevens gaat het? U kunt meerdere mogelijkheden aangeven.
a. Naam-, adres- en woonplaatsgegevens
b. Telefoonnummers
c. E-mailadressen en andere adressen voor elektronische communicatie
d. Toegangs- en identificatiegegevens (bijv. inlognaam, wachtwoord of klantnummer)
e. Financiële gegevens (bijv. rekeningnummer, creditcardnummer)
f. Burgerservicenummer (BSN) of sofinummer
g. Paspoortkopieën of kopieën van andere legitimatiebewijzen
h. Geslacht, geboortedatum en/of leeftijd
i. Bijzondere persoonsgegevens (bijv. ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens).
j. Overige gegevens, namelijk (vul aan)

8. Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? U kunt meerdere mogelijkheden aangeven.

a. Stigmatisering of uitsluiting
b. Schade aan de gezondheid
c. Blootstelling aan (identiteits)fraude
d. Blootstelling aan spam of phishing
e. Anders, namelijk (vul aan)

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

10. Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? Kies een van de volgende opties en vul aan waar nodig.
a. Ja
b. Nee
c. Deels, namelijk (vul aan)

11. Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? Beantwoord deze vraag, als u bij vraag 10 gekozen hebt voor optie a. of c. Als u gebruik hebt gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.

12. Heeft de inbreuk betrekking op personen in andere EU-landen? Kies een van de volgende opties.
a. Ja
b. Nee
c. Nog niet bekend

Bijlage 2 – Informatie voor de leden Data-incidentcommissie

Inleiding
De algemeen directeur van het IFV heeft vastgesteld dat er sprake is van een datalek, dat op grond van de AVG is gemeld aan de Autoriteit Persoonsgegevens (AP). De algemeen directeur verwacht uiterlijk binnen 6 weken, nadat de melding van het datalek is gedaan, de rapportage over de feitelijke toedracht van het datalek en een voorstel hoe een dergelijk incident in de toekomst te voorkomen. Om tot een goede rapportage te komen is het noodzakelijk dat een onderzoek door de Data-incidentcommissie wordt verricht.

U heeft ingestemd met deelname aan een ad hoc samengestelde Data-incidentcommissie. U bent inmiddels uitgenodigd voor een toelichtend gesprek bij de directeur Bedrijfsvoering. Ter voorbereiding op dit gesprek ontvangt u de volgende informatie die voor u relevant is. Vragen kunt u tijdens het gesprek en lopende het onderzoek stellen.

Inzet tijd
Afhankelijk van de complexiteit van het datalek en de ervaring van de commissieleden, zal 10 tot 24 uur per persoon nodig zijn in een periode van vier weken.

Documenten/informatie
U ontvangt hierbij:
- een afschrift van het meldformulier aan de AP;
- een schriftelijke opdracht van de directeur Bedrijfsvoering, voor het doen van een onderzoek, waarin een termijn is gesteld waarbinnen het rapport beschikbaar moet voor toezending aan de genodigden;
- indien aanwezig, de eigen verslagen van betrokkenen die op verzoek van de betrokken manager zijn opgesteld;
- de Procedure meldplicht datalekken van het IFV incl. bijlagen. Hierin zijn alle processtappen en ieders bevoegdheden en verantwoordelijkheden beschreven.

Bevoegdheden
Als onderzoeker heeft u de bevoegdheid met iedereen te spreken, alle documenten in te zien en heeft u toegang tot alle plaatsen voor zover van belang voor het onderzoek. Mocht het onderzoek daartoe aanleiding geven, dan heeft u, na voorafgaand overleg met de algemeen directeur, de bevoegdheid een extern deskundige te betrekken bij uw onderzoek. De directeur Bedrijfsvoering zal u informeren over uw bevoegdheden in relatie tot de verwerker op grond van de verwerkersovereenkomst tussen het IFV en de verwerker.

Gesprekken (intern en extern) betrokkenen
Als onderzoeker zult u naast het doen van onderzoek ook gesprekken met (intern) betrokkenen houden, inclusief (indien van toepassing) derde partijen die voor het IFV werken. Ook kan het noodzakelijk zijn om een gesprek te voeren met betrokkene(n) volgens de definitie van AVG (ofwel de personen om wiens gegevens het gaat).

Een methode om in korte tijd de gesprekken met betrokkenen te houden is de zogenaamde 'carrouselmethode'. Dit houdt in dat u achter elkaar de betrokkenen voor een gesprek ontvangt.

