POLITIE

Procesbeschrijving meldplicht datalekken

AVG en Wpg

5.1.2.e / 5.1.2.e

Definitief

Versie: Definitief

Versie datum 12 augustus 2019

Rubricering politie intern

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing
0.1	14-12-2018	Eerste opzet.
0.2	09-01-2019	Opmerkingen uit collegiale review verwerkt.
0.3	15-01-2019	Aanscherpen werkwijze en RACI
0.4	21-01-2019	Wijzigingen periodiek overleg protocol datalekken verwerkt en stroomschema nader uitgewerkt.
0.5	31-01-2019	Wijzigingen uit bespreking d.d. 29-01-2019 verwerkt en verwerkersrol politie toegevoegd.
1.0	14-02-2019	Reviewopmerkingen verwerkt. Rapportagestructuur toegevoegd.
1.1	18-02-2019	Opmerkingen uit periodiek overleg protocol datalekken verwerkt.
1.2	18-04-2019	Opmerkingen van TIB verwerkt, als bijlage de werkwijze van Dienstverlening Partners toegevoegd en de werkwijze voor VIK aangescherpt.
DEF t/m DEF (2)	07-05-2019	Besproken en behandeld in MT Directie IV en Driehoek IV
DEF (3)	12-08-2019	Naar BBVO ter besluitingvorming.

Distributie

Versie	Verzend datum	Naam
0.3	17-01-2019	Deelnemers periodiek overleg protocol datalekken : 5.1.2.e , Piet Deelman, 5.1.2.e , 5.1.2.e i, 5.1.2.e , 5.1.2.e Ter kennisname naar: 5.1.2.e en 5.1.2.e .
0.4	24-01-2019	Deze versie is verstuurd naar 5.1.2.e , 5.1.2.e en 5.1.2.e ter voorbereiding op een bespreking d.d. 29-01-2019. Ook is deze versie verstuurd naar 5.1.2.e en 5.1.2.e van TIB.
0.5	01-02-2019	5.1.2.e , Piet Deelman, 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e l, 5.1.2.e en 5.1.2.e .
1.0	14-02-2019	Deelnemers periodiek overleg protocol datalekken : 5.1.2.e , Piet Deelman, 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e . Ter kennisname naar: 5.1.2.e en 5.1.2.e .
1.1	22-02-2019	Piet Deelman (FG), 5.1.2.e (GA) en MT-leden Directie IV
DEF	07-05-2019	Piet Deelman (FG), 5.1.2.e (GA), 5.1.2.e (PDC) en MT-leden Directie IV
DEF (3)	12-08-2019	Driehoek IV en BBVO

Review commentaar

Versie	Wanneer	Wie	Functie
0.1	08-01-2019	5.1.2.e	Riskmanager
0.2	14-01-2019	5.1.2.e	Change Agent Informatiebeveiliging
0.3	18-01-2019	Deelnemers periodiek overleg protocol datalekken	Divers
0.4	29-01-2019	5.1.2.e	Beleidsadviseur wet- en regelgeving
	31-01-2019	5.1.2.e , medewerker DP	Privacy-adviseur
0.5	06-02-2019	5.1.2.e	Beleidsadviseur wet- en regelgeving
0.5	11-02-2019	Piet Deelman	Functionaris voor de gegevensbescherming
1.0	15-02-2019	5.1.2.e , 5.1.2.e en 5.1.2.e	Gegevensautoriteit / Functionaris voor de Gegevensbescherming

Referentiedocumenten

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken.pdf
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf
Rijksoverheid / Inlichtingenbureau: Procedure Meldplicht Datalekken 1.1.pdf, maart 2016

Gerelateerde documenten

Beleid datalekken 2018.014 datalek ciso aw.doc, 25 mei 2018
Beleid Informatiebeveiligingsincidenten, januari 2014
Proces melden datalek Dienstverlening Partners (nog te formaliseren na april 2019)

Inhoudsopgave

Inleiding

De meldplicht datalekken houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra zij een ernstig datalek hebben. En soms moet het datalek ook gemeld worden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).
Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie.

Bij de uitvoering van haar taak, en als werkgever van 65.000 medewerkers , verzamelt en verwerkt de politie persoonsgegevens, zowel in de rol van verwerkingsverantwoordelijke als in de rol van verwerker. Met al die gegevens wordt integer omgegaan, met respect voor ieders privacy en met de grootst mogelijke zorgvuldigheid.
Bij het verwerken van al deze gegevens moet de politie zich houden aan de Algemene verordening gegevensbescherming (AVG) en de Wet politiegegevens (Wpg).

Conform het interne beleid (Beleid informatiebeveiligingsincidenten) werkt de politie met een decentraal incident afhandelingsproces. Verantwoordelijkheden en bevoegdheden worden zo laag mogelijk in de organisatie belegd, inclusief de registratie van de incidenten. Reden is om zo snel mogelijk handelen te stimuleren en het incident en de gevolgen daarvan te beperken.

Doel

Het doel van deze procesbeschrijving is op gecontroleerde wijze omgaan met de gevolgen van een beveiligingsincident met potentieel datalek.
Deze procesbeschrijving is aanvullend op de in werking zijnde incidentprocedures bij

- De diverse servicedesken (ICT, Team Mobiel etc.) binnen de organisatie waar incidentmeldingen worden ontvangen, dan wel geregistreerd. In dit document worden zij aangeduid als decentraal meldpunt.
- Security Operations Center
- Team Informatiebeveiliging PDC
- Afdeling Veiligheid & Continuïteit
- Privacy functionarissen bij de eenheden
- Afdelingen Veiligheid, Integriteit en Klachten

Meldplicht

Binnen de politieorganisatie geldt de interne meldplicht (bij de in dit document genoemde meldpunten) voor iedereen die een datalek constateert.
De wet verplicht, op een uitzondering na, tot melding van een datalek aan de AP en in bepaalde gevallen ook aan de betrokkene(n). Dit laatste is afhankelijk van de ernst van de zaak en de mogelijke gevolgen voor de betrokkene(n).

Bij 'niet tijdige' melding kan de AP:

- een (bindende) aanwijzing geven om alsnog te melden;
- per overtreding een bestuurlijke boete opleggen, welke kan oplopen tot 83.000 euro in het kader van de Wpg en tot 10.000.000 euro in het kader van de AVG.

In deze procesbeschrijving worden begrippen uit de privacywetgeving als bekend verondersteld. Voor eventuele naslag kan de intranetpagina AVG bij de politie en het Praktijkhandboek Wpg worden geraadpleegd.

1. Wat is een datalek?

Bij een datalek gaat het om ongeoorloofde of onbedoelde toegang tot persoonsgegevens bij een organisatie.
De term ‘datalek’ komt niet voor in de wet. In de plaats daarvan heeft de wet het over een ‘inbreuk in verband met persoonsgegevens’.

Artikel 4. AVG geeft de volgende definitie:
“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 33a. Wpg geeft de volgende definitie:
“een inbreuk op de beveiliging die een risico voor de rechten en vrijheden van personen met zich meebrengt.”

Binnen de politie is zowel sprake van verwerkingen van persoonsgegevens waarop de AVG van toepassing is, als van verwerkingen van persoonsgegevens waarop de Wpg van toepassing is. In het laatste geval betreft dat verwerking van persoonsgegevens in het kader van de uitoefening van de politietaak.
Voor beide (AVG en Wpg) verwerkingen van persoonsgegevens moeten datalekken gemeld worden bij de AP.

1.1 Categorieën

Er zijn drie categorieën datalekken te onderscheiden:

Inbreuk op de vertrouwelijkheid
Wanneer er sprake is van een onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens.
Inbreuk op de integriteit
Wanneer er sprake is van een onbevoegde of onopzettelijke wijziging van persoonsgegevens.
Inbreuk op de beschikbaarheid
Wanneer er sprake is van een onbevoegd of onopzettelijk verlies van toegang tot, of vernietiging van, persoonsgegevens.

Een datalek kan, afhankelijk van de omstandigheden, in meer dan één van deze drie categorieën vallen.

