BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 1147

24 december 2021

Officiële uitgave van de gemeenschappelijke regeling Peelgemeenten

# Beleid informatiebeveiligingsincidenten Gemeenschappelijke regeling Peelgemeenten

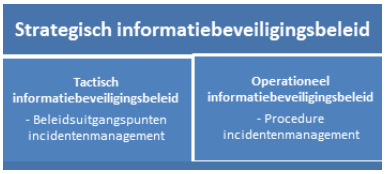
## 1. Inleiding

Het hebben van een adequaat proces incidentmanagement is belangrijk. Dit verkleint de impact van een informatiebeveiligingsincident (hierna incident), omdat adequaat gereageerd kan worden en de schade en impact hierdoor minimaal kunnen blijven. Daarnaast zorgt het ervoor dat lering wordt getrokken uit incidenten, waardoor de kans op herhaling ook wordt verkleind. Alle medewerkers zijn verantwoordelijk voor informatiebeveiliging en dienen een incident te herkennen en weten waar ze dat moeten melden.

De GR Peelgemeenten verwerkt in haar dienstverlenings- en bedrijfsvoeringprocessen persoonsgegevens van bijvoorbeeld burgers en medewerkers. Er moet adequaat worden gereageerd op incidenten die de continuïteit van de bedrijfsvoering en dienstverlening verstoren en de vertrouwelijkheid en juistheid van informatie bedreigen. Om mogelijke schade snel op te sporen en te voorkomen is het noodzakelijk dat iedere medewerker (vermoedelijke) incidenten tijdig en volgens een vastgestelde procedure meldt.

### 1.1 Leeswijzer

Dit document beschrijft het 'proces incidentenmanagement' dat van toepassing is voor de GR Peelgemeenten. Dit document start met het uitleggen van de termen informatiebeveiligingsincidenten en datalekken. Vervolgens is er beleid opgenomen waarin de beleidsuitgangspunten zijn geformuleerd en wordt er aandacht besteed aan de rollen, taken en verantwoordelijkheden. De beleidsuitgangspunten zijn ontleend aan het strategisch informatiebeveiligingsbeleid. Tot slot is er een procedure opgenomen waarin stapsgewijs wordt uitgelegd welke processtappen gemaakt moeten worden binnen het incidentenmanagement en wie de betrokkenen zijn in dit proces. Dit ziet er schematisch uit als weergeven in de volgende figuur:




### 1.2 Definities

***Wat is een informatiebeveiligingsincident?***

Een informatiebeveiligingsincident is een gebeurtenis die een inbreuk vormt op de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening. Het hoeft niet alleen te gaan om ICT-aangelegenheden, zoals het uitvoeren van beveiligingspatches en updates. Een slecht wachtwoord(beleid), het niet vergrendelen van je scherm of het klikken op verdachte mails zijn bedreigingen voor de informatievoorziening. Andere voorbeelden zijn:

- Een malware-besmetting[1];
- Een ransomware aanval;
- Een calamiteit zoals een brand in een datacentrum;
- Klikken op een phishing[2] e-mail;
- Een inbraak(poging) door een hacker;
- Toegangspas laten rondslingeren op de afdeling;

1) Malware is elke software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot computersystemen. Het woord is een samentrekking van het Engelse malicious software. Malware veronderstelt kwade opzet.
2) Phishing is een vorm van internetfraude. Het bestaat uit het oplichten van mensen door ze te lokken naar een valse website, die een kopie is van de echte website, om ze daar – nietsvermoedend – te laten inloggen met hun inlognaam en wachtwoord of hun bankgegevens.

- Verlies of diefstal van een laptop of andere (mobiele) gegevensdrager.

***Wat is een datalek?***
Als er in het geval van een incident sprake is van een inbreuk in verband met persoonsgegevens wordt er gesproken van een datalek. Elk datalek is een incident maar niet elk incident is een datalek.

De term 'datalek' komt niet voor in de wet. In plaats daarvan heeft de Algemene Verordening Gegevensbescherming (hierna AVG) het over een 'inbreuk in verband met persoonsgegevens'. Van een inbreuk in verband met persoonsgegevens is sprake in het geval van 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 toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens (artikel 4, punt 12, AVG). Er is dus sprake van een datalek als vertrouwelijke gegevens verloren kunnen zijn gegaan door een inbreuk op de beveiliging, of als niet uitgesloten is dat deze door onbevoegden zijn verwerkt.

