Richtlijnen i.v.m. het beveiligen van gegevens en documenten op basis van classificatie.

KMS PROC
OP-ICT-PB-IB

Inhoud

1 Doel

Dit document beschrijft de richtlijnen voor het classificeren van de Pidpa-gegevens en bevat de checklist met te nemen beveiligingsmaatregelen voor de geclassificeerde gegevens. Het gaat over zowel de gegevens in digitale vorm (data) als gegevens in afgedrukte vorm (documenten).

2 Classificatie als methodiek voor een 'passende' beveiliging

Elke organisatie is in toenemende mate afhankelijk van haar gegevens; dit geldt ook zo voor de Pidpa. Teneinde de continuïteit van onze dienstverlening te verzekeren en schade aan onze goede werking te voorkomen of te beperken is een gepaste beveiliging dan ook aangewezen. Bovendien zijn er wettelijke verplichtingen aangaande de bescherming van persoonsgegevens. Daarom moeten beveiligingsmaatregelen getroffen worden voor wat betreft de vertrouwelijkheid, de beschikbaarheid en de integriteit van de aanwezige informatie.

- Vertrouwelijkheid van informatie wil zeggen er voor zorgen dat alleen personen die daarvoor toelating hebben toegang krijgen tot de informatie.
- Beschikbaarheid van informatie wil zeggen er voor zorgen dat de gebruiker toegang heeft tot de informatie op het moment dat hij de informatie nodig heeft.
- Integriteit van informatie wil zeggen er voor zorgen dat de informatie juist, volledig en bijgevolg betrouwbaar is.

Speciale aandacht dient te gaan naar de ontsluiting van informatie naar buiten de traditionele kantooromgeving, wat als gevolg een aantal mogelijke zwakke plekken met zich mee kan brengen. Denk hierbij aan de toenemende diversiteit aan beschikbare toestellen (PC, laptop, tablet, smartphone, USB-stick, enz. ...) en de verhoogde flexibiliteit naar werkplek (Kantoor, op het terrein, wifi, thuiswerken, enz. ...).

2.1 Classificatie van gegevens

Het hulpmiddel bij uitstek voor het bepalen van geschikte beveiligingsmaatregelen is de classificatie van gegevens. Dit is het indelen in gelijkaardige groepen of klassen van de gegevens die dan het beschermingsniveau bepalen. Niet alle gegevens hebben immers dezelfde waarde of zijn even gevoelig of kritisch. Voor elke klasse wordt verderop in de vorm van een checklist vastgelegd waaruit de minimale beveiliging moet bestaan. Hoe hoger de klasse, hoe hoger de beveiliging. Het is belangrijk dat iedere medewerker (ook externe) zich bewust is van de classificatie en de bijhorende maatregelen.

2.1.1 Classificatie van gegevens naar vertrouwelijkheid

De classificatie van gegevens naar vertrouwelijkheid gebeurt op basis van de betekenis of inhoud (content) van de gegevens. Het is immers de content die bepalend is voor de schade die opgelopen wordt indien de gegevens in verkeerde handen vallen. Voor de gegevens die informatie over personen bevatten is bijzondere aandacht nodig omdat deze onder de wet op de privacy vallen.

- Klasse 1 - Publieke gegevens : de gegevens die openbaar zijn of geen vertrouwelijke inhoud hebben. Een voorbeeld hiervan zijn de publieke gegevens op de website van Pidpa.
- Klasse 2 - Interne bedrijfsgegevens : de gegevens waarvan het gebruik beperkt moet worden tot intern het bedrijf. Deze gegevens zijn niet bestemd voor publieke bekendmaking zonder voorafgaande goedkeuring door de directie. In principe vallen hier alle gegevens onder die aanwezig zijn in Pidpa-documenten of ingebracht in ICT-systemen.
- Klasse 3 - Vertrouwelijke bedrijfsgegevens : dit zijn de bedrijfsgegevens die ofwel binnen de context van de Pidpa of de partners een vertrouwelijk karakter hebben. Deze gegevens zijn niet bestemd voor verspreiding, zowel binnen als buiten het bedrijf, zonder voorafgaande goedkeuring van de beheerder

van de gegevens of de directie. Het kan hier gaan over de meest diverse gegevens als financiële gegevens, operationele gegevens, commerciële gegevens, enz.

