Datum
6 oktober 2022

Van
Bureau
Gegevensbescherming
5.1 lid 2 sub e @uwv.nl

Handreiking bij impactvolle datalekken UWV

Een leidraad voor het optreden bij een impactvol datalek

Opgesteld door Bureau Gegevensbescherming

Inhoud

Versiebeheer

Datum versie	Actie
Conceptversie 3 mei 2019	Voor review voorgelegd aan JZ en SBK
Conceptversie 7 mei 2019	Mondeling besproken in Datalekoverleg met BSO's op 15/5
Conceptversie 4 juni 2019	Mondeling besproken met BSO's van WB, K&S, UITK en GD
Conceptversie 9 juli 2019	Voor review voorgelegd aan JZ, SBK, CC, C-ICT en 5.1 lid 2 sub e
Conceptversie 8 augustus 2019	Voor schriftelijke review voorgelegd aan Tactische Overleg van de Coalitie IB&P
Conceptversie 4 oktober 2019	Schriftelijke review van Tactische Overleg verwerkt
Conceptversie 29 november 2019	Opmerking van CISO verwerkt en voorgelegd aan Strategisch Overleg van de Coalitie IB&P (5/12/2019)
Definitief (versie 1.0) 17 januari 2020	Akkoord van Strategisch Overleg. Opmerking van FB DIV verwerkt.
Definitief (versie 1.1) 25 november 2021	Bijlage contactpersonen aangepast
Conceptversie Review Q4 2021 en Q2 2022 22 juni 2022	Evaluatie BG, SMZ, Uitkeren, K&S verwerkt. Ter review voorgelegd
Concept versie 1.3 7 juli 2022	Reviewcommentaar verwerkt
Concept versie 1.92 26 augustus 2022	Reviewcommentaar versie 1.3 verwerkt
Concept versie 1.93 1 september 2022	Reviewcommentaar versie 1.93 verwerkt en ter informatie gedeeld in Inhoudstafel
Concept versie 1.99 27 september 2022	Ter informatie geagendeerd voor Beleidstafel
Definitief versie 2.0 6 oktober 2022	Ter informatie geagendeerd voor Thematafel IB&P

1 Inleiding

1.1 Doel van deze handreiking

Beveiligingsincidenten die mogelijk een datalek zijn, dienen altijd via het reguliere datalekproces gemeld te worden. Wanneer blijkt dat een datalek een relatief grote impact heeft op de vertrouwelijkheid, beschikbaarheid of integriteit van gegevens, dan is het reguliere datalekproces vaak niet afdoende om het datalek tijdig en effectief af te handelen. Deze handreiking heeft daarom tot doel om binnen UWV duidelijkheid te geven over welke stappen moeten worden ondernomen wanneer zich een impactvol datalek heeft voorgedaan. Voor de duiding van een impactvol datalek: zie paragraaf 3.1. Het streven is door goede afstemming en coördinatie van (herstel)acties de gevolgen van een impactvol datalek te beheersen. Het in deze handreiking beschreven proces treedt dan ook alleen in werking als een datalek wordt opgeschaald van incident naar calamiteit, zoals verder toegelicht in hoofdstuk 3.

Dit document bevat geen in steen gebeitelde procedure, maar vormt een leidraad die afhankelijk van de specifieke situatie en behoeften kan worden aangepast en verder ingevuld. Ook staat het organisatieonderdelen vrij om voor hun eigen onderdeel een nadere uitwerking te maken op basis van deze handreiking Wanneer een organisatieonderdeel hiertoe besluit, is het raadzaam de collega's die zich met bedrijfscontinuïteitsmanagement (BCM) binnen het eigen onderdeel bezighouden hierbij te betrekken.

Verder is het belangrijk om op te merken dat binnen UWV wordt gewerkt aan de verdere professionalisering van BCM. Op dit moment zijn de BCM-processen binnen de diverse organisatieonderdelen nog niet zodanig uitgekristalliseerd en belegd, dat het optreden bij een impactvol datalek binnen die processen wordt opgepakt. Daarom is ervoor gekozen deze handreiking voor impactvolle datalekken op te stellen. Het streven is echter om dit proces een regulier onderdeel te laten vormen van de BCM-structuur.

1.2 Definitie datalek

De term 'datalek'[1] wordt binnen UWV vaak gehanteerd. De formele omschrijving in de Algemene verordening gegevensbescherming (AVG) is "een inbreuk in verband met persoonsgegevens"[2]. Daarbij kan onderscheid gemaakt worden tussen drie soorten inbreuken die kunnen leiden tot een zogezegd datalek:

- Inbreuk op de **vertrouwelijkheid** van persoonsgegevens: in geval van een onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens.
- Inbreuk op de **integriteit** van persoonsgegevens: in geval van een onbevoegde of onopzettelijke wijziging van persoonsgegevens.
- Inbreuk op de **beschikbaarheid** van persoonsgegevens: in geval van een onbevoegd of onopzettelijk verlies of vernietiging van persoonsgegevens.

1.3 Melding beveiligingsincidenten met persoonsgegevens

Beveiligingsincidenten die mogelijk een datalek zijn, moeten altijd via het reguliere datalekproces worden gemeld met het interne meldformulier. Alle meldingen worden geregistreerd door het BIS-team[3] van de

[1] Deze term vindt z'n oorsprong in de Wet Meldplicht Datalekken die sinds 1 januari 2016 in werking is getreden en is vervangen door de komst van de AVG.

[2] Onder 'inbreuk in verband met persoonsgegevens' wordt verstaan: 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, onder 12, AVG).

[3] BIS staat voor Bedrijfskritische Incidenten & Service requests en is onderdeel van de Servicedesk IV.

Servicedesk IV en vervolgens doorgezet naar de relevante IB&P-teams. Nadat alle beschikbare informatie is verzameld wordt het interne meldformulier doorgestuurd naar Bureau Gegevensbescherming. Bureau Gegevensbescherming beoordeelt (indien nodig met advies van JZ) of het beveiligingsincident als datalek moet worden gemeld aan de Autoriteit Persoonsgegevens (AP) en draagt vervolgens zorg voor die melding.