Alleen een dreiging of tekortkoming in de beveiliging is niet voldoende. Er moeten daadwerkelijk persoonsgegevens gelekt zijn. Onder een datalek verstaat de Autoriteit Persoonsgegevens (AP) persoonsgegevens die gelekt of vernietigd zijn als gevolg van een beveiligingsincident.
Een inbreuk op de beveiliging van persoonsgegevens moet dus ruim worden genomen. Dit betreft alle incidenten waardoor de bescherming van persoonsgegevens op enig moment is doorbroken en de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking van persoonsgegevens. Het is daarbij niet van belang of de verwerkingsverantwoordelijke passende beveiligingsmaatregelen had getroffen of niet.

Voorbeelden van inbreuken in verband met persoonsgegevens (hierna datalekken) zijn:
- Een kwijtgeraakte, niet-versleutelde USB-stick met persoonsgegevens;
- Verzending van e-mail waarin de e-mailadressen van alle geadresseerden onnodig zichtbaar zijn voor alle andere geadresseerden;
- Achtergelaten kopie met persoonsgegevens in de printer;
- Een medewerker verliest een laptop met daarop niet-versleutelde persoonsgegevens

### 1.3 Scope
Alle typen (vermoedelijke) incidenten en daarmee datalekken kunnen binnen dit proces en de bijbehorende procedure worden behandeld. Het gaat om incidenten die bijvoorbeeld worden gemeld door een medewerker, stagiair of iemand die via inhuur werkzaam is. Ook binnen beschouwing vallen (vermoedelijke) incidenten die worden geconstateerd door ICT tijdens controle en monitoring werkzaamheden en (vermoedelijke) incidenten die worden ontvangen vanuit bijvoorbeeld de Informatiebeveiligingsdienst (IBD) of andere organisaties. Ook is dit proces van toepassing voor incidenten en daarmee datalekken die door een externe partij worden gemeld via bijvoorbeeld e-mail, telefoon of de Coordinated Vulnerability Disclosure (CVD)[3].

## 2. Beleidsuitgangspunten informatiebeveiligingsincidenten

Met het proces incidentmanagement geven we richting aan de wijze waarop we wensen om te gaan met alle (vermoedelijke) incidenten op het gebied van informatiebeveiliging en privacy. We onderschrijven het belang van een adequate behandeling van incidenten en de reactie daarop om daarmee de gevolgen voor de bedrijfsvoering te minimaliseren. Incidenten dienen gestructureerd te worden behandeld en er moeten procedures worden vastgesteld om de reactie op incidenten doeltreffend en ordelijk te laten plaatsvinden. De organisatie wil leren van incidenten, en daarom moeten incidenten geëvalueerd worden. Onderstaande uitgangspunten zijn van toepassing op iedereen die werkzaam is voor de organisatie, ongeacht de contract-vorm.

Iedere medewerker, zowel vast als tijdelijk, intern of extern is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken. De volgende

3) Regelmatig worden nieuwe kwetsbaarheden in producten of diensten gevonden door onderzoekers of organisaties. De vinder kan door een Coordinated Vulnerability Disclosure de eigenaren van die producten of diensten op de hoogte stellen. Eigenaren kunnen dan maatregelen nemen voordat de kwetsbaarheden actief misbruikt zullen worden door derden.

uitgangspunten zijn vastgesteld en ontleend aan het strategisch informatiebeveiligingsbeleid en de Baseline Informatiebeveiliging Overheid (BIO):