1.2 Voorbeelden

Een datalek kan zijn:

- een kwijtgeraakte USB-stick waar zich persoonsgegevens (o.a. emailadressen) op bevinden;
- een gestolen/verloren werklaptop, telefoon en/of toegangspas;
- aanval en inbraak op politienetwerk door een hacker;
- verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden;
- HRM-gegevens politiemedewerkers onbedoeld inzichtelijk voor ketenpartners;
- een besmetting met ransomware waarbij persoonsgegevens ontoegankelijk zijn gemaakt;
- wachtwoord politie-account doorgeven aan een ander;
- hard copy rapporten met persoonsgegevens in de trein achterlaten;
- papieren met persoonsgegevens belanden op straat;
- een kwetsbaarheid in een applicatie waardoor persoonsgegevens gelekt worden;
- mail verstuurd naar verkeerde persoon;
- poststuk niet ontvangen of retourzending van een geopend poststuk.

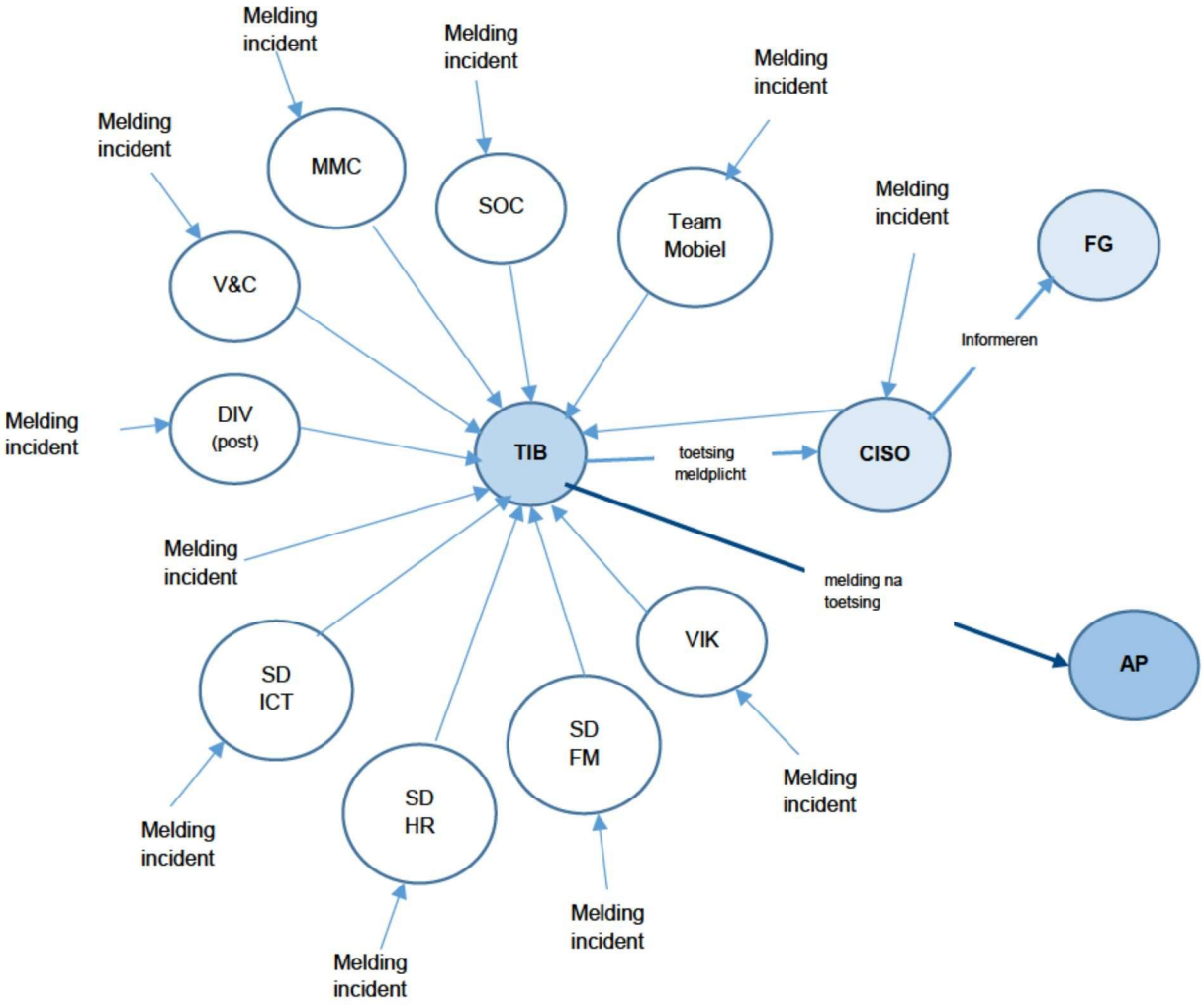
2. Werkwijze politie als verwerkingsverantwoordelijke

De politie is de officiële verwerkingsverantwoordelijke als het gaat om de verwerking van persoonsgegevens voor de politietaak (Wpg) maar ook voor de verwerking van persoonsgegevens in de zin van de AVG, denk aan alle gegevens die over medewerkers worden verwerkt, de korpscheftaken en de vreemdelingentaak.
Dit hoofdstuk beschrijft de werkwijze die de politie als verwerkingsverantwoordelijke hanteert, indien zich een incident voordoet waarbij mogelijk persoonsgegevens zijn betrokken.

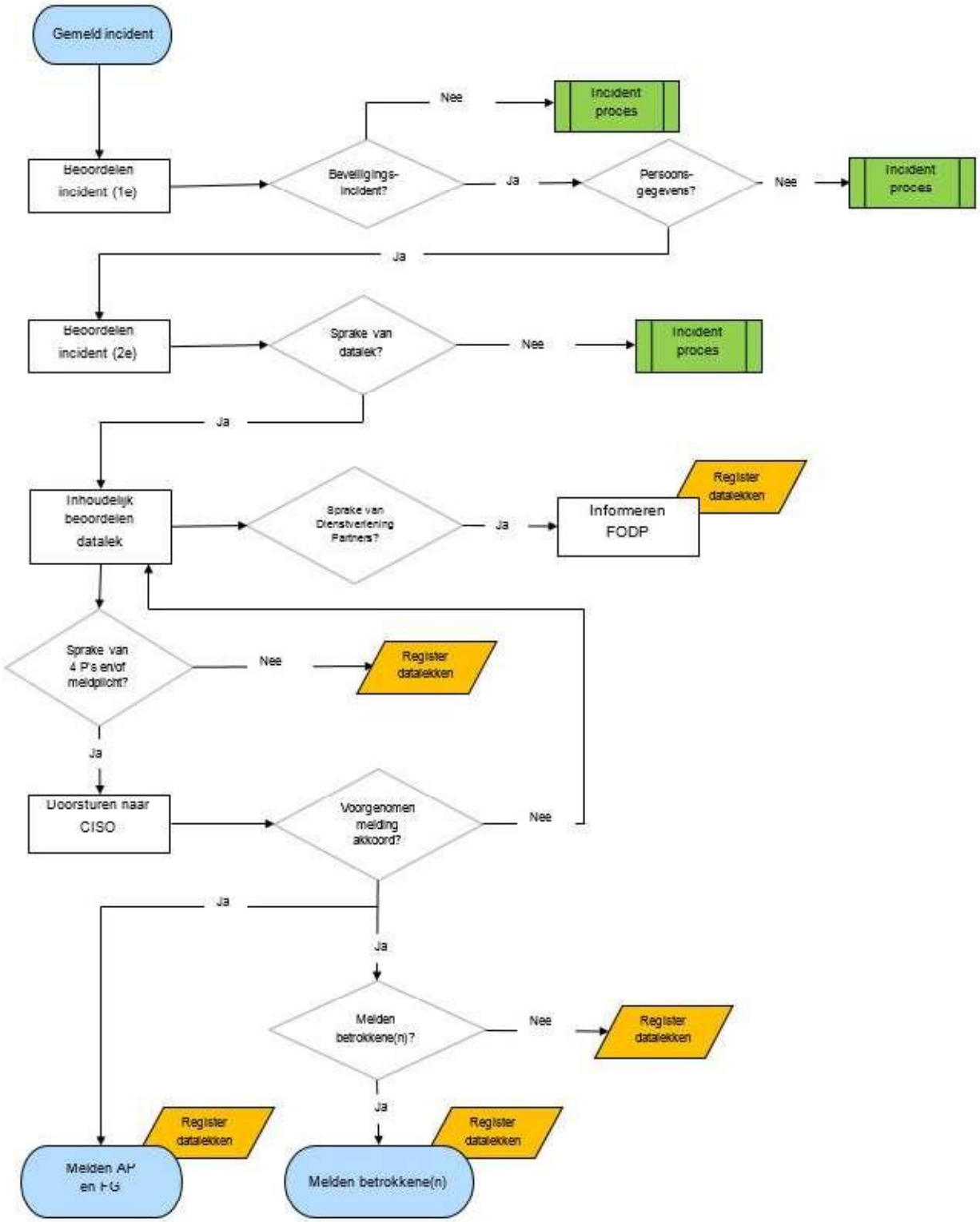
Uitgangspunt van de politie is dat de meldplicht datalekken zo efficiënt mogelijk wordt gerealiseerd en de belasting van de operatie zo beperkt mogelijk is. Dit betekent dat de medewerkers van de politie op hoofdlijnen geïnformeerd worden over datalekken en de mogelijke consequenties daarvan en welke handelingen van hen verwacht worden. De hoofdinspanning wordt gelegd bij de decentrale meldpunten zijnde de reeds bestaande servicedesken. Deze medewerkers worden gericht opgeleid om alle meldingen te kunnen duiden in het kader van potentiële datalekken.

