CompLions Data Pro Richtlijn: Datalekken

CompLions-GRC B.V.

CompLions-GRC B.V.
Keulenstraat 8E, 7418 ET Deventer
Postbus 2147, 7420 AC Deventer

T 0570 – 63 47 17
W www.complions.com
E secretariaat@complions.com

NL12 RABO 0319 7046 61
KvK-nr.: 68855753

DOCUMENTGEGEVENS

CompLions Richtlijn Datalekken v1.0

Auteur:	CompLions-GRC B.V.
Versie:	1.0
Datum:	Juli 2021
Documentnaam:	Data Pro - CompLions Richtlijn Datalekken v1.0

Documenthistorie

Versie	Status	Toelichting	Auteur	Datum
0.1	Herziening	Directiebeoordeling	Ron Boscu	Juli 2021
1.0	Definitief	Herziening	Ron Boscu	Juli 2021

Uitgegeven door:

CompLions-GRC B.V.

Bezoekadres: Keulenstraat 8E, 7418 ET Deventer

Postadres: Postbus 2147, 7420 AC Deventer

Contactgegevens:

support@complions.com

Telefoon: 0570 – 62 19 34

Inhoud

1. Documentbeheer

1.1 Doel en reikwijdte

Op basis van de AVG geldt een meldplicht, deze houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken onverwijld moeten melden aan de Autoriteit Persoonsgegevens (AP), en in bepaalde gevallen ook aan de betrokkene(n). De betrokkene is degene van wie persoonsgegevens zijn gelekt. Eventuele inbreuken die niet worden gemeld, moeten wel worden gedocumenteerd ter bewijsvoering. Dit document geeft richting aan de procedure omtrent het zien van een mogelijk incident, tot het opschalen naar een datalek en het melden hiervan.

1.2 Doelstelling en doelgroep

De doelstelling is om duidelijkheid te creëren in de procesflow omtrent incidenten en datalekken. De doelgroep zijn de medewerkers van CompLions (inclusief tijdelijke medewerkers en werknemers van derden welke toegang hebben tot CompLions netwerken, systemen en applicaties).

De meldplicht is eveneens van toepassing als het datalek bij een derde is ontstaan, bijvoorbeeld bij één van onze datacenters of hostingpartijen.

Dit document is ingericht als leidraad.

1.3 Verantwoordelijkheden, goedkeuring en controle

Verantwoordelijke voor het onderhoud van deze beleidsrichtlijn is het Security Team bestaande uit Manager consultancy, servicedelivery, ISO, privacy coördinator, MT lid. Via gedelegeerde taken zullen zij toezien op naleving en controle van de beleidsrichtlijn. Door ondertekening van dit document geeft de directie goedkeuring aan deze beleidsrichtlijn.
Deze beleidsrichtlijn zal periodiek worden herzien op volledigheid, mede op basis van de veranderingen in de infrastructuur. Deze veranderingen worden uitgevoerd via een change- managementproces, waarin de belanghebbende vertegenwoordigd zijn.
Controle op de beleidsrichtlijn zal periodiek door middel van assessmentsaudits worden uitgevoerd door het Security Team in opdracht van de directie, hiervan wordt verslaglegging gedaan.