1. De proceseigenaar is verantwoordelijk voor het oplossen van incidenten.
2. In het digitaal meldloket worden de incidenten gemeld. In een bijbehorende meldprocedure staan de taken en verantwoordelijkheden van het meldloket beschreven.
3. (Vermoedelijke) incidenten die verband houden met processen en ondersteunende informatiesystemen worden zodanig kenbaar gemaakt dat tijdig en adequaat corrigerende maatregelen genomen kunnen worden. Dit omvat ook het regelmatig beoordelen van loggegevens van informatiesystemen.
4. Alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen en diensten, moeten alle (vermoedelijke) incidenten melden volgens de procedure en binnen 24 uur vanaf ontdekking. Indien het incident er om vraagt wordt de leidinggevende en/of de CISO direct benaderd.
5. (Vermoedelijke) incidenten moeten vastgelegd en beheerd worden volgens de hiervoor vastgestelde procedure. Deze procedure moet bekend zijn bij alle werknemers. In deze procedure moeten de verantwoordelijkheden belegd worden.
6. Indien vereist worden datalekken binnen 72 uur vanaf ontdekking gemeld bij de Autoriteit Persoonsgegevens. Incidenten waarbij persoonsgegevens betrokken zijn worden altijd intern geregistreerd.
7. De voortgang en de effectiviteit van de implementatie van de verbetermaatregelen moet worden gemonitord.
8. Incidenten moeten geëvalueerd worden zodat de procedure kan worden bijgesteld en beheersmaatregelen kunnen worden verbeterd.
9. Incidenten kennen soms een vervolgprocedure, daarom moet zoveel als mogelijk bewijsmateriaal verzameld worden.
10. Het proces incidentenmanagement en de bijbehorende procedure moeten jaarlijks worden getoetst op effectiviteit.
11. Over de (opvolging van) incidenten wordt periodiek gerapporteerd aan het management en de portefeuillehouder.

In bijlage 4 staan alle controls en maatregelen vanuit de BIO die betrekking hebben op incidenten. Bij het uitvoeren van het incidentenmanagement staan deze controls en maatregelen centraal.

## 3. Rollen, taken en verantwoordelijkheden

Hieronder volgt een toelichting op de rollen, taken en verantwoordelijkheden binnen het proces incidentenmanagement.

- **De medewerker** (in elke laag van de organisatie) die direct of indirect kennis draagt van een (vermoedelijk) incident of datalek meldt dit direct, doch binnen 24 uur vanaf ontdekking, via het daarvoor aangewezen digitaal formulier. De medewerker vult hiervoor het digitale formulier in, bijvoorbeeld via Topdesk, en zorgt voor een volledige omschrijving van het incident, conform een checklist.
- **De manager** is verantwoordelijk voor een gepaste beveiliging (op basis van risicomanagement en naar de stand van de techniek) van de onder zijn/haar verantwoordelijkheid uitgevoerde processen en de daarbij gebruikte processen en informatiesystemen en verleent alle medewerking bij de analyse van het incident en de implementatie van de verbetermaatregelen. De verantwoordelijk manager verleent alle medewerking aan het onderzoek en is verantwoordelijk voor het ondernemen van preventieve en repressieve beveiligingsacties. Hiernaast is de manager of een ondergeschikte aan zet als het gaat om de risicoanalyse van het incident en het formuleren en eventueel implementeren van de verbetermaatregelen of anders de organisatie hiervan. Hierbij is de manager eindverantwoordelijke en hebben de CISO en PO een adviserende rol. De manager beoordeelt, na advies van de CISO, PO en FG, of een incident een grote impact kan hebben en/of een incident bestuurlijk/politiek gevoelig ligt. Hiernaast neemt de manager de beslissing of er gemeld wordt aan de AP en betrokkene(n) als er geen sprake is van grote incidenten of bestuurlijk/politieke gevoelige incidenten. Als de manager niet aanwezig is neemt de vervangend manager deze taak over. Als een incident buiten de organisatie is ontstaan, blijft de manager die voor de uitvoering van zijn/haar proces een externe partij heeft ingeschakeld zelf verantwoordelijk voor de behandeling van het incident.
- **De Chief Information Security Officer (CISO) en Privacy Officer (PO)** vormen samen de beveiligingsfunctionarissen. Zij onderzoeken het incident en de PO beoordeelt of er sprake is van een

inbreuk op persoonsgegevens. De rol beveiligingsfunctionaris is geen formele rol maar een functionele. De CISO en PO zijn verantwoordelijk voor registratie van het informatiebeveiligingsincident (CISO) en datalek (PO) en het informeren van de FG over een incident. Bij afwezigheid van de CISO en/of PO is de FG achtervang.
- **De CISO** is verantwoordelijk voor het jaarlijks actualiseren van het proces en de procedure.
- **De Functionaris Gegevensbescherming (FG)** onderzoekt of het incident ernstige nadelige gevolgen heeft (of kan hebben) voor de persoonlijke levenssfeer van de betrokkene(n) en adviseert management en/of de **directie** over het doen van de meldingen aan de AP en aan de betrokkenen.
- **ICT** biedt ondersteuning bij het onderzoeken van incidenten en indien nodig ook het implementeren van verbetermaatregelen.
- **De directie** neemt beslissingen bij grote incidenten. Een beslissing kan bijvoorbeeld zijn het uitzetten van kritische informatiesystemen vanwege een aanval. **De directie** moet als een incident bestuurlijk/politiek gevoelig ligt keuzes en beslissingen nemen.
- **Team communicatie** informeert indien van toepassing in samenwerking met de CISO en PO de extern betrokkene(n) over het incident.
- **Juridische Zaken** heeft een rol bij de woordvoering over incidenten omdat de aard en inhoud van de communicatie gevolgen kan hebben voor aansprakelijkheid.