- Klasse 4 - Persoonsgegevens : een persoonsgegeven is iedere informatie over een geïdentificeerd of identificeerbaar natuurlijk persoon. Alle persoonsgegevens hebben een min of meer vertrouwelijk karakter en zijn gebonden aan de richtlijnen uit de wet op de privacy. Ook ogenschijnlijk triviale gegevens als vb. naam, adres en telefoonnummer zijn persoonsgegevens.
- Klasse 5 - Vertrouwelijke persoonsgegevens : dit zijn de persoonsgegevens die een vertrouwelijk karakter hebben. Voor deze gegevens hebben we ons te houden aan de privacywet (cf. persoonsgegevens), maar eveneens aan bijzondere bijkomende behandeling ter bescherming ervan. Voorbeelden hiervan zijn gegevens i.v.m. verloning, evaluaties, wanbetalers, enz...
- Klasse 6 - Gevoelige persoonsgegevens : het gaat om gegevens over ras, politieke opvattingen, godsdienstige of levensbeschouwelijke overtuigingen, lidmaatschap van een vakvereniging, gezondheid, seksuele leven, verdenkingen, vervolgingen, strafrechtelijke of bestuurlijke veroordelingen. De wetgever heeft bepaald dat het verboden is om dergelijke gegevens te verwerken.

In deze classificatie zijn, op uitzondering van de publieke gegevens (klasse 1) en interne bedrijfsgegevens (klasse 2), alle gegevens vertrouwelijk. Voor deze vertrouwelijke gegevens zijn extra maatregelen van toepassing, afhankelijk van de klasse. De maatregelen kan U verderop in dit document vinden.

2.1.2 Classificatie van gegevens naar beschikbaarheid

De classificatie van gegevens naar beschikbaarheid gebeurt op basis van de schade die het niet (meer) ter beschikking hebben van de gegevens op het moment dat ze nodig zijn veroorzaakt. Het tijdsaspect is hierbij een belangrijk element en dient men geval per geval te bekijken.

- Klasse 1 - Niet vitaal : verlies of niet beschikbaar zijn van de gegevens brengt geen of aanvaardbare schade toe aan de onderneming.
- Klasse 2 - Vitaal : verlies of niet beschikbaar zijn van de gegevens brengt ernstige schade toe aan de onderneming.
- Klasse 3 - Zeer vitaal : verlies of niet beschikbaar zijn van de gegevens vormen een bedreiging voor de onderneming.

Een minimale bescherming naar beschikbaarheid is steeds aangewezen voor digitale gegevensdragers, ook voor niet-vitale gegevens (klasse 1). Alle gegevens hebben immers hun betekenis en zijn van waarde voor Pidpa. Voor de vitale (klasse 2) en zeer vitale (klasse 3) gegevens zijn extra maatregelen te voorzien. De maatregelen kan U verderop in dit document vinden.

2.1.3 Classificatie van gegevens naar integriteit

Er is geen classificatie naar integriteit voorzien. Ten behoeve van de bewaking van de integriteit van de gegevens zal eerder gewerkt worden met een aantal aanbevelingen (best practices) die de verantwoordelijken in staat stellen om de nodige initiatieven te nemen zodat de gegevens juist, volledig en bijgevolg betrouwbaar aanwezig zijn in de respectievelijke ICT-systemen. De aanbevelingen kan U verderop in dit document vinden.

3 Maatregelen van toepassing afhankelijk van de classificatie

Checklist
Hierna volgt de checklist van te implementeren maatregelen i.v.m. de vertrouwelijkheid en i.v.m. de beschikbaarheid. Het is een mix van maatregelen rond veilig gedrag en de beveiliging op niveau van de fysieke toegang, ICT-systemen, de applicaties en het netwerk die onze veiligheid moet verzekeren.

De maatregelen die voor een component van toepassing zijn, worden bepaald door de classificatie voor deze component. De maatregelen zijn cumulatief, of m.a.w. hoe hoger de klasse hoe meer aanvullende maatregelen gelden.