Bij de melding aan de AP wordt een onderscheid gemaakt tussen een voorlopige melding en een definitieve melding. Omdat een datalek in principe uiterlijk 72 uur nadat UWV daarvan kennis heeft genomen aan de AP moet worden gemeld[4], wordt meestal eerst een voorlopige melding gedaan. Als alle relevante informatie is verzameld, kan de melding definitief worden gemaakt of – indien is gebleken dat het incident bij nader inzien niet onder de meldplicht valt –worden ingetrokken.

Verder kan het ook nodig zijn dat de betrokkenen (de personen van wie gegevens zijn 'gelekt') over het datalek wordt geïnformeerd.[5] Of de betrokkene moet worden geïnformeerd wordt ook beoordeeld door Bureau Gegevensbescherming (indien nodig met advies van JZ). In de regel worden betrokkenen geïnformeerd als het waarschijnlijk is dat er door het datalek een hoog risico op inbreuk op de rechten en vrijheden van betrokkenen is ontstaan.

1.4 Onderscheid incident, calamiteit en crisis

UWV onderscheidt drie niveaus van onbedoelde en ongewenste gebeurtenissen. Deze zijn in 2018 door de RvB vastgesteld in het kader van het bedrijfscontinuïteitsmanagement (BCM). De drie niveaus zijn:

Incident: Dit is een gebeurtenis die afwijkt van de normale situatie, met (mogelijk) verstoring van de dienstverlening, letsel en/of (imago)schade maar op beperkte schaal. De situatie verstoort de reguliere dienstverlening van korte duur.

Calamiteit: Dit is een bedrijfsincident dat (mogelijk) leidt tot zwaardere consequenties, zoals (mogelijk) ernstige verstoring van de dienstverlening, letsel en/of (imago)schade. Dit incident is bedreigend voor delen van de organisatie en verstoort de reguliere dienstverlening voor langere tijd. De situatie vraagt toepassing van een (keten)calamiteitenplan door het desbetreffende organisatieonderdeel om terug te keren naar de normale situatie.

Crisis: Dit is een calamiteit die (mogelijk) leidt tot zwaardere consequenties en die niet (snel genoeg) kan worden opgelost binnen de bestaande processen en (overleg)structuren. Dit betekent dat naast de toepassing van een calamiteitenplan, besturing op het hoogste niveau van de organisatie (centrale crisisorganisatie) noodzakelijk is om terug te keren naar de normale situatie.

In het kader van deze handreiking is het van belang te benadrukken dat hierbij de aandacht met name gericht is op de schade aan (de persoonlijke levenssfeer van) betrokkenen. Zie ook paragraaf 3.1.

1.5 Scope van deze handreiking

Beveiligingsincidenten die mogelijk een datalek zijn, dienen altijd via de reguliere datalekprocedure gemeld te worden. Een datalek dat wordt gekwalificeerd als incident wordt binnen het reguliere datalekproces afgehandeld, zoals te vinden op DWU en in de werkinstructies.

[4] Artikel 33 AVG.
[5] Artikel 34 AVG.

Deze handreiking heeft betrekking op het optreden bij datalekken die een zodanige impact hebben dat zij als calamiteit moeten worden opgeschaald, zoals toegelicht in hoofdstuk 3.

De afhandeling van een zeer ernstig datalek dat leidt tot een zodanige verstoring dat sprake is van een crisis wordt beschreven in het centraal crisismanagement plan. Meer informatie over de centrale crisisorganisatie is te vinden op de DWU-pagina Crisismanagement UWV.

2 Schematisch stappenplan

Onderstaand schema beschrijft op hoofdlijnen de stappen die moeten worden doorlopen wanneer zich een datalek voordoet dat mogelijk grote impact heeft en dus als calamiteit moet worden aangemerkt. In de hoofdstukken 3 tot en met 6 volgt een toelichting op deze stappen.

START	**Meld het beveiligingsincident/datalek via de geldende meldprocedure.**
	Beveiligingsincidenten die mogelijk een datalek zijn, moeten altijd via de daarvoor geldende procedure worden gemeld. De melding gebeurt door een medewerker die een beveiligingsincident constateert waar mogelijk persoonsgegevens betrokken zijn. Dit kan een medewerker ook doen n.a.v. een signaal vanuit een klant of werkgever. De melder downloadt het interne meldformulier, vult deze in en stuurt dit naar 5.1 lid 2 sub e @uwv.nl. Alle meldingen worden ontvangen door de Servicedesk IV en doorgezet naar het relevante IB&P-team. Nadat de beschikbare informatie is verzameld, beoordeelt Bureau Gegevensbescherming of het beveiligingsincident als datalek moet worden gemeld aan de Autoriteit Persoonsgegevens (AP) en eventueel ook aan de betrokkene (indien nodig met advies van JZ). *Voor verdere toelichting op het reguliere datalekproces, zie de DWU-pagina over datalekken*.
STAP 1	**Bepaal of het datalek moet worden opgeschaald tot calamiteit**
	De BSO of een IB&P-coördinator signaleert of mogelijk sprake is van een calamiteit, eventueel na raadplegen van Bureau Gegevensbescherming. De BSO/IB&P coördinator informeert de verantwoordelijke directeur en deze schaalt het incident indien nodig op naar calamiteit. Daarnaast heeft de Functionaris Gegevensbescherming de mogelijkheid om een incident te escaleren richting de directeur of de RvB indien er vanuit het organisatieonderdeel geen actie daartoe wordt ondernomen. Zie paragraaf 5.3 ‘Besluitvorming’. De volgende vragen kunnen behulpzaam zijn: - Wat is de aard van de getroffen persoonsgegevens? Gaat het om gevoelige gegevens? Van wie zijn gegevens gelekt of verstoord, bv. gegevens van VIP’s? - Wat is de omvang van het datalek? Hoeveel gedupeerden en hoeveel ontvangers? Duurt het datalek nog voort of is deze reeds gedicht? - Hoe heeft het beveiligingsincident kunnen plaatsvinden? Wie heeft toegang gehad tot de gegevens? Bv. een grootschalige hack door criminelen? - Is er mogelijk sprake van een “opzettelijk datalek” met betrokkenheid van een of meerdere UWV-medewerkers of externe partijen?

