Regio Gooi en Vechtstreek

MEMO

Interne procedure afhandeling meldingen datalekken AVG

Algemeen	
Aan	CMT
Van	Anne Cnossen
Datum	21 oktober 2019
Verspreiden	Nee
Kenmerk	19.0013519

Inleiding

Sinds 1 januari 2016 is er met de Wet meldplicht datalekken een verplichting voor organisaties om datalekken zorgvuldig af te handelen. Met de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) is het afhandelen van datalekken ook een Europese verplichting geworden. Deze plicht om datalekken goed af te handelen betekent voor de Regio onder meer dat zij als verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens bij informatieveiligheidsincidenten met persoonsgegevens moet beoordelen of er sprake is van een datalek.
Als vast is gesteld dat inderdaad sprake is van een datalek (in de AVG inbreuk in verband met persoonsgegevens geheten) moet vervolgens mogelijk worden gemeld aan de Autoriteit Persoonsgegevens (AP) en de gedupeerde (in de AVG betrokkene). Ook bestaat er een verplichting alle datalekken vast te leggen in een datalekkenregister. Het register geeft inzicht in het aantal en de soorten datalekken dat heeft plaatsgevonden binnen de organisatie en dient ook als controlemiddel voor de AP of de organisatie aan de meldplicht heeft voldaan.
Datalekken kunnen zich in de gehele organisatie voordoen, maar de kans is het grootst daar waar veel met persoonsgegevens wordt gewerkt, zoals bij P&O en de uitvoerende RVE's.
Het onterecht niet aanmerken als datalek, het onterecht niet melden aan AP of betrokkene en het niet (op de juiste wijze) registreren van datalekken kan aanleiding zijn tot het opleggen van boetes door de AP aan de Regio.
In dit document worden de intern te zetten processtappen ten aanzien van een mogelijk datalek beschreven.
Voor de beoordeling of sprake is van een datalek en zo ja, om vervolgens te bepalen wat er moet gebeuren, wordt verwezen naar de Handreiking beoordeling datalekken AVG.

De procedure

In deze paragraaf wordt beschreven welke stappen achtereenvolgens gezet moeten worden als bij de Regio bekend wordt dat er sprake is of is geweest van een (mogelijk) datalek.
Allereerst is een overzicht opgenomen waarin de meest voorkomende stappen in relatie tot de actoren in een 'swimlane' schematisch zijn weergegeven.
Daarna volgt een tweede overzicht waarin de stappen voor interne en Regio-overstijgende opschaling in een 'swimlane' zijn weergegeven. Deze stappen zijn apart gevisualiseerd omdat opschaling zich niet vaak zal voordoen maar de kenbaarheid voor de organisatie (w.o. het bestuur) wel heel belangrijk is.

