Informatieveiligheid:

Incidentenprocedure

Inhoud

1. Inleiding 3
2. Regelgevend kader 3
3. Voor alle medewerkers 4
   3.1. Wat is een incident ? 4
   3.2. Detectie van een incident 4
   3.3. Stappenplan: Hoe meld je een incident in MIPS? 4
4. Voor de IV-cel en verantwoordelijken 5
   4.1. Behandeling van een incident 5
   4.2. Ontvangst en dispatch 5
   4.3. Incidentenbehandeling 6
   4.4. Incidenten melden 7
   4.4.1. Melding aan de toezichthoudende autoriteit 7
   4.4.2. Melding aan betrokkenen 8
   4.4.3. Meldingsplicht Politie 9
   4.5. Het stappenplan voor de IV-Cel 9

1. Inleiding

Elke organisatie krijgt vroeg of laat te maken met incidenten: een fout, een technisch probleem of een onvoorziene gebeurtenis waarbij informatie in het gedrang komt. Soms gaat het om een klein misverstand, soms om een ernstige bedreiging zoals een IT-aanval. Snel en correct reageren is in elk geval essentieel.

Deze incidentenprocedure helpt alle medewerkers van Stad Turnhout om op een uniforme en correcte manier te reageren bij zulke situaties. Ze beschrijft:

- Wat je moet doen als medewerker wanneer je een (mogelijk) incident vaststelt
- Hoe het incident verder wordt opgevolgd door de informatieveiligheidscel (IV-cel) en andere verantwoordelijken

Door incidenten op een consequente manier te behandelen, zorgen we samen voor:

- de bescherming van persoonsgegevens en systemen,
- het beperken van de impact van fouten of inbreuken,
- en het voldoen aan onze wettelijke verplichtingen, zoals de meldplicht bij de Gegevensbeschermingsautoriteit.

Deze procedure bestaat uit twee delen:

- Deel 1 – Voor alle medewerkers
  Toegankelijke richtlijnen over hoe je een incident herkent, meldt en opvolgt.
- Deel 2 – Voor de IV-cel en verantwoordelijken
  Technische en juridische richtlijnen voor de analyse, opvolging en eventuele melding van incidenten.

Bij twijfel: meld altijd. Liever één melding te veel dan één te weinig.

2. Regelgevend kader

De procedure is gebaseerd op de onderstaande wetgeving:

- De wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens
- De Europese Verordening 2016/679 van 27 april 2016 betreffende de bescherming van de natuurlijke personen m.b.t. het verwerken van persoonlijke gegevens en het vrije verkeer van deze gegevens.

Welke verplichtingen heeft het bestuur volgens deze wetgeving:

- Het bestuur moet een procedure hebben en alle medewerkers moeten deze kennen
- Als een incident zich voordoet of er bestaat een risico op een incident moeten medewerkers dit onmiddellijk melden aan hun diensthoofd of andere verantwoordelijke
- Het bestuur moet een procedure hebben om bij incidenten die een inbreuk vormen op de privacy van personen deze te behandelen en dit binnen de 72 uren na kennisname van het incident te melden bij de toezichthoudende autoriteit (Vlaamse Toezichtcommissie en Gegevensbeschermingsautoriteit)
- De DPO en de algemeen directeur moeten steeds op de hoogte gebracht worden van incidenten of mogelijke risico's.

3. Voor alle medewerkers

3.1. Wat is een incident ?

Een incident is een fout, vergissing of onverwachte gebeurtenis waarbij persoonsgegevens of informatiesystemen in gevaar komen. Denk aan een verkeerd verstuurde e-mail met vertrouwelijke info, een gestolen laptop, een phishingmail, of iemand die zonder toestemming toegang heeft tot dossiers.

Deze procedure is van toepassing op alle incidenten die te maken hebben met:

- Persoonsgegevens: zoals naam, adres, rijksregisternummer, e-mailadres, foto's, rekeningnummer enz.
- Informatiesystemen: zoals je computer, mailbox, bestanden, of toepassingen waarmee gegevens worden beheerd.

Ook als er (nog) geen schade is, maar een risico bestaat (bv. een nooddeur die vaak open staat), spreken we van een bijna-incident. Ook dat moet gemeld worden.