3.1 Maatregelen i.v.m. de vertrouwelijkheid

- Klasse 1 - Publieke gegevens
- Klasse 2 - Interne bedrijfsgegevens
- Klasse 3 - Vertrouwelijke bedrijfsgegevens
- Klasse 4 - Persoonsgegevens
- Klasse 5 - Vertrouwelijke persoonsgegevens
- Klasse 6 - Gevoelige persoonsgegevens

Het 'Need to know'-principe
Om de vertrouwelijkheid van gegevens zo goed als mogelijk te ondersteunen geldt als algemene regel het 'Need to know'-principe. Dit principe stelt dat uit beveiligingsoverweging toegang tot gegevens slechts mag verstrekt worden aan de personen die deze nodig hebben voor het uitvoeren van hun taken. Het 'Need to know'-principe is o.a. toe te passen op de toegang tot de ICT-systemen, de toekenning van toegangsrechten tot documenten in het documentensystemen (eDocs) en het verzenden van mails aan medewerkers. Ook een op rollen gebaseerde toegang tot specifieke gegevens binnen een ICT-systeem is een toepassing van dit principe en is in een systeem met gevoelige gegevens sterk aan te bevelen.

Toegangscontrole – identificatie, authenticatie en autorisatie
Voor de toegang tot gegevens in informatiesystemen wordt bepaald of - en welke - identificatie, authenticatie en autorisatie vereist is ... en dit vooraleer de toegang wordt verleend.
- Bij de 'identificatie' wordt gevraagd wie U bent. dit gebeurt door vb. het opgeven van een gebruikersnaam.
- Bij de 'authenticatie' wordt nagegaan of diegene die zich geïdentificeerd heeft, wel effectief de persoon is voor wie hij zich uitgeeft. Dit gebeurt vb. door het opgeven van een paswoord, of het controleren van een vingerafdruk.
- Na authenticatie zorgt de 'autorisatie' er voor dat de geïdentificeerde en geauthentiseerde gebruiker enkel toegang krijgt tot voor hem ter beschikking gestelde gegevens of diensten.

Belangrijke opmerking i.v.m. het uitvoeren van testen
Voor de testen die met kopieën van productiegegevens worden uitgevoerd dient men dezelfde maatregelen te implementeren als voor de productiegegevens zelf. Vanaf klasse 6 is het verboden om deze productiegegevens te gebruiken voor testdoeleinden. Er moeten m.a.w. in dit geval fictieve gegevens gebruikt worden.

3.1.1 Checklist voor gegevens

Klasse >=	Minimale Maatregel
1	Computerruimten zijn voorzien van een degelijke inbraakbeveiliging. Toegang tot deze ruimten is verboden zonder begeleiding van een ICT-systeemmedewerker die toezicht houdt tijdens de aanwezigheid van derden.

1	Op elke PC is een antivirusprogramma aanwezig; de virusdefinities worden regelmatig up-to-date gebracht.
1	Er moet steeds een authenticatie via een gebruikersnaam en wachtwoord aanwezig zijn om toegang te bekomen tot een ICT-systeem.
1	Het ICT-systeem wordt na een beperkt aantal mislukte aanmeldpogingen uitgeschakeld.
1	De authenticatie is steeds persoonsgebonden.
1	Het wachtwoord voor de toegang tot het systeem staat versleuteld opgeslagen.
1	Een toestel wordt na een beperkte tijd van inactiviteit vergrendeld.
2	Toegang tot de gegevens wordt verleend op basis van het 'Need to know'-principe.
2	Gegevens worden niet verspreid zonder de toelating van de verantwoordelijke ervoor.
2	Testgegevens krijgen - indien het kopieën zijn van productiegegevens - dezelfde bescherming als de productiegegevens.
3	Het wachtwoord voor de toegang tot het systeem is een sterk wachtwoord, wat wil zeggen dat het bestaat uit minstens 8 posities en een combinatie is van kleine en grote letters en cijfers. Hierop moet het systeem een controle uitoefenen. Het wachtwoord is maximaal 1 jaar geldig.
3	Het wachtwoord wordt via een veilige versleutelde verbinding verstuurd.
3	De toegang tot het ICT-systeem is traceerbaar op gebruikersnaam
3	De back-up van de gegevens wordt fysiek beveiligd en procedures voor toegang en restore worden voorzien van de nodige regels om de vertrouwelijkheid te waarborgen.
3	Indien een toestel met gegevensopslag ingeleverd wordt, moet het deze gegevens via volledige formattering vernietigen (niet alleen de indexering)
3	Indien een toestel met gegevensopslag defect is, moet het vernietigd worden.
3	Versleuteling van datatransport wordt toegepast om afluisteren te voorkomen. De gegevens mogen dus niet via het publieke netwerk (internet) benaderbaar zijn tenzij via een beveiligde netwerkprotocol (https, imaps, pop3s,…).
3	De gegevens mogen niet op mobiele apparaten (laptop, USB, CD, ...) worden geplaatst zonder versleuteling ervan (encryptering).
4	De wetgeving op de privacy is van toepassing. Alle medewerkers moeten hiervan op de hoogte gebracht worden.
5	De toegang tot deze gegevens is traceerbaar op gebruikersnaam.
6	Deze gegevens mogen niet buiten het lokale netwerk te benaderen zijn.
6	Voor testdoeleinden mogen geen productiegegeven of kopieën ervan gebruikt worden.
6	De opslag van deze gegevens is steeds geëncrypteerd.
6	Een specifieke risicoanalyse is voor deze gegevens vereist, wat kan resulteren in bijkomende maatregelen.