Binnen onze organisatie worden incidenten door medewerkers vooral gemeld bij decentrale meldpunten. Een decentraal meldpunt doet de 1e beoordeling van een incident en zorgt voor verdere afhandeling conform de voor het betreffende meldpunt in werking zijnde incidentprocedure. Als blijkt dat het een beveiligingsincident betreft waarbij persoonsgegevens betrokken zijn dan wordt dit aangemeld bij Team Informatiebeveiliging PDC (TIB).
Privacyfunctionarissen en VIK-medewerkers zullen bij het vermoeden van een beveiligingsincident, waarbij persoonsgegevens zijn betrokken, (meestal) direct een melding doen bij TIB of de CISO.
TIB doet de 2e beoordeling en bij het vermoeden van een datalek wordt het stappenplan uit hoofdstuk 4 gevolgd. Indien het een datalek betreft dan draagt TIB zorg voor het verzamelen van de benodigde informatie (impact, gevolgen, juridisch advies, acties enz.) en legt dit voor aan de CISO. De CISO maakt, in afstemming met JZ, de afweging of het een meldplichtig datalek is en informeert de FG.
TIB doet vervolgens de melding aan de AP, tenzij het de 4 P's (zie hoofdstuk 3. Taken, verantwoordelijkheden en bevoegdheden) betreft, dan zal de CISO, na de afweging, direct de melding aan de AP doen.

2.1 Decentrale meldpunten en flow meldingen



2.2 Stroomschema



3. Taken, verantwoordelijkheden en bevoegdheden

Proceseigenaar meldplicht datalekken:	CIO
Toezichthouder proces meldplicht datalekken:	FG
Regie proces meldplicht datalekken:	CISO
Uitvoering meldplicht datalekken:	TIB

De eerste verantwoordelijkheid voor het melden van een beveiligingsincident ligt bij iedere medewerker.
Bij een beveiligingsincident waarbij persoonsgegevens betrokken zijn neemt het Team Informatiebeveiliging (TIB) van de Dienst IM contact op met de juridische medewerker en/of privacyfunctionaris van de betreffende eenheid.
Indien het beveiligingsincident betrekking heeft op het verwerken van persoonsgegevens voor een andere verwerkingsverantwoordelijke dan informeert TIB de Front Office Dienstverlening Partners[1] (zie hoofdstuk 5. Werkwijze politie als verwerker).
Voor nadere afstemming neemt TIB contact op met de CISO en deze ontvangt noodzakelijke informatie.
De CISO informeert de FG en toetst, op basis van de geleverde informatie en het initiële advies door TIB, of het datalek meldplichtig is. Vervolgens draagt TIB zorg voor de melding aan de AP.

De CISO let op naleving van de afhandeling van de uitvoering door TIB.
De FG toetst bij de CISO of de afspraken rondom het proces meldplicht datalekken leiden tot een effectief systeem.

Echter, als een beveiligingsincident één of meerdere van de onderstaande P's (mogelijk) raakt, dan moet het direct gemeld worden aan de CISO / Informatiebeveiligingsautoriteit:

> de veiligheid of privacy van het **P**ubliek, van burger(s), komt in gevaar;
> de veiligheid of privacy van het eigen **P**ersoneel komt in gevaar;
> het komt in de **P**ers;
> het ligt **P**olitiek gevoelig.

De CISO neemt dan de regie over van de incidentafhandeling en stemt, indien nodig, af met andere disciplines over de mogelijke gevolgen en te nemen acties. TIB blijft verantwoordelijk voor de melding aan de AP.

De informatievoorziening omtrent een datalek wordt in principe alleen gedeeld met de rollen die zijn genoemd in paragraaf 3.1 RACI-model. Alle communicatie (waarbij persoonsgegevens betrokken zijn) met andere partijen dan genoemd in het RACI-model dient afgewogen te worden tegen het belang en het risico. Deze informatieverstrekking dient functioneel te zijn in het kader van het betreffende datalek.

[1] Als verwerker heeft de politie andere verplichtingen dan als verwerkingsverantwoordelijke. Dit heeft ook gevolgen voor de meldplicht datalekken. Het is dan belangrijk om bij alle (vermoedens van) datalekken na te gaan of het een beveiligingsincident betreft die valt binnen de Dienstverlening Partners.

3.1 RACI-model

Taak \ Rol	Medew.	Leiding	SD	TIB	CISO	VIK	FG	PF	GA	JZ	RSLM	Comm.	CIO
Informeren/stimuleren medewerkers tot melden van een datalek	I	A											
Melden datalek	A		I										
Regie meldplicht datalekken					A								
Toezicht houden op proces meldplicht datalekken							A						
Signaleren mogelijke inbreuk op persoonsgegevens	R	R	R	R	A	R	I	R					
Beoordelen inbreuk op persoonsgegevens				R	A			C		C			
Adviseren bij inbreuk op persoonsgegevens				R	A		I	R					
Verrichten nader onderzoek				R	A		I	C					
Terugmelden wijze afhandeling incident				R	A								
Documenteren incident				R	A			C		C			
Beoordelen of incident leidt tot oriënterend onderzoek naar medewerker						A							
Melden datalek aan AP				R	A		I		C				
Informeren betrokkene(n)				R	A								
Adviseren over grote groep betrokkenen				R	C							A	I
Betrekken relevante partijen		I		R	A							I	I
Bepalen invloed op reguliere dienstverlening				R	A						R	I	I
Voorbereiden woordvoeringslijn				I	I						R	A	C
Beschikbaar stellen managementrapportage datalekken		I		R	A		I	I	I				I

R = Responsible (Verantwoordelijk) A = Accountable (Eindverantwoordelijk) C = Consulted (Geraadpleegd) I = Informed (Geïnformeerd)

3.2 Rollen en taken

Medewerker / Leidinggevende / Eenheidsleiding

- Leidinggevende / Eenheidsleiding stimuleren medewerkers voor het doen van melding.
- Medewerkers melden een beveiligingsincident zo spoedig mogelijk bij hun leidinggevende.
- De leidinggevende verricht samen met de medewerker al die handelingen die noodzakelijk zijn om de consequenties van het beveiligingsincident te beperken en betrekt hierbij (zonodig) de privacyfunctionaris, de beveiliging coördinator en/of informatiebeveiligingsfunctionaris.
- De leidinggevende zorgt ervoor dat het Team Informatiebeveiliging, of in geval van één van de vier P's de CISO / Informatiebeveiligingsautoriteit, zo snel mogelijk wordt geïnformeerd.
- De leidinggevende (eenheidsleiding) beoordeeld of bij een beveiligingsincident het team Veiligheid, Integriteit en Klachten (VIK) wordt betrokken.
- Ontvangt een managementrapportage datalekken.

Servicedesk (= decentraal meldpunt: ICT, MMC, FM, DIV (poststukken), V&C, SOC en Team Mobiel)

- Signaleert mogelijke beveiligingsincidenten.
- Informeert in geval van een mogelijk beveiligingsincident waarbij persoonsgegevens zijn betrokken het Team Informatiebeveiliging.