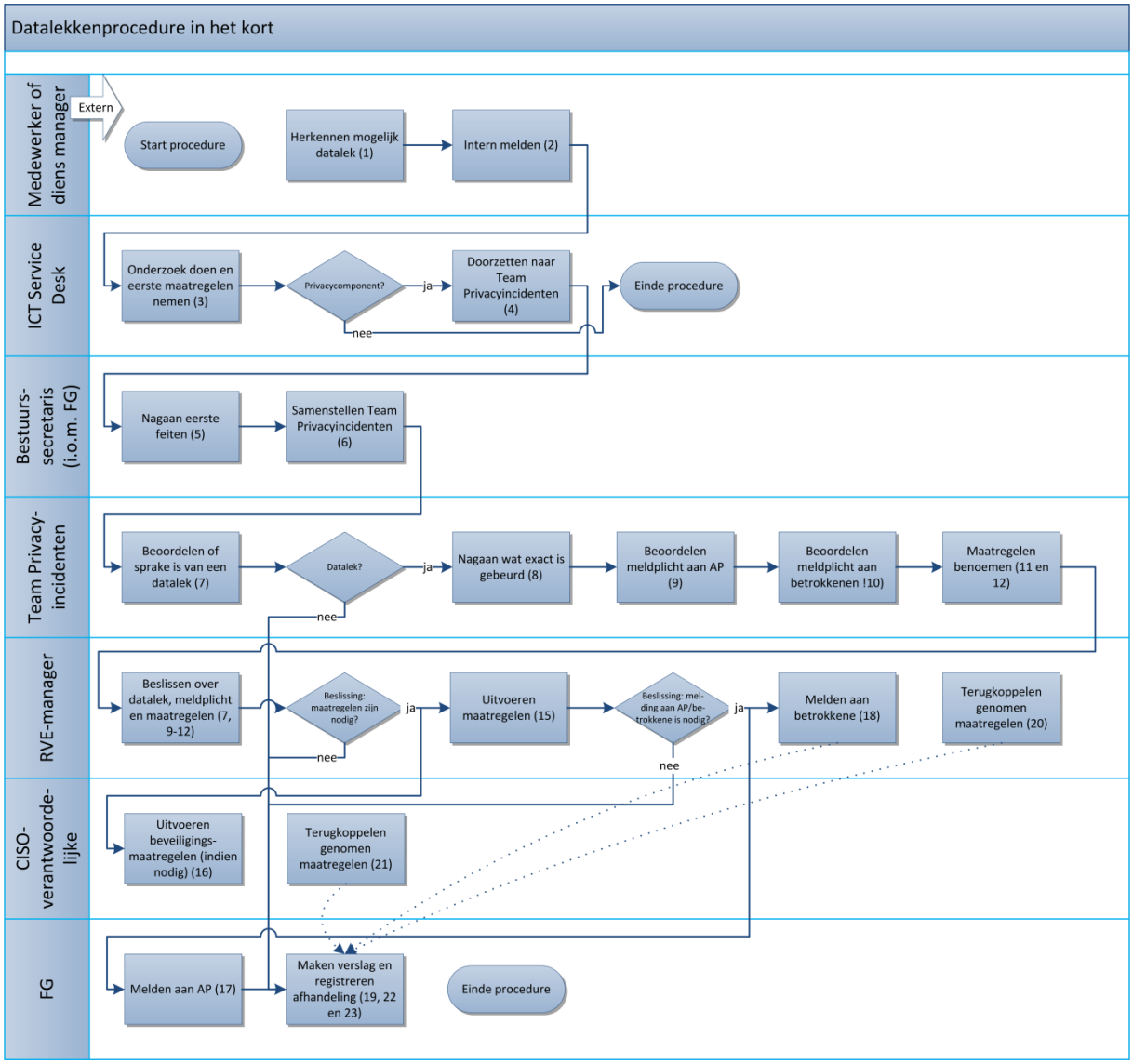
Na de schema's worden de stappen in detail uitgewerkt (waarbij de nummers van de stappen corresponderen met de nummers in de overzichten).
De processtappen zijn een uitwerking van de volgende aandachtspunten bij een datalek:

- Herkennen van mogelijk datalek
- Interne melding
- Eerste maatregelen door ICT (bij betrokkenheid device)
- Samenstelling van het Team Privacyincidenten
- Beoordelen datalek
- Overzicht verkrijgen
- Beoordelen meldplichtigheid aan AP
- Beoordelen meldplichtigheid aan betrokkene
- Maatregelen benoemen
- Interne en Regio-overstijgende opschaling
- Uitvoeren van maatregelen
- Daadwerkelijk melden
- Registratie van het datalek

