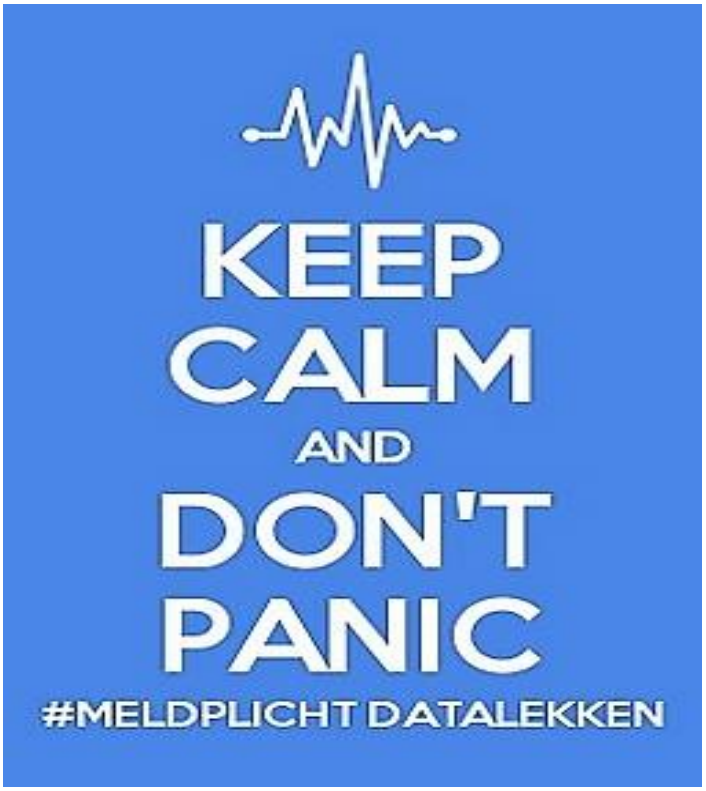
Ministerie van Veiligheid en Justitie

Datalek scenario's

Handreiking voor de afhandeling van (vermoedelijke) datalekken



Datum	15 augustus 2016
Status	versie 1.2

Colofon

Afzendgegevens	**Directie Informatisering en Inkoop** Turfmarkt 147 2511 DP Den Haag Postbus 20301 2500 EH Den Haag www.rijksoverheid.nl/venj
Contactpersoon	H.J.K.W. van der Molen (070) 370 7911
Projectnaam	Implementatie Meldplicht datalekken
Auteurs	Dirk Rinkel, Pieter de Groot, Bram Lamens, Ellen Beem, Just Stam, Eric Grobbe, Henk-Jan van der Molen

Versiehistorie

Versienr	Datum	Globale inhoud wijziging
0.1	21-4-2016	Initiële versie, waarin: • De separate scenario documenten zijn samengevoegd; • De stappen (incl. verwijzingen) consistent zijn genummerd en teksten daarop aangepast; • Hoofdstuk 1 (Aanleiding, Doelgroep, Evaluatie, Referten) toegevoegd; • Stap 7 (evaluatie) toegevoegd.
0.2	28-4-2016	Commentaar Werkgroep Privacy verwerkt, o.a. • Generieke stappen omgenummerd van [1-7].[1-6] naar [1-7].[a-f] voor onderscheid met paragrafen; • Scenario in H8 aangevuld met wie hun eigen betrokkenen het datalek meldt; • Generieke stap '8. Afsluiting' toegevoegd; • Diverse tekstuele verbeteringen en aanvullingen.
0.3	16-6-2016	Commentaar uit CISO overleg verwerkt.
1.0	23-6-2016	Versie als 'best practice' vastgesteld door CIO-Raad VenJ.

1.1	01-08-2016	Commentaar NP, BVC's en CIO Raad verwerkt; o.a.:
		• Hoofdstuk 'Voorbereiding afhandelen datalek' (H2) toegevoegd;
		• Generiek datalek scenario omgezet naar algemene procedure voor het afhandelen van datalekken; de specifieke scenario's zijn ingekort tot aandachtspunten, dubbele tekst verwijderd;
		• Relevante verbeteringen overgenomen uit:
		  • IND Procesbeschrijving datalekken versie 13-01-2016;
		  • CJIB Memo Proces Handelen bij Calamiteiten 20150203;
		  • NP Proces Meldplicht datalekken versie 15-03-2016.

1.2	15-08-2016	Aanvullend commentaar verwerkt o.a. van de werkgroep Privacy; bestandsnaam aangepast.
16-08-2016		Publicatie op VenJ-intranet

Inhoud

1 Inleiding

1.1 Aanleiding

Met ingang van 1 januari 2016 is de gewijzigde Wet bescherming persoonsgegevens (Wbp) in werking getreden, die een meldplicht invoert voor datalekken. Deze meldplicht houdt in dat organisaties die op grond van deze wet persoonsgegevens verwerken beveiligingsincidenten met (mogelijk) ernstige gevolgen voor de bescherming van persoonsgegevens onverwijld moeten melden aan de Autoriteit Persoonsgegevens. En organisaties moeten in bepaalde gevallen een datalek ook melden aan degenen van wie persoonsgegevens zijn gelekt (=betrokkenen).

Op de lange termijn zijn beveiligingsincidenten onvermijdelijk. De mogelijk daaruit resulterende datalekken kunnen grote financiële schade veroorzaken, voor zowel de eigen organisatie als voor een groot aantal betrokkenen. Naast de directe schade kan ook de imagoschade erg groot zijn, vooral binnen een politieke context.
Om schade te minimaliseren, is het nodig een procedure voor het afhandelen van een datalek vooraf uit te werken. Deze handreiking geeft handvatten voor het ontwikkelen van zo'n procedure en bevat alle verplichte onderdelen van de Wbp.

Onderdelen worden steeds afhankelijker van de data van andere organisaties. Het gebruik van deze handreiking voor de procedure van afhandeling van datalekken biedt dan meerwaarde. Zo ontstaat nl. een gemeenschappelijke basis die het risico verkleint dat VenJ datalekken met gedeelde data niet effectief of inefficiënt afhandelt.

1.2 Doelgroep en leeswijzer

De doelgroep van dit document vormen alle medewerkers die direct meewerken aan de afhandeling van een datalek, zoals:

- Medewerkers frontoffice en backoffice van ICT-dienstverlener en bewerker;
- Leidinggevenden;
- Technisch beheerders van VenJ-systemen;
- Chief Information Security Officers (CISO);
- Privacy Officers;
- Beveiligingscoördinatoren (BVC);
- Informatiebeveiligingsfunctionarissen van dienstonderdelen van VenJ;
- (Medewerkers) Beveiligingsautoriteit VenJ;
- Medewerkers van de directie Voorlichting;
- Medewerkers van de afdeling Juridische Zaken;
- De *Senior Responsible Owner* als eigenaar van een (generieke) applicatie, systeem of voorziening;
- Degenen die conform het Organisatiebesluit VenJ en daarop gebaseerde mandaatregelingen zijn aan te merken als 'verantwoordelijke' in de zin van de Wbp voor de verwerking van persoonsgegevens. Deze persoon stelt uiteindelijk het doel en de middelen voor de verwerking van persoonsgegevens vast (hierna te noemen: de verantwoordelijke).

In hoofdstuk 2 zijn de voorbereiding beschreven die een organisatie kan treffen om datalekken effectief en efficiënt af te handelen.

In hoofdstuk 3 staat het generieke proces voor het afhandelen van datalekken beschreven. Deze beschrijving vermeldt de te nemen stappen, de acties die actoren kunnen nemen en te registreren informatie.

In hoofdstuk 4 tot en met 10 staan de aandachtpunten van de volgende scenario's beschreven:

- Opvallend gedrag netwerk of systemen (H4);
- Verlies drager met persoonsgegevens (H5);
- Persoonsgegevens verkeerd geadresseerd (H6);
- Systeem-hack (H7);
- Extern bericht over datalek (H8);
- Melden datalek aan veel betrokkenen (H9);
- Datalek in gemeenschappelijke voorziening (H10).