Je hoeft zelf niet in te schatten hoe ernstig het is. **Meld altijd als je twijfelt.**

3.2. Detectie van een incident

Medewerkers moeten onmiddellijk alle incidenten en risico's melden.

Alle meldingen moeten zo snel mogelijk gemeld worden via een MIPS-melding onder de categorie Informatieveiligheid.

Bij kritische incidenten waar er onmiddellijke schade is aan de ICT-middelen, bijvoorbeeld als het interne netwerk uitvalt, de stroom onderbroken is, er een virus of malware op de computer is vastgesteld, moeten medewerkers de ICT-verantwoordelijke contacteren zodat onmiddellijke actie kan genomen worden.

3.3. Stappenplan: Hoe meld je een incident in MIPS?

Stap 1: Open MIPS en kies de juiste categorie

1. Ga naar mips.turnhout.be.
2. Klik op "Privacy meldingen".
3. Klik op "Nieuwe privacy melding".

Stap 2: Vul de melding in

- Titel → Geef een korte en duidelijke titel.
- Categorie → Selecteer "Melding incident".
- Prioriteit → Kies "Hoog" (incidenten zijn altijd hoog).
- Beschrijving → Geef zo veel mogelijk details:
    - Wat is er gebeurd?
    - Welke gegevens of systemen zijn betrokken?
    - Wanneer en hoe heb je het ontdekt?

Stap 3: Verzend de melding

- Klik op "Verzend melding".
- De DPO neemt het incident vanaf hier over.

Bij een kritisch incident (bv. ransomware, groot datalek, netwerkuitval): Bel onmiddellijk ICT en de DPO, en meld het incident in MIPS.

4. Voor de IV-cel en verantwoordelijken

4.1. Behandeling van een incident

De behandeling van incidenten gebeurt onder verantwoordelijkheid van de informatieveiligheidscel. Onderstaande werkwijze beschrijft hoe incidenten intern worden geanalyseerd, geclassificeerd, opgevolgd en, indien nodig, gemeld aan de bevoegde instanties en betrokkenen.

Bij de behandeling van de incidenten maken we een onderscheid tussen

Incident	Wat
Kritische incidenten	Incident met onmiddellijke schade aan de ICT-middelen. De schade zal escaleren als er niet onmiddellijk ingegrepen wordt. Bijvoorbeeld, er is een virus of malware op de computer vastgesteld.
Niet-kritische incidenten	Incident met beperkte schade en waarvan de schade niet escaleert als ze niet onmiddellijk verholpen is.
Incidenten met impact op rechten en vrijheden betrokkenen	Kritisch incident waarbij er een impact is op de privacy van burgers.
Risico's of bijna-incidenten	Er is geen onmiddellijke schade maar deze kan in de toekomst wel optreden

De aanpak verloopt in volgende stappen, namelijk de ontvangst en dispatch, de incidentenbehandeling en eventueel het melden van het incident.

4.2. Ontvangst en dispatch

- Alle meldingen worden verzameld via het MIPS-systeem.
- De Coördinator strategie & beleid in samenspraak met de DPO beoordelen tot welke categorie een incident behoort.
- De DPO informeert de betrokkenen volgens de ernst van het incident.

Incident	Melding bezorgen aan
Kritische incidenten	Algemeen directeur, Coördinator strategie & beleid, ICT en DPO + betrokken diensthoofd
Niet-kritische incidenten	Coördinator strategie & beleid en DPO
Incidenten met impact op rechten en vrijheden betrokkenen	Algemeen directeur, Coördinator strategie & beleid en DPO
Risico's of bijna-incidenten	Coördinator strategie & beleid en DPO

- Alle incidenten en bijna incidenten worden genoteerd in het incidentenregister. In dit register dienen de volgende gegevens te worden vermeld:
    - Wanneer het lek plaatsvond.
    - Een korte beschrijving van het lek.
    - Wat er gebeurd is met de gegevens.
    - Hoeveel gegevens gelekt zijn.
    - Van welke categorie personen de gegevens gelekt zijn.
    - Welke soort gegevens.
    - Gevolgen van de inbreuk.
    - Genomen maatregelen (zowel schade beperkend als preventief).
    - Wanneer de meldplicht voldaan werd en indien niet, de reden daarvoor.