1.4 Definities

AP
Autoriteit Persoonsgegevens, de Nederlandse gegevensbeschermingsautoriteit.
Bestand
Elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid (artikel 4, lid 6, AVG).
Betrokkene
Degene op wie een persoonsgegeven betrekking heeft.
Beveiligingslek
Een inbreuk op de beveiliging (zoals bedoeld in artikel 34, lid 1, AVG) waarbij persoonsgegevens niet worden blootgesteld aan verlies of onrechtmatige verwerking; er is dan geen sprake van een datalek.
Datalek
Een inbreuk op de beveiliging (zoals bedoeld in artikel 34, lid 1, AVG) waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking; dus blootgesteld aan datgene waartegen beveiligingsmaatregelen (artikel 32, lid 1, AVG) bescherming moesten bieden.
Datalekken Commissie
Een door de Security Manager tijdelijk ingestelde onderzoekscommissie, die zorgdraagt voor een onderzoek en over de uitkomsten rapporteert aan de directie.
Derden
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken (artikel 4, lid 10, AVG).
Genodigden
Interne betrokkenen die uitgenodigd zijn bij de bespreking(en) van het incident.
FG
Functionaris Gegevensbescherming (artikel 37, AVG). CompLions-GRC heeft geen FG, maar een coördinator Privacy.
Incident
Een mogelijk beveiligingsincident, waardoor de bescherming van persoonsgegevens op enig moment is doorbroken en waardoor de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Het is daarbij niet van belang of de verantwoordelijke passende technische of organisatorische beschermingsmaatregelen heeft getroffen of niet. Ieder datalek is een incident, niet ieder incident is een datalek.
ISO
Information Security Officer, tevens de manager, die vanuit de portefeuille Informatieveiligheid belast is met de interne coördinatie van de procedure Meldplicht Datalekken.
Persoonsgegeven
Informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (artikel 4, lid 1, AVG).
Verwerkingsverantwoordelijke

Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen (artikel 4, lid 7, AVG).

Verwerker

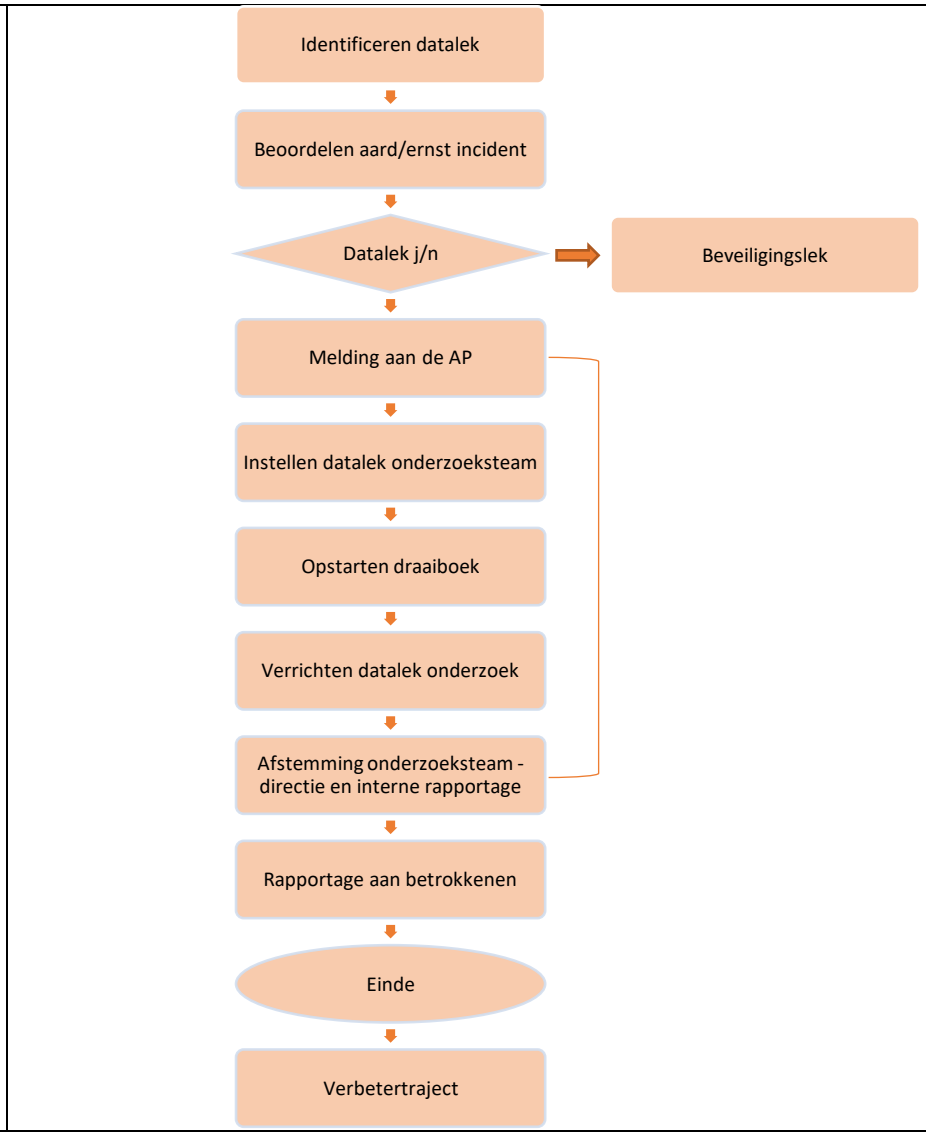
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt (artikel 4, lid 8, AVG)