1.3 Positionering van dit document

Dit document is gebaseerd op de Wbp bepalingen over de meldplicht. In sommige situaties kan andere wetgeving prevaleren. In de gezondheidszorg geldt bijvoorbeeld dat de zorgprofessional inhoudelijk verantwoordelijk is voor de medische dossiers van eigen patiënten. Bij een datalek zal de zorgprofessional vanuit die verantwoordelijkheid regie willen voeren over de melding naar betrokkenen.

In de praktijk heeft de dominante wetgeving geen invloed op de inhoud van de te nemen stappen zoals beschreven. Wel kan dit invloed hebben op **wie** er melding doet aan betrokkenen en **hoe** dit gebeurt. In sommige gevallen kan onduidelijk zijn wie van de lijnmanagers de verantwoordelijke is. Consulteer in dat geval de FG, Privacy Officer of de bedrijfsjurist.

1.4 Evaluatie van dit document

Deze handreiking is een levend document en nooit af, verbeteringen voor en aanvullingen op deze handreiking zijn daarom altijd welkom.

Om de actualiteit te borgen zal de Functionaris voor de Gegevensbescherming van VenJ als eigenaar dit document jaarlijks bijwerken. De eigenaar zal dit document ook aanpassen nadat de EU Algemene Verordening Gegevensbescherming van kracht wordt (25 mei 2018).

Daarnaast is het mogelijk dat een opgetreden datalek tussentijdse wijzigingen nodig maakt, bijvoorbeeld als blijkt dat dit document onvoldoende aansluit bij de werkelijkheid. We vragen de gebruikers van deze handreiking daarom expliciet om verbeteringen op de inhoud aan te dragen. Dit kan bij de volgende contactpersoon:

Functionaris voor de Gegevensbescherming Ministerie van VenJ
SG Cluster / Bureau Secretaris Generaal / Bureau Beveiligingsautoriteit
Mr. Pieter de Groot
p.j.de.groot@minvenj.nl | (06) 4810 0101

1.5 Referentiedocumenten

- Wet Bescherming Persoonsgegevens (Wbp) geldig vanaf 1-1-2016
- Beleidsregels Meldplicht Datalekken - versie 8-12-2015
- VenJ Circulaire Meldingsplicht Datalekken - versie 15-12-2015
- VenJ Incidentenregeling Integrale Beveiliging - versie 16-06-2011
- VenJ Procedure Escalatie van Incidenten - versie 0.1 (concept)
- Organisatiebesluit VenJ 2015 en onderliggende mandaatregelingen
- **Algemene Verordening Gegevensbescherming - versie 27-04-2016**

2 Voorbereiding afhandelen datalek

2.1 Wat is een datalek?

Volgens de definitie van de Autoriteit Persoonsgegevens[1] spreken we van een datalek als het gaat om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.

We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking - dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

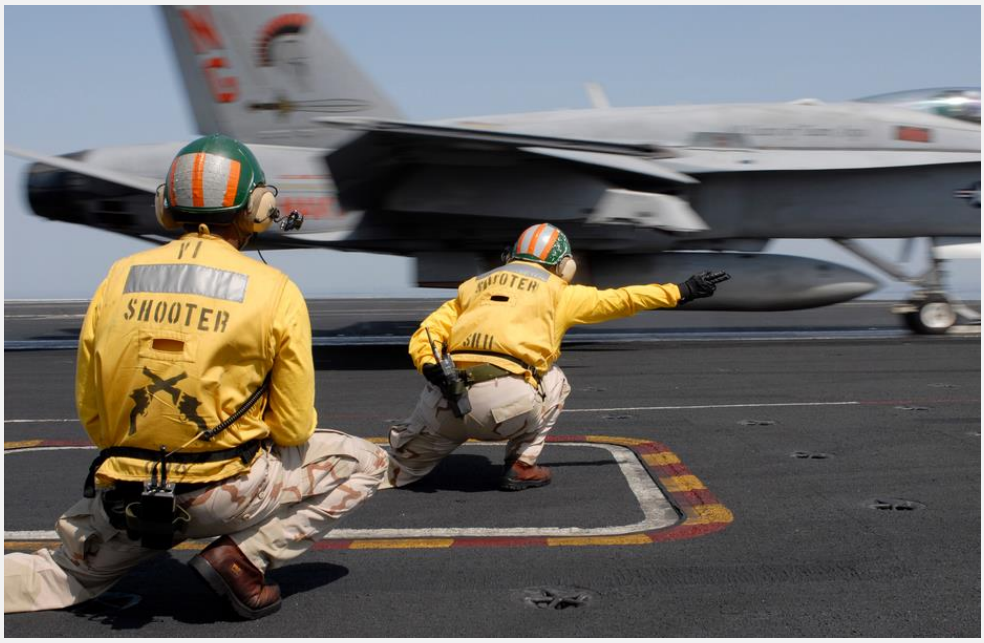
Op de lange termijn zijn beveiligingsincidenten en datalekken onvermijdelijk, elke organisatie krijgt ermee te maken. Voorbereiding op een datalek vertaalt zich dan terug in snellere afhandeling, minder schade en een beter imago van de organisatie.

2.2 Cultuur, attitude en vaardigheden

De voorbereiding start met dat er aandacht is voor gedrag, houding en cultuur t.a.v. incidenten, zodat de organisatie een veilige omgeving biedt om datalekken te melden. Illustratief hiervoor is de volgende anekdote.

> Op een nucleair vliegdekschip brak een boordwerktuigkundige een essentiële regel: hij hield niet bij welke gereedschappen hij gebruikte op het landingsdek. Na de reparatie ontdekt hij dat zijn gereedschap niet meer compleet was en meldde dit onmiddellijk aan zijn leidinggevende. Alle vliegtuigen in de lucht werden vervolgens omgeleid, totdat het vermiste gereedschap was gevonden.
>
> De dag erna werd de boordwerktuigkundige naar voren geroepen, voor het oog van de voltallige bemanning. Toen hij daar in zijn eentje voor de troep stond, kreeg hij een daverend applaus, omdat hij de moed had getoond zijn fout te melden voordat er schade kon ontstaan.
> Daarna werd het incident gebruikt als signaal dat de veiligheid kan verbeteren, waarbij iedereen van hoog tot laag werd ingeschakeld. Was het onoplettendheid? Klopt het systeem nog wel? Moeten medewerkers anders trainen of moet er een nieuwe standaard komen?
>
> [lees verder]

[1] Bron: website Autoriteit Persoonsgegevens (https://autoriteitpersoonsgegevens.nl)



Op een vliegdekschip houdt de werkvloer het schip operationeel. Het operationele personeel op een vliegdekschip traint daarom voortdurend en zwaar. Zij weten precies wat wel en niet werkt om risico's te verkleinen. Ondanks de militaire hiërarchie, heeft het personeel de bevoegdheid om **onmiddellijk** in te grijpen als er iets mis dreigt te gaan. Als zij merken dat een piloot tijdens de landing te nerveus is, kunnen ze zelfstandig de piloot opdracht geven om door te vliegen en het later opnieuw te proberen. Wachten op instructies van boven zou zoveel tijd kosten dat het vliegtuig intussen kan verongelukken.