Team Informatiebeveiliging PDC

- Beoordeelt of persoonsgegevens onherstelbaar verloren zijn gegaan, of inzage door onbevoegden, onbevoegde verstrekking of onrechtmatige verwerking heeft plaatsgevonden.
- Verricht zo nodig nader onderzoek naar de aard en gevolgen van het beveiligingsincident.
- Als sprake is van een (vermoeden van een) inbreuk in verband met persoonsgegevens dan neemt Team Informatiebeveiliging contact op met de CISO / Informatiebeveiligingsautoriteit.
- Indien het beveiligingsincident betrekking heeft op het verwerken van persoonsgegevens voor een andere verwerkingsverantwoordelijke dan informeert TIB de FODP.
- Meldt een datalek, na afstemming met de CISO / Informatiebeveiligingsautoriteit, zonder onnodige vertraging binnen 72 uur na ontdekking van het datalek bij de AP.
- Informeert zo nodig onverwijld de betrokkene over de inbreuk in verband met zijn/haar persoonsgegevens.
- Meldt de wijze van afhandeling van het beveiligingsincident terug aan de melder en overige betrokkenen.
- Documenteert de relevante gegevens met betrekking tot het beveiligingsincident in het daarvoor bestemde register.
- Stemt met de privacyfunctionaris af over de documentatieplicht.

Veiligheid Integriteit en Klachten (VIK)

- Signaleert mogelijke beveiligingsincidenten.
- Beoordeelt of het beveiligingsincident aanleiding geeft tot een verzoek om oriënterend onderzoek naar een medewerker.
- Informeert in geval van een mogelijk beveiligingsincident waarbij persoonsgegevens zijn betrokken de CISO/Informatiebeveiligingsautoriteit.

CISO / Informatiebeveiligingsautoriteit

- Heeft de regie over het proces rond de meldplicht datalekken.
- Wordt geïnformeerd over mogelijke beveiligingsincidenten.
- Informeert de Functionaris voor Gegevensbescherming (FG) en stemt met deze persoon af over de beoordeling van het beveiligingsincident en het mogelijke datalek, de gevolgen daarvan en de te nemen maatregelen.
- Meldt, indien sprake is van de 4 P's, een datalek zonder onnodige vertraging en binnen 72 uur na ontdekking van het datalek bij de AP.
- Informeert zo nodig onverwijld de betrokkene over de inbreuk in verband met zijn/haar persoonsgegevens.
- Betrekt zo nodig relevante partijen, zoals de korpsleiding, woordvoering, bestuurszaken, leidinggevenden, landelijk portefeuillehouders, DGpol, Europol etc.
- Meldt, indien sprake is van de 4 P's, de wijze van afhandeling van het beveiligingsincident terug aan de melder en overige betrokkenen.
- Documenteert de relevante gegevens met betrekking tot het datalek in het daarvoor bestemde register.

- Betrekt Communicatie in het geval van een gevoelig beveiligingsincident waarbij de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt .
- Voorziet de CIO van een managementrapportage datalekken.
- Voorziet de eenheidsleiding van een managementrapportage datalekken.

Privacyfunctionaris

- Stemt met het Team Informatiebeveiliging af over de juiste vulling van het incidentregister in het kader van de documentatieplicht.[2]
- Adviseert het Team Informatiebeveiliging zo nodig bij de beoordeling van het beveiligingsincident en het mogelijke datalek, de gevolgen daarvan en de te nemen maatregelen.

Functionaris voor de Gegevensbescherming

- Wordt zo spoedig mogelijk geïnformeerd over (mogelijke) datalekken.
- Houdt toezicht op het proces rond de meldplicht datalekken.
- Heeft toegang tot de managementrapportage datalekken.
- Is voor de AP het 1e loket als de AP vragen heeft over datalekken.

Gegevensautoriteit

- Heeft toegang tot de managementrapportage datalekken.

RSLM

- Mocht het datalek invloed – dreigen te - hebben op de reguliere dienstverlening, dan wordt RSLM hiervan verwittigd door de CISO.
- RSLM kan zo nodig de interne communicatie verzorgen.

Communicatie

- Bereidt de woordvoeringslijn voor in geval van een gevoelig beveiligingsincident waarbij de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt en stemt dit af met de CIO.
- Adviseert over de wijze waarop een grote groep van betrokkenen geïnformeerd moet worden over de inbreuk in verband met hun persoonsgegevens.

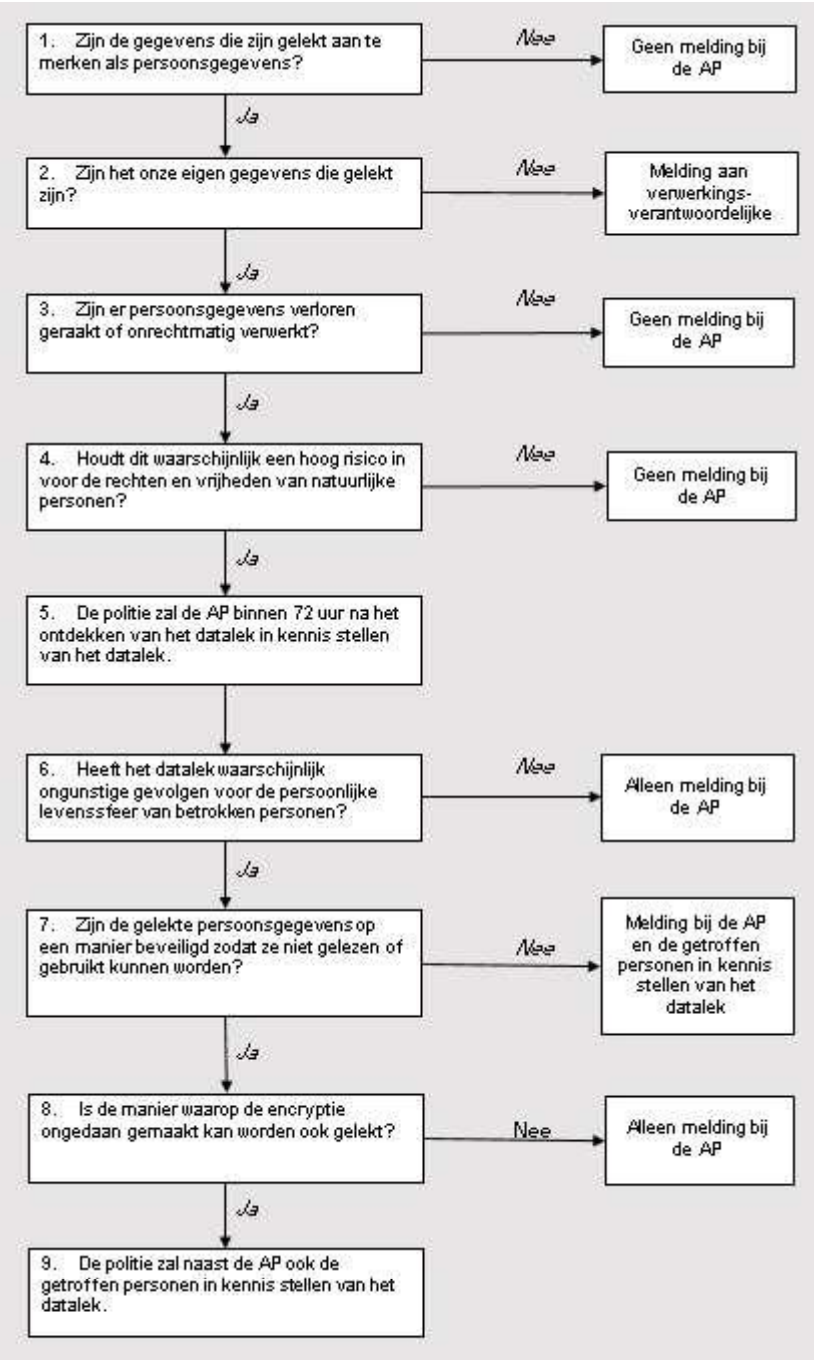
CIO

- Is proceseigenaar Meldplicht Datalekken.
- Wordt geïnformeerd indien het een grote groep betrokkenen betreft.
- Wordt geïnformeerd over het betrekken van relevante partijen.
- Wordt geïnformeerd over de consequenties voor de reguliere dienstverlening.
- Wordt geconsulteerd m.b.t. de woordvoeringslijn.
- Ontvangt een managementrapportage datalekken.