Verwerking van persoonsgegevens

Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens (artikel 4, lid 2, AVG).

1.5 Werkwijze melding datalek

1.5.1 Proces flow melding datalek

Betrokken medewerkers CompLions Information Security Officer/ Security Team (ISO) i.o.m. Directie Coördinator Privacy/ Directie Manager Service Delivery (SD) i.s.m. manager SW development (SWD) Managers SD en SWD, directie en Coördinator Privacy / ISO Directie	

2. Toelichting flow

2.1 Identificeren van een datalek

De medewerker die een (mogelijk) datalek constateert, meldt dit incident per omgaande bij zijn organisatorisch hoofd, en deze meldt het incident per omgaande aan het integraal management of daarmee gelijkgesteld manager. Deze zorgt dat de ISO / Coördinator Privacy direct wordt geïnformeerd.

De procedure Meldplicht Datalekken wordt dan gestart.

2.2 Beoordeling aard/ernst incident: datalek ja/nee

- De ISO / Coördinator Privacy draagt zorg voor volledige en juiste informatie.
- Op basis van de verkregen informatie en bij vermoeden van een datalek wordt in overleg met de Directie en eventueel management en de ISO / Coördinator Privacy zo spoedig mogelijk de beoordeling gemaakt of er daadwerkelijk sprake is van een datalek.
- Tevens kan in dit overleg worden beoordeeld of er per direct maatregelen genomen moeten worden om de schade te beperken, waaronder het doen van een (voorlopige) melding aan betrokkenen.
- Tevens kan worden beoordeeld of het datalek meldingsplicht is voor de politie in geval van vermoeden van een strafbaar feit (zie ook hierna onder 2.3).
- De beoordeling of er sprake is van een incident, dat gemeld moet worden aan de AP kan tot stand komen met behulp van de schema's te vinden in de beleidsregels "Guidelines Meldplicht Datalekken" van de AP.
  Bij de beoordeling spelen o.a. een rol:
  - is er sprake van verlies van persoonsgegevens; dit houdt in dat [naam organisatie] deze gegevens niet meer heeft, omdat deze zijn vernietigd of op een andere wijze verloren zijn gegaan;
  - is er sprake van onrechtmatige verwerking van persoonsgegevens; hier onder vallen de onbedoelde of onwettige vernietiging, verlies of wijziging van verwerkte persoonsgegevens, of een niet geautoriseerde toegang tot verwerkte persoonsgegevens of verstrekking daarvan;
  - is er sprake van een enkele tekortkoming of kwetsbaarheid in de beveiliging;
  - kan redelijkerwijs worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid;
  - zijn er persoonsgegevens van gevoelige aard gelekt;
    - bijzondere persoonsgegevens conform artikel 9, AVG;
    - gegevens over de financiële of economische situatie van de betrokkene;
    - gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
    - gebruikersnamen, wachtwoorden en andere inloggegevens;
    - gegevens die kunnen worden gebruikt voor (identiteits)fraude;
  - leiden de aard en de omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen; betrek hierbij factoren als
    - de omvang van de verwerking; gaat het om veel persoonsgegevens per persoon, en om gegevens van grote groepen betrokkenen;
    - de impact van verlies of onrechtmatige verwerking;
    - het delen van de persoonsgegevens binnen (zorg)ketens; dit betekent dat de gevolgen van verlies en onbevoegde wijziging van persoonsgegevens door de hele keten kunnen op- treden;

- betrokkenheid van kwetsbare groepen; denk aan verstandelijk gehandicapten;
- In geval geoordeeld wordt, dat sprake is van een (mogelijk) datalek, wordt tevens het communicatietraject richting betrokkene(n) en indien van toepassing de bewerker besproken;
- In geval dat het incident niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens is er geen sprake van een datalek maar van een beveiligingslek. Melding aan de AP is dan niet aan de orde. Wel kan in het overleg besloten worden, dat het zinvol is om het beveiligingslek te onderzoeken om herhaling te voorkomen.