2.3 Termijnen voor afhandeling datalek

Stap	Actor	Deadline
1. Signaleren incident / risico	Medewerker	0 uur
2. Beoordeling mogelijk datalek	(externe) datalekdeskundige	72 uur
3. Nader onderzoek	Onderzoeksteam	
4. Melding datalek aan AP	d.z.v. verantwoordelijke	
5. Treffen tegenmaatregelen	d.z.v. verantwoordelijke	z.s.m. daarna
6. Melding datalek aan betrokkenen	d.z.v. verantwoordelijke	
7. Evaluatie afhandeling datalek	Verantwoordelijke	N.t.b.
8. Afsluiting datalek	Verantwoordelijke	

Toelichting: *Voor* ***het melden van een datalek*** *bij de Autoriteit Persoons is een termijn gesteld van 72 uur nadat het datalek werd gesignaleerd.*

De verantwoordelijke moet zo snel mogelijk maatregelen treffen om het incident met ***correctieve maatregelen*** *op te lossen. Daarnaast zullen betrokkenen mogelijk ook maatregelen moeten nemen, zoals hun wachtwoord vernieuwen. Door beide acties zo snel mogelijk uit te voeren, minimaliseert de verantwoordelijke de impact van het datalek voor alle betrokkenen.*

Om het risico van datalekken te verminderen, zijn effectieve preventieve maatregelen nodig. De ***evaluatie*** *is nodig om verbeterpunten op te stellen voor:*

- *De preventieve maatregelen, om de kans op herhaling te minimaliseren;*
- *Het gevolgde proces voor het afhandelen van het datalek;*
- *De correctieve maatregelen die tijdens de afhandeling van het datalek werden getroffen.*

*Zodra de verantwoordelijke de **nazorg** voor betrokkenen over kan dragen naar reguliere bedrijfsprocessen, kan de verantwoordelijke het datalek formeel afsluiten.*

2.4 Actoren

De actoren die samenwerken bij de afhandeling van een datalek, zullen meestal maar een deel van de stappen uitvoeren. Het is aan te raden **vooraf** met deze actoren de procedure door te spreken voor het afhandelen van toekomstige datalekken.

Soort actor	**Stap**
Medewerkers VenJ	1
Leidinggevenden	1, 3, 7
Medewerkers front- en backoffice ICT-dienstverlener en bewerker, Technisch beheerders van VenJ-systemen	2
(Externe) datalek deskundige: Chief Information Security Officers (CISO), Beveiligingscoördinator (BVC), Privacy Officers, medewerkers van de afdeling Juridische Zaken, informatiebeveiligingsfunctionarissen	2 - 5, 7, 8
(Medewerkers) Beveiligingsautoriteit VenJ	1 - 2
Wbp verantwoordelijke	3 - 8
Functionaris voor de Gegevensbescherming (FG)	2
Medewerker van de directie Voorlichting	1, 6
Senior Responsible Owner die is aangemerkt als eigenaar van een (generieke) applicatie, systeem of voorziening	3 - 6

2.5 Registratie van handelingen en beslissingen

De aangelegde registratie van het datalek maakt het mogelijk dat de verantwoordelijke achteraf verantwoording kan afleggen over de afhandeling van het datalek. Om dat mogelijk te maken, moet de verzamelde registratie elke significante handeling bevatten van VenJ medewerkers.

Meer precies gaat het dan om **wie, wat, waar en wanneer** deed voor de afhandeling van het incident, de opstelling en evaluatie van (voorlopige) adviezen en het formele besluit om het datalek wel of niet te melden aan de AP en betrokkenen. Vanuit efficiency moet het register tevens de contactgegevens van medewerkers bevatten. Uit de registratie blijkt ook de op- en afbouw van de zorg naar betrokkenen en de formele afsluiting van het datalek.

De registratie genoemd in dit handboek kan uit de volgende bronnen bestaan:

- Het incidentenregister van het eigen dienstonderdeel;
- Het incidentregister van de ICT Helpdesk;
- Het logboek(en) van de medewerkers die hebben meegewerkt aan de afhandeling van het incident;
- De uitgewisselde communicatie zoals e-mails, webpagina's, advertenties, brieven.

3 Generiek proces voor afhandelen datalek

In dit hoofdstuk staan de generieke processtappen en de acties waaruit die bestaan. De verantwoordelijke kan deze stappen parallel laten uitvoeren.

Stap 1. Signaleren (mogelijk) incident / risico

Een signaal of een geconstateerde fout kan een aanwijzing zijn dat persoonsgegevens waarvoor VenJ verantwoordelijk is, verloren zijn gegaan, gestolen zijn of onrechtmatig zijn verwerkt.

Actie 1.a Informeren direct leidinggevende

De medewerker die het signaal of de opgetreden fout waarneemt, geeft dat aan bij zijn direct leidinggevende. Hij doet dat ook als hij niet direct kan vaststellen of de bedrijfsinformatie van VenJ daadwerkelijk gevaar loopt.

De leidinggevende vraagt (door) naar de toedracht, omstandigheden, soort en omvang van de persoonsgegevens die mogelijk zijn blootgesteld aan onrechtmatige verwerking.

De leidinggevende bepaalt op basis van de informatie van de medewerkers of hij dit incident meldt aan de (externe) datalekdeskundige binnen het organisatieonderdeel waar hij werkzaam is.

Actie 1.b Informeren (externe) datalekdeskundige

De direct leidinggevende meldt de signalen aan de (externe) datalekdeskundige binnen het dienstonderdeel en vraagt hem om een nadere beoordeling daarvan. De direct leidinggevende geeft de datalekdeskundige eventueel het mandaat om binnen het onderdeel zelfstandig voorlopige maatregelen te (laten) treffen.

Stap 2. Beoordeling mogelijk datalek door (extern) datalekdeskundige

Actie 2.a Opvragen (extra) informatie

De (externe) datalekdeskundige neemt kennis van de signalen en vraagt alle relevante informatie op bij degene die het mogelijke datalek heeft gesignaleerd.

De (externe) datalekdeskundige bepaalt aan de hand van een beschikbare referentielijst wie op grond van het Organisatiebesluit VenJ 2015 en onderliggende mandaatregelingen als (gemandateerde) verantwoordelijke is aan te merken.

Actie 2.b Nemen voorlopige maatregelen (monitoring / preventief / correctief)

De (externe) datalekdeskundige geeft op basis van de ontvangen informatie zo nodig opdracht om:

- Het betreffende systeem gedurende een bepaalde periode nauwkeurig te monitoren en hem te informeren over de resultaten daarvan;
- Het systeem dat de persoonsgegevens verwerkt tijdelijk stil te leggen, maar **alleen** als de impact voor de gebruikers van het systeem gering is ten opzichte van de toenemende schade van het doordraaien van het systeem.

Actie 2.c Opstellen voorlopig advies

Conform par. 3 van de Beleidsregels van de Autoriteit Persoonsgegevens (AP) voor toepassing van artikel 34a van de Wbp (hierna te noemen: Beleidsregels) zijn er twee mogelijkheden:

- De (externe) datalekdeskundige concludeert op basis van de informatie uit stappen 2.a en 2.b dat de **melding** in het kader van de meldplicht datalekken **achterwege kan blijven**. Hij legt deze conclusie vast in het incidentenregister van zijn dienstonderdeel,
  – OF –
- De (externe) datalekdeskundige concludeert op basis van de opgevraagde informatie **dat er sprake is van een mogelijk datalek**. Hij legt deze conclusie vast in het incidentenregister van zijn dienstonderdeel. Hij adviseert vervolgens ***onverwijld*** de Wbp verantwoordelijke voor de verwerking van persoonsgegevens nader onderzoek te laten uitvoeren om vast te stellen of er

sprake is van een datalek en, zo ja, om conform par. 4 van de Beleidsregels vast te stellen of er sprake is van een datalek met (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

Stap 3. Nader onderzoek

Dit onderzoek beantwoordt de volgende vragen:

- Of het incident een datalek betreft dat de verantwoordelijke moet (laten) melden aan de Autoriteit Persoonsgegevens;
- Of de verantwoordelijke het datalek moet (laten) melden aan de betrokkenen van wie de persoonsgegevens zijn gelekt.

Daarnaast levert het onderzoek de gegevens op die inhoudelijk nodig zijn voor de (voorlopige) melding aan de AP en betrokkenen.