	- Is het datalek al bekend in de pers? Is er in de politiek of vanuit het ministerie al aandacht voor? - Zijn er meerdere organisatieonderdelen van UWV betrokken en/of externe ketenpartijen? Zijn er eventueel al maatregelen genomen om de gevolgen te beperken? *Voor verdere toelichting, zie hoofdstuk 3.*
STAP 2	**Samenstellen van het calamiteitenteam (CT) en het plannen van de eerste bijeenkomst.**

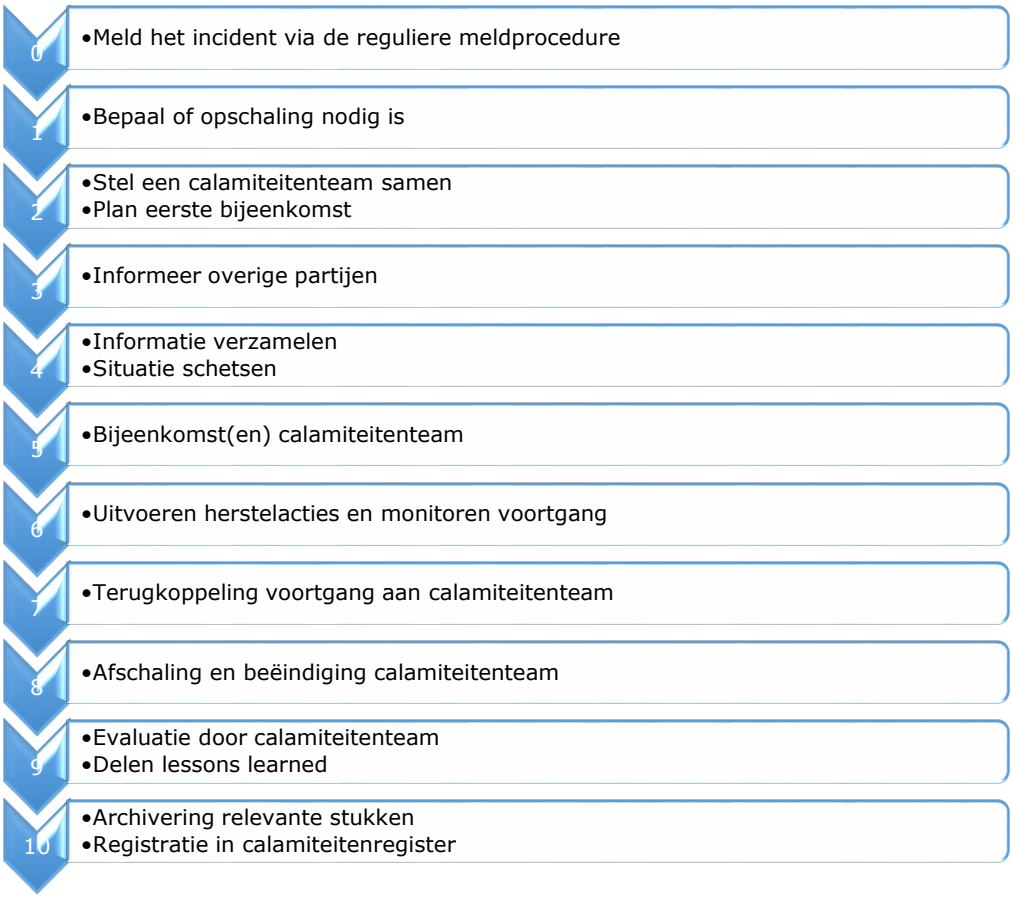
	Het calamiteitenteam is verantwoordelijk voor de afstemming en coördinatie van de benodigde (herstel)acties om de impact van het datalek te beperken. De directeur van het getroffen onderdeel is voorzitter van het calamiteitenteam, tenzij hij of zij deze taak heeft gedelegeerd aan een andere persoon.
	
	De voorzitter van het calamiteitenteam beslist, mede op advies van de BSO, over de samenstelling van het team. De algemene stelregel is: hoe kleiner het team, hoe slagvaardiger. Daarbij kan onderscheid gemaakt worden tussen de benodigde deelnemers voor de vaste kern en deelnemers voor de flexibele schil. De voorzitter zorgt ervoor dat de eerste bijeenkomst op (zeer) korte termijn wordt gepland.
	
	De volgende vragen kunnen behulpzaam zijn bij het bepalen wie deel moeten nemen aan het calamiteitenteam:
	- Raakt het datalek meerdere organisatieonderdelen? Zijn andere organisatieonderdelen nodig om het datalek te herstellen?
	- Wordt (veel) aandacht in de pers of vanuit Den Haag verwacht?
	  - Is specifieke expertise nodig om herstelacties te bepalen?
	  Bureau Integriteit (BI) is door de RvB als enige afdeling 'bevoegd verklaard' om onderzoeken in te stellen naar de rol van een UWV-medewerker bij een integriteits-issue. Als er sprake is van een mogelijk opzettelijk datalek of van een grove fout (waarop een medewerker aangesproken MOET worden), dan zal BI een rol moeten spelen bij en aanwezig moeten zijn in het calamiteitenteam.
	
	Voor verdere toelichting, zie paragraaf 4.1 en 4.2

STAP 3	**Informeer overige partijen over het opstarten en de voortgang van het calamiteitenteam.**
	Niet iedereen die geïnformeerd dient te worden, hoeft lid te zijn van het calamiteitenteam. Informatie kan bijvoorbeeld ook periodiek aan een groep betrokkenen worden gemaild. Het organisatieonderdeel dat het calamiteitenteam start is verantwoordelijk voor het zo spoedig mogelijk informeren van andere partijen die niet deelnemen aan het calamiteitenteam, maar wel hierover geïnformeerd moeten worden. Denk hierbij aan de volgende partijen: - Raad van Bestuur - SBK - CISO - Juridische Zaken - Functionaris Gegevensbescherming - Klantcontactcentrum (KCC), FB DIV en andere organisatieonderdelen die betrokken zijn bij het oplossen van het datalek.