2.3 Maatregelen om het (actieve) lek te stoppen of de gevolgen te beperken

Het draaiboek is geënt op bovenstaand flow van activiteiten. Het is toegespitst op de organisatie en software dienstverlening o.b.v. het samenbrengen van expertise (het Security Team met relevante stakeholders) binnen de organisatie. Er worden voor specifieke situaties keuzes en beslissingen genomen omtrent het te nemen maatregelen en verbeteracties.

2.3.1 Mogelijke maatregelen

Er zijn maatregelen die genomen kunnen worden om een (actief) lek te stoppen of de gevolgen te beperken, namelijk:

- Het loskoppelen of offline halen van het computernetwerk/NAS/servers en/of werkstations;
- Het activeren van filters op netwerkrouters;
- Het blokkeren van bepaalde gebruikersaccounts;
- Het verplaatsen van data naar een veilige locatie;
- Het uitschakelen van het systeem;
- Het isoleren van een indringer van buitenaf;
- Het aanpassen van firewallconfiguraties;
- Het wijzigen van wachtwoorden van beheerders of onderhouders;
- Het tijdelijk stopzetten van diensten zoals FTP, webdiensten of e-mails;
- Remote wiping (bijvoorbeeld bij een gestolen laptop);
- Foutief geadresseerde personen contacteren met het verzoek om te verwijderen wat hij/zij heeft ontvangen;
- Fysiek zoeken (bijvoorbeeld bij kwijtgeraakte USB-stick of harde schijf);
- (Hot)fixes en/of patches aanbrengen;
- Het formatteren/herinstalleren van een systeem d.m.v. Back-ups (bij bijvoorbeeld hackaanvallen);
- Mogelijkheden om externe expertise of professionals in te roepen.

2.4 Bewijs verzamelen en data veiligstellen

Voor zover mogelijk het bijhouden van een Audittrail (logging) van de constateringen en genomen stappen, het maken van back-ups van logbestanden en het hele systeem en eventueel andere maatregelen nemen om het bewijsmateriaal en de data veilig te stellen.

2.5 Melden aan de Autoriteit Persoonsgegevens

- MT of ISO/ Coördinator Privacy verzorgt de tijdige (onverwijld, zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek) elektronische melding bij de AP volgens het online meldingsformulier van de AP. (https://datalekken.autoriteitpersoonsgegevens.nl)
- Dit met inachtneming van richtlijnen van de AP terzake. De ISO / Coördinator Privacy zorg voor volledige en juiste informatie zoals opgenomen in het 'Formulier t.b.v. melding datalek' op grond waarvan feitelijk gemeld zal worden. De ISO / Coördinator Privacy fungeert als contactpersoon inzake de communicatie naar de AP. Dit geldt ook ingeval nog niet duidelijk is dat het incident een datalek is. Dan is de mogelijkheid aanwezig om na vaststelling van de aard van het incident de melding aan te vullen, dan wel in te trekken.
- De directie is eindverantwoordelijk, de ISO / Coördinator Privacy is gedelegeerd regievoerder over de interne afhandeling van het (mogelijke) datalek in al zijn facetten, over de externe afhandeling, waaronder het AP, betrokkenen en bewerker.
- Het direct betrokken management draagt zorg dat de bij het incident betrokken medewerkers worden geïnformeerd. Het direct betrokken (integraal) management zorgt ervoor dat de betrokken medewerkers bij het incident, het mogelijke datalek, zo snel mogelijk een eigen verslag opstellen over de toedracht van het incident. Deze schriftelijke informatie wordt aan de directie verstrekt ten behoeve van de leden van het Security Team (zie 2.6) en het datalekken dossier.
- De AP zal na het melden van een datalek een ontvangstbevestiging sturen. Alleen indien de melding daartoe aanleiding geeft zal de AP contact opnemen.
- Bij een datalek als gevolg van een (niet-ethische) hack (art. 138ab van het Wetboek van Strafrecht), is van belang wat de aard van de gelekte persoonsgegevens is, en wat de risico's van misbruik voor de betrokkene(n) zijn. Bij een hack ligt naast melding bij de AP, ook aangifte bij de politie in de rede in verband met de opsporing van de daders. Aangifte loopt via een eventueel beschikbare contactfunctionaris richting politie.