Actie 3.a Overdracht advies aan Wbp verantwoordelijke

De verantwoordelijke neemt kennis van het advies van de (externe) datalekdeskundige en de aangereikte informatie.

Actie 3.b Evaluatie voorlopig advies

De verantwoordelijke wijst het voorlopige advies af, of hij neemt het over. In beide gevallen legt de verantwoordelijke deze beslissing vast in het incidentenregister van zijn dienstonderdeel.

Actie 3.c Inrichten onderzoeksteam

De verantwoordelijke stelt voor het onderzoek een team van (externe) datalekdeskundigen (zie paragraaf 2.4 op blz 9) samen. Hiervoor kan hij een beroep doen op de CISO van VenJ, de Functionaris voor de Gegevensbescherming van VenJ. Voor de bedrijfsjuridische aspecten van het onderzoek roept hij de ondersteuning in van zijn afdeling Juridische Zaken en eventueel de bedrijfsjuristen bij de directie Informatisering en Inkoop.

Actie 3.d Vaststellen onderzoeksopdracht

Het team onderzoekt het incident om de verantwoordelijke zo snel mogelijk, zo mogelijk niet later dan 48 uur na het conform stap 2.c uitgebrachte advies, antwoord te geven op de vraag:

- Of er sprake is van een datalek dat de verantwoordelijke het datalek moet (laten) melden aan de Autoriteit Persoonsgegevens en, zo ja,
- Of er bovendien sprake is van een datalek met (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Zo ja, dan heeft de verantwoordelijke de plicht de betrokkenen het datalek te melden;
- Welke preventieve en correctieve maatregelen de organisatie en de betrokkenen kunnen treffen.

De verantwoordelijke accordeert de opdracht voor het onderzoek, wijst een opdrachtnemer aan, wijst middelen en mensen toe aan het onderzoek en ziet toe op de uitvoering van het onderzoek.

Actie 3.e Opvragen extra informatie

Het team vraagt meer en actuele informatie op voor hun onderzoek, bijvoorbeeld op basis van de voorlopige maatregelen in stap 2.b.

Actie 3.f Opstellen advies over melding datalek aan AP / betrokkenen en te nemen maatregelen

Het team stelt een definitief advies op dat de onderzoeksopdracht en draagt het advies over aan de verantwoordelijke.

Stap 4. Melding aan AP

Actie 4.a Beslissing verantwoordelijke op gegeven advies

Hierbij zijn drie mogelijkheden:

- De verantwoordelijke komt op basis van de uitkomst van het onderzoek tot de conclusie dat er geen sprake is van een datalek,
  – OF –
- De verantwoordelijke komt op basis van de uitkomst van het onderzoek tot de conclusie dat er wel sprake is van een datalek, maar geen datalek met (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens,
  - OF –
- De verantwoordelijke komt op basis van de uitkomst van het onderzoek tot de conclusie dat er sprake is van een datalek met (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

In alle gevallen legt de verantwoordelijke deze beslissing vast in het incidentenregister van zijn dienstonderdeel.

Actie 4.b Opstellen / muteren (voorlopige) melding aan AP

Als een datalek (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, dan moet de verantwoordelijke dit datalek tijdig melden bij de AP. De verantwoordelijke meldt het datalek zo snel mogelijk, bij voorkeur niet later dan 72 uur na het conform stap 2.c uitgebrachte advies. Paragraaf 5 van de Beleidsregels schrijft voor hoe de verantwoordelijke een datalek moet melden bij de Autoriteit Persoonsgegevens (AP). De AP heeft daarvoor een online Meldloket ingericht.

Indien de verantwoordelijke het datalek later dan 72 uur na het conform stap 2.c uitgebrachte advies meldt bij de AP, dan kan hij desgevraagd motiveren waarom hij de melding later heeft gedaan.

Indien de verantwoordelijke 72 uur na het conform stap 2.c uitgebrachte advies nog niet volledig zicht heeft op wat er is gebeurd en om welke persoonsgegevens het gaat, doet de verantwoordelijke de melding op basis van de gegevens waarover hij op dat moment beschikt.

Eventueel vult de verantwoordelijke de melding naderhand nog aan of trekt hij deze in.

Actie 4.c Vervolgstappen melding

De verantwoordelijke volgt de relevante stappen conform het addendum op de incidentenregeling Integrale Veiligheid zoals opgenomen in de Circulaire meldplicht datalekken.

Stap 5. Treffen tegenmaatregelen

De verantwoordelijke geeft opdracht om binnen zijn onderdeel (aanvullende) technische en/of organisatorische maatregelen te nemen om het risico te mitigeren dat persoonsgegevens daadwerkelijk blootstaan aan verlies, diefstal of onrechtmatige verwerking.

Om het risico van datalekken daadwerkelijk te verminderen, zijn effectieve maatregelen nodig. De verantwoordelijke kan de effectiviteit van de genomen maatregelen (laten) vaststellen met de 4xO systematiek. Als de tijd het niet toelaat, kan verantwoordelijke de 4xO systematiek toepassen in stap 7 'Evaluatie'.

De 4xO analyse systematiek bestaat uit:

- **Oorzaak**: analyseer de grondoorzaak van het incident / risico; is er sprake van een structureel gebrek aan kwaliteit in het proces of is hier sprake van een nieuw verschijnsel?
- **Omvang**: bepaal de impact van het incident / risico in termen van locaties, processen en levenssfeer van betrokkenen. Dit bepaalt de scope van corrigerende maatregelen.

- **Oplossing**: specificeer vanuit de Oorzaak en Omvang analyse de corrigerende maatregelen, zowel preventief naar de grondoorzaak als correctief naar de omvang van het incident / risico.
- **Operationaliteit**: verifieer objectief de effectiviteit van de getroffen maatregelen, bijvoorbeeld met een interne controle, Peer Review of audit.

Actie 5.a Preventieve maatregelen
Deze maatregelen zijn erop gericht om vanuit de Oorzaak analyse in stap 3 in de toekomst de kans te verminderen dat een dergelijk incident zich opnieuw kan voordoen. Hieronder vallen ook maatregelen om de detectie en afhandeling van dergelijke incidenten in te toekomst te verbeteren.

En voorbeeld van een preventieve maatregel: *Periodieke beveiligingsaudits worden uitgevoerd in opdracht van het lijnmanagement* (zie BIR 6.1.8.2 - Beoordeling van het informatiebeveiligingsbeleid).

Het treffen van preventieve maatregelen heeft in principe prioriteit boven correctieve maatregelen, vanuit de logica dat je beter eerst de kraan kunt dichtdraaien VOORDAT je begint met dweilen.

Actie 5.b Correctieve maatregelen
Correctieve maatregelen betreffen het herstellen van de schade veroorzaakt door het datalek. Vanuit de Omvang analyse in stap 3 kunnen alle benodigde maatregelen worden afgeleid. In eerste instantie betreft dat de schade voor betrokkenen, maar ook het imago van de verantwoordelijke en de organisatie kan herstel nodig hebben.

Een voorbeeld van een correctieve maatregel: *de vastgestelde procedure uitvoeren nadat een crypto sleutel is gecompromitteerd.* (zie BIR 12.3.2 - Sleutelbeheer).

Stap 6. Melding datalek aan betrokkenen

Actie 6.a Voorbereiding
Tegelijk met de verlening van de in stap 3.d bedoelde opdracht vraagt de verantwoordelijke het onderzoeksteam conform par. 7 van de Beleidsregels ook te beoordelen of het datalek waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van betrokkenen.
Zodra het onderzoeksteam tot een bevestigend oordeel is gekomen en de verantwoordelijke dit oordeel heeft overgenomen, meldt de verantwoordelijke het datalek conform par. 8 en 9 van de Beleidsregels onverwijld aan betrokkenen.

Actie 6.b Uitvoering
De verantwoordelijke handelt verder conform de Circulaire meldplicht datalekken, het daarin opgenomen addendum op de incidentenregeling Integrale Veiligheid.