[2] Artikel 33, lid 5 AVG en artikel 32, lid 1, onder d Wpg

4. Stappenplan

Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als er onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs uit te sluiten zijn.
Bij de beslissing of een gebeurtenis , die zich heeft voorgedaan, meldplichtig is , moet een aantal afwegingen worden gemaakt. Het onderstaande schema geeft in de vorm van een stappenplan deze afwegingen weer.



STAP 1: Persoonsgegevens

Zijn de gegevens die zijn gelekt aan te merken als persoonsgegevens (= alle informatie over een geïdentificeerde of identificeerbare natuurlijk persoon)?
Een gegeven is geen persoonsgegeven, indien doeltreffende technische en organisatorische maatregelen getroffen zijn waardoor een daadwerkelijke identificatie van individuele personen redelijkerwijs wordt uitgesloten (informatie is geanonimiseerd). Een persoon is wel identificeerbaar als zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Bevatten de gegevens bijvoorbeeld namen, (e-mail)adressen of BSN's?

JA: ga naar stap 2
NEE: je hoeft geen melding te doen

STAP 2: Verwerkingsverantwoordelijke / Verwerker[3]?

Zijn het onze eigen gegevens die gelekt zijn?
De *verwerkingsverantwoordelijke* is degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Het gaat hierbij om de vraag wie uiteindelijk bepaalt welke verwerking er plaatsvindt van welke persoonsgegevens en voor welk doel. Ook is van belang wie er beslist over de middelen voor die verwerking: de vraag op welke manier de gegevensverwerking zal plaatsvinden. Deze bevoegdheden kunnen soms in verschillende handen liggen. In dat geval is er sprake van gezamenlijke verantwoordelijkheid.

JA: *Verwerkingsverantwoordelijke:* Ga naar stap 3.
NEE: *Verwerker:* De meldplicht datalekken richt zich alleen tot de *verwerkingsverantwoordelijke* voor de verwerking van persoonsgegevens. Er hoeft dus geen melding bij de AP te worden gedaan. Als *verwerker* heb je wel je verantwoordelijkheid richting de *verwerkingsverantwoordelijke*, zodat deze op tijd melding kan maken. De richtlijn is dit binnen 4 uur door te geven, omdat de *verwerkingsverantwoordelijke* binnen 72 uur de melding moet doen bij de AP. Zie verder Hoofdstuk 5.

De politie levert hierbij alle informatie aan die nodig is voor de *verwerkingsverantwoordelijke* om aan de verplichting te voldoen. Daarnaast houdt zij de *verwerkingsverantwoordelijke* op de hoogte van eventuele nieuwe ontwikkelingen rond het incident, en van de maatregelen die de politie treft om aan haar eigen kant de gevolgen van het beveiligingsincident te beperken en herhaling te voorkomen.

STAP 3: Datalek?

In deze stap zijn er verschillende vragen om rekening mee te houden:

Stap 3A: is er sprake van een inbreuk op de beveiliging?

Een inbreuk op de beveiliging houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Er is niet uitsluitend sprake van een dreiging, of van een tekortkoming in de beveiliging (ook wel aangeduid als een beveiligingslek) die zou kunnen leiden tot een beveiligingsincident. Er heeft zich daadwerkelijk een beveiligingsincident voorgedaan, en de preventieve maatregelen die de politie eventueel heeft getroffen waren niet toereikend om dit te voorkomen.

JA: (wel inbreuk) dit is een beveiligingslek. Er kan tevens sprake zijn van een datalek, ga naar stap 3B.
NEE: (geen inbreuk) dit is geen datalek. Je hoeft geen melding te doen.

[3] Zie voor meer informatie: art. 33, lid 2 AVG en art. 33a. lid 1, Wpg

Stap 3B: zijn er persoonsgegevens verloren gegaan?

Verlies houdt in dat de politie de persoonsgegevens niet meer heeft. Bij het beveiligingsincident zijn de persoonsgegevens vernietigd of op een andere manier verloren gegaan, en de politie beschikt niet over een complete en actuele reservekopie van de gegevens.

JA: (wel verloren) dit is een datalek, ga naar stap 4.
NEE: (niet verloren) er kan toch sprake zijn van een datalek, ga naar stap 3C.

Stap 3C: kan er uitgesloten worden dat er persoonsgegevens onrechtmatig zijn verwerkt?

Onder onrechtmatige vormen van verwerking vallen de aantasting van de persoonsgegevens, onbevoegde kennisneming, wijziging, of verstrekking daarvan. Als de politie redelijkerwijs niet kan uitsluiten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid, dan moet u de inbreuk beschouwen als een datalek.

JA: (kan uitgesloten worden) dit is geen datalek. Je hoeft geen melding te doen.
NEE: (kan niet uitgesloten worden) dit is een datalek, ga naar stap 4.

Meldplicht AP

De meldplicht valt uiteen in de meldplicht aan de AP en die aan de betrokkene(n).
Hierna wordt omschreven wanneer en hoe er aan de AP moet worden gemeld.

STAP 4: Melden aan AP?

In deze stap zijn twee vragen om rekening mee te houden:

Stap 4A: zijn er persoonsgegevens van gevoelige aard gelekt?

Bij het beantwoorden van de vraag of er sprake is van het waarschijnlijk inhouden van een hoog risico voor de rechten en vrijheden van natuurlijke personen, moet er in ieder geval gekeken worden naar de aard van de getroffen gegevens. Is er sprake van bijzondere persoonsgegevens of van persoonsgegevens die anderszins van gevoelige aard zijn? Bij dit laatste moet je bijvoorbeeld denken aan gegevens over betalingsachterstanden.
Bij een aantal categorieën van persoonsgegevens, in dit kader aangeduid als persoonsgegevens van gevoelige aard, kunnen verlies of onrechtmatige verwerking onder meer leiden tot stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, financiële schade of tot (identiteits)fraude. Tot deze categorieën[4] van persoonsgegevens moeten in ieder geval worden gerekend:

- *Politiegegevens.* Het betreft hier alle persoonsgegevens die in het kader van de politietaak worden verwerkt. Dat zijn persoonsgegevens over verdachten, maar ook aangevers en getuigen.
- *Bijzondere persoonsgegevens.* Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
- *Gegevens over de financiële of economische situatie van de betrokkene.* Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
- *(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene.* Hieronder vallen bijvoorbeeld gegevens over (verdenking van) crimineel gedrag, gokverslaving, prestaties op school of werk of relatieproblemen.
- *Gebruikersnamen, wachtwoorden en andere inloggegevens.* De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens

[4] Strafrechtelijke gegevens (strafrechtelijke veroordelingen en strafbare feiten) worden niet aangemerkt als een bijzondere categorie van persoonsgegevens. Artikel 10 van de AVG.

toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.

- *Gegevens die kunnen worden misbruikt voor (identiteits)fraude.* Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (BSN).

JA: (wel gevoelige gegevens) dit moet gemeld worden bij de AP, ga naar stap 5. Mogelijk moet dit ook gemeld worden aan de betrokkenen, ga daarna naar stap 6.
NEE: (geen gevoelige gegevens) ga naar stap 4B.

Stap 4B: leiden de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?

De aard en omvang van de getroffen verwerking is mede bepalend voor de beantwoording van de vraag of er bij een datalek sprake is van het waarschijnlijk inhouden van een hoog risico voor de rechten en vrijheden van natuurlijke personen. Een datalek bij instellingen als de Belastingdienst, de Sociale Verzekeringsbank (SVB) of bij een commerciële bank of verzekeraar kan leiden tot financieel nadeel voor de betrokkene of tot de compromittering van gegevens die beschermd worden door een geheimhoudingsplicht. Beveiligingslekken in de omvangrijke verwerkingen van persoonsgegevens waarover de overheid beschikt kunnen ook zeer grote gevolgen hebben voor de betrokkenen. Afgezien van de gevoelige aard van de verwerkte gegevens, die in de voorgaande paragraaf al aan de orde kwam, is voor het waarschijnlijk inhouden van een hoog risico voor de rechten en vrijheden van natuurlijke personen verder het volgende relevant:

- De omvang van de hierboven beschreven verwerkingen betekent dat het bij datalekken kan gaan om veel persoonsgegevens per persoon, en om gegevens van grote groepen betrokkenen. Deze beide factoren maken een gelekte dataset aantrekkelijk voor misbruik in het criminele circuit. De kans dat de gelekte dataset wordt doorverkocht, wordt daardoor ook groter, met als gevolg dat de betrokkenen langer last houden van het datalek.