2.6 Startbijeenkomst Security Team

- De ISO / Coördinator Privacy plant een startbijeenkomst ter bespreking van de opdracht aan het Security Team. Deze startbijeenkomst vindt in geval van een datalek plaats binnen één week na de melding van het datalek aan het AP.
- De ISO / Coördinator Privacy draagt zorg voor openstelling van beschikbare informatie inzake het datalek t.b.v. de leden van het Security Team.

2.7 Verrichten datalek onderzoek

- Het Security Team stelt binnen de gestelde termijn en opdrachtverlening een (systematisch) (intern) onderzoek in naar de feitelijke toedracht van het (mogelijke) datalek.
- Het Security Team onderzoekt verder of en zo ja hoe dergelijke incidenten in de toekomst kunnen worden voorkomen (het vermijdbaarheidsaspect).
- De bevoegdheden van het Security Team zijn:
    - de mogelijkheid met iedereen te spreken;
    - alle relevante documenten in te zien;
    - toegang te hebben tot alle plaatsen. Dit alles in het kader van wat de commissie nodig acht ten behoeve van een zorgvuldige analyse;

- in relatie tot de externe bewerker gelden de afspraken zoals vastgelegd in de bewerkersovereenkomst

- Het Security Team heeft binnen 4 weken na de startbijeenkomst het onderzoek afgerond.
- Het Security Team kan in overleg met, of op instigatie van [bestuur van de organisatie] besluiten om externe deskundigen te betrekken bij het onderzoek.
- Het Security Team analyseert de gegevens.
- Vervolgens stuurt het Security Team het conceptrapport ter verdere bespreking aan de ISO/ Coördinator Privacy.
- De ISO / Coördinator Privacy plant, voordat de slotbijeenkomst plaatsvindt, een overleg met de leden van het Security Team ter voorbespreking van het conceptrapport.
- Het Security Team legt het conceptrapport ter correctie op feitelijke onjuistheden voor aan de interne en externe geïnterviewde.
- Het Security Team stelt vervolgens het rapport vast.

2.8 Beoordeling of datalek gemeld dient te worden aan betrokkene(n)

- Indien een datalek is gemeld aan de AP dient tevens vast gesteld te worden of het datalek ook moeten worden gemeld aan degenen om wiens gegevens het gaat.
- Dit ter beoordeling van en advisering door het Security Team.
  De beoordeling of er sprake is van een incident dat gemeld moet worden aan de betrokkenen kan tot stand komen met behulp van de schema's te vinden in de beleidsregels "Meldplicht datalekken in de Wet bescherming persoonsgegevens" van de AP
  Bij de beoordeling speelt onder meer een rol:
  - Indien CompLions passende technische beschermingsmaatregelen heeft genomen, waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens, dan kan de melding aan de betrokkene(n) achterwege blijven (artikel 34, lid 3, sub a, AVG). Bij twijfel hierover dient het datalek gemeld te worden aan de betrokkene(n).
  - Het datalek moet aan de betrokkene(n) worden gemeld, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (artikel 34, lid 1, AVG).
    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 bijvoorbeeld gedacht worden 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.
  - De melding aan de betrokkene(n) mag achterwege blijven, als daarvoor zwaarwegende redenen aanwezig zijn (artikel 23, AVG). Daarbij geldt wel dat de melding aan de betrokkene alleen achterwege mag blijven als dit *noodzakelijk* is met het oog op de belangen die worden genoemd in dit artikel. Op grond van artikel 23, lid 1, sub i, AVG mag van de melding aan de betrokkene worden afgezien voor zover dit noodzakelijk is in het belang van de bescherming van de betrokkene.

