PROCEDURE DATALEKKEN NGR

Procedure van de NVOG voor het reageren op (potentiële) datalekken bij de NGR zodat passende maatregelen genomen worden en voor het melden aan de mede-verantwoordelijke waarmee deze kan voldoen aan de verplichtingen ten aanzien van het melden aan Autoriteit Persoonsgegevens en de Betrokkene(n) zoals bepaald in de Algemene Verordening Gegevensbescherming

Inhoudsopgave

Samenvatting

1. De deelnemende beroepsbeoefenaar en de verwerker (SBD groep) melden een mogelijke datalek zo spoedig mogelijk. Dit doen zij aan de contactpersoon van de NVOG. De contactpersoon wordt aan de NVOG leden en de verwerker bekend gemaakt. De NVOG zorgt steeds voor een vervanger, zodat altijd iemand bereikbaar is.
2. De NVOG heeft de centrale regie bij de omgang met incidenten in de beveiliging.
3. De NVOG doet onderzoek en betrekt daar in voorkomende gevallen de verwerker bij. De meldende beroepsbeoefenaar wordt van het onderzoek op de hoogte gehouden en kan ook zelf input geven.
4. Het onderzoek is er op gericht om:
    a. Vast te stellen of het incident ook een inbreuk op de beveiliging is in de zin van artikel 4.12 AVG, met andere woorden een datalek;
    b. Of dit ook een meldingsplichtige datalek betreft en zo ja, of deze ook aan de betrokkenen moet worden gemeld;
    c. Of onmiddellijk maatregelen om moeten worden genomen om verdere datalekken te voorkomen zoals het stilleggen van de gehele NGR of beperkingen in de uitvoer, afsluiten bepaalde accounts, etc.;
    d. De oorzaken te achterhalen en verbetermaatregelen voor te stellen en te implementeren indien aan de orde.
5. De NVOG richt de onderdelen a en b van het onderzoek zo in dat tijdig, dat wil zeggen binnen 72 uur, een melding kan worden gedaan indien het incident een meldingsplichtige datalek betreft. Onderdeel c van het onderzoek kan per direct worden geïmplementeerd en eventueel vervolgens worden gemitigeerd of opgeheven.
6. Indien de datalek de veiligheid van de gehele NGR betreft, wordt de melding aan de AP door de NVOG als mede verantwoordelijke gedaan. Indien de datalek uitsluitend één Beroepsbeoefenaar betreft, wordt de melding aan de AP door deze Beroepsbeoefenaar gedaan. In alle gevallen die daar tussen in liggen, beslissen de NVOG en Beroepsbeoefenaar in onderling overleg wie de melding doet. Een eventuele melding aan de betrokkenen vindt altijd vanuit de Beroepsbeoefenaar plaats.
7. Na de melding ontvangen de betrokken beroepsbeoefenaren een rapportage van de NVOG met een uitleg over de datalek en de verbetermaatregelen, indien aan de orde. Bij een ernstige datalek kan de NVOG hiertoe een onderzoekscommissie instellen.

Reikwijdte en doel procedure datalekken

Deze procedure beschrijft hoe de Landelijke Registratie Orthopedische Implantaten (NGR) handelt indien sprake is van een datalek of wanneer een datalek wordt vermoed. Onder een datalek wordt verstaan een ‘inbreuk in verband met persoonsgegevens’ in de zin van artikel 4.12 AVG. Deze procedure omvat dus zowel:

- Vermoedelijke datalekken;
- Een datalek die aan de Autoriteit Persoonsgegevens moet worden gemeld;
- Een datalek die tevens aan de betrokkenen (zijnde de personen op wie de persoonsgegevens betrekking hebben) moet worden gemeld.

De overkoepelende term is ‘een incident’.

De procedure is van toepassing op incidenten bij het gehele proces van gegevensverwerking in het kader van de NGR, dus uiteraard inclusief de gegevensverwerking bij de door de NVOG ingeschakelde verwerker van de NGR, zijnde de SBP groep.

Het doel van deze procedure dat de NVOG als mede verantwoordelijke voor de gegevensverwerking van de NGR zo spoedig mogelijk op een adequate wijze kan reageren al dan niet samen met de betrokken beroepsbeoefenaar. Soms zal de beroepsbeoefenaar als eerste een incident constateren. Deze procedure richt zijn daarom tevens tot de beroepsbeoefenaar. Zij vormt een Bijlage bij het Reglement NGR. De procedure werkt door naar de verwerkersovereenkomst tussen de NVOG en de SBD groep en vormt daar eveneens een Bijlage.

