

Protocol Meldplicht Datalekken

*Procedure rondom (mogelijke) datalekken bij
Octras Raadschap BV*

Datum: 6 april 2018

Wilhelm de Haas

Jordan Hidalgo

Inhoud

1. Doel	3
2. Definities.....	4
3. Toepassingsgebied	5
4. Werkwijze	5
4.1. Identificeren van een datalek.....	7
4.2. Beoordeling aard/ernst incident; datalek ja/nee.....	7
4.3. Melden aan de Autoriteit Persoonsgegevens	8
4.4. Instellen Datalekken Commissie.....	8
4.5. Startbijeenkomst Datalekken Commissie.....	9
4.6. Verrichten datalek onderzoek.....	9
4.7. Beoordeling of datalek gemeld dient te worden aan betrokkene(n).....	9
4.8. Slotbijeenkomst in geval van een datalek: bespreking rapport en vaststellen verbetermaatregelen	10
4.9. Rapporteren aan de betrokkene(n).....	10
4.10. Implementeren verbetermaatregelen	11
4.11. Sluiten melding en vastlegging.....	11
Bronnen.....	11

1. Doel

Met ingang van 1 januari 2016 is de Wet bescherming persoonsgegevens (Wbp) gewijzigd. Sindsdien geldt een meldplicht voor datalekken. Deze meldplicht 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. De bedrijven, overheden en andere organisaties tot wie de meldplicht datalekken zich richt, moeten zelf een beredeneerde afweging maken of een concreet datalek dat hen ter kennis komt onder het bereik van de wettelijke meldplicht valt. Deze procedure beschrijft hoe te handelen binnen Octras Raadschap B.V. (hierna te noemen: OCTRAS), indien er sprake is van een datalek of wanneer een datalek vermoed wordt. Deze procedure is mede gebaseerd op de beleidsregels van de AP inzake de meldplicht datalekken in de Wet bescherming persoonsgegevens.

Per gemeld datalek behoudt de directie de vrijheid te beoordelen of de procedure gevolgd kan worden, dan wel afwijking van deze procedure gerechtvaardigd is.

Het doel van deze procedure is vast te leggen, welke stappen genomen moeten worden door OCTRAS bij het vermoeden van of kennis nemen van een incident dat (mogelijk) aangemerkt kan worden als een datalek.

Het volgende resultaat wordt hiermee nagestreefd:

- het steeds volgen van een eenduidige procedure;
- het zorgvuldig waarborgen van de belangen van OCTRAS, het individu dan wel een ander bedrijf dat betrokken is bij het incident, zijnde (mogelijk) datalek;
- het op zorgvuldige en systematische wijze analyseren van een incident, zijnde mogelijk datalek, zodat aanwezige risicomomenten in het proces zichtbaar worden. Centraal staat
- hierbij het vaststellen van de onvolkomenheden in de (toepassing van) technische en organisatorische beveiligingsmaatregelen, die (mogelijk) hebben kunnen leiden tot het incident;
- het bevorderen van het nemen van passende verbetermaatregelen en het structureel borgen
- van deze verbetermaatregelen;
- het realiseren van een voldoende en eenduidige interne en op verzoek externe
- verantwoording over de afhandeling van een incident, zijnde (mogelijk) datalek.

In de procedurebeschrijving zijn de te doorlopen stappen verwoord.

2. Definities

AP

Autoriteit Persoonsgegevens, de nieuwe naam van het College Bescherming Persoonsgegevens (CBP) m.i.v. 1-1-2016.

Bestand

Elk gestructureerd geheel van persoonsgegevens (op papier als digitaal ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze), dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen (artikel 1c, Wbp).

Betrokkene

Degene op wie een persoonsgegeven betrekking heeft (artikel 1f, Wbp).

Beveiligingslek

Een inbreuk op de beveiliging (zoals bedoeld in artikel 34a, lid 1, Wbp) waarbij persoonsgegevens niet worden blootgesteld aan verlies of onrechtmatige verwerking; er is dan geen sprake van een datalek.