- Naarmate de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpender zijn, is ook de impact van verlies of onrechtmatige verwerking groter. Bijvoorbeeld: als een organisatie financiële gegevens gebruikt om iemands kredietwaardigheid te bepalen zijn de gevolgen van verlies en onbevoegde wijziging van de gegevens ingrijpender dan bij gebruik van dezelfde gegevens voor marketingdoeleinden.

- Bij omvangrijke verwerkingen van de overheid is vaak sprake van persoonsgegevens die binnen ketens worden gedeeld. Dit betekent dat de gevolgen van verlies en onbevoegde wijziging van persoonsgegevens door de hele keten heen kunnen optreden. Voor de betrokkenen wordt het hierdoor moeilijker om de mogelijke gevolgen van een datalek te overzien en om zich daar waar mogelijk aan te onttrekken.

Als de aard en omvang van de getroffen verwerking voldoen aan het bovenstaande, dan moet de politie ervan uitgaan dat er waarschijnlijk sprake is van een hoog risico voor de rechten en vrijheden van natuurlijke personen.

JA: (wel ernstige gevolgen) dit moet gemeld worden bij de AP, ga naar stap 5. Mogelijk moet dit ook gemeld worden aan de betrokkenen, ga daarna naar stap 6.
NEE: (geen ernstige gevolgen) dit datalek hoeft niet gemeld te worden aan de AP

STAP 5: Melding AP

De AP stelt een webformulier beschikbaar waarmee datalekken moeten worden gemeld.

- Er kan melding worden gemaakt van een datalek op de website *https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?1*.
- Het datalek zal zonder onnodige vertraging en indien mogelijk niet later dan 72 uur gemeld moeten worden . Mogelijk is er na 72 uur geen volledig zicht op het incident. De melding bij de AP kan achteraf worden bijgewerkt of zelfs ingetrokken. Als er later dan 72 uur wordt gemeld, wordt er gemotiveerd waarom.
- De ontvangstbevestiging wordt direct verstuurd door de AP. Deze registeren in het register datalekken.
- Bij die meldingen die aanleiding geven tot nadere actie door de Autoriteit Persoonsgegevens, zal deze contact met de politie opnemen om de herkomst van de melding te verifiëren.
- Mogelijk moet er naast een melding bij de AP, ook gemeld worden aan betrokkenen, ga door naar stap 6.

Meldplicht betrokkenen

De meldplicht valt uiteen in de meldplicht aan de AP en die aan de betrokkenen. Hierna wordt omschreven wanneer en hoe er aan de betrokkenen moet worden gemeld. De wijze waarop (individueel of via media) hangt af van het geval.

STAP 6: Persoonlijke levenssfeer

Heeft het datalek waarschijnlijk een hoog risico voor de rechten en vrijheden van personen?
Het datalek moet aan de betrokkene worden gemeld als de inbreuk waarschijnlijk een hoog risico voor de rechten en vrijheden van betrokkene inhoudt.
Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik van persoonsgegevens in hun belangen worden geschaad. De schade kan van materiële of van immateriële aard zijn. Bij dit laatste moet je bijvoorbeeld denken aan onrechtmatige publicatie, aantasting in eer en goede naam, identiteitsfraude of discriminatie. Identiteitsfraude kan overigens niet alleen leiden tot immateriële gevolgen, maar ook tot materiële gevolgen.

Het is aan de politie om te beoordelen of een datalek aan de betrokkene gemeld moet worden.
Indien er persoonsgegevens van gevoelige aard zijn gelekt, dan moet je er van uitgaan dat je het datalek niet alleen moet melden aan de Autoriteit Persoonsgegevens, maar ook aan de betrokkene. Verlies of onrechtmatige verwerking van dergelijke gegevens kunnen onder meer leiden tot stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, financiële schade of (identiteits)fraude.
In alle overige gevallen zal je op basis van de omstandigheden van het geval een afweging moeten maken.

JA: (wel gevolgen voor persoonlijke levenssfeer) ga naar stap 7.
NEE: (geen gevolgen voor persoonlijke levenssfeer) er hoeft alleen aan de AP en niet aan de betrokkenen gemeld te worden.

STAP 7: Goed beveiligd?

Zijn de gelekte persoonsgegevens op een manier beveiligd zodat ze niet gelezen of gebruikt kunnen worden?
Als door de crypto grafische bewerkingen die de politie heeft toegepast de gelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kan je de melding aan de betrokkene achterwege laten. Dit is een strenge norm, die je van geval tot geval toe moet passen op basis van de actuele stand van de techniek. Als je twijfelt over de adequaatheid van de technische beschermingsmaatregelen die je hebt getroffen, dan moet je het datalek melden aan de betrokkene.

JA: (wel goed beveiligd) ga door naar stap 8.
NEE: (niet goed beveiligd) Er moet naast aan de AP ook aan betrokkenen worden gemeld, ga door naar stap 9.

STAP 8: Ongedaan maken van encryptie[5] gelekt?

Is de manier waarop de encryptie ongedaan gemaakt kan worden bekend gemaakt?
Aandachtspunten bij de beoordeling zijn:

- Het algoritme zelf, of de wijze waarop dit is toegepast, kunnen kwetsbaarheden vertonen waardoor de encryptie of de hashing niet de bescherming biedt die je daarvan verwacht.
- Encryptie is omkeerbaar. Een onbevoegde die over de juiste sleutel beschikt, of deze zonder al te veel moeite kan vinden, kan de gelekte gegevens ontsleutelen.
- Hashing is herhaalbaar. Als er bij hashing geen salt is toegepast, of als een onbevoegde over de gebruikte salt beschikt of deze zonder al te veel moeite kan vinden, kan hij de gebruikte hashingmethode toepassen op een lijst met veelgebruikte waarden en daardoor bijvoorbeeld gestolen wachtwoorden achterhalen.

NEE: Er moet alleen aan de AP gemeld worden en niet aan de betrokkenen gemeld worden.
JA: Er moet naast aan de AP ook aan betrokkenen worden gemeld, ga naar stap 9.

[5] Het toepassen van encryptie is een taak van de Dienst ICT. Het SOC draagt zorg voor monitoring op deze maatregel.

STAP 9: Melding betrokkenen

Er moet ook worden gemeld aan de *betrokkenen*. Dit moet 'onverwijld' gebeuren. Bij de melding aan de AP wordt een termijn afgesproken waarbinnen dit moet gebeuren. Deze termijn moet nagekomen worden. Bij melding worden minimaal de volgende gegevens verstrekt:

- de aard van de inbreuk (algemene omschrijving)
- de instanties waar de *betrokkene* meer informatie over de inbreuk kan krijgen (contactgegevens politiefunctionaris)
- en de maatregelen die de politie de *betrokkene* aanbeveelt om te nemen om de negatieve gevolgen van de inbreuk te beperken (bijvoorbeeld wachtwoord wijzigen).

Afhankelijk van waar (eenheid/directie/dienst) de inbreuk heeft plaatsgevonden zal de betreffende teamchef of privacyfunctionaris of VIK-medewerker de melding aan betrokkene(n) doen. Dit gebeurt na overleg en afstemming met TIB / CISO.

5. Werkwijze politie als verwerker

Naast de rol als verwerkingsverantwoordelijke voor politiegegevens (Wpg) en persoonsgegevens in de zin van de AVG, heeft de politieorganisatie soms ook de rol van verwerker van persoonsgegevens voor een andere verwerkingsverantwoordelijke.

Als verwerker heeft de politie andere verplichtingen met betrekking tot de inbreuken in verband met persoonsgegevens. Deze afspraken zijn vastgelegd in de desbetreffende verwerkersovereenkomst , dienstverleningsdocumentatie en eventuele specifieke werkinstructies.
In de verwerkersovereenkomst is de informatieplicht opgenomen en staat aangegeven hoe en wanneer de verwerkingsverantwoordelijke wordt geïnformeerd.

Indien ketenpartners of andere partijen verwerker zijn van gegevens waarvoor de politie de verwerkingsverantwoordelijke is, dan dient in de verwerkersovereenkomsten ook expliciet aangegeven te zijn (door een clausule/artikel Meldplicht) waar gemeld moet worden indien een verwerker een inbreuk in verband met persoonsgegevens heeft geconstateerd.