In concreto beoogt deze procedure te bereiken:

- Optimale samenwerking tussen de NVOG en de Beroepsbeoefenaar teneinde de veiligheid van de gegevensverwerking rond de NGR te optimaliseren en de naleving van de wettelijke bepalingen te borgen;
- Het op zorgvuldige en systematische wijze analyseren van een incident zodat aanwezige risicomomenten in het proces zichtbaar worden en kunnen worden verminderd, cq. beheerst;
- Het bevorderen van compliance met de meldplicht datalekken indien het incident ook een meldingsplichtige datalek in de zin van artikel van artikel 33 AVG blijkt te zijn;
- Het optimaal beschermen van de belangen van de betrokkenen voor wie de NGR uiteindelijk is bedoeld.

Definities

AP	Autoriteit Persoonsgegevens
Betrokkene	Een geïdentificeerde of identificeerbare natuurlijke persoon, op wie een persoonsgegeven betrekking heeft (artikel 4 sub 1, AVG).
Datalek	Een incident dat tevens een inbreuk in verband met persoonsgegevens is in de zin van artikel 4. 12 AVG. Dat wil zeggen: een inbreuk op de beveiliging die per ongeluk of onrechtmatig leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens. Een datalek kan een meldingsplichtige datalek betreffen of een die niet hoeft te worden gemeld.
Meldingsplichtige datalek	Een datalek waarbij het waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen
Beroepsbeoefenaar	Het NVOG lid dat gegevens in de NGR invoert of doet invoeren en toegang heeft tot de ingevoerde gegevens.
Derden	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken (artikel 4 sub 10, AVG).
Incident	Een mogelijke datalek of een beveiligingsincident die tot een datalek had kunnen leiden had kunnen leiden dan wel een datalek.

NGR	De (tijdelijke) Nederlandse Gynaecologische Registratie, zoals bepaald in het reglement NGR.
Onderzoekscommissie	De onderzoekscommissie die kan worden ingesteld om het datalek verder te onderzoeken en het definitieve Datalekken Rapport mee opstellen. De onderzoekscommissie wordt ingesteld door NVOG.
Persoonsgegeven	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (‘de betrokkene’). (artikel 4 sub 1, AVG).
SBD groep	De door de NVOG aangewezen verwerker van de NGR database.
NVOG	De Nederlandse Vereniging voor Obstetrie en Genaecologie, gevestigd aan Mercatorlaan 1200 te Utrecht, geregistreerd in het Handelsregister van de Kamer van Koophandel onder nummer 40532508.
Verwerkingsverantwoordelijke	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan dit/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 4 sub 7, AVG).
Verwerker	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt (artikel 4 sub 8, AVG)
Verwerking	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren,

afschermen, wissen of vernietigen van gegevens (artikel 4 sub 2, AVG).

Stappenplan

Uitgangspunten

Contactpersonen

Het begint er mee dat men elkaar snel kan bereiken bij zorgen omtrent de gegevensbescherming, of het nu een incident is of niet. De contactpersonen van de NVOG zijn opgenomen in Bijlage 1 bij dit document. Een wijziging wordt tijdig aan de Beroepsbeoefenaar doorgegeven.

Open dialoog

Het doel van dit document is om de gegevensbescherming te verbeteren waar nodig en compliant te handelen met betrekking tot een datalek indien aan de orde. Daartoe is een open dialoog tussen de melders, SBD groep en de NVOG noodzakelijk. Het gaat uitdrukkelijk niet om ‘verwijten’ of een ‘schuldige’ aan te wijzen maar om gezamenlijk aan optimale gegevensbescherming voor de doelen van de NGR bij te dragen. Die doelen dienen de patiëntenzorg waarvan de huidige betrokkenen en toekomstige patiënten kunnen profiteren.

Op basis van een onderzoek van een onderzoekscommissie zoals hierna beschreven, zal eventueel door juristen kunnen worden besloten dat een bepaalde partij juridisch voor een datalek aansprakelijk gesteld kan worden. Dat valt buiten deze procedure.

Centrale regie

Centrale regie is noodzakelijk voor een tijdige respons op een incident. De centrale regie is bij de contactpersoon van de NVOG belegd. Uiteraard in nauw overleg met de ook betrokken Beroepsbeoefenaren indien aan de orde.

Een ieder meldt een incident zo spoedig mogelijk aan de contactpersoon van de NVOG.