Het secretariaat van de directeur Bedrijfsvoering (of het secretariaat van de betrokken afdeling waar het datalek zich voordeed) regelt vergaderruimtes en afspraken voor gesprekken met betrokkenen. Bij bevestiging van de afspraak moet Bijlage 3 bij de Datalekken procedure meegezonden worden aan de interne personen die worden geïnterviewd en Bijlage 4 voor de externe personen (medewerkers van derden). Deze bijlage bevat relevante informatie voor de te interviewen personen.

Van belang is een schriftelijk verslag te maken van een gesprek met een (intern of extern) betrokkene en ter beoordeling op feitelijke onjuistheden toe te zenden aan de betrokkene. Zij ontvangen niet de (concept) rapportage.
U kunt daar waar nodig de ontvangen informatie verwerken in uw rapportage aan de algemeen directeur.

(Eind)rapportage Data-incidentcommissie
Bijlage 5, rapportage Data-incidentcommissie dient als handvat tijdens het uitvoeren van het onderzoek en is voor u leidend bij het opstellen van uw rapportage aan de algemeen directeur.
Vervolgens wordt de conceptrapportage doorgestuurd naar de directeur Bedrijfsvoering die tezamen met uw commissie het conceptrapport bespreekt. U ontvangt daartoe een uitnodiging van de directeur Bedrijfsvoering.
Uw definitieve rapport moet u toezenden aan de directeur Bedrijfsvoering binnen de in de opdrachtformulering gestelde termijn.
Uw definitieve rapportage wordt vervolgens besproken met de algemeen directeur, de directeur Bedrijfsvoering, de manager en/of leidinggevende, de leden van de Data-incidentcommissie, de communicatieadviseur en de juridisch adviseur.

De algemeen directeur besluit of de uitkomsten van uw rapport al dan niet worden overgenomen en besluit tevens welke verbetermaatregelen worden doorgevoerd.
Tevens stelt de directeur Bedrijfsvoering, in opdracht van de algemeen directeur een kennisgeving aan betrokkene(n) volgens de AVG op, in overleg met de communicatieadviseur en de juridisch adviseur.

Als lid van de Data-incidentcommissie moet u daarna alle papieren en digitale documenten die verband houden met het datalek, vernietigen. Het datalekken dossier wordt gedurende minimaal één jaar digitaal gearchiveerd bij het secretariaat van de directeur Bedrijfsvoering.

Evalueren eindrapportage en procesgang Datalekken onderzoek
De directeur Bedrijfsvoering evalueert de procesgang van het onderzoek en de eindrapportage met de Data-incidentcommissie.

Aanspreekpunten
De betrokken manager/leidinggevende is aanspreekpunt wat betreft inhoudelijke zaken rondom het datalek en afstemming naar de betrokken afdeling(en).
De directeur Bedrijfsvoering coördineert intern het Datalekken onderzoek. Hij is beschikbaar in geval u bijvoorbeeld vragen heeft of overleg wilt over de gegeven opdracht, de (concept)rapportage, gestelde termijnen en/of de werkwijze van de AP.

Met vriendelijke groet,

Directeur Bedrijfsvoering

Bijlage 3 – Informatie voor te interviewen interne personen door de Data-incidentcommissie

(Aparte e-mail maken met bevestiging afspraak, wanneer, waar, met wie, hoeveel tijdsbeslag, met deze brief als bijlage.)

Beste collega,

U bent gevraagd mee te werken aan een incidentonderzoek. Hieronder geven wij u informatie over de aanleiding van ons verzoek, de wijze waarop het onderzoek wordt uitgevoerd, uw rol en positie in het onderzoek en het verdere verloop van de procedure.

Aanleiding van ons verzoek
Op grond van de Algemene Verordening Gegevensbescherming (AVG) is de directie van het IFV verplicht om datalekken te melden aan de Autoriteit Persoonsgegevens (AP). Het IFV moet ieder datalek melden waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Binnen onze organisatie is daartoe vastgesteld de Procedure meldplicht datalekken' (bijlage). Recentelijk heeft zich een gebeurtenis binnen onze organisatie voorgedaan, die door de algemeen directeur is gemeld aan de AP. Op grond van deze procedure heeft de directeur Bedrijfsvoering een Data-incidentcommissie ingesteld, die bestaat uit de volgende personen: _____ (invullen personen).