In de rol van politie als verwerker moeten alle beveiligingsincidenten worden gemeld aan de Frontoffice Dienstverlening Partners (FODP). FODP behandelt deze meldingen volgens het incidentprotocol in de DAP behorende bij de specifieke dienstverlening .

Belangrijke onderwerpen (die verschillen van de werkwijze in hoofdstuk 2) zijn:

Definitie datalek	Iedere (pogingen tot) een inbreuk in verband met persoonsgegevens, een onrechtmatige of anderszins ongeautoriseerde verwerking van de persoonsgegevens wordt beschouwd als een beveiligingsincident dat gemeld moet worden. Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.
Meldpunt	Datalekken moeten in eerste instantie altijd worden gemeld bij TIB (= 2e lijns beoordeling). Na afweging stuurt TIB de melding door naar **FODP**: Tel: 088 5.1.2.i (e-mail: 5.1.2.i @politie.nl)
Registeren	• TIB registreert melding waaronder de incidenten politie in de rol als verwerker en stemt af met FODP. • Datalekken omtrent Dienstverlening Partners worden ook geregistreerd door **FODP.**
Melden aan	FODP meldt alle incidenten aan **verwerkingsverantwoordelijke.** ***De politie meldt dergelijke incidenten dus niet zelf aan de AP of aan betrokkene.***

6. Registratie datalekken

Alle datalekken moeten worden geregistreerd. Per datalek bevat de registratie in ieder geval feiten, gegevens omtrent de aard van de inbreuk en de wijze waarop de inbreuk is afgehandeld. Dit register hoeft niet openbaar te worden gemaakt.
De documentatie stelt de AP in staat de naleving van de AVG en Wpg te controleren.

In de Wpg is expliciet bepaald dat de verantwoordelijke zorgdraagt voor de vastlegging en de privacyfunctionaris houdt daarvan overzicht bij. Zij doen dit door gebruik te maken van de rapportagemogelijkheid die geboden wordt op het register. Voor de inzichtelijkheid van alle datalekken wordt gebruik gemaakt van de rapportages die geboden worden op het register.

Er moet rekening mee worden gehouden dat een vervolgprocedure na een datalek juridische maatregelen kan omvatten (civiel- of strafrechtelijk), en dat de politie waar dat aan de orde is het bewijsmateriaal moet verzamelen, bewaren en presenteren overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

6.1 Politie als verwerkingsverantwoordelijke

Als verwerkingsverantwoordelijke documenteert de politie:

a) alle inbreuken in verband met persoonsgegevens;
b) met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens;
c) de omvang (hoeveel personen worden geraakt);
d) de gevolgen daarvan en
e) de genomen corrigerende maatregelen;
f) of gemeld is aan de AP;
g) of gemeld is aan betrokkene.

Als het datalek is gemeld aan de *betrokkene*, dan wordt ook de tekst van de kennisgeving aan de *betrokkene* opgenomen in het overzicht.

6.2 Politie als verwerker

Als verwerker documenteert de politie alle informatie die relevant is voor de verwerkingsverantwoordelijke. Daarvoor is een **eigen frontoffice** beschikbaar. De afspraken daarover zijn vastgelegd in de verwerkersafspraken, dienstendocumentatie en eventuele werkinstructies.

7. Rapportage

Uit het register datalekken worden de managementrapportages opgesteld.
Deze rapportages bevatten de volgende gegevens:

Informatielevering
Aantal meldingen datalekken - cumulatief
Aantal meldingen datalekken - periode
Aantal meldingen AVG - cumulatief
Aantal meldingen AVG - periode
Aantal meldingen Wpg -cumulatief
Aantal meldingen Wpg -periode
Aantal meldplichtig -cumulatief
Aantal meldplichtig -periode
Aantal gemelde potentiele datalekken die geen datalek zijn - cumulatief
Aantal gemelde potentiele datalekken die geen datalek zijn - periode
Aantal datalekken gemeld bij AP - cumulatief
Aantal datalekken gemeld bij AP - periode
Aantal datalekken in behandeling - cumulatief
Aantal datalekken in behandeling - periode
Aantal datalekken afgerond - cumulatief
Aantal datalekken afgerond - periode

Bijlage 1 – Afkortingen en termen

Afkorting	Omschrijving
AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming
Betrokkene	Degene op wie een persoonsgegeven betrekking heeft
BSN	Burger Service Nummer
CISO	Concern Information Security Officer
DIV	Documentaire informatievoorziening
FODP	Frontoffice DP
FG	Functionaris voor de Gegevensbescherming
GA	Gegevensautoriteit
Persoonsgegeven	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon
RSLM	Relatie en Service Level Management
SD FM	Servicedesk Facilitair Management
SD ICT	Servicedesk ICT
SOC	Security Operations Center
Team Mobiel	Team mobiele apparatuur
TIB	Team Informatiebeveiliging
V&C	Team Veiligheid & Continuïteit
Verwerkingsverantwoordelijke	Degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt
Verwerker	Een verwerker is een persoon of organisatie aan wie de verwerkingsverantwoordelijke de gegevensverwerking heeft uitbesteed. Bijvoorbeeld een administratiekantoor. Een verwerker is niet zelfstandig verantwoordelijk voor de verwerking van de persoonsgegevens. Maar de verwerker heeft wel een aantal afgeleide verplichtingen, voor onder meer beveiliging en geheimhouding van de gegevens.
Verwerking	Een bewerking of een geheel van bewerkingen in het kader van de Dienstverlening met betrekking tot Persoonsgegevens, of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen.
Wpg	Wet politiegegevens

Bijlage 2 – Contactgegevens

Politie als verwerkingsverantwoordelijke

Informatiebeveiligingsorganisatie

Informatiebeveiligingsincidenten worden hoofdzakelijk gemeld via de servicedesken (decentrale meldpunten) van het korps (met name ICT, HR, FM) of aan het Team Informatiebeveiliging PDC (088 5.1.2.i). Melding geschiedt telefonisch (warm contact) en mag pas als gemeld worden beschouwd als de ontvangende partij deze bevestigd heeft. Zo nodig dient de melding op de e-mail toegelicht te worden.

Bij overschrijding van de P's (Pers, Publiek, Personeel, Politiek) wordt het beveiligingsincident door bijvoorbeeld Team Informatiebeveiliging of een servicedesk direct warm (via telefoon) aan de CISO/Informatiebeveiligingsautoriteit gemeld. De CISO (06 5.1.2.e) heeft dan de regie voor de verdere afhandeling, en informeert ook de FG.

5

Bijlage 3 – Addendum

Politie als verwerker

Dit document is in hoofdzaak opgesteld op basis van de **politie in de rol als verwerkingsverantwoordelijke van persoonsgegevens**. In het kort is de **politie in de rol als verwerker van persoonsgegevens** beschreven.
Het addendum zorgt ervoor dat de taken, verantwoordelijkheden en bevoegdheden van de **politie in de rol als verwerker van persoonsgegevens** ingebed zijn in het proces meldplicht datalekken.

Inleiding

Het addendum op de procesbeschrijving meldplicht datalekken richt zich op de politie in haar rol als verwerker van persoonsgegevens (bijvoorbeeld in de migratieketen en voor het ketendeel van de BVID-voorziening) en betreft de Dienstverlening Partners (DP)
Dit addendum op de procesbeschrijving is aanvullend op de in werking zijnde incidentprocedures bij

- De Frontoffice DP
- Team Informatiebeveiliging
- Dienstenmanagers BVV en BVID

Werkwijze politie als verwerker in migratieketen

In sommige gevallen heeft de politieorganisatie een rol als verwerker van persoonsgegevens. Als verwerker is de politie niet zelfstandig verantwoordelijk voor de verwerking van de persoonsgegevens, maar heeft wel een aantal afgeleide verplichtingen voor onder meer beveiliging en geheimhouding van persoonsgegevens.
Dat is het geval in de migratieketen. De Dienst ICT verzorgt de doorontwikkeling en het onderhoud van de centrale ICT-voorzieningen BVV, EUVIS en EURODAC (scv-local omgeving).
De directie Regie Migratieketen van het ministerie van Justitie en Veiligheid (DRM/DGM) is bij wet aangewezen als verwerkingsverantwoordelijke voor de persoonsgegevens in de migratieketen.