3.1.2 Checklist voor documenten

Klasse >=	Minimale Maatregel
2	Afdrukken of kopiëren van documenten kan slechts na toelating van de verantwoordelijke ervoor.
3	Documenten mogen niet onbeheerd achtergelaten worden op de werkplek. Voor deze documenten geldt dus het 'clean desk'-principe.
3	Documenten mogen niet in de prullenmand belanden. Vernietiging is verplicht.
4	De wetgeving op de privacy is van toepassing. Alle medewerkers moeten hiervan op de hoogte gebracht worden.
5	Afdrukken of kopiëren van deze documenten is niet toegelaten tenzij voor specifieke doeleinden. Hiervan is een inventaris beschikbaar bij de verantwoordelijke, bevattende de gemandateerde(n) voor het afdrukken.

5	Afdrukken of kopiëren van de documenten gebeurt steeds onder toezicht.
5	Documenten moeten achter gesloten deur bewaard worden. Dit geldt ook voor archieven.
5	Documenten mogen het gebouw niet verlaten zonder bijkomende maatregelen. Er moet steeds toezicht zijn op het document tot aan de bestemming.
6	Documenten mogen het gebouw niet verlaten zonder dat deze in een beveiligde verpakking opgeborgen zit.

3.2 Maatregelen i.v.m. de beschikbaarheid

- Klasse 1 - Niet vitaal
- Klasse 2 - Vitaal
- Klasse 3 - Zeer vitaal

Maatregelen i.v.m. de beschikbaarheid moeten ervoor zorgen dat we het verlies van gegevens of de onbeschikbaarheid ervan voorkomen of zo veel mogelijk beperken. Zowel preventieve maatregelen als curatieve maatregelen moeten meegenomen worden in de beveiliging. Hoe waardevoller een systeem, hoe meer men zal trachten om preventieve maatregelen te voorzien. Preventieve maatregelen zijn over het algemeen echter wel duurder dan curatieve. Een goede afweging is dus aan de orde.

Single-point-of-failure (SPOF).
ICT-systemen bestaan uit een aantal technische componenten die allen op de één of andere manier kwetsbaar zijn en kunnen falen. De schade kan op zulk moment beperkt worden door een alternatief (redundantie) te voorzien. Enkele voorbeelden van redundantie zijn :

- Noodstroomvoorzieningen : Dit kan een algemene noodstroomvoorziening zijn (op het ganse net of een deel ervan) middels een stroomgenerator, of een specifieke voorziening voor een bepaald toestel d.m.v. een UPS.
- Reserve(onderdelen) : Onderdelen of volledige systemen kunnen op stock gehouden worden in een magazijn. Men moet wel rekening met de tijd die de installatie en configuratie ervan vergt.
- Cold standby : Dit betekent dat er een tweede systeem volledig geïnstalleerd klaar staat om de taken van het defecte systeem over te nemen. De overname gebeurt nog wel manueel.
- Fail-over : Dit is een techniek waarbij de taken van het defecte systeem direct en automatisch - dus zonder tussenkomst van medewerkers - worden overgenomen door een ander systeem. Dit is volledig transparant voor de gebruiker.

Het ultieme redmiddel
De reddingsboei bij uitstek als gegevens gecorrumpeerd geraken, is het back-up en restore systeem. Een dergelijk systeem dat niet deugdelijk is, geeft een onterecht gevoel van veiligheid. Essentieel is dus de controle op de goede werking ervan. Zowel de back-up als de restore-systematiek moeten procedureel vastgelegd worden, inclusief de testscenario's.