Deze commissie verricht onderzoek naar de feitelijke toedracht van het incident en adviseert over eventueel te nemen maatregelen ter voorkoming van het incident in de toekomst. Deze commissie heeft, om haar werk goed te kunnen uitvoeren, de bevoegdheid gekregen om met iedereen te spreken, alle documenten in te zien, en heeft ook toegang tot alle plaatsen. De Data-incidentcommissie analyseert alle gegevens en stelt daarna een in beginsel geanonimiseerd intern rapport op aan de directie.

Wat betekent dat voor u?
Om een datalek goed te kunnen analyseren wordt tijdens het onderzoek zoveel mogelijk gebruik gemaakt van de kennis van betrokken medewerkers en deskundigen op het gebied waarop een incident zich afspeelde.
De Data-incidentcommissie heeft daarom een afspraak met u gemaakt. Het doel is van u te leren wat er is gebeurd en welke maatregelen genomen kunnen worden om herhaling van vergelijkbare incidenten te voorkomen.

Wat gebeurt er met de informatie die u geeft?
Openheid is essentieel in een dergelijk onderzoek. Alleen bij volledige openheid kunnen de echte oorzaken van incidenten worden achterhaald en beoordeeld.
De Data-incidentcommissie maakt een schriftelijk verslag van het gesprek met u. Dit wordt ter beoordeling op feitelijke onjuistheden aan u toegezonden.

De informatie die u geeft, kan gebruikt worden voor het rapport van de Data-incidentcommissie aan de directie. Het integrale rapport wordt niet aan u verstrekt.
Het doel van het rapport is inzicht te geven in het incident en om aanbevelingen te doen voor maatregelen om herhaling te voorkomen. Het rapport is vertrouwelijk en in beginsel volledig anoniem. Het rapport wordt aangeboden aan de algemeen directeur, waarna het rapport wordt besproken. Vervolgens besluit de algemeen directeur of hij kan instemmen met de uitkomsten van het rapport en welke verbetermaatregelen genomen moeten worden. Het management is verantwoordelijk voor de uitvoering van de maatregelen.

Wie ontvangt een afschrift van het rapport?
In de procedure Melding Datalekken staat beschreven wie een afschrift ontvangt van de rapportage. De informatie uit de rapportage is vaak abstract en organisatie overstijgend. Het is noodzakelijk dat de betrokken manager/leidinggevende zorgt voor een vertaling naar de afdeling en uitleg geeft. Stilgestaan wordt bij de ervaringen van intern betrokkenen en wat op de afdeling beter of anders kan naar aanleiding van het datalek.

Kan ik vrijuit praten of kan ik hier later nog problemen mee krijgen?
Het is wenselijk dat u de Data-incidentcommissie alle benodigde informatie verstrekt om een goede analyse te kunnen maken van het gebeuren en passende verbetermaatregelen te kunnen nemen. Er zullen uitsluitend sanctiemogelijkheden van toepassing zijn, bijvoorbeeld in arbeidsrechtelijke zin, indien het geheel van omstandigheden dit rechtvaardigt.

Overige partijen die belang hebben bij de informatie
Ook de betrokkene(n) volgens de AVG (degene op wie een persoonsgegeven betrekking heeft), of diens wettelijk vertegenwoordiger(s) ontvangen informatie van het IFV over het datalek, de uitkomsten van het verrichte interne onderzoek, en de eventuele genomen verbetermaatregelen.

Bewaren onderzoeksgegevens/rapportages
Uitsluitend de rapportage aan de AP en het definitieve rapport van de Data-incidentcommissie worden gedurende minimaal één jaar digitaal gearchiveerd bij het secretariaat van de directeur Bedrijfsvoering.

Wij danken u bij voorbaat voor het feit dat u uw medewerking wilt verlenen aan het onderzoek.

Met vriendelijke groeten,

De Data-incidentcommissie

Bijlage: Procedure meldplicht datalekken

Bijlage 4 - Informatie voor te interviewen externe personen door de Data-incidentcommissie

(Aparte e-mail maken met bevestiging afspraak, wanneer, waar, met wie, hoeveel tijdsbeslag, met als bijlage deze brief.)

Geachte (naam invullen),

U heeft een verzoek ontvangen om mee te werken aan het incidentonderzoek waarbij XXXX (invullen wat van toepassing is) is betrokken. Hieronder geven wij u informatie over de aanleiding van ons verzoek, de methode van onderzoek, uw rol en positie in het onderzoek en het verdere verloop van de procedure.