	Voor verdere toelichting, zie paragraaf 4.3
STAP 4	**Verzamelen van relevante informatie en een beeld vormen van de situatie.**
	Van belang is om zoveel mogelijk relevante informatie over het datalek te verzamelen voorafgaand aan de eerste bijeenkomst van het calamiteitenteam. Daarbij blijft het van belang om zo snel mogelijk alle informatie te verzamelen in het kader van de melding aan de AP. Bepaal welke informatie nog ontbreekt en wie deze informatie moet verzamelen. Zo kan het calamiteitenteam starten met een gemeenschappelijk beeld van de situatie. Een deel van de relevante informatie is meestal al verzameld in het kader van de voorlopige melding van het datalek door Bureau Gegevensbescherming aan de AP. Zorg ervoor dat deze informatie ook beschikbaar is voor het calamiteitenteam. Het is van belang om direct bij de start een duidelijke, begrijpelijke probleemschets op te stellen. Hierbij moet het sjabloon van het meldformulier gebruikt worden. *Voor verdere toelichting, zie paragraaf 5.1*
STAP 5	**Start van het Calamiteitenteam.**
	Kom bijeen met het calamiteitenteam en bepaal wie de notulen maakt. Start met een voorstelrondje en benoem ieders rol in het team. Deel alle relevante informatie met elkaar en stel vast of er een gemeenschappelijk beeld is: hebben alle leden van het calamiteitenteam eenzelfde informatieniveau (zie stap 4)? Nadat er een gedeeld informatieniveau is, bespreek vervolgens de benodigde acties zo concreet mogelijk, benoem specifieke actiehouders en bepaal een datum waarop een actie moet zijn uitgevoerd. Tot slot, stel vast wanneer het calamiteitenteam weer bijeenkomt. Van cruciaal belang is goede afstemming over communicatie naar buiten. Stem binnen het calamiteitenteam af wie, wat, wanneer, aan wie communiceert. Gebrek aan afstemming leidt tot gebrek aan controle en onnodige verrassingen voor betrokken partijen. *Voor verdere toelichting, zie paragraaf 5.2.*
STAP 6	**Uitvoeren van (herstel)acties en monitoring hiervan.**
	Uitvoering van de (herstel)acties geschiedt door een of meer herstelteams. Zij voeren acties uit binnen de betrokken organisatieonderdelen. *Voor verdere toelichting, zie paragraaf 5.3*
STAP 7	**Terugkoppeling voortgang (herstel)acties in het calamiteitenteam.**
	Zorg ervoor dat het calamiteitenteam steeds zoveel mogelijk over dezelfde informatie beschikt over de voortgang van de herstelacties. Informeer zo nodig de flexibele schil en andere organisatieonderdelen daarover.

	Herhaal zo nodig de stappen 5, 6 en 7 om het datalek te beheersen.
STAP 8	**Beëindigen calamiteitenteam**
	Als de calamiteit/het datalek en de benodigde (herstel)acties onder controle zijn en de acties die nog nodig zijn binnen de bestaande structuren kunnen worden uitgevoerd, kan de calamiteit worden afgeschaald en het calamiteitenteam beëindigd. De voorzitter van het calamiteitenteam beslist over het afschalen van de calamiteit en het beëindigen van het calamiteitenteam. Hij kan hierover worden geadviseerd door de BSO of andere adviseurs. Formele beëindiging van het calamiteitenteam kan ook plaatsvinden nadat de evaluatie (stap 9) heeft plaatsgevonden. Dit dient dan ook schriftelijk vastgelegd te worden in de notulen.
STAP 9	**Evaluatie van het datalek en aanbevelingen.**
	Na afronding van de benodigde (herstel)acties, wordt het calamiteitenteam beëindigd. Elk datalek dat als een calamiteit is behandeld, dient na afloop met het CT te worden geëvalueerd. Dit is van belang om vast te stellen welke maatregelen nodig zijn om soortgelijke datalekken in de toekomst te voorkomen en mogelijke verbeterpunten voor het optreden van het calamiteitenteam. Om herhaling te voorkomen verdient het de aanbeveling om de benodigde maatregelen in het DT van het desbetreffende organisatieonderdeel te bespreken en hierover besluitvorming te laten plaatsvinden. *Voor verdere toelichting, zie paragraaf 6.1*
STAP 10	**Archiveren besluitvorming en registratie van de calamiteit.**
	Het organisatieonderdeel waar het datalek zich heeft voorgedaan is verantwoordelijk voor het archiveren van de relevante stukken omtrent de besluitvorming en uitgevoerde (herstel)acties. Op deze wijze kan er op een later moment verantwoording worden afgelegd worden over de keuzes die zijn gemaakt om het datalek op te lossen. Denk hierbij aan: - Verslagen van de bijeenkomsten van het calamiteitenteam - Andere relevante gespreksverslagen - Overwegingen die aan besluitvorming ten grondslag hebben gelegen (voor zover deze niet uit de verslagen blijken) - Besluitenlijsten en actiepuntenlijsten Registreer de calamiteit/datalek in het calamiteitenregister. *Voor verdere toelichting, zie paragraaf 6.2*

Hieronder een schematische weergave van bovenstaande stappenplan. Een aantal stappen zal, afhankelijk van de specifieke situatie, vaker worden doorlopen. Dit hoeft niet per se chronologisch te zijn. Maar elke stap wordt tenminste één maal uitgevoerd.



3 Opschalen van incident naar calamiteit

Deze handreiking gaat over het optreden bij impactvolle datalekken die worden geëscaleerd van incident naar calamiteit, dat wil zeggen zodra duidelijk wordt dat een datalek een relatief grote impact heeft en de regulier (overleg)structuren en processen niet afdoende zijn.