Het register is een nuttig document om het aantal incidenten te monitoren en daar gevolgen uit te trekken. Het overzicht hoeft niet openbaar te worden gemaakt. Wel is het een verantwoordingsdocument ten aanzien van de Gegevensbeschermingsautoriteit (GBA) en de Vlaamse Toezichtcommissie (VTC) om aan te tonen dat het bestuur bewust omgaat met incidenten.

4.3. Incidentenbehandeling

De behandeling van een incident hangt af van de ernst en de impact. De coördinator strategie & beleid maakt in overleg met de DPO een inschatting van de juiste categorie. Per categorie gelden onderstaande werkwijzen.

a) Kritische incidenten
Dit zijn incidenten met onmiddellijke schade aan de ICT-middelen of dienstverlening, waarbij snel handelen nodig is om verdere schade te voorkomen.

- De betrokken diensten nemen onmiddellijk maatregelen om schade te beperken en te herstellen.
- De coördinator strategie & beleid en ICT coördineren de technische afhandeling, in samenspraak met de DPO.
- Indien nodig roept de algemeen directeur de informatieveiligheidscel (IV-cel) samen voor crisisoverleg.
- Het incident wordt geregistreerd in het incidentenregister.

b) Incidenten met impact op rechten en vrijheden van betrokkenen
Dit zijn incidenten waarbij persoonsgegevens gelekt of blootgesteld zijn, met mogelijk ernstige gevolgen voor burgers.

- De betrokken diensten beperken en herstellen de schade.
- De coördinator strategie & beleid, de DPO en de ICT-verantwoordelijke documenteren de oorzaak en verzamelen bewijsmateriaal (zoals logs of e-mails).
- De DPO beoordeelt, in overleg met de algemeen directeur, of het incident gemeld moet worden aan de Gegevensbeschermingsautoriteit en/of de Vlaamse Toezichtcommissie.
- Indien nodig worden ook de betrokken burgers geïnformeerd op duidelijke wijze.
- Het incident wordt opgenomen in het incidentenregister.

c) Niet-kritische incidenten
Dit zijn incidenten waarbij de schade beperkt is en geen onmiddellijke actie vereist is.

- De coördinator strategie & beleid en de DPO beoordelen de melding en nemen gepaste maatregelen.
- Indien nodig wordt een voorstel voorbereid voor bespreking op de eerstvolgende IV-cel.
- Het incident wordt geregistreerd in het incidentenregister.

d) Risico's of bijna-incidenten
Dit zijn situaties waarbij geen schade is vastgesteld, maar wel een zwakke plek werd ontdekt die in de toekomst tot incidenten kan leiden.

- De melding wordt onderzocht door de coördinator strategie & beleid en de DPO.
- Gepaste preventieve maatregelen worden genomen om toekomstige incidenten te vermijden.
- De IV-cel bespreekt deze risico's op periodieke basis, met het oog op structurele verbeteringen.
- Ook risico's worden genoteerd in het incidentenregister, om trends en terugkerende zwakke plekken te kunnen detecteren.

4.4. Incidenten melden

4.4.1. Melding aan de toezichthoudende autoriteit

Het melden van een incident aan de GBA en VTC is niet altijd verplicht. De melding dient alleen te gebeuren wanneer het waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een **risico** inhoudt voor de rechten en vrijheden van natuurlijke personen. Om uit te maken of het incident gemeld moet worden, kunnen volgende vragen doorlopen worden:

- *Zijn er effectief data gelekt?*
  Als een incident het risico op een lek inhield, maar in feite geen data publiek gemaakt zijn of bij verkeerde personen terechtgekomen, blijft het bij een incident. Het incident wordt wel in het interne incidentenregister genoteerd, maar aangifte bij de VTC of GBA is niet nodig.

- *Is er waarschijnlijk geen risico?*
  Als data buiten de beveiligde zones of buiten je organisatie terechtgekomen zijn, is het nog steeds mogelijk dat er dankzij de beschermingsmaatregelen eigenlijk geen risico is. De data kunnen bijvoorbeeld degelijk geëncrypteerd zijn of beveiligd op een andere manier en zullen dus door buitenstaanders niet gebruikt kunnen worden. De sleutel om de beveiliging te kraken mag natuurlijk ook niet gelekt zijn. In geval van laag risico is een melding bij de VTC of GBA niet noodzakelijk.