Actie 6.c Nazorg
Nadat de voorgenomen acties zijn uitgevoerd, zal de verantwoordelijke de gebruikte resources (mensen en voorzieningen) verminderen of geheel vrijgeven.
De verantwoordelijke legt elke significante wijziging vast in het incidentenregister.

Stap 7. Evaluatie afhandeling datalek
Een opgetreden incident of een gemeld risico kan een aanwijzing zijn dat het 'systeem' in de organisatie niet werkt zoals bedoeld. Het is daarom in het belang van de organisatie als de verantwoordelijke voor een (onafhankelijke) controle laat uitvoeren op de uitgevoerde acties t.o.v. Incidentenregeling, Circulaire en beleidsregels. Een ADR audit of een evaluatie door medewerkers die buiten de afhandeling van dit incident stonden, kan deze evaluatie in- of aanvullen.

Voor de evaluatie kunnen verschillende informatiebronnen worden gebruikt, zoals de ingevulde logboeken, verstuurde e-mails en interviews met medewerkers en betrokkenen. Daarnaast kan het zinvol zijn externe partijen te betrekken bij de evaluatie, zoals het NCSC bij cyberincidenten.

Actie 7.a Verbetering preventieve maatregelen
De evaluatie kan verbeteringen op maatregelen voorstellen die de kans op soortgelijke incidenten te verminderen, zoals
- Het beperken van de sets van persoonsgegevens die de organisatie verwerkt;
- Het tijdig signaleren van beveiligingsincidenten voordat er schade ontstaat.

Actie 7.b Verbetering correctieve maatregelen
Uit de evaluatie kunnen verbeteringen op maatregelen volgen die de schade kunnen beperken, zoals:
- Het beter afhandelen van een beveiligingsincident (bijvoorbeeld door het verbeteren van deze Datalek scenario's);
- Het verhogen van de frequentie en omvang van te maken back-ups.

Actie 7.c Verbetering eigen procedures
De processtappen die de medewerkers hebben uitgevoerd bij de afhandeling van dit datalek worden vergeleken met de beschreven procedure. Als terecht is afgeweken van de eigen procedure, kan de procedure (en deze handreiking) mogelijk worden verbeterd.

Actie 7.d Opstellen en communicatie van Lessons Learned
Om het leereffect te maximaliseren, is een document nodig over de afhandeling van dit incident. Dit document bevat zoveel mogelijk feitelijke informatie (zie paragraaf 2.4 - Documentatie), waarbij eventuele persoonsgegevens moeten worden geanonimiseerd.

Het ligt voor de hand de *lessons learned* te delen met alle mogelijke actoren binnen de organisatie.

Stap 8. Afsluiting datalek
Zodra alle voorgenomen acties om het datalek af te handelen zijn uitgevoerd, neemt de verantwoordelijke het besluit om het incident formeel af te sluiten.
De verantwoordelijke legt de afsluiting vast in het incidentenregister.

4 Datalek scenario Opvallend gedrag netwerk of systemen[2]

4.1 Omschrijving scenario

Technisch beheerders van de VenJ netwerkcomponenten signaleren afwijkingen en/of opvallend verkeer op bijvoorbeeld de volgende componenten:

- Webservers of mailservers;
- Firewalls en AntiVirus;
- Intrusion Detection Systems / Intrusion Prevention Systems (IDS / IPS);
- Systeem voor Incident en Event Management (SIEM);
- Informatiesystemen / applicaties en databases;
- Fileshares, routers en printers;

De afwijkingen en/of het opvallende dataverkeer hebben bijvoorbeeld betrekking op de volumes, tijdstippen en de bestemmingen van het in- en uitgaande dataverkeer.

4.2 Aandachtspunten

Stap 1. Signaleren incident / risico

De gesignaleerde afwijkingen kunnen een poging zijn om toegang te krijgen tot de bedrijfsinformatie van VenJ respectievelijk mogelijke blootstelling aan verlies, diefstal of onrechtmatige verwerking van persoonsgegevens waarvoor VenJ verantwoordelijk is.

Actie 1.a Informeren direct leidinggevende

Als de technisch beheerders deze signalen niet direct kunnen interpreteren als een poging om toegang te krijgen tot bedrijfsinformatie van VenJ, dan geven de technische beheerders dat aan in hun melding.

Actie 1.b Informeren (externe) datalekdeskundige

De technisch beheerders melden signalen van afwijkingen en/of opvallend verkeer op netwerkcomponenten van VenJ aan de (externe) datalekdeskundige binnen het dienstonderdeel die de desbetreffende netwerkcomponenten gebruikt. Er zijn drie situaties denkbaar:

- Het dienstonderdeel heeft een eigen ICT-beheerorganisatie/dienstverlener (DJI, CJIB, Justid);
- Het dienstonderdeel neemt ICT-diensten af van een Rijks SSO (Bestuursdepartement, IND, DT&V) of van een ander onderdeel van VenJ (RvdK);
- Het dienstonderdeel neemt ICT diensten af van een marktpartij (OM => Atos en Capgemini).

In alle drie de situaties nemen de technisch beheerders - eventueel na ruggenspraak met hun leidinggevende(n) - rechtstreeks contact op met de verantwoordelijke CISO of (informatie)beveiligingsfunctionaris.

[2] Dit scenario gaat ervan uit dat in de bewerkersovereenkomst is vastgelegd dat de bewerker de verantwoordelijke onverwijld meldt als er een datalak aan de orde is.

5 Datalek scenario Verlies drager met persoonsgegevens

5.1 Omschrijving scenario

Als gevolg van het handelen/nalaten van een medewerker van Veiligheid en Justitie zijn persoonsgegevens waarvoor VenJ verantwoordelijk is mogelijk blootgesteld aan verlies, diefstal of onrechtmatige verwerking. Het gaat hier om de volgende situaties:

- Verlies of diefstal van digitale gegevensdragers zoals een smartphone, tablet, laptop of usb-stick;
- Verlies of diefstal van papieren dossiers met persoonsgegevens;
- Papieren stukken met persoonsgegevens laten slingeren of zijn niet in de juiste containers afgevoerd.

5.2 Aandachtspunten

Stap 1. Signaleren incident / risico

Actie 1.a Informeren direct leidinggevende

De medewerker meldt het verlies of diefstal van de digitale gegevensdrager dan wel verlies of diefstal van papieren dossiers met persoonsgegevens of het laten slingeren, dan wel niet in de juiste containers afvoeren daarvan onverwijld aan zijn leidinggevende.

De leidinggevende vraagt (door) of er een real time back-up is van gegevens die verloren zijn gegaan, dan wel wat de impact is als de back-up verouderd of afwezig is.

De leidinggevende bepaalt op basis van de door melder verstrekte informatie over de aard en omvang van de gegevens die verloren zijn gegaan, of hij dit incident meldt aan de ICT Helpdesk, of de (externe) datalekdeskundige binnen het organisatieonderdeel waar hij werkzaam is.

Stap 2. Beoordeling mogelijk datalek door (externe) datalekdeskundige

De medewerker helpdesk c.q. (externe) datalekdeskundige neemt de melding in ontvangst en registreert de gegevens over dit incident.

Actie 2.a Opvragen (extra) informatie

De medewerker helpdesk c.q. (externe) datalekdeskundige checkt:

- Of de ontvangen informatie compleet en actueel is;
- Of verloren gegane gegevens op het medium adequaat zijn vercijferd (bijvoorbeeld usb-stick verstrekt door VenJ).

Actie 2.b Nemen voorlopige maatregelen (monitoring / preventief / correctief)

In geval van verlies of diefstal van smartphone of tablet gaat de medewerker Helpdesk onverwijld over tot het op afstand wissen van deze gegevensdragers. Daarmee verwijdert de Helpdesk medewerker alle gegevens en apps die lokaal waren opgeslagen op de smartphone of tablet.