Als verwerker heeft de politie andere verplichtingen dan als verwerkingsverantwoordelijke. Dit heeft ook gevolgen voor de meldplicht datalekken. Het is dan ook belangrijk om bij alle (vermoedens van) datalekken na te gaan of het een beveiligingsincident betreft in de migratieketen of niet.

Globale werkwijze[6] meldplicht datalekken DP

Belangrijke onderwerpen (die verschillen van de werkwijze politie als verwerkingsverantwoordelijke) zijn:

Definitie datalek	Iedere (pogingen tot) een inbreuk in verband met persoonsgegevens, een onrechtmatige of anderszins ongeautoriseerde verwerking van de persoonsgegevens wordt beschouwd als een beveiligingsincident dat gemeld moet worden. Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.
Meldpunt	Datalekken moeten worden gemeld aan FODP.
Registeren	Datalekken worden geregistreerd door FODP.
Melden aan	FODP meldt alle incidenten aan DRM/DGM.
Termijn waarbinnen gemeld moet worden	FODP meldt meteen of binnen 24 uur na ontdekking van het datalek aan DRM / DGM.
Melden aan AP	DRM/DGM maakt de afweging om wel/niet te melden aan de AP en aan betrokkenen.

[6] Details van deze werkwijze zijn op te vragen bij FODP.

Informeren CIO Politie	DRM/DGM stelt de CIO Politie op de hoogte als een datalek is gemeld aan de AP en/of aan betrokkenen.

Registratie datalekken in de migratieketen

Als verwerker in de migratieketen documenteert de politie:

a. alle beveiligingsincidenten, d.w.z. iedere gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen, inclusief iedere (pogingen tot) inbreuk in verband met persoonsgegevens, een onrechtmatige of anderszins ongeautoriseerde verwerking van persoonsgegevens;
b. met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens
c. aard van de inbreuk in verband met persoonsgegevens
d. persoonsgegevens en betrokkenen
e. waarschijnlijke gevolgen van de inbreuk
f. maatregelen die verwerker heeft voorgesteld of genomen om de inbreuk aan te pakken, waaronder, in voorkomend geval, de maatrgelen ter beperking van de eventuele nadelige gevolgen daarvan.

Het overzicht hoeft niet openbaar gemaakt te worden, wel is het altijd inzichtelijk voor DRM/DGM.

DRM/DGM is verantwoordelijk voor het bijhouden van het register datalekken voor de migratieketen.

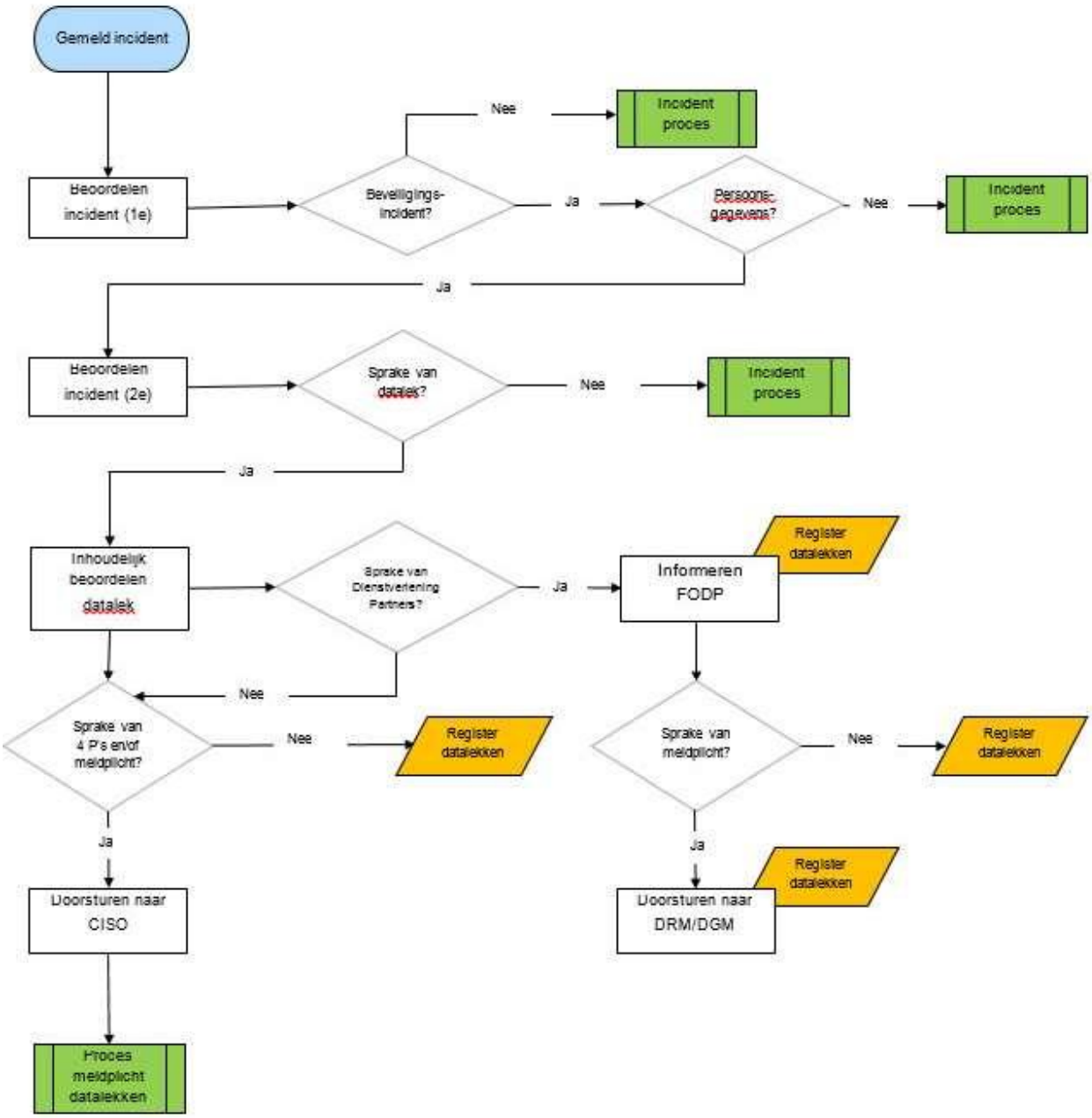
Contactgegevens

Beveiligingsincidenten op de scv-local omgeving moeten gemeld bij de frontoffice van Dienstverlening Partners.

Tel. 088-5.1.2.I (e-mail: 5.1.2.I@politie.nl)

Melding geschiedt telefonisch (warm contact) en mag pas als gemeld worden beschouwd als de ontvangende partij deze bevestigd heeft . Zo nodig dient de melding op de e-mail toegelicht te worden.

Stroomschema



Bijlage 4 – VIK-onderzoeken

De meldplicht datalekken geldt ook binnen de opsporingstaak en/of inlichtingen- of informatietaak van de politie. Indien er door VIK een intern onderzoek wordt gestart en er blijkt sprake te zijn van het 'lekken van informatie' dan kan er sprake zijn van een datalek.

Bij een mogelijk datalek moet er in ieder geval sprake zijn van:

- persoonsgegevens
- technisch of organisatorisch falen bij de verwerkingsverantwoordelijke.

Indien een volledig bevoegde en geautoriseerde medewerker (politie)informatie (persoonsgegevens) willens en wetens verkoopt aan criminelen dan is dit **geen** datalek.
Indien de organisatie verzuimd heeft om bij functiewijziging autorisaties in te trekken en medewerker verkoopt dan (politie)informatie dan is dit **wel** een datalek.

De uiteindelijke afweging of het een informatiebeveiligingsincident dan wel een (meldplichtig) datalek is, wordt gedaan door de beveiligingsorganisatie.

Bijvoorbeeld: De meldplicht is er NIET wanneer vanuit die politietaken (vermeende) datalekken worden waargenomen bij andere 'verwerkingsverantwoordelijken' dan de politie zelf. De meldplicht is er wel wanneer vanuit die politietaken (vermeende) datalekken worden waargenomen bij de politie (zelf) als verwerkingsverantwoordelijke. Zie bijlage 3 politie als verwerker)

Voor de verdere afweging/beoordeling of er sprake is van een meldplichtig datalek kan VIK contact opnemen met Team Informatiebeveiliging PDC (zie Bijlage 2 – Contactgegevens).