Naast bovengenoemde rollen moet er ook een **Incident Management Team (IMT)** worden opgericht. Het IMT moet worden ingesteld om voorbereid te zijn en om snel en adequaat te kunnen reageren op een beveiligingsincident dat bijvoorbeeld buiten de scope van de servicedesk valt. Het gaat dan om beveiligingsincidenten met een hoge classificatie (zie bijlage 1) die directe mobilisering van het IMT vereist. Dit team bestaat uit een vaste kern medewerkers van de organisatie die afhankelijk van het incident gebruik maakt van andere noodzakelijke competenties/disciplines waaronder eventuele externe inhuur. Het IMT moet 24/7 bereikbaar zijn omdat een incident met een hoge classificatie zich niet houdt aan werktijden. Voor de vaste kern van het IMT moet tijdig tijdelijke vervanging worden aangewezen. Er moet ook een bereikbaarheidslijst worden gemaakt van alle teamleden van de IMT. Deze bereikbaarheidslijst moet ook offline te raadplegen zijn. Het IMT moet geïntegreerd worden met het nog te ontwikkelen business continuïteitsplan.

## 4. Procedure melden van informatiebeveiligingsincidenten en datalekken

De procedure legt stapsgewijs uit welke acties ondernomen moeten worden om incidenten tijdig te detecteren zodat passende en risico verkleinende maatregelen getroffen kunnen worden. In deze procedure komen ook de rollen zoals hierboven beschreven aan bod. Deze procedure is gedetailleerd beschreven ten behoeve van uniformiteit en om te voorkomen dat er discussie ontstaat over wie, wat en wanneer iets moet doen. Een algemeen beschrijvende procedure is niet adequaat genoeg. Bijlage 2 bevat de schematische weergave van de procedure in de vorm van een stappenplan. Een tekstuele toelichting op deze schematische weergave van de procedure volgt hier beneden.

### 4.1. Melding van een informatiebeveiligingsincident

Elke laag in de organisatie dient alert te zijn op bedreigingen met betrekking tot informatiebeveiliging en privacy en is verplicht om alle (vermoedelijke) incidenten die hij/zij ontdekt te melden via de daarvoor aangewezen meldmethode. Deze incidenten worden beheerd door de beveiligingsfunctionarissen. De CISO en Privacy Officer vervullen de rol van de beveiligingsfunctionaris binnen deze procedure.

Niet in alle gevallen zal de beveiligingsfunctionaris als primaire behandelaar optreden, immers het technisch verhelpen van een incident gebeurt niet altijd door de beveiligingsfunctionaris, maar door een technisch specialist (medewerker ICT) of door een medewerker die de eigen processen beter kent dan de beveiligingsfunctionaris. Het hiervoor aangewezen systeem ondersteunt in deze wisselwerking tussen de verschillende rollen in de informatiebeveiligingsorganisatie. De beveiligingsfunctionarissen kunnen op twee manieren worden ingeschakeld door een melder:

- De beveiligingsfunctionarissen moeten altijd op de hoogte worden gebracht dat een incident heeft plaatsgevonden of dat er sprake was van een vermoedelijk incident. Registratie van deze (vermoedelijke) incidenten gebeurt in het hiervoor aangewezen systeem.
- De beveiligingsfunctionarissen moeten een incident met hoge prioriteit direct oplossen, dan wel coördineren of over adviseren. In dit geval neemt de melder telefonisch contact op met de beveiligingsfunctionarissen (of vervanger). Hierna moet het incident ook nog worden geregistreerd door de melder in hiervoor aangewezen systeem.