Aanleiding van ons verzoek
Op grond van de Algemene Verordening Gegevensbescherming (AVG) is de directie van het IFV verplicht om datalekken te melden aan de Autoriteit Persoonsgegevens (AP). Gemeld moet worden ieder datalek waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Recentelijk heeft zich een gebeurtenis voorgedaan waarbij XXXX betrokken is geweest (kort vermelden wie/wat het incident betreft). Dit incident is door de algemeen directeur als datalek gemeld aan de AP. De directeur Bedrijfsvoering heeft een Data-incidentcommissie ingesteld, die bestaat uit de volgende personen: XXXX (leden Data-incidentcommissie invullen, naam en functie). Deze commissie verricht onderzoek naar de feitelijke toedracht van het datalek en adviseert over eventueel noodzakelijk te nemen maatregelen ter voorkoming van een dergelijk incident in de toekomst. Deze commissie heeft, om haar werk goed te kunnen uitvoeren, de bevoegdheid gekregen om met iedereen te spreken, alle documenten in te zien en heeft ook toegang tot alle plaatsen. De Data-incidentcommissie analyseert alle gegevens en stelt daarna een in beginsel geanonimiseerd intern rapport op voor de algemeen directeur.

Wat betekent dat voor u ?
Om een datalek goed te kunnen analyseren wordt tijdens het onderzoek zoveel als mogelijk gebruik gemaakt van de kennis van betrokkenen bij het incident. De Data-incidentcommissie heeft daarom een afspraak met u gemaakt om ook uw ervaringen te horen. Het doel is van u te vernemen wat er is gebeurd en welke maatregelen genomen kunnen worden om herhaling van vergelijkbare incidenten te voorkomen.

Wat gebeurt er met de informatie die u geeft ?
Openheid is essentieel in een dergelijk onderzoek. Alleen bij volledige openheid kunnen de echte oorzaken van incidenten worden achterhaald en beoordeeld. De Data-incidentcommissie maakt een schriftelijk verslag van het gesprek met u. Dit wordt ter beoordeling op feitelijke onjuistheden aan u toe gezonden. De informatie die u geeft, kan gebruikt worden voor het rapport van de Data-incidentcommissie aan de algemeen directeur.

Het doel van het rapport is inzicht te geven in het incident en om aanbevelingen te doen voor maatregelen om herhaling te voorkomen. Het rapport betreft een intern rapport, is vertrouwelijk en in beginsel volledig anoniem. Het rapport wordt aangeboden aan de algemeen directeur, waarna het rapport wordt besproken. Vervolgens besluit de algemeen directeur of hij kan instemmen met de uitkomsten van het rapport en welke verbetermaatregelen genomen moeten worden.
De algemeen directeur zal de uitkomsten van het rapport en de te nemen verbeter-maatregelen op passende wijze bespreken met de verwerker/de verantwoordelijke leidinggevende van uw bedrijf.

Mocht u nog vragen hebben, dan kunt u deze tijdens het gesprek stellen aan de leden van de Data-incidentcommissie.

Wij danken u bij voorbaat voor het feit dat u uw medewerking wilt verlenen.

Met vriendelijke groeten,

De Data-incidentcommissie

Bijlage 5 – Format rapportage Data-incidentcommissie

Datalekken rapportage

<Afdeling(en) invullen>

IFV

Datum concept: <invullen>
Datum bespreking directie: <invullen>
Datum definitief: <invullen>

Data-incidentcommissie:
- <naam invullen>
- <naam invullen>
- <naam invullen>

1. Opdracht en taakstelling

Hieronder wordt een korte toelichting gegeven bij het schrijven van de rapportage.
- Schrijf een korte en bondige rapportage.
- Gebruik het lettertype en de lay-out van deze voorbeeldrapportage.
- Draag zorg voor een logische opbouw passend in dit format, probeer zo weinig mogelijk te herhalen.
- In de opbouw is met name van belang dat de omschrijving van het incident, de beschrijving van de oorzaken, de beoordeling daarvan en de geadviseerde verbetermaatregelen een logisch gevolg van elkaar zijn.
- Draag zorg voor een rapport zonder spel- en zinsbouwfouten (gebruik spellingscontrole).
- Hoofdstukken hoeven niet op een nieuwe pagina te beginnen, dat is alleen in dit voorbeeld aangehouden voor de leesbaarheid;
- Gebruik dezelfde tijd bij het schrijven van je rapportage (voltooid tegenwoordige tijd).
- Verduidelijk complexe medische terminologie.
- Maak het incident visueel waar mogelijk, denk aan een foto of tekening.