Actie 3.e Opvragen extra informatie

In voorkomend geval vraagt het team informatie op over de veiligheid van de encryptie (methode en wachtwoord).

Stap 5. Te nemen maatregelen

Actie 5.a Preventieve maatregelen

Als blijkt dat vergelijkbare persoonsgegevens op andere gegevensdragers staan waarvoor hetzelfde risico geldt, dan is het wenselijk maatregelen te treffen om de impact van het lekken van deze data te verminderen. Hierbij vallen maatregelen zoals goede encryptie van data of een biometrisch 'wachtwoord' met een scanner voor vingerafdrukken.

Actie 5.bCorrectieve maatregelen
Uitgangspunt in deze paragraaf is dat een kopie van de vermiste gegevens beschikbaar is.
De laatste back-up van de gegevens komt beschikbaar voor de gebruiker die de gegevensdrager is verloren. Dat kan een actie zijn die via de Helpdesk loopt, soms kan gebruiker zelf een kopie maken van gegevens die op het interne netwerk staan.

Is er geen (recente) back-up beschikbaar, dan kan het nodig zijn de gegevens opnieuw samen te stellen. Mogelijk moeten mutaties op de gegevens sinds de laatste back-up opnieuw worden doorgevoerd. In dat geval is de hersteltijd groter, zodat de verantwoordelijke mogelijk aan betrokkenen moet melden dat het langer duurt om de afgesproken service te herstellen.

6 Datalek scenario Persoonsgegevens verkeerd geadresseerd

6.1 Omschrijving scenario

Als gevolg van het handelen/nalaten van een medewerker van Veiligheid en Justitie zijn persoonsgegevens waarvoor VenJ verantwoordelijk is mogelijk blootgesteld aan verlies, diefstal of onrechtmatige verwerking:

- Medewerker heeft intentie om (gedigitaliseerde) documenten met persoonsgegevens van persoon A te sturen naar (de gemachtigde van) persoon A, maar constateert achteraf dat ze feitelijk zijn verzonden naar (de gemachtigde van) persoon B;
- Medewerker vertrouwt voor de verzending van (gedigitaliseerde) documenten met betrekking tot persoon A op de adresgegevens van persoon A in de Gemeenschappelijke Basis Administratie (GBA), maar constateert achteraf dat deze niet juist zijn en dat iemand anders deze persoonsgegevens zal kunnen inzien.

6.2 Aandachtspunten

Stap 1. Signaleren incident / risico

Actie 1.a Informeren direct leidinggevende

De medewerker constateert de adresseringsfout, waardoor persoonsgegevens mogelijk toegankelijk zijn geworden voor onbevoegde personen. Hij meldt dit onverwijld aan zijn leidinggevende.

7 Datalek scenario Systeem hack

7.1 Omschrijving scenario

De beheerders van de applicatie of het systeem waarmee de bewerker persoonsgegevens verwerkt ten behoeve van de verantwoordelijke, constateren dat (persoons) gegevens die deze applicatie of dit systeem verwerkt:

- Zijn blootgesteld aan verlies (bijvoorbeeld ransomware) of diefstal (zoals hacker), of
- Door eigen handelen of nalaten van de beheerders zijn blootgesteld aan verlies, diefstal of onrechtmatige verwerking, of
- Door een ander technisch of organisatorisch falen zijn blootgesteld aan verlies, diefstal of onrechtmatige verwerking.

7.2 Aandachtspunten

Stap 1. Signaleren incident / risico

Actie 1.a Informeren direct leidinggevende

De beheerders van de applicatie of het systeem waarmee de bewerker persoonsgegevens verwerkt ten behoeve van de verantwoordelijke, melden aan de eigenaar de dat (persoons) gegevens die deze applicatie of dit systeem verwerkt mogelijk zijn blootgesteld aan verlies, diefstal of onrechtmatige verwerking.

Actie 1.b Informeren (extern) datalekdeskundige

De beheerders melden dit incident onverwijld aan de (extern) datalekdeskundige binnen het dienstonderdeel van VenJ dat de verwerking van deze persoonsgegevens heeft uitbesteed aan de bewerker ten behoeve van wie zij werkzaam zijn.

Stap 5. Te nemen maatregelen

De verantwoordelijke geeft aan de bewerker opdracht om binnen de mogelijkheden die op dat moment beschikbaar zijn (aanvullende) technische en/of organisatorische maatregelen te nemen om het risico te mitigeren dat persoonsgegevens (daadwerkelijk) blootstaan aan verlies, diefstal of onrechtmatige verwerking.

Actie 5.b Correctieve maatregelen

De verantwoordelijke geeft aan de afdeling Juridische Zaken/bedrijfsjurist van zijn dienstonderdeel opdracht om te onderzoeken of, en zo ja hoe de bewerker op grond van de met bewerker gesloten overeenkomst(en):

- En/of op grond van enige wettelijke verplichting VenJ de bewerker aansprakelijk kan stellen voor de eventuele gevolgschade van het datalek;
- VenJ de bewerker in gebreke kan stellen voor het niet nakomen van verplichtingen ingevolge deze overeenkomst(en).

De verantwoordelijke kan voor dit onderzoek tevens een beroep doen op de bedrijfsjuristen van de directie Informatisering en Inkoop en de Functionaris voor de Gegevensbescherming.

Indien de verantwoordelijke op basis van het bovenstaande onderzoek concludeert dat VenJ de bewerker op grond van de met bewerker gesloten overeenkomst(en) en/of op grond van enige wettelijke verplichting aansprakelijk kan stellen voor de eventuele gevolgschade van het datalek, stelt hij de bewerker op de vereiste wijze aansprakelijk voor (gehele of gedeeltelijke) vergoeding van de geleden gevolgschade van het datalek.

Indien de verantwoordelijke op basis van het onderzoek in stap 5.b concludeert dat VenJ de bewerker op grond van de met bewerker gesloten overeenkomst(en) in gebreke kan stellen wegens het niet nakomen van verplichtingen ingevolge deze overeenkomst, stelt hij de bewerker op de vereiste wijze in gebreke.

8 Datalek scenario Extern bericht over datalek

8.1 Omschrijving scenario

De organisatie krijgt van buiten een bericht waaruit is af te leiden dat er mogelijk sprake is van een datalek. Er is aan dit bericht geen interne melding vooraf gegaan overeenkomstig de circulaire meldplicht datalekken van de SG en het addendum incidentenregeling Integrale Veiligheid.

Voorbeeld 1: bericht in media waarin stond dat het dossier van een gedetineerde zou zijn ontvreemd uit zijn cel in een PI.

Voorbeeld 2: bericht in media waarin stond dat een vrouw van een regionale politie-eenheid abusievelijk vuilniszakken met onder meer persoonsgegevens ontving in plaats van haar -eerder in beslag genomen- persoonlijke eigendommen.

Voorbeeld 3: bij het NCSC komt een melding binnen waarin een externe onderzoeker via *Responsible Disclosure* de VenJ organisatie wijst op een beveiligingsrisico.

8.2 Aandachtspunten

Stap 1. Signaleren incident / risico

Actie 1.a Informeren direct leidinggevende

De medewerker van de directie Voorlichting en/of het bureau Beveiligingsautoriteit neemt kennis van een extern bericht waaruit is af te leiden dat er mogelijk sprake is van blootstelling aan verlies, diefstal of onrechtmatige verwerking van persoonsgegevens, voor de verwerking waarvan de minister van Veiligheid en Justitie de politiek eindverantwoordelijke is.

Actie 1.b Informeren (extern) datalekdeskundige

De medewerker van de directie Voorlichting en/of van het bureau Beveiligingsautoriteit stuurt het bericht onverwijld door naar de BVA en de Functionaris voor de Gegevensbescherming van het ministerie.