3.1 Factoren voor opschaling

Bij het bepalen of een datalek moet worden opgeschaald van een incident naar een calamiteit, zijn de volgende factoren van belang:

- Significante impact voor de betrokkene vanwege de **gevoeligheid (aard) van de getroffen gegevens**. Denk bijvoorbeeld aan gevoelige persoonsgegevens zoals financiële gegevens, gezondheidsgegevens, medische dossiers, BSN's of VIP-gegevens.[6]
- Significante impact van het datalek vanwege de **omvang van de getroffen gegevens**, namelijk het aantal betrokkenen. Denk bijvoorbeeld aan de situatie dat het datalek betrekking heeft op een grote groep betrokkenen van wie persoonsgegevens zijn 'gelekt' of aangetast. De omvang kan ook groot zijn doordat een bepaalde set persoonsgegevens onbedoeld bij een grote groep personen of verschillende organisaties terecht is gekomen.
- De **aard van de inbreuk**. Hoe heeft het datalek kunnen plaatsvinden en wie heeft toegang gehad tot deze gegevens? Is er bijvoorbeeld sprake van een grootschalige hack door criminelen? Zijn andere (overheids)organisaties tevens slachtoffer?
- **Langdurige verstoring** van de dienstverlening door de gebeurtenis. Denk aan het gedurende lange tijd niet beschikbaar zijn van bepaalde cruciale gegevens.
- Aandacht in **media en politiek** voor de gebeurtenis. Denk aan aandacht in de pers, Kamervragen of vragen vanuit het ministerie SZW.
- Interne urgentie door **complexiteit** van het datalek of de herstelacties. Het datalek en/of de herstelacties raken bijvoorbeeld meerdere organisatieonderdelen en/of externe (keten)partijen en dus moet actie worden gecoördineerd.

3.2 Risicobeoordeling

Bovenstaande factoren spelen een rol bij het bepalen of een datalek moet worden opgeschaald tot calamiteit. De factoren kunnen niet in een simpele beslisboom worden ondergebracht, maar moeten altijd worden gewogen in de specifieke context van het geval. Gezond verstand is daarbij een goede raadgever. Zo kan de omvang van een datalek heel klein zijn (bijvoorbeeld maar één VIP-klant betreffen), terwijl de impact ervan (het betrof gevoelige gegevens die vanuit UWV naar de roddelpers zijn gelekt) heel groot kan zijn en weer kan leiden tot Kamervragen. Omgekeerd kan een groot bestand met gegevens van 10.000 klanten onbedoeld bij één organisatie terecht zijn gekomen die het meteen heeft vernietigd. In dat geval zal de impact weer klein zijn. Harde criteria voor aantallen worden daarom hier niet voorgesteld. Dat laat overigens onverlet dat het organisatieonderdelen vrij staat om voor hun eigen processen wel bepaalde hardere criteria als richtlijn vast te stellen.

BG is eindverantwoordelijk voor de risicobeoordeling m.b.t. de melding aan de AP. Het is aan de bedrijfsonderdelen om de noodzakelijke informatie op te halen op basis waarvan de beoordeling wordt gedaan. Hiervoor is communicatie uiteraard belangrijk.

---

[6] Als niet meteen duidelijk is om welke vertrouwelijkheidsklasse het gaat, kunnen de Fugems/het Canoniek gegevensmodel waarin de vertrouwelijkheidsklasse is geregistreerd bij het vaststellen hiervan behulpzaam zijn.

3.3 Besluitvorming

De Algemeen directeur (of een door hem gemandateerd ander lid van het directieteam) van het organisatieonderdeel waar het datalek zich voordoet, beslist of het datalek moet worden opgeschaald tot calamiteit. Dit is van belang omdat deze beslissing ook gevolgen heeft voor de inzet van capaciteit en prioritering van werkzaamheden. Alleen een directeur (of gemandateerde) kan hier een besluit over nemen omdat hij of zij eindverantwoordelijk is voor het desbetreffende organisatieonderdeel.

In de praktijk heeft de BSO heeft een belangrijke signalerende en adviserende rol richting de directeur (of gemandateerde) voor het opschalen naar een calamiteit. Desgewenst kan ook advies worden ingewonnen bij andere organisatieonderdelen, zoals SBK of BZ (Juridische Zaken en/of Bureau Gegevensbescherming). Daarnaast heeft de Functionaris Gegevensbescherming de mogelijkheid om een incident te escaleren richting de Algemeen directeur of de RvB

Het besluit om een datalek als **crisis** aan te merken wordt genomen door de voorzitter van het centrale crisisteam (dit is een lid van RvB), al dan niet op advies van de directeur van het desbetreffende organisatieonderdeel. Als een datalek als calamiteit is aangemerkt en gaandeweg blijkt dat deze verder zou moeten worden opgeschaald tot crisis, kan de directeur van het desbetreffende organisatieonderdeel hierover advies uitbrengen aan de voorzitter van het centrale crisisteam.

4 Inrichten en opstarten calamiteitenteam

Indien een datalek is opgeschaald tot calamiteit, dient een calamiteitenteam (CT) te worden samengesteld en opgestart. Het calamiteitenteam is verantwoordelijk voor de afstemming en coördinatie van de benodigde (herstel)acties.

Het calamiteitenteam heeft een flexibele invulling naar gelang de situationele context. In paragraaf 4.1. worden de rollen beschreven die onderdeel vormen van een vaste kern van het calamiteitenteam. In paragraaf 4.2 wordt de flexibele schil beschreven. Deze bestaat uit rollen die naar eigen inzicht en afhankelijk van de situatie aan het calamiteitenteam kunnen deelnemen.

Algemeen advies luidt om de omvang van het calamiteitenteam zo klein mogelijk te houden. Dat bevordert de besluitvorming. Denk daarbij dat organisatieonderdelen die geïnformeerd moeten worden niet per se aan het calamiteitenteam hoeven deel te nemen.

De directeur of een door de directeur gemandateerd ander lid van het directieteam beslist over de exacte samenstelling van het calamiteitenteam. De BSO kan hem hierover adviseren.

Voor zover de leden van het calamiteitenteam nog niet bekend zijn met deze handreiking, verdient het aanbeveling dit document bij de uitnodiging van de eerste bijeenkomst ter informatie mee te sturen.