- *Is het onmiddellijke risico op schade voor de betrokkenen groot?*
  Een datalek moet gemeld worden als dit leidt tot een risico voor de rechten en vrijheden van betrokkenen. Dit risico bestaat als de inbreuk kan leiden tot lichamelijke, materiële of immateriële schade voor de personen wier gegevens het voorwerp van de inbreuk zijn. Wanneer de inbreuk betrekking heeft op gevoelige persoonsgegevens, moet dergelijke schade als waarschijnlijk worden beschouwd. Voorbeelden van dergelijke schade zijn discriminatie, identiteitsdiefstal of -fraude, financieel verlies en reputatieschade. Bij een datalek met betaalkaartgegevens is er kans op financiële schade en moeten de betrokkenen zo snel mogelijk verwittigd worden, zodat ze zelf maatregelen kunnen nemen. Dit kan ook het geval zijn als het gaat om diverse soorten gevoelige informatie.

In dat geval dient de melding te gebeuren **binnen de 72 uren na kennisname** van het lek door de verwerkingsverantwoordelijke. Maar deze verantwoording moet aangetoond kunnen worden.

De melding aan de toezichthoudende autoriteit moet de volgende gegevens bevatten (art 33, lid 3 AVG):

- de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
- de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;

- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Het bestuur moet zelf een beredeneerde afweging maken of een informatiebeveiligingsincident dat hen ter kennis komt een incident is en binnen het bereik van de wettelijke meldplicht valt. Bij twijfel wordt er aangeraden om het incident te melden aan de GBA en VTC.

4.4.2. Melding aan betrokkenen

Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk **een hoog risico** inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee (art. 34, lid 1 AVG).

Deze mededeling moet een omschrijving bevatten van de aard van het incident, in passende en eenvoudige taal. Tevens moeten de contactgegevens van de functionaris van gegevensbescherming of een andere contactpersoon worden bezorgd, de (mogelijke) gevolgen van de inbreuk, de vermoedelijke datum van de inbreuk, een beschrijving van de waarschijnlijke gevolgen en de getroffen maatregelen.
Onder volgende voorwaarden is een meldplicht niet vereist (art. 34, lid 3 AVG):

- *de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals **versleuteling**;*
- *de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;*
- *de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.*