## 4.2 Identificatie

De beveiligingsfunctionaris en/of manager of een ondergeschikte zal veelal ICT betrekken bij het controleren of er een kwetsbaarheid aanwezig is en/of een incident daadwerkelijk heeft plaatsgevonden. Identificatie kan ook het gevolg zijn van proactieve detectie van incidenten door de ICT-beveiliging of systeembeheer of doordat bij de controle van de logging iets naar boven komt. Indien wordt vastgesteld dat het inderdaad een kwetsbaarheid of incident is, dan moeten de betreffende belanghebbenden gewaarschuwd worden. Indien het om incidenten gaat zonder technische component zullen de beveiligingsfunctionarissen, afhankelijk van de casus een onderzoeksmethode gebruiken om het incident te identificeren.

Het is bij de identificatie belangrijk om in beeld te brengen wie of welke teams binnen de organisatie betrokken zijn. Een ander belangrijk onderdeel binnen deze fase is het beoordelen of er een verwerker of verwerkersverantwoordelijke betrokken is bij het incident. Zo ja dan dient deze bij het proces betrokken te worden. Dit zijn taken van de beveiligingsfunctionaris(se)n. Hiernaast moet er een onderzoek plaatsvinden of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden. Dit is een taak van de privacy officer.

## 4.3 Schade indamming

Nadat het incident is opgemerkt en gemeld gaan de manager of een ondergeschikte en de beveiligingsfunctionaris ermee aan de slag. Afhankelijk van de casus moet ICT gaan handelen om de schade van het incident te beperken. ICT stelt waar nodig een team aan om het incident te verhelpen en heeft hiervoor soms ook de CISO en PO nodig. Dit team is belast met het beperken van verdere schade als gevolg van het incident. Bij grote informatiebeveiligingsincidenten heeft de directie ook een belangrijke rol. De IBD kan worden ingeschakeld voor advies. De ondernomen acties worden vastgelegd zodat aantoonbaar is hoe er is gehandeld.

*1. Vaststellen impact incident*

In deze fase moet het incident en de gevolgen daarvan worden onderzocht. Hierbij moet bijvoorbeeld worden onderzocht wat de aard is van de gegevens die gelekt zijn. Bijv. gezondheidsgegevens, wachtwoorden, gegevens over financiële situatie of die kunnen leiden tot stigmatisering/misbruik. Hierna moet worden onderzocht hoe groot de omvang van de gelekte gegevens is en wat de impact van het incident kan zijn op de betrokken persoon of de organisatie. Stel vast wat de nadelige gevolgen kunnen zijn. De beveiligingsfunctionarissen coördineren het onderzoek.

Vervolgens is het belangrijk om te bepalen wat de urgentie is (snelheid waarmee het incident moet worden opgelost) en te bepalen hoe groot de impact (het effect) is dat het incident en bijbehorende risico met zich meebrengen. Bijlage 1 beschrijft hoe deze incidenten en bijbehorende risico's op basis van urgentie en impact kunnen worden geclassificeerd. Op basis van deze classificatie wordt de reactietijd en oplossingstijd bepaald.

## 4.4 Herstel

Er moeten maatregelen worden getroffen om de oorzaak van het incident te blokkeren of te verwijderen en er moet worden gekeken hoe de impact door verdere blootstelling van de gevoelige gegevens kan worden voorkomen. Eventueel moeten de bedrijfsprocessen worden herstart als deze gestopt waren als gevolg van het incident. Risico's die verband houden met het incident moeten worden verkleind. Als er diensten zijn uitbesteed is het noodzakelijk om goede afspraken te maken met de leverancier om incidenten goed op te pakken.

Nadat een incident zich heeft voorgedaan en nadat de risicoanalyse heeft plaatsgevonden kan een manager ervoor kiezen om het risico te accepteren. Dit moet schriftelijk worden vastgelegd. Als de manager het risico niet accepteert moeten er maatregelen worden geformuleerd en worden geïmplementeerd. Dit is afhankelijk van het incident een samenwerking tussen de beveiligingsfunctionarissen, ICT, leverancier, de manager en eventueel een ondergeschikte van de manager. Als een manager niet betrokken is bij het formuleren van de maatregel wordt deze gevraagd of hij of zij akkoord gaat met de maatregel. Na akkoord wordt er overgegaan tot implementatie van deze maatregel.