1.1 Datum incident
Geef hier aan gedurende welke periode het datalek heeft plaatsgevonden en wanneer het datalek is opgemerkt. Vermeld hier ook op welke datum de melding door de algemeen directeur is gedaan bij de Autoriteit Persoonsgegevens.

1.2 Samenstelling Data-incidentcommissie
De samenstelling van de Data-incidentcommissie is als volgt:
- titulatuur, voorletters, achternaam (functie, eventueel relevante werkachtergrond benoemen)
- ….

De leden van de Data-incidentcommissie hebben het onderzoek volledig onafhankelijk kunnen uitvoeren en zijn niet betrokken geweest bij het incident en niet werkzaam op de afdeling waar het incident is geweest.

1.3 Volledige beschrijving van incident
Geef hier een omschrijving van het incident. Omschrijf helder wat er heeft plaatsgevonden, waarbij je de gebeurtenissen en data omschrijft. Ga nog niet in op eventuele oorzaken, dit komt later aan bod.

1.4 Opdracht aan Data-incidentcommissie
De opdracht wordt omschreven door de directie en kan letterlijk worden overgenomen uit het opdrachtformulier dat de Data-incidentcommissie ontvangt bij de start van het onderzoek.

2. Algemene informatie

2.1 Persoonsgegevens
Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.
Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
Wanneer vond de inbreuk plaats?
Om welk type persoonsgegevens gaat het?

Noot: bij de beantwoording kunt u gebruik maken van de bijlage 1 “Formulier melding datalek”.

2.2 Aard van inbreuk
Omschrijf de aard van de inbreuk, bij de beantwoording kunt u gebruik maken van de bijlage 1 “Formulier melding datalek”.

2.3 Gevolgen voor de betrokkene(n)
Met betrokkene(n) is bedoeld degene(n) op wie de persoonsgegevens betrekking hebben, conform de definitie volgens AVG.
Omschrijf welke gevolgen de inbreuk kan hebben voor de persoonlijke levenssfeer van de betrokkene(n).
Bij de beantwoording kunt u gebruik maken van de bijlage 1 “Formulier melding datalek”.

2.4 Informeren betrokkenen
Zijn de betrokkene(n) of diens wettelijk vertegenwoordiger(s) geïnformeerd over het datalekincident en de melding aan de AP? Zo ja, door wie en wanneer is dit besproken.

2.5 Volledig overzicht intern en extern betrokken medewerkers
Geef in onderstaand overzicht aan welke medewerkers allemaal intern en extern (bij derden) betrokken zijn. De echte beginletters van de achternamen mogen niet terugkomen in het rapport, geef iedereen een letter op alfabetische volgorde.

Naam	**Functie**
Mevrouw A.	…
De heer B.	…
Etc.	

2.6 Interviews met intern en extern betrokken medewerkers
Voor dit datalekkenonderzoek zijn de volgende interviews gehouden:
- Mevrouw A. (functie)
- De heer B. (functie)
- Etc.

Indien betrokkene conform definitie van de AVG (de persoon wiens gegevens het betreft) en/of diens wettelijk vertegenwoordiger niet gehoord zijn, geef een toelichting waarom niet.

3. Het onderzoek

3.1 Focus onderzoek
Omschrijf naar aanleiding van het verloop van het datalek waar de focus van het incidentonderzoek is komen te liggen. Gebruik hierbij de volgende hulpvragen:
1. Wat waren de belangrijkste gebeurtenissen waardoor het incident ontstond?
2. Welk kritiek moment of gebeurtenis mag nooit meer plaatsvinden? Hiermee wordt niet de schade voor de betrokkene bedoeld, maar het moment (oorzaak) waardoor de schade (vervolg) kon ontstaan.
3. Wat moet dit onderzoek in de toekomst voorkomen?

Beantwoording van deze vragen hoeven niet letterlijk terug te komen in het rapport, maar zijn bedoeld om de Data-incidentcommissie te helpen bij het schrijven van het rapport en het onderzoek.

4. Basisoorzaken incident

4.1 Oorzakenboom
Maak een oorzakenboom (bij voorkeur in Powerpoint of Visio) behorend bij de casus en voeg deze toe als bijlage.