Voorbeelden en opschaling

Deze procedure heeft een zeer brede reikwijdte. Niet elk incident eindigt in een meldingsplichtige datalek. Een incident kan bijvoorbeeld betreffen dat een bepaalde account van een medewerker van een Beroepsbeoefenaar bij de NGR had moeten worden afgesloten terwijl dat niet tijdig is gebeurd. Indien blijkt dat geen verkeer op dat account heeft plaatsgevonden, is dat geen meldingsplichtige datalek. Maar wel een incident waarvan moet worden geleerd voor de NGR procedures in het algemeen.

Het kan ook voorkomen dat van een account bij een Beroepsbeoefenaar door een niet bevoegde medewerker van die Beroepsbeoefenaar onrechtmatig gebruik is gemaakt. Dit zou door de SBP groep kunnen zijn opgemerkt door bijvoorbeeld verkeer op dat account tijdens niet gebruikelijke tijden. Het account kan dan tijdelijk worden afgesloten. In dit geval liggen de follow-up en verbeteringsprocessen voornamelijk bij de Beroepsbeoefenaar. Indien inderdaad sprake is van meldingsplichtige datalek

(inbreuk op de gegevensbescherming) zal de Beroepsbeoefenaar dit melden. Mogelijk heeft het onrechtmatige gebruik zelfs tevens ook betrekking op andere registraties dan de NGR waaraan de beroepsbeoefenaar deelneemt.

Een mogelijke hack van een account door een derde partij is weer een geheel ander scenario dat centraal onder regie van de NVOG NGR breed moet worden onderzocht en waarschijnlijk leidt tot het instellen van een onderzoekscommissie.
Een onderzoekscommissie wordt ingesteld indien de aard of de omvang van het incident gerede aanleiding geeft om de gegevensbescherming (op het onderdeel waar het incident op betrekking heeft) nader te onderzoeken. De NVOG neemt het initiatief tot het instellen van de commissie. Elke Beroepsbeoefenaar kan daartoe na de melding van een incident en het eerste onderzoek een gemotiveerd voorstel doen.

Wie meldt
De NVOG meldt een datalek dat aan de voorwaarden voor de meldplicht voldoet aan de AP, indien de datalek betrekking heeft op de gegevensbescherming bij de NGR als geheel en waarschijnlijk meerdere Beroepsbeoefenaars zijn getroffen.
Een Beroepsbeoefenaar meldt indien het datalek uitsluitend betrekking heeft op de gegevensverwerking en daarmee verbonden procedures binnen de Beroepsbeoefenaar.
Voor alle situaties die tussen beide uitersten inliggen, overleggen de NVOG en Beroepsbeoefenaar(s) wie de melding zal doen.

Schema

1. Melding incident
Melding van een incident kan zowel vanuit de NVOG, SBP groep, de Beroepsbeoefenaar als extern (bijv. vanuit een patiënt) komen. Elke melding zal worden onderzocht.

2. Identificeren incident
Een ieder die een incident constateert, meldt dit zo spoedig mogelijk aan de contactpersoon van de NVOG of diens plaatsvervanger. Deze zorgt er voor dat ook de directeur van de NVOG direct wordt geïnformeerd indien deze functies niet samenvallen. De procedure is vervolgens als volgt.

3. Beoordelen aard/ernst incident
- De contactpersoon van de NVOG en voorzover van toepassing in samenspraak met de verwerker en/of de Beroepsbeoefenaar, zo spoedig mogelijk zorg voor volledige en juiste informatie zoals opgenomen in Bijlage 1 'Formulier t.b.v. melding datalek'.