Stap 2. Beoordeling mogelijk datalek door (externe) deskundige

Actie 2.a Opvragen (extra) informatie

De BVA en Functionaris voor de Gegevensbescherming checken of het desbetreffende mogelijke datalek al is gemeld aan BVA en Functionaris voor de Gegevensbescherming overeenkomstig de Circulaire meldplicht datalekken van de SG en het daarin opgenomen addendum op de Incidentenregeling Integrale Veiligheid:

- Zo nee, dan verder naar stap 2.b;
- Zo ja, geen aanvullende actie van BVA en Functionaris voor de Gegevensbescherming vereist, anders dan in Circulaire en addendum al zijn beschreven.

Actie 2.b Nemen voorlopige maatregelen (monitoring / preventief / correctief)

De BVA en Functionaris voor de Gegevensbescherming vragen de afdeling Voorlichting om eventuele nieuwe berichten in de media te registreren en naar hen door te sturen.

9 Datalek scenario Melden datalek aan veel betrokkenen

9.1 Omschrijving scenario

De verantwoordelijke voor de desbetreffende gegevensverwerking heeft conform par. 7 van de Beleidsregels van de Autoriteit Persoonsgegevens geconcludeerd dat een door hem geconstateerd datalek waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van een groot aantal (lees: duizenden) betrokkenen. Dat betekent dat de verantwoordelijke dit datalek zo snel mogelijk moet gaan melden aan al die betrokkenen.

Bij het melden van het datalek aan betrokkenen kan het voorkomen dat de contactgegevens van een aantal betrokkenen niet meer actueel zijn. Volgens de wet is een verantwoordelijke verplicht een **redelijke** inspanning te doen (meer is niet vereist) om betrokkenen te informeren. Als de juiste contactgegevens van een betrokkene moeilijk te achterhalen zijn, dan volstaat het kunnen aantonen van die redelijke inspanning.

9.2 Aandachtspunten

De aandachtpunten voor dit scenario hebben alleen betrekking op stap 6 - Melding aan betrokkenen.

Actie 6.a Voorbereiding

De verantwoordelijke installeert een 'incidententafel'. Deze tafel heeft de volgende leden:

- De directeur (of diens plaatsvervanger) van de beheerorganisatie die verantwoordelijk is voor het beheer van het systeem of de applicatie waarmee de desbetreffende gegevensverwerking plaatsvindt en daarmee ook verantwoordelijk is voor het treffen van adequate informatiebeveiligingsmaatregelen op het desbetreffende systeem of applicatie;
- De directeur die binnen het organisatieonderdeel verantwoordelijk is voor de uitvoering van het bedrijfsproces dat dit systeem of de applicatie ondersteunt;
- De voorlichter van het desbetreffende organisatieonderdeel;
- De bedrijfsjurist van het desbetreffende organisatieonderdeel.

Verder maken van deze tafel deel uit:

- De voorlichter van het bestuursdepartement;
- De functionaris voor de gegevensbescherming;
- De bedrijfsjurist en juridisch adviseur van het bestuursdepartement.

De verantwoordelijke beoordeelt, in lijn met stap 3.2.19 van de incidentenregeling Integrale Veiligheid of (aanvullend op de 'incidententafel') hij een 'DG-tafel' inricht:

DG-tafel
Indien het incident daartoe aanleiding geeft beoordeelt een DG of hij een DG-tafel bijeen zal roepen. Een DG bepaalt of het nodig is de bewindslieden te informeren.
Deze incidentenregeling beschrijft niet de opschalingstap van het informeren van de bewindslieden. Zie hiervoor de schematische procesbeschrijving 'Haagse hectiek, procesbeschrijving Incidentenroutine, pagina 2 en 3, van een Ander Justitie, project Incidentenstrategie, maart 2006'. Deze incidentenroutine beschrijft in feite het intern verloop van de incidentmelding vanaf het moment dat een veldorganisatie (en/of hoofdkantoor) een incident meldt aan de DG van hun specifieke sector.

Zo ja, dan adviseert de verantwoordelijke de DG in zijn lijn een DG-tafel in te richten. Indien de DG dit advies overneemt, dan treedt deze voor de verdere afwikkeling van dit incident in het kader van de meldplicht datalekken op als verantwoordelijke en volgt deze de stappen 4 tot en met 10.

Actie 6.b Uitvoering

De verantwoordelijke brengt in ieder geval nauwkeurig in kaart:

- Welke gegevens van welke betrokkenen zijn gelekt;
- Welke gevolgen en risico's een kwaadwillende (potentieel) kan inroepen voor de betrokkenen door het beschikbaar hebben van deze gegevens;
- Of, en zo ja, hoe deze gevolgen en risico's zich daadwerkelijk hebben voltrokken dan wel nog kunnen voltrekken;
- Welke maatregelen VenJ al heeft getroffen, dan wel VenJ en de betrokkenen nog kunnen treffen om deze gevolgen en risico's te voorkomen of mitigeren;
- Met welke personen of instanties de betrokkenen contact op kunnen nemen voor meer informatie;
- Hoeveel tijd, geld, middelen en kwaliteit noodzakelijk zijn om deze maatregelen te treffen;
- Hoeveel tijd, geld, middelen en kwaliteit noodzakelijk zijn en beschikbaar komen om betrokkenen volledig, adequaat en juist te informeren en ondersteunen;
- Of tijd, geld, middelen en kwaliteit van elders binnen VenJ beschikbaar kunnen worden gesteld.

De beslissing over hoeveel tijd, geld, middelen en kwaliteit worden aangewend om mitigerende maatregelen te treffen en betrokkenen te informeren worden op DG en/of SG-niveau genomen.

De verantwoordelijke informeert betrokkenen per brief en/of mail. Daarvoor zijn nodig: NAW-gegevens en e-mailadres. De brief en/of mail bevat in ieder geval informatie over:

- Welke gegevens zijn gelekt;
- Oorzaak van het lek;
- (Mogelijke) gevolgen en risico's van het lek voor de betrokkene;
- Welke maatregelen al zijn getroffen om deze gevolgen en risico's te voorkomen of mitigeren;
- Welke maatregelen betrokkenen zelf kunnen nemen om gevolgen en risico's te voorkomen of mitigeren en hoe ze dit kunnen doen;
- Verwijzen naar website voor nadere informatie en FAQ's;
- Verwijzen naar helpdesk (telefoon, mail);
- Of, en zo ja welke nadere informatie, hoe en wanneer nog volgt;
- Of, en zo ja, welke hulp of schadevergoeding de verantwoordelijke aanbiedt, gegeven de aard en de ernst van de gelekte gegevens en de daaruit voortvloeiende gevolgschade voor betrokkenen.

De verantwoordelijke richt een helpdesk in (telefoonnummer en mailbox), beschikbaar/open gedurende werkdagen en kantooruren. De medewerkers van de helpdesk zijn in ieder geval in staat om algemene informatie te verstrekken aan betrokkenen op de volgende items:

- Welke gegevens zijn gelekt;
- Oorzaak van het lek;
- (Mogelijke) gevolgen en risico's van het lek voor betrokkene;
- Welke maatregelen VenJ al heeft getroffen om deze gevolgen en risico's te voorkomen of mitigeren;
- Welke maatregelen betrokkenen zelf kunnen nemen om gevolgen en risico's te voorkomen of mitigeren en hoe ze dit kunnen doen;
- Of, en zo ja welke nadere informatie, hoe en wanneer nog volgt;
- Of, en zo ja, welke hulp of schadevergoeding de verantwoordelijke aanbiedt.

Indien en voor zover mogelijk zijn de medewerkers van de helpdesk ook in staat om aan betrokkenen meer specifieke informatie te verstrekken over hun persoonlijke situatie naar aanleiding van het ontstane datalek.