2.9 Slotbijeenkomst - verbeterplan

Security Team en MT plant een slotbijeenkomst ter bespreking van het rapport.
• Voor de slotbijeenkomst worden uitgenodigd het Security Team en

- Security Team bespreekt tijdens de slotbijeenkomst de bevindingen (rapport) en de voorgestelde verbetermaatregelen.
- Tijdens de bijeenkomst wordt het standpunt van Security Team t.a.v. het rapport vastgesteld en worden afspraken over verbetermaatregelen vastgelegd. Tijdens de bijeenkomst wordt vastgesteld of en hoe het datalek aan de betrokkene(n) wordt gemeld.
- Na de bijeenkomst ontvangen de genodigden het definitieve rapport inclusief besluitvorming.

2.10 Rapporteren aan de betrokkene(n)

- In opdracht van het MT stelt de [ISO of Coördinator Privacy] in samenspraak en kennisgeving aan betrokkene(n) op.
- Binnen het MT wordt bepaald wat aan de betrokkene(n) wordt gemeld.
- De melding bevat in ieder geval de aard van de inbreuk, contactgegevens van [naam organisatie] informatiepunt waar de betrokkene(n) meer informatie over de inbreuk kan krijgen, en de maatregelen die [naam organisatie] de betrokkene(n) aanbeveelt om te nemen om de negatieve gevolgen van de in- breuk te beperken.
- De betrokkene(n) worden individueel geïnformeerd.
- Het datalek moet onverwijld gemeld worden aan de betrokkene(n). Dit houdt in dat [naam organisatie], na het ontdekken van het datalek, enige tijd mag nemen voor nader onderzoek zodat [naam organisatie] de betrokkene op een behoorlijke en zorgvuldige manier kan informeren. Wel dient hierbij rekening gehouden te worden dat de betrokkene(n) naar aanleiding van de melding mogelijk maatregelen moet(en) nemen om zich te beschermen tegen de ge- volgen van het datalek. Hoe eerder [naam organisatie] de betrokkene(n) daarover informeert, hoe eerder deze in actie kan komen.
- In de melding aan de AP is al aangegeven of [naam organisatie] het datalek al aan de betrokkenen heeft gemeld en, zo niet, wanneer [naam organisatie] dat gaat doen. De termijn die [naam organisatie] in de melding aan het AP aangeeft, moet [naam organisatie] ook nakomen. Mocht deze termijn bij na- der inzien niet haalbaar blijken te zijn, dan laat [naam organisatie] dit aan de AP weten door middel van een aanpassing van de melding

2.11 Implementeren verbetermaatregelen

- De manager in wiens domein de verbetermaatregelen liggen is verantwoordelijk dat de vastgestelde verbetermaatregelen worden geïmplementeerd, ziet toe op de communicatie rondom en de uitvoering van de verbetermaatregelen, zorgt dat de genomen maatregelen worden geëvalueerd op bruikbaarheid en procesverbetering, en rapporteert over de voortgang aan [bestuur van de organisatie].
- Indien bij een bewerker verbetermaatregelen nodig zijn, is de manager die opdrachtgever is van deze bewerker daartoe verantwoordelijk.
- Het MT bewaakt de voortgang, onder eindverantwoordelijkheid van het Security Team.

2.12 Sluiten melding en vastlegging

- De ISO/ Coördinator Privacy informeert het MT op het moment dat het datalek definitief afgehandeld is en de melding is gesloten.
- De leden van de Datalekken Commissie vernietigen de nog in bezit zijnde documentatie.
- Het datalek dossier wordt digitaal bij ISO/ Coördinator Privacy het secretariaat gearchiveerd voor de duur van minimaal 1 jaar. Er kunnen redenen zijn om gedurende langere tijd te archiveren.