Nadat de maatregel is geïmplementeerd wordt er beoordeeld of de maatregel adequaat genoeg was. Indien dit niet het geval is, is er sprake van een restrisico. Ook hier kan de manager ervoor kiezen om dit restrisico te accepteren. Ook dit moet worden vastgelegd. Als de manager het restrisico niet accepteert moeten er aanvullende of andere maatregelen worden geformuleerd en worden geïmplementeerd. Dit

is afhankelijk van het incident een samenwerking tussen de beveiligingsfunctionarissen, ICT, leverancier, de manager en eventueel een ondergeschikte van de manager. Als een manager niet betrokken is bij het formuleren van de maatregel wordt deze gevraagd of hij of zij akkoord gaat met de maatregel. Na akkoord wordt er overgegaan tot implementatie van deze maatregel.

De stappen en de te formuleren maatregelen in deze fase zijn afhankelijk van de reeds genomen maatregelen uit de fase schade indamming.

### 4.5 Kennisgeving

Nadat is bepaald welke gegevens mogelijk zijn blootgesteld door het incident, moet worden bepaald of dit incident gemeld moet worden bij de toezichthoudende autoriteit (AP) en of de getroffenen ('betrokkenen") in kennis moeten worden gesteld van het feit dat hun gegevens blootgesteld zijn. Indien noodzakelijk moeten ook andere overheidsinstanties, zoals de IBD en/of de politie worden geïnformeerd. Het is ook raadzaam om bij de woordvoering over een incident een jurist te betrekken, de aard en inhoud van de communicatie kan gevolgen hebben voor aansprakelijkheid.

***Melding bij de AP***

Melding aan de AP kan alleen achterwege blijven als het onwaarschijnlijk is dat het datalek leidt tot een risico voor de rechten en vrijheden van de betrokkenen. Of hiervan sprake is hangt mede af van de aard en omvang van de gelekte persoonsgegevens. De PO en FG beoordelen of sprake is van een meldingsplichtig datalek en adviseren de verantwoordelijke manager. Besluit de manager om over te gaan tot melding, dan zorgt de FG daar voor. De PO en FG kunnen eventueel escaleren naar de directie als de manager het advies niet opvolgt.

***Betrokkene(n) informeren***

Indien het datalek waarschijnlijk een hoog risico voor de rechten en vrijheden van de betrokkenen veroorzaakt, moet het datalek gemeld worden bij de betrokkene(n). De verwerkingsverantwoordelijke moet daar een inschatting voor maken. Het risico moet bijvoorbeeld worden beoordeeld aan de hand van de aard en de hoeveelheid van de gelekte gegevens. Ongunstige gevolgen zijn er al snel als een onbevoegde kennis heeft genomen van de zogenaamde bijzondere gegevens. Dit betreft gegevens over bijvoorbeeld gezondheid, seksuele leven of godsdienst. Strafrechtelijke gegevens vallen niet onder het begrip "bijzondere gegevens". Dit is een aparte categorie. Deze gegevens zijn privacygevoeliger dan gegevens als naam en geboortedatum en kunnen bij verlies of misbruik ernstige gevolgen hebben voor de betrokkene. De PO en FG beoordelen of, wanneer en hoe de betrokkene dient te worden geïnformeerd. De manager van het team waarbinnen het datalek heeft plaatsgevonden zorgt ervoor dat de betrokkene op passende wijze wordt geïnformeerd en laat zich hierbij adviseren door de PO, de FG, communicatie en indien nodig een jurist. Deze verantwoordelijkheid van de manager geldt ook voor incidenten die ontstaan bij uitbestede diensten en processen.

### 4.6 Registratie, rapportage en evaluatie

Als verwerkingsverantwoordelijke is het wettelijk verplicht om een register op te stellen waarin inbreuken in verband met persoonsgegevens (datalekken) worden geregistreerd. Ook de datalekken die niet gemeld zijn bij de AP of de betrokkenen moeten hierin worden vastgelegd. Voor informatiebeveiligingsincidenten moet er eveneens een registratie worden bijgehouden. Dit gebeurt in het hiervoor aangewezen systeem.