- Afhankelijk van de ernst zullen direct maatregelen kunnen worden genomen, eventueel tijdelijk, zoals blokkeren account.
- Op basis van de verkregen informatie wordt in overleg tussen NVOG contactpersoon, de constaterende Beroepsbeoefenaar (indien van toepassing) en verantwoordelijke medewerkers bij de SBD groep zo spoedig mogelijk de beoordeling gemaakt of er daadwerkelijk sprake is van een datalek. Indien er twijfel is over de beoordeling van een datalek wordt de FG van NVOG en/of van de Beroepsbeoefenaar die het incident heeft geconstateerd bij de beoordeling betrokken. Blijft de twijfel bestaan, wordt uitgegaan van een datalek (maar mogelijk niet een meldingsplichtige datalek).
- Tevens kan in dit overleg worden beoordeeld of er per direct (technische) maatregelen genomen moeten worden om de schade te beperken, waaronder het doen van een (voorlopige) melding aan betrokken Beroepsbeoefenaren. Zie ook bij punt 4.
- Van de datalek en de genomen maatregelen wordt aantekening gemaakt bij de NVOG en, indien van toepassing, de beroepsbeoefenaar die het betreft. Bij de beoordeling of er sprake is van een datalek dat gemeld moet worden aan de AP, wordt gebruik gemaakt de Richtsnoeren van de (toenmalige) artikel 29 Werkgroep voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679[1] Bij de beoordeling spelen o.a. een rol:
    - Is er sprake van verlies van persoonsgegevens; dit houdt in dat NVOG deze gegevens niet meer heeft, omdat deze zijn vernietigd of op een andere wijze verloren zijn gegaan > melden;
    - Is er sprake van onrechtmatige verwerking van persoonsgegevens; hier onder vallen de onbedoelde of onwettige vernietiging, verlies of wijziging van verwerkte persoonsgegevens, of een niet geautoriseerde toegang tot verwerkte persoonsgegevens of verstrekking daarvan > melden;
    - Is er sprake van een enkele tekortkoming of kwetsbaarheid in de beveiliging zonder verdere consequenties, blijkt uiteindelijk een beveiligingsprobleem, niet melden ;
    - Kan met aan zekerheid grenzende waarschijnlijkheid worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid dus toch beveiligingsprobleem, niet melden. Anders wel melden;
    - Zijn er persoonsgegevens van gevoelige aard gelekt, toegespitst op de NGR;
        - Bijzondere persoonsgegevens in de zin van artikel 9 AVG;
        - Gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
        - Gebruikersnamen, wachtwoorden en andere inloggegevens;
        - Gegevens die kunnen worden gebruikt voor (identiteits-)fraude; melden
- In geval dat het incident niet heeft geleid tot een risico voor de rechten en vrijheden van de betrokkenen is er geen sprake van een meldingsplichtige datalek maar van een beveiligingsprobleem. Melding aan de AP is dan niet aan de orde. Wel kan in het overleg

[1] WP 250, rev. 01, laatste versie 6 februari 2018.

besloten worden, dat het zinvol is om het beveiligingsprobleem te onderzoeken om herhaling te voorkomen.

- Is een en ander binnen de 72 uur nog niet duidelijk, kan een voorlopige melding aan de AP worden gedaan die later met nieuwe informatie wordt aangevuld of eventueel zelfs wordt ingetrokken.
- Een volgende stap is, indien het meldingsplichtige datalek betreft, of deze ook aan de betrokkenen moet worden gemeld. De factoren die daarbij een rol spelen zijn:
    - 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 het 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;
        - De gegevens zijn niet geëncrypteerd of gepseudonimiseerd.
    - In het geval van de NGR zijn deze omstandigheden bijzonder onwaarschijnlijk. Zij dienen volledigheidshalve wel te worden te worden onderzocht.

4. Directe maatregelen m.b.t datalek

Tijdens de beoordeling van het datalek zullen directe maatregelen worden genomen om de schade van het datalek zoveel mogelijk te beperken. Denk daarbij aan het stilleggen van de NGR omgeving, het deactiveren van een account of andere acties waardoor het datalek niet meer op kan treden. Indien de oorzaak van het datalek niet duidelijk is of de oorzaak niet direct kan worden opgelost, dan zal de gehele NGR omgeving worden stilgelegd tot er meer duidelijk is over de oorzaak, de schade, de omvang en de oplossing.

5. Melding aan betrokken Beroepsbeoefenaren

Indien bij de beoordeling van het incident naar voren is gekomen dat het inderdaad gaat om een meldingsplichtige datalek, dan meldt NVOG dit aan de betrokken Beroepsbeoefenaren. Dit zal binnen 48 uur na de ontdekking gemeld worden. Bij melding aan de betrokken Beroepsbeoefenaren zal de volledige en juiste, en op dat moment beschikbare, informatie worden verstrekt zoals opgenomen in Bijlage 1 'Formulier t.b.v. melding datalek'.

Bij een datalek als gevolg van een (niet-ethische) hack (art. 138ab van het Wetboek van Strafrecht), is van extra 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 betrokken Zorgaanbieder, ook aangifte bij de politie en/of het National Cyber Security Centrum in de rede onder meer in verband met

de opsporing van de daders. Deze aangifte kan ook plaatsvinden indien de hack door de encryptie of andere maatregelen geen meldingsplichtige datalek betreft, met andere woorden niet is geslaagd.