4.1 Vaste kern calamiteitenteam

De volgende rollen maken doorgaans onderdeel uit van de vaste kern van het CT:

- ***Voorzitter***

De voorzitter verdeelt de rollen onder de teamleden, leidt de bijeenkomsten en neemt de operationele besluiten, daarbij geadviseerd door de overige leden van het calamiteitenteam. Als uitgangspunt geldt dat de directeur (of gemandateerde) de rol van voorzitter van het calamiteitenteam vervult. De directeur kan deze rol delegeren aan een ander lid van het directieteam (bijv. een IV-directeur), een calamiteiten-/escalatiemanager, de BSO of een andere medewerker die hiervoor geschikt is.

- ***BSO van het getroffen organisatieonderdeel***

In veruit de meeste gevallen zal de BSO deel uitmaken van het calamiteitenteam. Indien binnen het getroffen organisatieonderdeel niet de BSO, maar de IB&P-coördinator verantwoordelijk is voor de datalekken, kan deze in plaats van de BSO deelnemen aan het CT.

De BSO kan verschillende taken vervullen, zoals:
- uitvragen van informatie binnen het eigen organisatieonderdeel over de feitelijke gebeurtenissen;
- adviseren over de herstelacties en maatregelen die nodig zijn om herhaling te voorkomen;
- liaison zijn richting andere organisatieonderdelen om hen te informeren, informatie uit te vragen en eventuele acties te coördineren;
- informeren van het eigen DT over de voortgang van het calamiteitenteam en (herstel)acties.

- ***Medewerker + adviseur (Bureau Gegevensbescherming)***

Deze collega's van Bureau Gegevensbescherming beoordelen of het datalek aan de Autoriteit Persoonsgegevens (AP) moet worden gemeld. Als dat het geval is, is Bureau Gegevensbescherming verantwoordelijk voor de voorlopige en definitieve melding bij de AP. Ook beoordeelt Bureau Gegevensbescherming, of de betrokkene(n) moeten worden geïnformeerd en de wijze waarop dit dient te gebeuren. De adviseur is één van de accounthouders van het betreffende organisatieonderdeel.

- ***Communicatieadviseur (Woordvoering en evt. organisatieonderdeel)***

De communicatieadviseur adviseert over de externe communicatie met de media rond het datalek en eventueel de interne communicatie (binnen UWV) die nodig is.[7] Daarvoor dient dus altijd een adviseur van Woordvoering onderdeel te zijn van het CT. Dit kan eventueel aangevuld worden met een communicatieadviseur van het eigen organisatieonderdeel.

- ***Vertegenwoordiging van herstelteam(s)***

De uitvoering van (herstel)acties geschiedt door een of meer herstelteams. De vertegenwoordiger van het herstelteam vormt de liaison tussen het calamiteitenteam en het herstelteam. Hij informeert het CT over de voortgang van de herstelacties en koppelt zo nodig nieuwe acties terug aan het herstelteam.

- ***Administratieve ondersteuning***

Administratieve ondersteuning is van belang voor de praktische kant van het calamiteitenteam. De medewerker die deze rol vervult regelt de benodigde faciliteiten, organiseert vergaderingen en notuleert zo nodig de overleggen van het team. Met name voor de verantwoording van gemaakte keuzes binnen het proces is dit van belang.

4.2 Flexibele schil calamiteitenteam

Afhankelijk van de specifieke situatie, kan het nodig zijn een of meer andere personen te laten deelnemen aan het calamiteitenteam.
Omdat vooraf niet altijd vastgesteld kan worden of aansluiting noodzakelijk is, wordt de flexibele schil in ieder geval geïnformeerd en gevraagd om aan te haken. Als blijkt dat input niet (meer) nodig is stappen ze uit het team. Dat voorkomt dat partijen ten onrechte niet betrokken worden, of te laat.

Het gaat dan om de volgende partijen:
- een adviseur van Communicatie: bijv. een medewerker van Public Affairs wanneer aanzienlijke media-aandacht wordt verwacht;
- Juridische Zaken (JZ): wanneer twijfel bestaat over de meldplichtigheid door UWV of een derde (partner), of wanneer sprake is van mogelijke aansprakelijkheid van UWV of een derde (partner, leverancier). Ook adviseert JZ over de risicobeoordeling en de onderbouwing daarvan.

[7] Communicatie met het ministerie van SZW over het datalek verloopt via SBK,

- een vertegenwoordiger van SBK: bijv. wanneer er Kamervragen zijn gesteld/worden verwacht of vanuit het ministerie van SZW is verzocht om rechtstreekse terugkoppeling;
- CISO-Office: Wanneer het datalek zich manifesteert in het informatiebeveiligingsdomein sluit CISO aan i.v.m. haar stelselverantwoordelijkheid voor IB&P, t.b.v. de PDCA op beleid, IB&P risico's en de strategische veranderagenda. Hierbij kan CISO expertise leveren t.b.v. het op te stellen plan van aanpak om herhaling te voorkomen.

Daarnaast kunnen optioneel de volgende partijen worden uitgenodigd:
- vertegenwoordiger van andere direct betrokken organisatieonderdelen: bijv. de BSO van een andere divisie wanneer het datalek ook aanzienlijke gevolgen heeft voor zijn/haar organisatieonderdeel;
- de Functionaris Gegevensbescherming: bijv. wanneer actieve betrokkenheid van de Autoriteit Persoonsgegevens wordt verwacht of wanneer zijn betrokkenheid gewenst is bij het adviseren over vervolgacties;
- een of meer inhoudelijke experts: bijv. wanneer specifieke kennis en/of kunde nodig is voor het verzamelen van relevante informatie of het bepalen van de benodigde (herstel)acties.