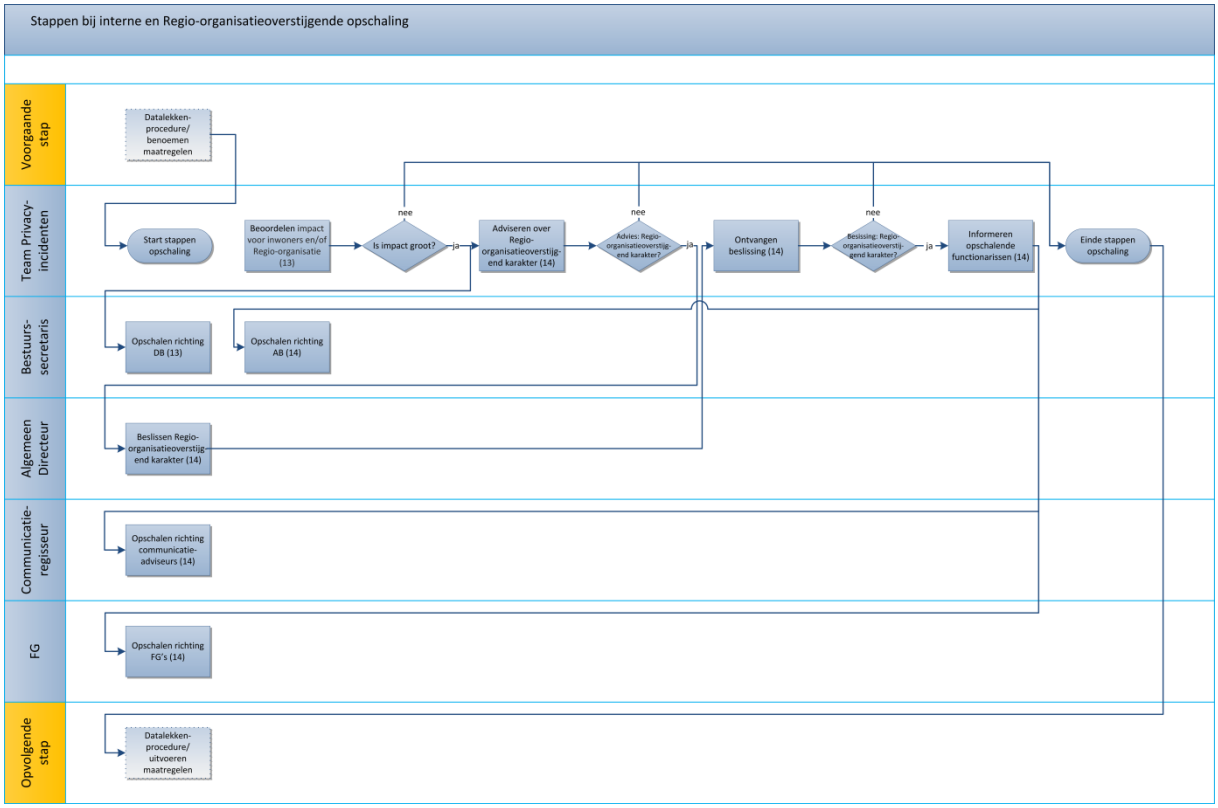
Algemeen

Het grootste deel van de onderstaande processtappen dient plaats te vinden voordat 72 uren zijn verstreken nadat bekend is geworden dat sprake is van een datalek.
In het algemeen is van belang dat er discreet met een datalek wordt omgegaan, zowel voor wat betreft de aanmelder als degene van wie de persoonsgegevens zijn gelekt. Van de gedupeerde persoon wordt in de beschrijving van het datalek niet de naam (en indien mogelijk ook geen andere identificerende gegevens) vermeld. Er is in het Document Management Systeem een vertrouwelijkheidsniveau (niveau datalekkenteam) voor het datalekkendossier (incl. brief aan betrokkene).
De rol van de betreffende RVE-manager bij beoordelen van een datalek is essentieel. De beslissing dat het een datalek is, dat al dan niet gemeld moet worden en het formuleren van de maatregelen ligt bij de verwerkingsverantwoordelijke, en dat is de RVE-manager. Uiteraard zullen de overige leden van het Team Privacyincidenten hier een advies over geven. Als de omstandigheden dit toelaten/vereisen (n.a.v. kennisniveau manager, specifieke omstandigheden van het lek) kan dit advies wat directiever van aard zijn. Indien manager advies niet overneemt, wordt dat geregistreerd. De FG kan eventueel escaleren via de lijn Algemeen Directeur – DB – AB.
Jaarlijks worden de datalekken en de werking van deze procedure geëvalueerd. De uitkomst van de evaluatie wordt gebruikt om het privacybewustzijn van de organisatie en deze procedure verder aan te scherpen.
Verder zal binnen de Regio de term datalek, vanwege de negatieve bijklank, zoveel mogelijk worden vervangen door de term privacyincident.