De verantwoordelijke richt een pagina in op de website van het eigen organisatieonderdeel en van het ministerie van VenJ respectievelijk Rijksoverheid. De website stelt betrokkenen in staat om algemene informatie te raadplegen over in ieder geval de volgende items:

- Welke gegevens zijn gelekt;
- Oorzaak van het lek;
- (Mogelijke) gevolgen en risico's van het lek voor betrokkene;

- Welke maatregelen al zijn getroffen om deze gevolgen en risico's te voorkomen of mitigeren;
- Welke maatregelen betrokkenen zelf kunnen nemen om gevolgen en risico's te voorkomen of mitigeren en hoe ze dit kunnen doen;
- Of, en zo ja welke nadere informatie, hoe en wanneer nog volgt;
- Of, en zo ja, welke hulp of schadevergoeding VenJ aanbiedt.

De verantwoordelijke informeert betrokkenen zo nodig met tussenberichten over de voortgang in de afwikkeling van het datalek, waaronder de getroffen maatregelen om het lek te dichten en de gevolgen en risico's voor de betrokkenen te voorkomen of mitigeren. Hij informeert betrokkenen zo nodig ook met een tussenbericht over de ondersteuning bij en/of vergoeding van de gevolgschade voor betrokkenen.

Actie 6.c Nazorg
De verantwoordelijke beoordeelt:
- Of het opgetreden datalek is gedicht;
- Of alle noodzakelijke maatregelen zijn getroffen om het risico te mitigeren van een herhaling van dit lek dan wel het optreden van een vergelijkbaar lek;
- Of alle noodzakelijke maatregelen zijn getroffen die volgen uit of verband houden met de meldplicht aan betrokkenen krachtens de Wbp en de beleidsregels meldplicht datalekken;
- Of hij dit incident en het oplossen van de impact daarvan kan afronden;

Zo ja, dan beslist de verantwoordelijke:
- Tot afronding van het incident;
- Tot het ontbinden van de 'incidententafel' of 'DG-tafel';
- Tot het ontmantelen van de helpdesk;
- Tot het deactiveren/niet langer vullen van de informatiepagina op de websites;

De verantwoordelijke stuurt betrokkenen per brief of e-mail een afloopbericht over de definitieve afwikkeling van het datalek, waaronder de getroffen maatregelen om het lek te dichten en de gevolgen en risico's voor de betrokkenen te voorkomen of mitigeren. Hij informeert betrokkenen zo nodig ook over de ondersteuning bij en/of vergoeding van de gevolgschade voor betrokkenen.

10 Datalek scenario Datalek in gemeenschappelijke voorziening

10.1 Omschrijving scenario

De beheerders van de gemeenschappelijke applicatie of voorziening constateren dat de (persoons) gegevens die deze applicatie of voorziening verwerkt:

- Zijn blootgesteld aan een hack, of;
- Door eigen handelen of nalaten van de beheerders zijn blootgesteld aan verlies, diefstal of onrechtmatige verwerking, of;

Door een ander technisch of organisatorisch falen zijn blootgesteld aan verlies, diefstal of onrechtmatige verwerking.

Toelichting: *Sommige dienstonderdelen van VenJ en externe ketenpartners maken in het kader van de uitoefening van hun publiekrechtelijke taak gebruik van een gemeenschappelijke ICT-applicatie of voorziening. Onder gemeenschappelijk wordt verstaan een applicatie of voorziening die meerdere – maar niet alle – dienstonderdelen van VenJ gebruiken. Daarnaast bestaat de mogelijkheid dat niet alleen meerdere dienstonderdelen van VenJ een gemeenschappelijke applicatie of voorziening gebruiken, maar ook externe ketenpartners.*

Een voorbeeld van een gemeenschappelijke voorziening is het Centraal Digitaal Depot (CDD+), in beheer bij Justid. Deze voorziening wordt gebruikt om dossiers (met persoonsgegevens) te bewaren en te ontsluiten voor dienstonderdelen die actief zijn in de strafrecht- of vreemdelingenketen. Een voorbeeld van een gemeenschappelijke voorziening die ook wordt benut door externe ketenpartners is het Generiek Casus Ondersteunend Systeem (GCOS). GCOS ondersteunt het werk in de zogeheten Veiligheidshuizen. Dit netwerksamenwerkingsverband verbindt partners uit de strafrechtketen, de zorgketen, gemeentelijke partners en bestuur, om gezamenlijk de overlast van huiselijk geweld en criminaliteit terug te dringen. Iedere ketenpartner legt (tijdelijk) een set van (persoons)gegevens vast in GCOS om op basis daarvan gezamenlijk een analyse en aanpak te bepalen voor elke individuele casus.

Uitgangspunt in dit scenario is dat iedere ketenpartner die een bepaalde set van persoonsgegevens vastlegt of bewaart of deelt met behulp van deze generieke of gemeenschappelijke applicatie of voorziening, zelf de verantwoordelijke is en blijft van deze vorm van gegevensverwerking en daarmee ten aanzien van deze gegevensverwerking verantwoordelijk is en blijft voor het:

- *Conform par. 3 van de Beleidsregels van de Autoriteit Persoonsgegevens (AP) voor toepassing van de Wbp Beleidsregels vast stellen of er sprake is van een datalek en,*
- *Conform par. 4 van de Beleidsregels vast stellen of sprake is van een datalek met (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens;*
- *Conform par. 7 van de Beleidsregels beoordelen of het datalek waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van betrokkenen.*

10.2 Aandachtpunten

Stap 1. Signaleren incident / risico

Actie 1.a Informeren direct leidinggevende

De beheerders van de generieke of gemeenschappelijke applicatie of voorziening constateren dat (persoons) gegevens die deze applicatie of voorziening verwerkt:

- Zijn blootgesteld aan een hack, of;
- Door eigen handelen of nalaten van de beheerders zijn blootgesteld aan verlies, diefstal of onrechtmatige verwerking, of;
- Door een ander technisch of organisatorisch falen zijn blootgesteld aan verlies, diefstal of onrechtmatige verwerking.

Alle verantwoordelijken binnen de context van het incident maken met elkaar een expliciete afspraak wie namens hen in de rol van *Senior Responsible Owner* (SRO)

optreedt als degene die een meldplichtig datalek meldt aan de Autoriteit Persoonsgegevens (AP). De SRO neemt de rol over van de verantwoordelijke in het generieke proces voor het afhandelen van het datalek (zie H3).

Toelichting: *Deze aanpak is te verkiezen boven die waarin iedere verantwoordelijke zelf melding doet aan de AP. Omdat een verantwoordelijke elk meldplichtig datalek onverwijld moet melden, is het essentieel dat er zo min mogelijk schakels zijn tussen de constatering van een mogelijk datalek en de uiteindelijke melding ervan aan de AP.*
Bovendien is het praktischer dat de AP één eenduidige melding in plaats van meerdere uit verschillende hoeken die betrekking hebben op één en hetzelfde beveiligingsincident.
Het ligt in de rede dat de verantwoordelijken met elkaar afspreken dat de SRO van de gemeenschappelijke applicatie of voorziening namens hen optreedt als degene die een datalek meldt aan de AP en dan ook voor de AP fungeert als aanspreekpunt voor dat datalek. De SRO is weliswaar niet per definitie zelf te beschouwen als verantwoordelijke voor de gegevensverwerkingen van deze applicatie of voorziening. Hij is echter wel degene die in de rol van opdrachtgever verantwoordelijk is voor het inrichten en toepassen van adequate technische en organisatorische maatregelen om de gegevensverwerkingen te beschermen tegen blootstelling aan verlies, diefstal of onrechtmatige verwerking.

Actie 1.bInformeren (externe) datalekdeskundige
De SRO bepaalt op basis van de door melder verstrekte informatie over de aard en omvang van de gegevens die mogelijk zijn blootgesteld aan onrechtmatige verwerking, of hij dit incident meldt aan de (externe) datalekdeskundige binnen het organisatieonderdeel waar hij werkzaam is.

11 Bijlage 1 - voorbeelden Communicatie

Teksten voor email, brief en webpagina - volgt.