Lessen uit het incident moeten worden geïdentificeerd en besproken worden met de belanghebbenden. Er moet ook, indien relevant, gerapporteerd worden over het incident en de genomen maatregelen. Incidenten, inclusief verbetermaatregelen, moeten goed worden geregistreerd zodat het proces incidentmanagement wordt verbeterd. Belangrijke incidenten moeten daarnaast ook gemeld worden aan de IBD en daarvoor moet een speciale interne contactpersoon binnen de organisatie aangewezen worden. Binnen een organisatie is dit de Vertrouwelijk Contactpersoon Informatiebeveiliging (VCIB). Incidenten melden bij de IBD geeft andere organisaties ook de mogelijkheid om de kans op en de eventuele impact van het incident te verkleinen. Mochten meerdere organisaties last hebben van hetzelfde incident dan kan de IBD eventueel optreden als contactpersoon richting de leverancier.

Tot slot is het belangrijk om de melder een terugkoppeling te geven over de uitkomsten van het incident. Zo wordt het signaal afgegeven dat melden loont.

## 5. Interne controle en evaluatie van de procedure

***De interne controle van de incidenten***
Elk kwartaal analyseert de CISO de incidenten en stelt op basis hiervan een verbeterplan op dat onderdeel is van het regulier informatiebeveiligingsplan. Op deze manier wordt er ook gegroeid van incidenten-management naar 'problem management'. Op het eerste gezicht losstaande incidenten kunnen namelijk voor grotere problemen zorgen. De PO analyseert en evalueert ook elke 3 maanden de datalekken en neemt n.a.v. hiervan verbetermaatregelen.

***De evaluatie van het proces***
Minimaal jaarlijks beoordeelt de CISO of het proces en de bijbehorende procedure en de uitvoering nog met elkaar in overeenstemming zijn. Indien deze niet met elkaar overeenkomen wordt beoordeeld of de procedure geactualiseerd moet worden of dat medewerkers geïnstrueerd moeten worden op een juiste toepassing van de procedure.

## 6. Aandachtspunten

***Voorbereiding***
In de voorbereiding is het ook belangrijk om iedereen die betrokken zal zijn bij het proces te informeren. Er is een overzicht met namen en functies en telefoonlijsten die ook offline beschikbaar is. Er is vervanging voor communicatie wanneer bijvoorbeeld de totale ICT-infrastructuur uitgevallen is of mobiele netwerken overbelast zijn vanwege grote drukte (bij calamiteiten).

***Externe relaties***
Incidenten staan vaak niet op zichzelf en kunnen een uitwerking hebben naar andere ketenpartners. Sommige incidenten doen zich niet bij één organisatie voor maar bij meerdere. Een incident moet behalve intern opgelost soms ook extern geëscaleerd worden zodat anderen gewaarschuwd kunnen worden en daarmee de impact van het incident zo klein als mogelijk gehouden kan worden. Extern escaleren (door de CISO) gebeurt naar de deelnemende gemeenten van de GR Peelgemeenten, de IBD en indien van toepassing de AP. Escaleren richting de deelnemende gemeenten van de GR Peelgemeenten gebeurt zodat zij ook op de hoogte worden gebracht van een (vermoedelijke ) kwetsbaarheid en zelf kunnen beoordelen of de kwetsbaarheid ook voor hen van toepassing is.

Als er sprake is van uitbesteding dan dienen er goede contractuele afspraken gemaakt te worden dat de leverancier op basis van prioriteit kwetsbaarheden snel moet oplossen. Afspraken bijvoorbeeld over wie de verantwoordelijkheid moet nemen voor elk van de stappen binnen het proces als een derde partij betrokken is.

***Verwerkersverantwoordelijke***
GR Peelgemeenten voert gemandateerde taken uit voor vijf lokale gemeenten. Deze gemeenten zijn verwerkingsverantwoordelijke en houden verantwoordelijkheid voor het datalek bij de verwerker. Bij een datalek waarin GR Peelgemeenten verwerker is, wordt de verwerkersverantwoordelijke gemeente bij de stappen betrokken. Via de verwerkersovereenkomst is opgenomen dat de GR Peelgemeenten incidenten meteen meldt bij de betrokken lokale gemeente(n). De GR Peelgemeenten meldt, wanneer van toepassing, het datalek bij de Autoriteit Persoonsgegevens namens de verwerkersverantwoordelijke gemeente.