Overzicht 1


Datalekkenprocedure in het kort
Medewerker of diens manager
Extern
Start procedure
Herkennen mogelijk datalek (1)
Intern melden (2)
ICT Service Desk
Onderzoek doen en eerste maatregelen nemen (3)
Privacycomponent?
ja
nee
Doorzetten naar Team Privacyincidenten (4)
Einde procedure
Bestuurs-secretaris (i.o.m. FG)
Nagaan eerste feiten (5)
Samenstellen Team Privacyincidenten (6)
Team Privacy-incidenten
Beoordelen of sprake is van een datalek (7)
Datalek?
ja
nee
Nagaan wat exact is gebeurd (8)
Beoordelen meldplicht aan AP (9)
Beoordelen meldplicht aan betrokkenen !10)
Maatregelen benoemen (11 en 12)
RVE-manager
Beslissen over datalek, meldplicht en maatregelen (7, 9-12)
Beslissing: maatregelen zijn nodig?
ja
nee
Uitvoeren maatregelen (15)
Beslissing: mel-ding aan AP/be-trokkene is nodig?
ja
nee
Melden aan betrokkene (18)
Terugkoppelen genomen maatregelen (20)
CISO-verantwoorde-lijke
Uitvoeren beveiligings-maatregelen (indien nodig) (16)
Terugkoppelen genomen maatregelen (21)
FG
Melden aan AP (17)
Maken verslag en registreren afhandeling (19, 22 en 23)
Einde procedure

Overzicht 2



Stap voor stap

Herkennen, interne melding en eerste maatregelen ICT

1. Een **medewerker** van de Regio constateert dat er sprake is geweest van een informatieveiligheidsincident dat mogelijk een datalek betreft. Ook is het mogelijk dat de constatering door een **manager** wordt gedaan of van buiten de organisatie van de Regio (bijv. via een inwoner of ICT-leverancier) komt.
2. De betrokken **medewerker** of diens **manager** meldt het (vermoeden van een) datalek z.s.m. intern bij de ICT servicedesk telefonisch op nummer 035-6926200 of per e-mail op meldpuntdatalek@regiogv.nl.
3. **ICT** stelt vast of er sprake is van omstandigheden waarbij elektronica (iPad, desktop, laptop Ericom Blaze, smartphone, USB-stick) betrokken is. Hierbij valt te denken aan een hack, malware of diefstal. Ook kan het zijn dat het een louter “fysiek datalek” (verlies of diefstal papieren dossier) betreft.
   Hiervoor start ICT een onderzoek. Hierbij wordt gekeken of er een afzonderlijk apparaat bij betrokken is. Zo ja, dan zal het betreffende apparaat zo spoedig mogelijk geïsoleerd worden van de elektronische systemen binnen de Regio.
   ICT onderneemt indien nodig nog andere acties die noodzakelijk zijn gelet op de aard van de melding. Denk hierbij aan het op afstand lokaliseren en/of wissen of versleutelen van een laptop, tablet, of smartphone of het op afstand blokkeren van de toegang tot een medewerkersaccount of clouddienst.
4. Indien **ICT** vermoedt dat het informatieveiligheidsincident een privacycomponent heeft, geeft zij de melding door aan het Team Privacyincidenten via de bestuurssecretaris (06-52578064).

Samenstellen van Team Privacyincidenten

5. De **bestuurssecretaris** of de **FG** gaat t.b.v. het overleg met het Team alvast de eerste feiten na bij de manager of medewerker
6. **Bestuurssecretaris** bepaalt (in overleg met de FG) de samenstelling van het Team en de wijze van afdoening en roept het Team bij elkaar. Samenstelling van het Team en aanpak hangen af van de ernst van het lek zowel voor de Regio als voor gedupeerde. Bij applicatie/systeemfouten is een grondigere afdoening nodig dan bij menselijke fouten. Wijze van aanpak kan variëren van schriftelijk (via mail) afdoen in kleinste samenstelling tot in volledige bezetting[1] bijeenkomen. Bij datalekken die wat complexer zijn en waarbij niet direct alle feiten boven tafel komen, is het gewenst nogmaals met het Team bij elkaar te komen op het moment dat alle feiten helder zijn.