4.3 Informeren van andere organisatieonderdelen

Voor zover de volgende partijen niet reeds deel uitmaken van het calamiteitenteam, moeten zij in ieder geval altijd worden geïnformeerd over het opstarten en de voortgang van het calamiteitenteam:

- Raad van Bestuur;
- SBK;
- Functionaris Gegevensbescherming;
- CISO
- De BSO van K&S, zodat het Klantcontactcentrum (KCC) zich kan voorbereiden op vragen van klanten;
- De BSO van FB DIV, zodat er voorbereidingen getroffen kunnen worden voor eventuele herstel-verzendingen;
- Indien van toepassing: De BSO van een ander betrokken organisatieonderdeel;
- Indien van toepassing: Bureau Integriteit, wanneer sprake is van verdenking van een strafbaar feit (bijv. diefstal, computervredebreuk of fraude) of verwijtbaar gedrag van een medewerker (mogelijke integriteitschending). Bureau Integriteit dient betrokken/geïnformeerd te zijn/te worden als er sprake is van een mogelijke integriteitschending gerelateerd aan het datalek. Bureau Integriteit stelt namelijk (als enige en onafhankelijke afdeling binnen UWV) onderzoeken in naar verwijtbare (mogelijke) integriteitschendingen, door UWV-medewerkers (en anderen). Denk daarbij bijvoorbeeld aan het 'opzettelijk' lekken van informatie, door UWV-medewerkers, maar ook door externe (hack-)partijen. Als dit lekken ook een strafbaar feit betreft dan bereidt Bureau Integriteit een aangifte voor, voor de Voorzitter van de Raad van Bestuur van UWV, die als enige binnen UWV bevoegd is om namens UWV aangifte te doen bij politie/OM van strafbare feiten gepleegd tegen of ten nadele van UWV.
- Indien van toepassing: KEREL, als het gaat om calamiteiten die ook impact (kunnen) hebben op de keten.

De voorzitter van het calamiteitenteam bepaalt samen met de BSO of IB&P-coördinator hoe en door wie deze partijen worden geïnformeerd.

5 Beheersing van de calamiteit en uitvoering van (herstel)acties

5.1 Beeldvorming – wat is de situatie?

Doel is om met elkaar een gemeenschappelijk beeld van (de chronologie van en betrokkenen bij) de gebeurtenissen vast te stellen zodat alle leden van het calamiteitenteam eenzelfde informatieniveau hebben. Ga hierbij na:

- Wat weten we? Kunnen we antwoord gegeven op de volgende vragen:
    - Wat is de startdatum van de inbreuk?
    - Wat is de einddatum van de inbreuk? Of duurt deze nog voort?
    - Wat is de aard van het de inbreuk? Kortom, wat is er gebeurd?
    - Welke persoonsgegevens zijn betrokken bij de inbreuk? Wat is de gevoeligheid van deze gegevens?[8]
    - Van welke groep mensen zijn de persoonsgegevens betrokken bij het datalek? En wat is de omvang van deze groep?
    - Wat zijn de gevolgen van het datalek voor betrokkenen en UWV?
    - Zijn er reeds (corrigerende) maatregelen genomen?
- Klopt alles wat we (denken te) weten?
- Welke informatie hebben we nog nodig om herstelacties te formuleren en tot een besluit te komen?
- Waar bevindt zich de ontbrekende informatie? Wie gaat deze verzamelen? Maak een (voorlopige risicobeschrijving.

[8] Een hulpmiddel hierbij is de in de Fugems/Canoniek gegevensmodel geregistreerde vertrouwelijkheidsklasse van de gegevens.

5.2 Oordeelsvorming – wat moet er gebeuren?

Als de leden van het calamiteitenteam een gemeenschappelijk beeld hebben van de situatie, wordt gesproken over wat er vervolgens moet gebeuren. Doel is om acties te formuleren waarover besluitvorming kan plaatsvinden.

Van groot belang hierbij is goede afstemming over communicatie naar buiten, zoals naar klanten, ketenpartners, ministerie of pers. Stem binnen het calamiteitenteam af wie, wat, wanneer, aan wie communiceert. Gebrek aan afstemming hierover leidt tot gebrek aan controle en onnodige verrassingen voor betrokken partijen.

De volgende vragen kunnen behulpzaam zijn bij het formuleren van benodigde acties:
- Is het datalek nog 'actief'? Zo ja, wat is nodig om het zo spoedig mogelijk te stoppen?
- Mocht het datalek nog niet zijn gemeld aan de Autoriteit Persoonsgegevens, moet dit alsnog gebeuren? Advies Bureau Gegevensbescherming.
- Moeten de betrokkenen/benadeelden worden geïnformeerd (conform art. 34 AVG)? Zo ja, hoe en wanneer? Terugbelactie en/of brief? Advies Bureau Gegevensbescherming en (Directie) Communicatie.
- Moeten melders (niet zijnde benadeelden) worden geïnformeerd? Denk bijvoorbeeld aan werkgevers.
- Welke herstelacties en herstelteams zijn nodig? Welke organisatieonderdelen zijn hierbij nodig?
- Welke informatie heeft KCC nodig om klanten te kunnen antwoorden?
- Is de RvB als op de hoogte? Wie informeert welk lid van de RvB en wanneer? Uitgangspunt is dat het RvB-lid dat verantwoordelijk is voor het betreffende bedrijfsonderdeel altijd z.s.m. door de betrokken directie geïnformeerd wordt wanneer een datalek aangemerkt wordt als calamiteit.
- Moeten andere directeuren worden geïnformeerd? Zo ja, wie doet dat wanneer?
- Zijn er externe partijen betrokken? Zo ja, wie informeert deze wanneer?
- Moet het ministerie van SZW door SBK van aanvullende informatie worden voorzien? Zo ja, wanneer?
- Moet een woordvoeringslijn/Q&A's worden opgesteld voor contact met de media? Advies van Woordvoering i.s.m. communicatieadviseur van divisie.
- Is er mogelijk sprake van een strafbaar feit? Zo ja, wie informeert Bureau Integriteit en wanneer gebeurt dit? Informeren van Centraal Meldpunt Identiteitsfraude?

Het resultaat van de oordeelvorming is een inzicht in benodigde vervolgacties (herstelplan) en inzicht in de besluiten die genomen moeten worden.