3.2.1 Checklist voor gegevens

Klasse >=	Minimale Maatregel
1	Er is een algemene noodstroomvoorziening aanwezig
1	Een periodieke back-up wordt voorzien
1	Een restore is op elk moment (tijdens de kantooruren) mogelijk op eenvoudig verzoek. De tijd nodig voor het terugzetten van gegevens is afhankelijk van het betrokken systeem.
1	Er wordt door de ICT-dienst voorzien in technische ondersteuning (tijdens de kantooruren) bij calamiteiten
2	Er is een UPS voor kritieke ICT-systemen voorzien.
2	Redundantie is voorzien voor de betrokken server(s).

2	Een capaciteitsplanning (naar performantie en volume) is aanwezig en wordt periodiek bijgewerkt.
2	Een dagelijkse back-up word voorzien of – bij statische gegevens - een back-up na belangrijke wijzigingen.
2	Onderhoud aan het ICT-systeem gebeurt waar mogelijk buiten de kantooruren
2	Er wordt door de ICT-dienst voorzien in technische ondersteuning (24/24 en 7/7) bij calamiteiten.
2	Onderhoudscontracten voorzien in regelmatige inspectie van cruciale onderdelen
2	Voor specifieke taken die niet door de eigen ICT-dienst kunnen opgenomen worden, wordt een serviceovereenkomst aangegaan met een externe partner.
3	Een specifieke risicoanalyse is voor deze gegevens vereist, wat kan resulteren in bijkomende maatregelen.
3	Een continuïteitsplan is aanwezig en wordt regelmatig (jaarlijks) geëvalueerd. Het continuïteitsplan houdt rekening met de risicoanalyse en de behoeften van de gebruiker.
3	Een restore is op elk moment (24/24 en 7/7) mogelijk op verzoek van de directie.
3	Er is een actieve meldingensystematiek (foutdetectie, capaciteitsproblemen, performantie,..) in de betrokken systemen ingebouwd, zodat tijdig inzichtelijk wordt welke preventieve acties moeten ondernomen worden om onderbrekingen te voorkomen.
3	Er worden reserveonderdelen voorzien (ofwel in eigen magazijn of gereserveerd bij een leverancier) of er wordt een uitwijkfaciliteit voorzien.

3.2.2 Checklist voor documenten

Klasse >=	Minimale Maatregel
2	Documenten worden achter gesloten deuren bewaard.
3	Documenten worden in een brandwerende kluis opgeborgen.

3.3 Maatregelen i.v.m. de integriteit

Kernbegrippen bij de integriteit van gegevens zijn juistheid en volledigheid. Het belang van de integriteit van gegevens is af te meten aan de schadelijke gevolgen die foutieve gegevens kunnen veroorzaken. Het gaat dan over vb. extra operationele kosten maar ook over gevolgen als foutieve beleidsbeslissingen. De integriteit van gegevens kan onbewust geschonden worden, maar kan ook het gevolg zijn van opzettelijke acties.

Er zijn geen stringente maatregelen voorzien wat betreft de integriteitsbewaking. Hierna volgen wel een aantal aanbevelingen die de verantwoordelijken in staat moeten stellen om de nodige initiatieven te nemen zodat de gegevens juist, volledig en bijgevolg betrouwbaar aanwezig zijn in de respectievelijke databanken.

3.3.1 Aanbevelingen ter voorkoming van het onbewuste schenden van de integriteit

Opleiding : ICT-systemen kunnen bijzonder complex zijn. Elke medewerker die een ICT-systeem gebruikt moet goed op de hoogte zijn van de werking ervan, de mogelijkheden van de software en de betekenis van de gegevens. Een gerichte opleiding is hiervoor noodzakelijk.

Autorisatie : Medewerkers dienen voldoende kennis te bezitten over de ICT-systemen om ze correct te kunnen gebruiken. Daarom is het aangewezen dat alleen de medewerkers die een opleiding hebben gevolgd, en zich voldoende bewust zijn van de betekenis van de gegevens die ze inbrengen, toegang krijgen tot een ICT-systeem. Elk systeem staat standaard dicht voor iedereen die geen autorisatie heeft.