6. Melding aan de AP

De NVOG meldt een meldingsplichtige datalek aan de AP, indien dit datalek betrekking heeft op de gegevensbescherming bij de NGR als geheel en meerdere Beroepsbeoefenaren zijn getroffen.
Een Beroepsbeoefenaar meldt indien het datalek uitsluitend betrekking heeft op de gegevensverwerking en daarmee verbonden procedures door de Beroepsbeoefenaar.
Voor alle situaties die tussen beide uitersten inliggen, overleggen de NVOG en Beroepsbeoefenaren wie de melding zal doen. Dit gebeurt door een mededeling van de NVOG aan de Beroepsbeoefenaren met daarin een voorstel door wie en hoe de melding zal worden gedaan. De Beroepsbeoefenaren reageren zo spoedig mogelijk op dit voorstel. Eventueel vindt telefonisch overleg plaats.
Bij een datalek dat tevens aan de betrokkenen moet worden gemeld, gebeurt dit via de Beroepsbeoefenaren mede omdat de NVOG niet over de daartoe noodzakelijke contactgegevens beschikt.

7. Verrichten datalek onderzoek

- Direct na melding stelt de NVOG een (systematisch) onderzoek in naar de feitelijke toedracht van het (mogelijke) datalek. Voor dit onderzoek kan een onderzoekscommissie worden ingesteld indien het een groter datalek betreft waar de oorzaken en verbetermaatregelen niet evident zijn.
- NVOG onderzoekt verder of en zo ja hoe dergelijke incidenten in de toekomst kunnen worden voorkomen (het vermijdbaarheidsaspect).
- Indien nodig stelt de SBD groep een technisch rapport op t.b.v. het datalek en de eventuele oplossingen ter voorkoming van een datalek in de toekomst.
- De Beroepsbeoefenaar die het incident heeft gemeld, wordt desgewenst bij het rapport betrokken.
- De NVOG zal indien nodig besluiten om een onderzoekscommissie in te stellen met externe deskundigen.
- De NVOG dan wel de onderzoekscommissie analyseert alle gegevens conform Bijlage 2 'Format rapportage Datalekken'.
- Het conceptrapport wordt ter verdere bespreking aan verantwoordelijke personen bij de SBD gezonden en indien nodig ook aan de betrokken Beroepsbeoefenaren
- Het bestuur van de NVOG stelt vervolgens het rapport vast.
- Het onderzoek wordt binnen 4 weken na de melding aan de betrokken Beroepsbeoefenaren afgerond.

8. Implementeren verbetermaatregelen

- De organisatie (bijv. NVOG of SBD groep) 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 NVOG en indien aan de orde, aan de Beroepsbeoefenaren.
- Indien bij SBD groep verbetermaatregelen nodig zijn, is de directeur van de NVOG, die opdrachtgever is van Reports, daartoe verantwoordelijk.
- De directeur van de NVOG bewaakt de voortgang, onder eindverantwoordelijkheid van het NVOG bestuur.

9. Sluiten melding en vastlegging

- De NVOG informeert de betrokken beroepsbeoefenaren, de verwerker en de persoon die het datalek heeft gemeld over de definitieve afhandeling van het datalek via de Rapportage datalekken.
- Het dossier wordt digitaal bij de NVOG gearchiveerd voor de duur van minimaal 1 jaar. Er kunnen redenen zijn om gedurende langere tijd te archiveren, de richtlijn zoals beschreven in “Meldplicht datalekken in de Wet bescherming persoonsgegevens; beleidsregels” zal worden gehanteerd.

Deze Procedure Meldplicht Datalekken is vastgesteld in de bestuursvergadering van NVOG van d.d. 16 December 2020

Handtekening [bestuur van de organisatie]

Astrid Vollebregt
Voorzitter NVOG

Bijlage 1 Formulier melding datalek

Deze bijlage bevat de gegevens die NVOG oplevert aan betrokken Beroepsbeoefenaars na constatering van een datalek. De Zorgaanbieder kan de gegevens gebruiken t.b.v. de melding aan de AP.

Melding van het incident

Door wie (incl. functie en werkgever) en wanneer (exacte datum en tijd) is het incident gemeld bij NVOG.

Was het incident ook een datalek ?

Zo neen, korte beschrijving en waarom geen datalek. Het formulier hoeft verder niet te worden ingevuld.