Bewerker

Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen (artikel 1e, Wbp)

Datalek

Een inbreuk op de beveiliging (zoals bedoeld in artikel 34a, lid 1, Wbp) waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking; dus blootgesteld aan datgene waartegen beveiligingsmaatregelen (artikel 13, Wbp) bescherming moesten bieden.

Datalekken Commissie

Een door de Security Officer tijdelijk ingestelde onderzoekscommissie, die zorgdraagt voor een onderzoek en over de uitkomsten rapporteert aan de directie van OCTRAS.

Derden

De bij het incident betrokken externe partij, anders dan betrokkene.

Genodigden

Interne betrokkenen die uitgenodigd zijn bij de bespreking(en) van het incident bij de directie van OCTRAS.

FG

Functionaris Gegevensbescherming (artikel 1-l, Wbp). Is als aparte rol niet aanwezig bij OCTRAS maar behoort tot de taak van de Security Officer.

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. Is bij OCTRAS de Security Officer.

Persoonsgegevens

Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon Wbp (artikel 1a, Wbp).

Wbp

Wet bescherming persoonsgegevens.

Verantwoordelijke

De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 1d, Wbp).

Verwerking van persoonsgegevens

Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 1b, Wbp).

Manager Informatieveiligheid

De manager, die vanuit de portefeuille Informatieveiligheid belast is met de interne coördinatie van de procedure Meldplicht Datalekken. Is bij OCTRAS belegd bij de Security Officer welke naam als zodanig wordt gebruikt in deze procedure.