***Verwerker***
Het kan gebeuren dat een datalek optreedt bij de verwerker. De GR Peelgemeenten is en blijft (als 'verwerkerssverantwoordelijke') altijd verantwoordelijk voor het datalek bij de verwerker. In dat geval moet in beginsel dezelfde procedure worden afgewerkt. De verwerker moet bij de stappen betrokken worden.
Via de verwerkersovereenkomst moet in ieder geval afgedwongen worden dat de verwerker incidenten gelijk meldt bij de GR Peelgemeenten, en de GR Peelgemeenten helpt bij het beoordelen of er gemeld moet worden en de afwikkeling van het incident. Belangrijk is dat de verwerker niet buiten de GR Peelgemeenten om een datalek meldt bij de Autoriteit Persoonsgegevens. De verwerker moet verder alle redelijke instructies van de GR Peelgemeenten opvolgen.

***Logging***
Bij het onderzoek naar mogelijke incidenten wordt veelvuldig gebruik gemaakt van de controle op logging uit systemen, netwerkapparatuur en programma's. Logbronnen worden gebruikt door een monitoring en responsedienst die detecteert of er kwetsbaarheden of incidenten hebben plaatsgevonden.

Los van de detectie, wordt logging ook veelvuldig achteraf gebruikt bij het reconstrueren van een incident of om te ontdekken welke systemen nog meer geraakt waren. Logs moeten bewaard worden volgens vaste regels en kennen per soort logging een bewaartermijn waarvan afgeweken kan worden (verlenging) als er een vermoeden is van een incident. Als logging op de juiste wijze bewaard en behandeld wordt, kan logging ook dienen als bewijsmateriaal voor de wet. De applicatiebeheerders en systeembeheerders moeten hierbij opletten dat logging persoonsgerelateerde of privacygevoelige informatie kan bevatten, en dat gelogde gegevens zodanig bewaard moet worden dat deze niet zomaar kan worden ingezien of worden gewijzigd. Zie hiervoor de handreiking 'Aanwijzing Logging' van de IBD.

## 7. Gouden uur en gouden tips

### 7.1 Gouden uur

Het 'gouden uur' is het eerste uur na de ontdekking van het incident. Het is essentieel om het incident in te perken maar ook geen informatie verloren te laten gaan die nodig is voor het onderzoek of het onderzoek achteraf. In het geval van bijvoorbeeld een computerinbraak, het wissen van een schijf en de diefstal van data, kan het nodig zijn om een digitaal forensisch expert in te huren. Deze kan alleen maar onderzoek doen als er zorgvuldig met bewijsmateriaal omgesprongen wordt. De handelingen uitgevoerd in het eerste uur zijn essentieel voor het welslagen van de reactie, maar ook op de bewijsvoering.

### 7.2 Gouden tips

- Vraag bij twijfel advies van een digitaal forensisch expert of bel de Helpdesk van de IBD: 070 2045511.
- Zorg voor volledig inzicht in de juridische consequenties van het incident en de betrokkenheid. Ga nooit verder dan je expertise zal toestaan.
- Denk verder dan het apparaat in kwestie en let ook op de papieren documentatie, die in het kantoor ligt en mogelijk ook moet worden beschermd om als mogelijk bewijs te dienen.
- Documenteer nauwkeurig de uitgevoerde acties, deze moeten ook datum en tijd bevatten.
- Vergeet niet om bij het onderzoek de apparatuur te isoleren vanuit elke netwerkverbinding (Bluetooth, bedraad of draadloos).
- Schakel nooit een apparaat aan als het uit staat.
- Als een apparaat is ingeschakeld en het lijkt zo te zijn dat dit actief bezig is met het verwijderen van gegevens of onder externe controle is, dan is het te overwegen het apparaat uit te schakelen door het snoer of de batterij weg te nemen. LET OP: niet uitzetten met de aan/uit knop, dan verdwijnen er mogelijk sporen. Win, indien mogelijk, deskundig advies in alvorens iets te doen.
- Maak desnoods foto's van externe aansluitingen aan het apparaat, zoals printers of USB-drives en van schermactiviteiten die u kunt zien.

## Vaststelling en inwerkingtreding

Dit beleid treedt in werking na publicatie in het publicatieblad van de Gemeenschappelijke regeling Peelgemeenten.

*Aldus vastgesteld door het Dagelijks bestuur van de Gemeenschappelijke regeling Peelgemeenten op 4 november 2021.*

*De voorzitter*

*M.M. Schlosser*

*De secretaris*

*C.L.C. Verberne*