Beoordelen of sprake is van een datalek en of gemeld moet worden

7. Het **Team Privacyincidenten** beoordeelt aan de hand van de Handreiking beoordeling datalekken AVG of er sprake is van een 'inbreuk in verband met persoonsgegevens', ofwel een datalek. Dit is 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 en adviseert de **RVE-manager** die beslist. Deze beoordeling moet zo spoedig mogelijk worden uitgevoerd. Als er wordt besloten dat geen sprake is van een datalek dan wordt het dossier m.b.t. het gemelde (mogelijke) datalek gesloten. Wordt er daarentegen besloten dat van een datalek wél sprake is, dan begint de termijn van 72 uren voor melden aan de AP vanaf nu te lopen.
8. Het **Team Privacyincidenten** gaat m.b.v. de Handreiking beoordeling datalekken AVG na wat er exact gebeurd is. Als de melding door de manager is gedaan of van buiten de Regio komt, dan loopt de afhandeling en terugkoppeling volledig via de manager. Indien de medewerker zelf heeft gemeld dan is hij of zij zelf de contactpersoon. De aanmelder wordt bedankt voor de melding. Bij de inventarisatie wordt o.a. bekeken welke persoonsgegevens zijn betrokken, wat de omvang van het datalek is en wie toegang hebben gekregen tot de persoonsgegevens. Hiervoor houdt de betrokken medewerker/manager zich beschikbaar en verleent alle medewerking die redelijkerwijs verwacht mag worden. De **RVE-manager** en de **CISO-verantwoordelijke** verstrekken de benodigde informatie. De verkregen informatie is nodig voor de vervolgstappen.
9. Het **Team Privacyincidenten** beoordeelt m.b.v. de Handreiking beoordeling datalekken AVG of het datalek gemeld moet worden aan de AP. Indien het Team dat wenselijk vindt, wordt de communicatieregisseur op de hoogte gesteld (als die niet al deel uitmaakt van het Team) van het feit dat gemeld gaat worden. Het Team adviseert de **RVE-manager** die beslist. Er moet binnen 72 uur worden bepaald of het datalek moet worden gemeld aan de AP en zo ja, moet ook binnen die termijn de melding zijn gedaan. Regel is dat er moet worden gemeld tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor rechten en vrijheden van natuurlijke personen.
10. Ook beoordeelt **Team Privacyincidenten** m.b.v. de Handreiking beoordeling datalekken AVG of het datalek gemeld moet worden aan de betrokkene. Indien gewenst wordt de communicatieregisseur erbij betrokken (als die niet al deel uitmaakt van het Team). Het Team

[1] Het volledige Team bestaat uit de FG, de CISO-verantwoordelijke, één van de juridisch adviseurs en de bestuurssecretaris. Per datalek wordt de betrokken manager aan het team datalekken toegevoegd. De bestuurssecretaris kan per geval bepalen dat andere personen aan het Team worden toegevoegd. De communicatieregisseur wordt erbij betrokken als de bestuurssecretaris het aannemelijk vindt dat er een melding aan AP (en betrokkene) gedaan moet worden.
Als een lid van het datalekkenteam de dupe is van het datalek of het datalek heeft veroorzaakt, wordt de beoordeling zonder deze persoon gedaan en wordt zo nodig het vertrouwelijkheidsniveau naar boven bijgesteld (bijv. alleen betreffende manager en FG).

adviseert de **RVE-manager** die beslist. De betrokkene moet worden geïnformeerd als het risico voor rechten en vrijheden van natuurlijke personen hoog is.

Maatregelen benoemen

11. Het **Team Privacyincidenten** formuleert (naast de maatregelen die ICT al heeft genomen) de maatregelen die direct getroffen moeten worden om het datalek te beëindigen en de schade te beperken en adviseert de **RVE-manager** die beslist.[2]
Voorbeelden van maatregelen om schade bij een datalek te beperken zijn:
- Een gepubliceerd bestand offline halen.
- Een verkeerde ontvanger vragen om een bevestiging dat de gegevens uit een brief of e-mail zijn vernietigd. Hoewel je op basis van zo'n bevestiging niet 100% zeker weet dat de gegevens vernietigd zijn, is het handig dit mee te nemen in de risico-inschatting.