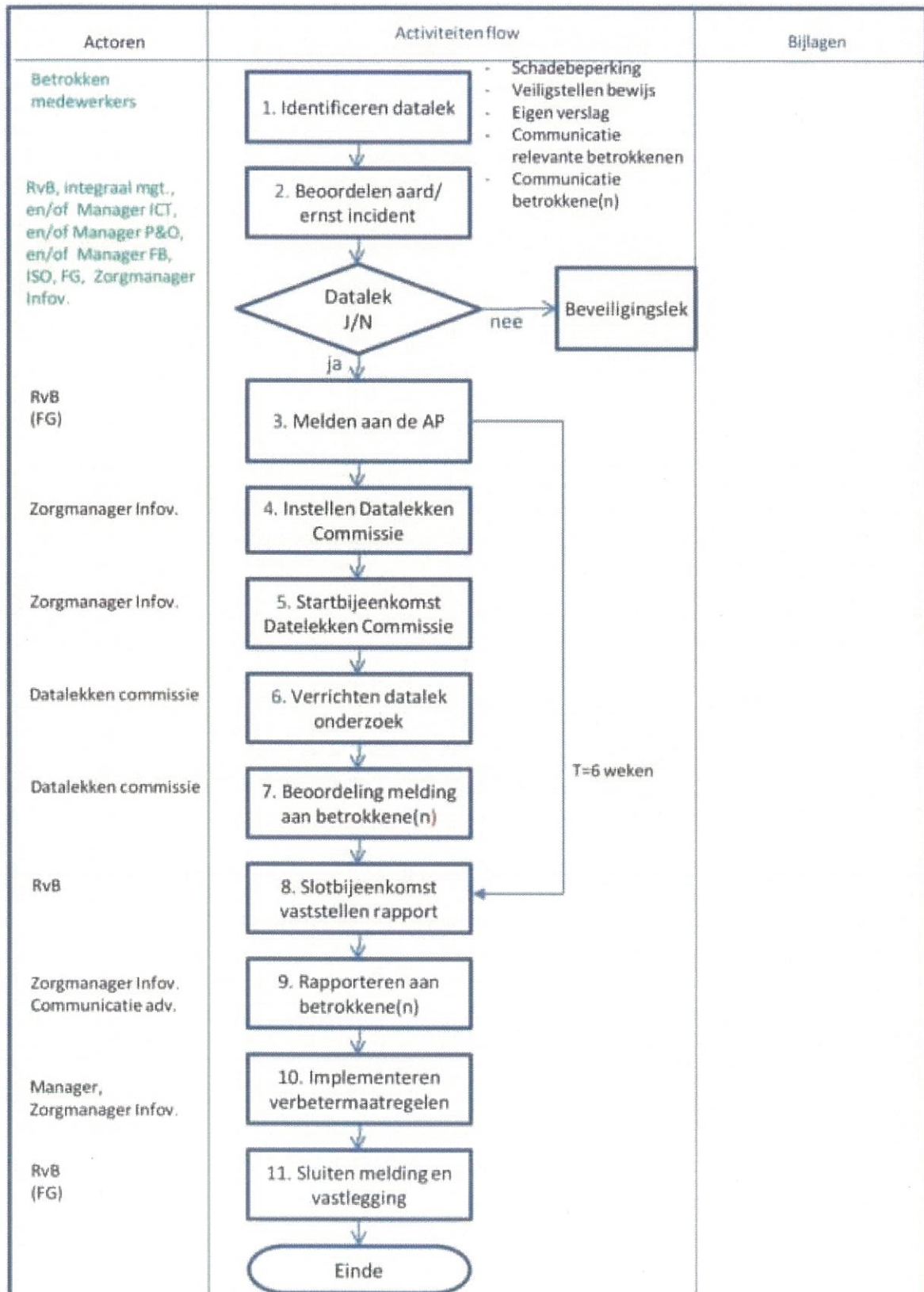
3. Toepassingsgebied

Deze procedure wordt gehanteerd bij het melden en afhandelen van (mogelijke) datalekken bij OCTRAS, dan wel van (mogelijke) datalekken die buiten OCTRAS hebben plaatsgevonden, doch waarvoor OCTRAS als Verantwoordelijke wel de eindverantwoordelijkheid draagt (bv. bij de IT beheerder of ons EPD-systeem).

4. Werkwijze

Ten behoeve van het totaal overzicht is een processchema opgesteld. Vervolgens wordt specifieke informatie per processtap over de te verrichten activiteiten en bijbehorende verantwoordelijkheden en bevoegdheden uitgewerkt.

Noot: De genoemde functiebenamingen zijn generiek gehouden en kunnen afwijken van de binnen OCTRAS gehanteerde functiebenamingen.



4.1. Identificeren van een datalek

De medewerker die een (mogelijk) datalek constateert, meldt dit incident per omgaande bij het management, en deze meldt het incident per omgaande aan de Security Officer.

Een medewerker is te allen tijde bevoegd zelfstandig een melding te doen aan de Security Officer. De procedure Meldplicht Datalekken wordt dan gestart.

Noot: Ook (de medewerker van) derden kunnen een datalek constateren en melden aan diens opdrachtgever OCTRAS.

4.2. Beoordeling aard/ernst incident; datalek ja/nee

- De Security Officer draagt zo spoedig mogelijk zorg voor volledige en juiste informatie zoals opgenomen in Bijlage 1 'Formulier t.b.v. melding datalek'.
- Op basis van de verkregen informatie en bij vermoeden van een datalek wordt in overleg met het management van OCTRAS 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 meldingsplichtig is voor de politie in geval van vermoeden van een strafbaar feit (zie ook hierna onder 4.3).
- 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 "Meldplicht datalekken in de Wet bescherming persoonsgegevens" van de AP (zie Bijlage 2).
- Bij de beoordeling spelen o.a. een rol:
 - is er sprake van verlies van persoonsgegevens; dit houdt in dat OCTRAS 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 gelect;
 - bijzondere persoonsgegevens conform artikel 16 Wbp;
 - 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 optreden;
 - 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.