Gegevens over de datalek

Inclusief:

- Een samenvatting van het incident waarbij de inbreuk in verband met de persoonsgegevens zich heeft voorgedaan.
- Indien bekend: Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
- De groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
- Wanneer de inbreuk plaats vond.
- De aard van de inbreuk. (Lezen (vertrouwelijkheid), Kopiëren, Veranderen (integriteit), Verwijderen of vernietigen (beschikbaarheid), Diefstal of Nog niet bekend)
- Om welk type persoonsgegevens het gaat.
- Waren de gegevens geëncrypteerd en/of gepseudonimiseerd en wat is de kans dat deze beveiliging wordt doorbroken
- Welke gevolgen de inbreuk kan hebben voor de persoonlijke levenssfeer van de betrokkenen.

Vervolgacties naar aanleiding van het datalek

De technische en organisatorische maatregelen die de NVOG en de SBD groep hebben getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen. Daarnaast zal er zo spoedig mogelijk een technisch rapport door SBD groep worden opgeleverd, indien de datalek zich in of vanuit de SBD omgeving heeft voorgedaan.

Bijlage 2 Format Rapportage Datalekken die hebben geleid tot het instellen van een onderzoekscommissie

1. Opdracht, samenstelling en taakstelling

De NVOG stelt een onderzoekscommissie in indien de datalek van een zodanige ernst is dat volgens de directeur de NVOG de gegevensverwerking in de NGR opnieuw moet worden beoordeeld en rapportage in het formulier datalekken niet volstaat. Daarnaast kan een Beroepsbeoefenaar uitdrukkelijk om het instellen van een onderzoekscommissie verzoeken. De NVOG geeft aan een dergelijk verzoek gehoor tenzij na overleg met het bestuur van de NVOG en de beroepsbeoefenaar een onderzoekscommissie disproportioneel zou blijken.

De NVOG stelt de onderzoekscommissie in overleg met de betrokken Beroepsbeoefenaren. De onderzoekscommissie bestaat uit ten hoogste vijf personen, waarvan tenminste 1 vanuit de Beroepsbeoefenaren en twee externe deskundigen.

2. Rapportage onderzoekscommissie

1 Algemeen

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 het Bestuur is gedaan bij de Autoriteit Persoonsgegevens.

1.2 Samenstelling Datalekken onderzoekscommissie

- titulatuur, voorletters, achternaam (functie, eventueel relevante werkachtergrond)

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 Datalekken onderzoeksgroep

De opdracht wordt omschreven door het Bestuur en kan letterlijk worden overgenomen uit het opdrachtformulier dat de Datalekken onderzoeksgroep ontvangt bij de start van het onderzoek.

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 voor melding datalek”, met name vraag 10 t/m 13 en vraag 15.

2.2 Aard van inbreuk

Omschrijf de aard van de inbreuk, bij de beantwoording kunt u gebruik maken van de bijlage 1 “Formulier voor melding datalek” met name vraag 14.

2.3 Gevolgen voor de betrokkene(n)

Met betrokkene(n) is bedoeld degene(n) op wie de persoonsgegeven(s) betrekking heeft (hebben), conform de definitie volgens Wet bescherming persoonsgegevens.
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 voor melding datalek”, met name vraag 16.

2.4 Informeren betrokkenen

Zijn de betrokkene(n) of diens wettelijk vertegenwoordiger(s) geïnformeerd over het datalek incident en de melding aan de AP?

2.5 Volledig overzicht intern en extern betrokken medewerkers

Geef in onderstaand overzicht aan welke medewerkers allemaal intern en extern (bij derden) bij de datalek 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 datalekken onderzoek zijn de volgende interviews gehouden:

- Mevrouw A. (functie)

- De heer B. (functie)
- Etc.

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?

4 basisoorzaken incident

4.1 Oorzakenboom

Maak een oorzakenboom 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 bewerker

Geef weer wat de schade is die de betrokkene(n) heeft opgelopen door het incident.

4.4 Nevenbevindingen

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 eventueel in de in de rapportage moeten worden meegnomen. 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 is er een aantal zaken die de overweging van de Datalekken Commissie verdient. 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

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

- Waren er technische tekortkomingen en zo ja welke?

7. Conclusie

Herhaal de onderzoeksvraag die gesteld is in paragraaf 1.4 en geef hier antwoord op. Om grote lappen 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 Datalekken Commissie doet op hoofdlijnen aanbevelingen en houd hierbij de volgende zaken in ogenschouw:

1. Zijn de verbetermaatregelen SMART (Specifiek/ Meetbaat/ Appelerend / 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?

9. Bronnen

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