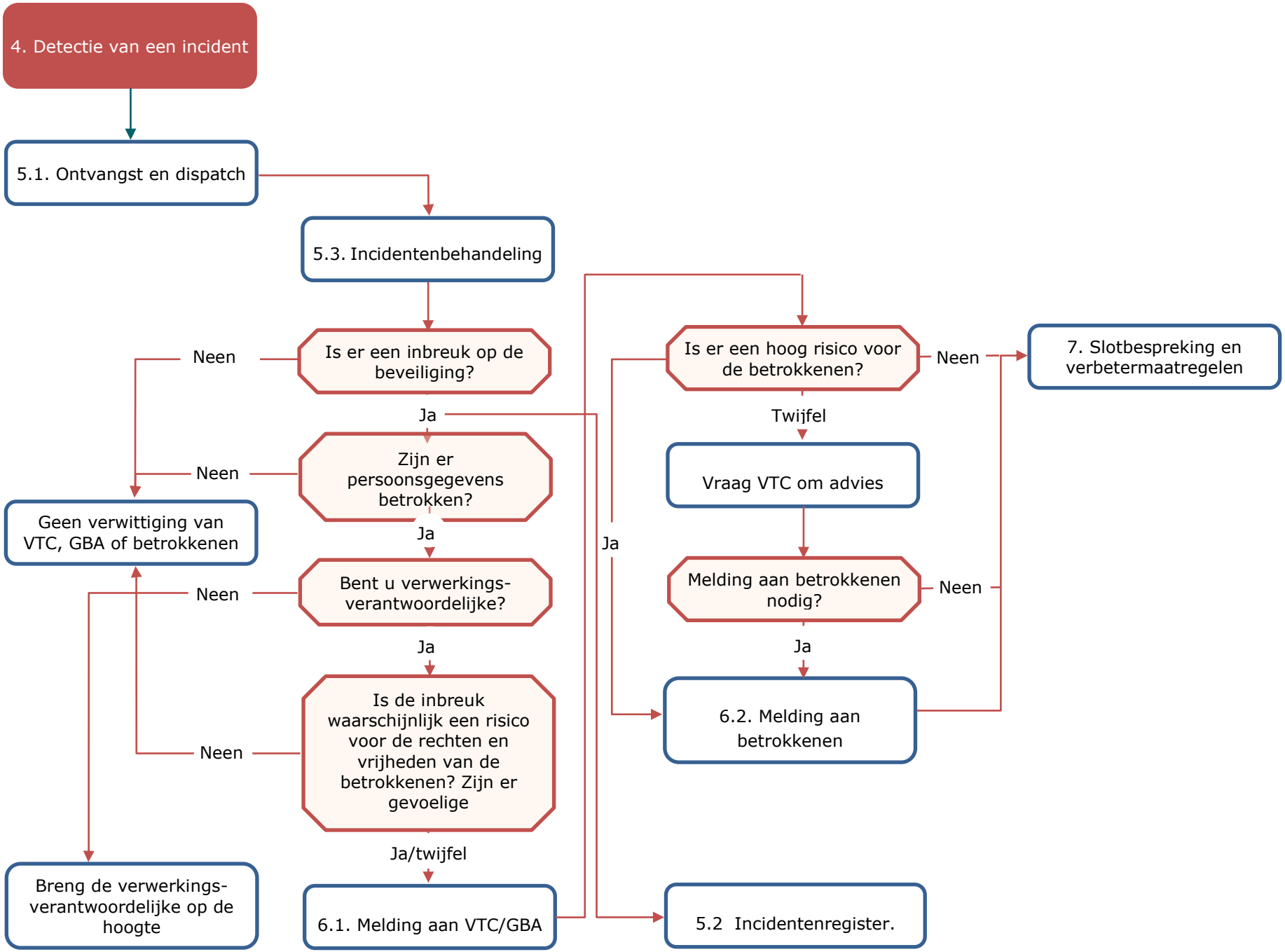
Welke zijn de risico's voor de betrokkenen?
Overweging 75 (AVG) levert een voorbeeldlijst van risico's die kunnen voortkomen uit een gegevensverwerking:

- *ernstige lichamelijke, materiële of immateriële schade, met name: waar de verwerking kan leiden tot discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, reputatieschade, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens, ongeoorloofde ongedaanmaking van pseudonimisering, of enig ander aanzienlijk economisch of maatschappelijk nadeel;*
- *wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen;*
- *wanneer persoonsgegevens worden verwerkt waaruit ras of etnische afkomst, politieke opvattingen, religie of levensbeschouwelijke overtuigingen, of vakbondslidmaatschap blijkt, en bij de verwerking van genetische gegevens of gegevens over gezondheid of seksueel gedrag of strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen;*
- *wanneer persoonlijke aspecten worden geëvalueerd, om met name beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;*
- *wanneer persoonsgegevens van kwetsbare natuurlijke personen, met name van kinderen, worden verwerkt;*
- *of wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.*

4.4.3. Meldingsplicht Politie

Afhankelijk van de situatie, waarbij sprake is van kwade wil en afpersing, wordt overwogen om hiervan melding te maken bij de politie.

4.5. Het stappenplan voor de IV-Cel


4. Detectie van een incident
5.1. Ontvangst en dispatch
5.3. Incidentenbehandeling
Is er een inbreuk op de beveiliging?
Neen
Ja
Zijn er persoonsgegevens betrokken?
Neen
Ja
Bent u verwerkings-verantwoordelijke?
Neen
Ja
Is de inbreuk waarschijnlijk een risico voor de rechten en vrijheden van de betrokkenen? Zijn er gevoelige
Neen
Ja/twijfel
Geen verwittiging van VTC, GBA of betrokkenen
Breng de verwerkings-verantwoordelijke op de hoogte
6.1. Melding aan VTC/GBA
Ja
5.2 Incidentenregister.
Is er een hoog risico voor de betrokkenen?
Neen
Twijfel
Vraag VTC om advies
Melding aan betrokkenen nodig?
Neen
Ja
6.2. Melding aan betrokkenen
7. Slotbespreking en verbetermaatregelen