4.3. Melden aan de Autoriteit Persoonsgegevens

- Het management van OCTRAS 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. Dit met inachtneming van richtlijnen van de AP terzake. De Security Officer draagt, zorg voor volledige en juiste informatie zoals opgenomen in Bijlage 1 'Formulier t.b.v. melding datalek' op grond waarvan feitelijk gemeld zal worden. Het management van OCTRAS 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.
- Het management van OCTRAS is eindverantwoordelijk, de Security Officer 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 management draagt ervoor zorg dat de bij het incident betrokken medewerkers worden geïnformeerd. Het 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 het management van OCTRAS verstrekt ten behoeve van de leden van de Datalekken Commissie (zie 4.4) 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.

4.4. Instellen Datalekken Commissie

- De Security Officer benoemt een Datalekken Commissie bestaande uit ten minste drie leden om verdergaand onderzoek te verrichten. Betrokkenen bij het incident, dan wel de afdeling waar het incident heeft plaatsgevonden, kunnen niet participeren in een commissie. Bij de samenstelling van de Datalekken Commissie wordt rekening gehouden met de aard van het incident. De Security Officer faciliteert waar nodig de Datalekken Commissie.
- De Security Officer formuleert een opdracht voor de Datalekken Commissie en informeert hierover schriftelijk de Datalekken Commissie, voorzien van de termijn waarbinnen het management van OCTRAS de rapportage wil ontvangen en voegt toe Bijlage 3 'Informatie voor leden van de Datalekken Commissie', Bijlage 4 'Informatie voor te interviewen interne personen door de Datalekken Commissie' en Bijlage 5 'Informatie voor te interviewen (medewerkers van) derden door de Datalekken Commissie'.

4.5. Startbijeenkomst Datalekken Commissie

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

4.6. Verrichten datalek onderzoek

- De Datalekken Commissie stelt binnen de gestelde termijn en opdrachtverlening een (systematisch) (intern) onderzoek in naar de feitelijke toedracht van het (mogelijke) datalek.
- De Datalekken Commissie onderzoekt verder of en zo ja hoe dergelijke incidenten in de toekomst kunnen worden voorkomen (het vermijdbaarheidsaspect).
- De bevoegdheden van de Datalekken Commissie 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
- De Datalekken Commissie heeft binnen 4 weken na de startbijeenkomst het onderzoek afgerond.
- De Datalekken Commissie kan in overleg met, of op instigatie van het management van OCTRAS besluiten om externe deskundigen te betrekken bij het onderzoek.
- De Datalekken Commissie analyseert alle gegevens conform Bijlage 6 'Format rapportage Datalekken Commissie' en Bijlage 2 Beleidsregels "Meldplicht datalekken in de Wet bescherming persoonsgegevens" van de AP.
- Vervolgens stuurt de Datalekken Commissie het conceptrapport ter verdere bespreking aan de Security Officer.
- De Security Officer plant, voordat de slotbijeenkomst plaatsvindt, een overleg met de leden van de Datalekken Commissie ter voorbespreking van het conceptrapport.
- De Datalekken Commissie legt het conceptrapport ter correctie op feitelijke onjuistheden voor aan de interne en externe geïnterviewden.
- De Datalekken Commissie stelt vervolgens het rapport vast.

4.7. 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 de Datalekken Commissie. 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 (zie Bijlage 2).
- Bij de beoordeling speelt onder meer een rol:
 - Indien OCTRAS passende technische beschermingsmaatregelen heeft genomen, waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor een ieder die geen recht heeft op kennisname van de gegevens, dan kan de melding aan de betrokkene(n) achterwege blijven (artikel 34a, lid 6, Wbp). 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 34a, lid 2, Wbp). 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 43 Wbp). 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 43, onder e, Wbp mag van de melding aan de betrokkene worden afgezien voor zover dit noodzakelijk is in het belang van de bescherming van de betrokkene.