12. Het **Team Privacyincidenten** formuleert voorstellen ter voorkoming van herhaling en adviseert de **RVE-manager** die beslist.

Interne en Regio-organisatieoverstijgende opschaling

13. Bij datalekken met mogelijk grote impact voor inwoners en/of de Regio-organisatie is het van belang dat het bestuur snel op de hoogte wordt gebracht. Het **Team Privacyincidenten** beoordeelt of deze mogelijk grote impact aanwezig is.
Overwegingen om te bepalen dat er grote impact is voor inwoners en/of de Regio-organisatie zijn:
- betrokkenheid meerdere RVE's
- maatschappelijke onrust / impact
- (dreigende) verstoring van functioneren van de Regio
- gevaar voor veiligheid medewerkers / inwoners
- bedreiging van reputatie
- betrokkenheid meerdere externe partners
- opschaling vanuit overheidszijde
- noodzaak grootschalige inzet
- (verwachte) mediaaandacht

Grote impact voor inwoners (en trouwens ook voor de Regio-organisatie) is er bijvoorbeeld wanneer volledige dossiers van inwoners voor onbevoegden toegankelijk zijn. Mogelijk grote impact voor de Regio-organisatie zelf kan aan de orde zijn wanneer de reputatie van de Regio in het geding is. Denk hierbij aan een in de landelijke media breed uitgemeten datalek dat zich vervolgens bij de Regio op een zelfde wijze voordoet.
De **bestuurssecretaris** draagt zorg voor opschaling richting DB.

14. Als het datalek (naast grote impact voor inwoners en/of de Regio-organisatie) ook een Regio-organisatieoverstijgend karakter heeft, moet mogelijk opgeschaald worden richting de Regiogemeenten. Het **Team Privacyincidenten** beoordeelt of al dan niet sprake is van een datalek met een Regio-organisatieoverstijgend karakter en adviseert de Algemeen Directeur. De **Algemeen Directeur** beslist en koppelt de beslissing terug aan het Team Privacyincidenten.
Om het Regio-organisatieoverstijgende karakter in te schatten wordt gekeken of het datalek afstraalt op de Regiogemeenten. Hiervan kan sprake zijn bij een datalek dat zich voordoet rondom taken waarvan de uitvoering deels bij de Regio en deels bij gemeenten ligt (zoals bij de taken van Inkoop en Contractbeheer). Of ten aanzien van taken waarvan niet helder is of de Regio daarvoor alleen of samen met Regiogemeenten verantwoordelijk is (zoals nieuwe taken waarvan de opdracht aan de Regio nog niet goed vast is gesteld).
Als de beslissing is dat het datalek een Regio-organisatieoverstijgend karakter heeft, zorgt het

[2] Team Privacyincidenten kan daarnaast voorstellen doen m.b.t. doen van aangifte en melden bij de verzekering, etc.

Team Privacyincidenten ervoor dat de **bestuurssecretaris** overgaat tot opschaling richting AB en de Regiogemeenten (op welk niveau is afhankelijk van de omstandigheden van het geval). Ook wordt de **communicatieregisseur** geïnformeerd die zorgt voor opschaling richting communicatieadviseurs van de Regiogemeenten en de **FG** zorgt voor opschaling richting FG's van de Regiogemeenten. In communicatie naar de buitenwereld heeft de communicatieregisseur van de Regio een coördinerende rol. Communicatieadviseurs vanuit de Regiogemeenten stemmen hun werkzaamheden m.b.t. het datalek af met de communicatieregisseur van de Regio. De Regio is verantwoordelijk voor de afhandeling van het datalek. Dit vanwege het praktische aspect dat de Regio waarschijnlijk het best op de hoogte is van de situatie, maar ook vanwege de veronderstelde verwerkingsverantwoordelijkheid van de uitgevoerde taak. Dit betekent o.a. dat de Regio de melding aan AP en betrokkenen verzorgt.

Uitvoeren van maatregelen

15. De **RVE-manager** treft de maatregelen waartoe hij/zij na advies van het Team heeft besloten. Maatregelen die onmiddellijk genomen moeten worden, hebben de eerste aandacht.