5.3 Besluitvorming – wie gaat wat doen?

Als de (herstel)acties zijn geformuleerd, volgt besluitvorming over de uitvoering ervan. De operationele besluiten worden in principe genomen door de voorzitter van het calamiteitenteam, daarover geadviseerd door de overige leden van calamiteitenteam.

Het calamiteitenteam neemt geen strategische besluiten, maar kan daarover wel adviseren. Strategische besluiten dienen te worden genomen door de algemeen directeur/het directieteam van het getroffen organisatieonderdeel of, afhankelijk van de aard van het besluit, door de Raad van Bestuur.

Zorg ervoor dat de besluiten/actiepunten zoveel mogelijk 'smart' zijn geformuleerd, dat wil zeggen:
- beschrijf concrete acties met een concreet resultaat;
- benoem een specifieke actiehouder;
- benoem een datum/tijdstip waarop de actie moet zijn uitgevoerd.

Uitvoering van herstelacties geschiedt door een of meer herstelteams. Het calamiteitenteam bepaalt welke herstelteams nodig zijn. De herstelteams zijn verantwoordelijk voor de operationele beheersing van de calamiteit. Elk herstelteam heeft zijn eigen scope en expertise. Herstelteams kunnen een technische focus hebben, bijvoorbeeld functioneel ontwerp/beheer of releasemanagement die voor

(snelle) aanpassing van systemen moeten zorgen. Herstelteams kunnen ook een functionele of procesmatige focus hebben (bijvoorbeeld het Klantcontactcentrum (KCC) voor terugbelacties).

6 Evaluatie en archivering

6.1 Evaluatie

Na afronding van de benodigde (herstel)acties, wordt het calamiteitenteam beëindigd. Elk datalek dat als een calamiteit is behandeld, dient na afloop met het CT te worden geëvalueerd. Dit is van belang om vast te stellen welke maatregelen nodig zijn om soortgelijke datalekken in de toekomst te voorkomen.

Ook het optreden van het CT zelf dient te worden geëvalueerd. Hierdoor kan van de opgedane ervaringen worden geleerd en kunnen zo nodig verbeteringen worden aangebracht in procesafspraken. In verband met dat laatste worden de uitkomsten van de evaluatie ondertekend door de directie en ook teruggekoppeld naar Bureau Gegevensbescherming bij Bestuurszaken, zodat deze handreiking zo nodig kan worden aangepast.

Vragen die bij de evaluatie behulpzaam kunnen zijn, zijn:
- Welke toekomstige maatregelen zijn nodig om herhaling van dit datalek te voorkomen?
- Hoe verliep de besluitvorming over het opstarten van een CT?
- Hoe wordt de samenstelling van het CT beoordeeld?
- Hoe verliep de samenwerking binnen het CT?
- Hoe verliep de informatie-uitwisseling?

Hierbij wordt het volgende geadviseerd:
- Bespreek de maatregelen die nodig zijn om herhaling van het datalek te voorkomen in het DT en zorg dat hierover besluitvorming plaatsvindt.
- Deel de belangrijkste bevindingen van de evaluatie in relevante overleggen, zoals het Tactisch Overleg van de coalitie IB&P en het maandelijkse Datalekken-overleg, zodat ook andere organisatieonderdelen hiervan kunnen leren.

6.2 Archivering en verantwoording

Van belang is dat de besluitvorming in het CT wordt vastgelegd en gearchiveerd. Zo nodig moet deze documentatie kunnen worden overlegd aan de Autoriteit Persoonsgegevens. Ook de FG kan hiernaar vragen als hij besluit zelf een onderzoek te doen naar het datalek.

De voorzitter van het calamiteitenteam zorgt ervoor dat archivering plaatsvindt.. In ieder geval dienen de volgende zaken schriftelijk te worden vastgelegd en gearchiveerd:
- verslagen van bijeenkomsten van het calamiteitenteam;
- andere belangrijke gesprekverslagen
- overwegingen die aan besluitvorming ten grondslag hebben gelegen (voor zover deze niet al uit een van de verslagen blijken);
- besluitenlijsten en actiepuntenlijsten.

Tot slot dient het datalek te worden geregistreerd in het calamiteitenregister van het organisatieonderdeel.[9]

[9] Het bedrijfscontinuïteitsmanagement schrijft voor dat ieder organisatieonderdeel een calamiteitenregister bijhoudt.

Bijlage – contactpersonen

CENTRAAL			
Onderdeel	**Naam en telefoon**	**E-mailadres**	**Naam en telefoon vervanger**
Bureau Gegevensbescherming	5.1 lid 2 sub e	5.1 lid 2 sub e @uwv.nl	5.1 lid 2 sub e
Juridische Zaken BZ	5.1 lid 2 sub e	5.1 lid 2 sub e @uwv.nl	5.1 lid 2 sub e
CC - Woordvoering	Perstelefoon: 5.1 lid 2 sub e	5.1 lid 2 sub e @uwv.nl	5.1 lid 2 sub e
CC - Public Affairs	5.1 lid 2 sub e	5.1 lid 2 sub e @uwv.nl	5.1 lid 2 sub e
SBK	5.1 lid 2 sub e	5.1 lid 2 sub e @uwv.nl	5.1 lid 2 sub e
CISO	5.1 lid 2 sub e	5.1 lid 2 sub e @uwv.nl	5.1 lid 2 sub e
Functionaris Gegevensbescherming	5.1 lid 2 sub e	5.1 lid 2 @uwv.nl	
Bureau Integriteit	Piketttelefoon 5.1 lid 2 sub e (bereikbaar op werkdagen van 8.30 tot 17.00 uur	5.1 lid 2 sub e @uwv.nl	5.1 lid 2 sub e

DECENTRAAL			
Onderdeel	**Naam en telefoon**	**E-mailadres**	**Naam en telefoon vervanger**
Business Security Officers / IB&P-teams	Voor namen en contactgegevens: klik hier		
Servicedesk IV – BIS team	Algemeen telefoonnummer: 5.1 lid 2 sub e (bereikbaar van 07.00 tot 19.00 uur)	5.1 lid 2 sub e @uwv.nl	5.1 lid 2 sub e