Inputvalidatie : Iedereen zal vroeg of laat wel eens foutieve gegevens inbrengen; vergissen is menselijk. Tot op zekere hoogte kan een ICT-systeem dit voorkomen door ingebouwde controles. Voorbeelden hiervan zijn

numerieke controles, controle op datum, pick-up-lijsten, controle op verbanden tussen gegevens, enz. … Niet alle systemen gaan even ver in het ter beschikking stellen van dergelijke inputvalidatie maar gezien hun efficiëntie is een maximale implementatie ervan aangewezen.

Gerichte foutdetectie : Indien de schade door foutieve of ontbrekende gegevens als ernstig wordt ingeschat, dan is het aangewezen om bijkomende controlesoftware te ontwikkelen. Deze software moet de kans op fouten verkleinen door gericht op zoek te gaan naar foutieve of ontbrekende gegevens.

Specificaties (SPECS) : Belangrijke schade kan ontstaan indien er conceptuele fouten in systemen sluipen tijdens het ontwerp ervan. Dit zijn fouten waardoor foutieve uitgangspunten worden gehanteerd waarddoor het systeem niet kan leveren wat ervan verwacht wordt, of - in het slechtste geval – onbewust foutieve output levert. Deze fouten zijn op een later tijdstip soms zeer moeilijk te corrigeren. Bovendien liggen de kosten om dergelijke fouten te herstellen meestal bijzonder hoog. Dit kan mogelijk vermeden worden door duidelijke en zo specifiek mogelijke specificaties (SPECS / functioneel en technisch ontwerp) op te stellen bij de aanvang van een informatiseringsproject.

Beheer van wijzigingen aan software : Wijzigingen die moeten aangebracht worden aan programmatuur door derden of door eigen ICT-medewerkers, worden steeds schriftelijk aangevraagd door de Pidpa-verantwoordelijke van de software of een gemandateerde. De verantwoordelijke staat in voor het uitvoeren van de testen en de acceptatie van de aangebrachte wijzigingen. Slechts na acceptatie van de wijzigingen worden deze in productie gebracht.

Synchronisatie : In principe zal een bepaald gegeven op slechts één plaats opgeslagen zijn. In sommige gevallen is dit echter niet haalbaar en zullen dezelfde gegevens op meerdere systemen - in gekopieerde vorm - ter beschikking gesteld worden. In dergelijk geval is het essentieel dat één gegevensbestand (in een bronsysteem) als basis wordt aangewezen, en dat de andere systemen schaduwbestanden bevatten. De synchronisatie kan on-the-fly, via buffering, of in batchverwerking. Dit moet met de systeembeheerder worden afgestemd en beschreven staan in de systeemdocumentatie.

3.3.2 Aanbevelingen ter voorkoming van het bewuste schenden van de integriteit

Antivirusprogramma : Hiervoor wordt verwezen naar het hoofdstuk 'Maatregelen i.v.m. vertrouwelijkheid'.

Toegangscontrole : Hiervoor wordt verwezen naar het hoofdstuk 'Maatregelen i.v.m. vertrouwelijkheid'.

Functiescheiding : De fraudegevoeligheid van processen kan verkleind worden door er voor te zorgen dat er meer dan één persoon nodig is om de fraude te kunnen plegen. Dit is dus een organisatorische maatregel. Belangrijk is om scheidingen aan te brengen tussen besluitvorming, uitvoering, controle, registratie en bewaring van middelen.

Servercertificaten / SSL : Door het gebruik van servercertificaten kunnen gebruikers weten of de website die ze benaderen ook de juiste website is en niet een website die door een hacker is nagebouwd. Daarnaast wordt informatie die de gebruiker met de server uitwisselt versleuteld (geëncrypteerd) over de lijn verzonden.

Digitale handtekening : Juridisch heeft een digitale handtekening dezelfde status als een gewone handtekening (Richtlijn 99/93/EG). Deze is dus ook geldig voor de ondertekening van contracten e.d. in digitale vorm. Een digitale handtekening werkt twee kanten uit, enerzijds weet de ontvanger met zekerheid wie het document verstuurd heeft en anderzijds kan de verzender niet ontkennen dat betreffende document door hem verstuurd is.

3.4 Incidenten

Externe partijen melden incidenten via een mail naar ivc@pidpa.be .