16. De **CISO-verantwoordelijke** treft de vereiste beveiligingsmaatregelen (indien nodig).

Daadwerkelijk melden

17. De **FG** draagt zorg voor melding aan de AP via https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken. Er moet een kopie van de melding worden opgeslagen. Melding vindt onverwijld plaats, zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking. Ook als nog niet alle informatie bekend is, moet zo mogelijk binnen 72 uur een voorlopige melding worden gedaan. Deze kan later worden aangevuld of ingetrokken. In zo'n geval kan het Team vóór aanvulling of intrekking nogmaals bij elkaar komen.

18. De FG stelt een tekst op voor mededeling aan betrokkene(n)[3]. Deze tekst wordt voorgelegd aan de communicatieregisseur. De tekst die FG en communicatieregisseur samen hebben opgesteld wordt aan de RVE-manager gestuurd. Als FG en communicatieregisseur het niet eens zijn over de tekst, beslist RVE-manager. De **RVE-manager** draagt zorg voor het mededelen aan betrokkene(n). De mededeling kan bijv. in een e-mail of brief aan betrokkenen worden gestuurd. Overwogen kan worden om de betrokkene eerst telefonisch op de hoogte te stellen. Afhankelijk van de omstandigheden van het geval kan telefonisch informeren voldoende zijn. Een vooraf door FG en communicatieregisseur opgestelde belinstructie is dan wel van belang.
Indien een eigen medewerker de dupe is van het datalek wordt, voordat een brief aan gedupeerde medewerker wordt gestuurd, de manager van gedupeerde medewerker op de hoogte gesteld, die de gedupeerde medewerker mondeling inlicht. Daarbij wordt de gedupeerde medewerker aangeboden actief te worden betrokken bij door de organisatie te treffen maatregelen.

Registratie

19. De **FG** zorgt (samen met het Team Privacyincidenten) voor het maken van een verslag (waarvoor een Word-sjabloon beschikbaar is) met daarin het feitenrelaas, de beoordeling en de maatregelen.

20. De **RVE-manager** laat per mail weten hoe en wanneer de geformuleerde maatregelen zijn uitgevoerd.

[3] De mededeling bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van het datalek, contactgegevens van de FG, de waarschijnlijke gevolgen van het datalek en de voorgestelde en getroffen maatregelen. Ook wordt aangegeven welke maatregelen betrokkene zelf kan nemen om de negatieve gevolgen te beperken.

21. De **CISO-verantwoordelijke** laat per mail weten hoe en wanneer de benodigde beveiligingsmaatregelen zijn uitgevoerd.
22. De **FG** registreert het in stap 19 bedoelde verslag en i.v.t. de melding aan AP en betrokkenen in het Document Management Systeem.
23. De **FG** neemt het gemelde informatieveiligheidsincident (waaronder naast de gemelde ook de niet-gemelde datalekken) met relevante kenmerken[4] op in het register van incidenten en datalekken dat de Regio op grond van de AVG in het Document Management Systeem bijhoudt.

Afronding

24. De **bestuurssecretaris** legt, indien naar zijn oordeel nodig, na afloop het verslag en de eventuele aanbevelingen voor aan de Algemeen Directeur. De Algemeen Directeur tekent voor gezien.

[4] In het register staat aangegeven of het een informatieveiligheidsincident of datalek betreft, een beschrijving van de inbreuk, het betrokken organisatieonderdeel, de mogelijke gevolgen van de inbreuk, de getroffen corrigerende maatregelen en of hiervan een melding is gedaan aan de AP en betrokkenen (plus inhoud van die melding). Ook staat aangegeven of de FG is betrokken bij afhandeling en of de RVE-manager het advies van het Team Privacyincidenten heeft opgevolgd en zo niet, waarom niet. De betrokkenheid van derde partijen die bij het datalek een rol hebben gehad wordt vermeld. Ten slotte is opgenomen een vermelding van de vindplaats van de documentatie aangaande verslag, melding aan AP en betrokkenen en de bevestiging van RVE-manager (en indien van toepassing van de CISO-verantwoordelijke) van daadwerkelijk genomen hebben van corrigerende (en preventieve) maatregelen.