4.8. Slotbijeenkomst in geval van een datalek: bespreking rapport en vaststellen verbetermaatregelen

- Het management van OCTRAS plant een slotbijeenkomst ter bespreking van het rapport van de Datalekken Commissie.
- Voor de slotbijeenkomst worden uitgenodigd het management van OCTRAS, de leden van de Datalekken Commissie en de Security Officer. De genodigden ontvangen van de Security Officer een afschrift van het conceptrapport.
- De directie van OCTRAS bespreekt tijdens de slotbijeenkomst het rapport en de voorgestelde SMART geformuleerde verbetermaatregelen.
- Tijdens de bijeenkomst wordt het standpunt van het management van OCTRAS t.a.v. het rapport van de Datalekken Commissie vastgesteld en worden afspraken over verbetermaatregelen vastgelegd. Tijdens de bijeenkomst wordt vast gesteld of en hoe het datalek aan de betrokkene(n) wordt gemeld.
- Na de bijeenkomst ontvangen de genodigden het definitieve rapport.

4.9. Rapporteren aan de betrokkene(n)

- In opdracht van de directie van OCTRAS stelt de Security Officer een kennisgeving aan betrokkene(n) op.
- De Security Officer bepaalt wat aan de betrokkene(n) wordt gemeld.
- De melding bevat in ieder geval de aard van de inbreuk, contactgegevens van OCTRAS, een informatiepunt waar de betrokkene(n) meer informatie over de inbreuk kan krijgen, en de maatregelen die OCTRAS de betrokkene(n) aanbeveelt om te nemen om de negatieve gevolgen van de inbreuk te beperken.
- De betrokkene(n) worden individueel geïnformeerd.
- Het datalek moet onverwijld gemeld worden aan de betrokkene(n). Dit houdt in dat OCTRAS, na het ontdekken van het datalek, enige tijd mag nemen voor nader onderzoek zodat OCTRAS 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 gevolgen van het datalek. Hoe eerder OCTRAS de betrokkene(n) daarover informeert, hoe eerder deze in actie kan komen. In de melding aan de AP is al aangegeven of OCTRAS het datalek al aan de betrokkenen heeft gemeld en, zo niet, wanneer OCTRAS dat gaat doen. De termijn die OCTRAS in de melding aan het AP aangeeft, moet OCTRAS ook nakomen. Mocht deze termijn bij nader inzien niet haalbaar blijken te zijn, dan laat OCTRAS dit aan de AP weten door middel van een aanpassing van de melding.

4.10. Implementeren verbetermaatregelen

- De manager en medewerker 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 het management van OCTRAS.
- Indien bij derden verbetermaatregelen nodig zijn, is de manager die opdrachtgever is van deze bewerker daartoe verantwoordelijk.
- De Security Officer bewaakt de voortgang, onder eindverantwoordelijkheid van het management van OCTRAS.

4.11. Sluiten melding en vastlegging

- De Security Officer informeert het management van OCTRAS, op het moment dat het datalek definitief afgehandeld is en de melding is gesloten.
- De Datalekken Commissie wordt door het management van OCTRAS ontbonden.
- De leden van de Datalekken Commissie vernietigen de nog in bezit zijnde documentatie.
- Het datalek dossier wordt digitaal op de T-schijf van OCTRAS gearchiveerd voor de duur van minimaal 1 jaar. Er kunnen redenen zijn om gedurende langere tijd te archiveren, de richtlijn zoals beschreven in Bijlage 2 "Meldplicht datalekken in de Wet bescherming persoonsgegevens; beleidsregels" zal worden gehanteerd.

Bronnen

Wet bescherming persoonsgegevens

Meldplicht datalekken in de Wet bescherming persoonsgegevens
beleidsregels.

Deze Procedure Meldplicht Datalekken is vastgesteld in de vergadering van het management van OCTRAS Raadschap BV op 6 april 2018.

Deze Procedure Meldplicht Datalekken is 6 april 2018 gepresenteerd aan de organisatie.

Handtekening Management van Octras Raadschap BV



Wilhelm de Haas
Directeur



Jordan Hidalgo
Security Officer