4.2 Bespreking oorzaak-en-gevolg factoren en veiligheidsbarrières
In deze paragraaf worden de diverse factoren besproken die hebben geleid tot het incident. Dit kan gezien worden als een verhalende toelichting op de oorzakenboom. Hierbij wordt nadrukkelijk gekeken naar oorzaak-gevolg en veiligheidsbarrières.

4.3 Schade voor de betrokkene(n) of de organisatie, regresrecht verwerker
Geef weer wat de schade is die de betrokkene(n) heeft opgelopen door het incident.

4.4 Overige bevindingen
Licht hier overige bevindingen toe die nog niet naar voren zijn gekomen in dit hoofdstuk, maar wel onderdeel moeten zijn van het rapport. Zijn er geen overige bevindingen? Dan kan deze paragraaf verwijderd worden.

4.5 Vermijdbaarheid
Licht hier toe of er sprake is van vermijdbaarheid.

5. Professionaliteit

5.1 Professionele standaarden en protocollen
Werd er volgens de professionele normen gewerkt? Werd er protocollair volgens afspraak gewerkt en zo niet, wat was de motivatie om af te wijken? Voeg aangehaalde normen of protocollen toe als bijlage.

5.2 Andere bevindingen rondom professionaliteit
Op het gebied van professionaliteit zijn er nog een aantal andere zaken die de overweging van de Data-incidentcommissie verdienen. Indien een van de onderstaande vragen van belangrijke invloed was op het incident, neem dat dan op onder deze paragraaf. Zijn er geen andere bevindingen op het vlak van professionaliteit? Dan kun je deze paragraaf weghalen.
- Wat was de rol en verantwoordelijkheid van de betrokken professionals en medewerkers? Heeft eenieder zijn rol en verantwoordelijkheid genomen of kunnen nemen? Geef hier een toelichting op.
- Was de bevoegdheid en bekwaamheid van de betrokkenen op niveau?
- Was er adequate overdracht van informatie?

6. Organisatorische aspecten

Op het gebied van organisatorische aspecten zijn er een aantal zaken die de overweging van de Data-incidentcommissie verdienen. Indien een van de onderstaande vragen van belangrijke invloed was op het incident en eerder in dit rapport nog onvoldoende besproken zijn, neem dat dan op onder dit hoofdstuk. Maak paragrafen indien er meerdere ‘losse’ punten besproken worden.

6.1 Bevindingen rondom organisatorische aspecten
Zijn er geen andere bevindingen op het vlak van organisatorische aspecten? Dan kun je deze paragraaf weghalen.
- Waren er organisatorische tekortkomingen en zo ja welke?
- Heeft het gedrag van de medewerker(s) een rol gespeeld?
- Heeft het kennis niveau van de medewerker(s) een rol gespeeld?

6.2 Bevindingen rondom technische aspecten

Waren er technische tekortkomingen en zo ja welke?

Zijn er geen andere bevindingen op het vlak van technische aspecten, dan kun je deze paragraaf weghalen.

7. Conclusie

Herhaal de onderzoeksvraag die gesteld is in paragraaf 1.4 en geef hier antwoord op. Om grote stukken tekst te voorkomen, kan het handig zijn de verschillende basisoorzaken te nummeren in dit hoofdstuk. Draag er zorg voor dat niet het hele rapport wordt herhaald, het gaat om een samenvattende conclusie.

8. Adviezen en verbetermaatregelen

In dit hoofdstuk worden de verbetermaatregelen weergegeven die uit het onderzoek zijn voortgekomen. De Data-incidentcommissie doet op hoofdlijnen aanbevelingen en houd hierbij de volgende zaken in ogenschouw:

1. Zijn de verbetermaatregelen SMART (Specifiek/ Meetbaat/ Appellerend / Realistisch/ Tijdgebonden)?
2. Is duidelijk voor wie de verbetermaatregelen zijn bestemd en hoe ze worden geborgd?
3. Op welke tijdstermijn moeten deze maatregelen worden opgepakt?

Gebruik onderstaande tabel om de verbetermaatregelen weer te geven.

Verbetermaatregel	Verantwoordelijke	Termijn afgerond

9. Bronnen

Vul hier alle bronnen in die gebruikt zijn bij het onderzoek. Voeg vervolgens onder bijlagen alle aangehaalde normen of protocollen toe. Bij uitgebreide protocollen of normen kan de betreffende passage ook voldoende zijn.