Handleiding BIV classificatie

IBPDOC14

GEBRUIKERSGROEP IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Verantwoording

Productie
Kennisnet / saMBO-ICT

Met dank aan
SURF. Het document “SCIPR Leidraad Classificatie” is de basis voor hoofdstuk 2.
CIP (Centrum voor informatiebeveiliging en privacybescherming). Het document “De privacy baseline” is de basis voor hoofdstuk 4.

Auteurs
Maurits Toet (Cerrix)
Ludo Cuijpers (Kennisnet)
Maart 2016

Review
Leo Bakker (Kennisnet)
Bram Bogers (Gebruikersgroep ibp)
Esther van der Hei (Gebruikersgroep ibp)
Maart 2016

Sommige rechten voorbehouden

Inhoudsopgave

`

1. Toelichting

1.1 Samenhang met andere documenten

De sleutel tot een succesvol beleid op het gebied van informatiebeveiliging en privacy is in handen van de medewerkers en studenten van onze mbo instellingen. Flyers, trainingen, awareness campagnes, etc. zorgen ervoor dat dit thema breed onderkend wordt. Het management, met name de proceseigenaren, zijn (mede-) verantwoordelijk voor de verdere formele implementatie van het beleid. Het “Model informatiebeveiligings- en privacy beleid voor de mbo sector (IBPDOC6)” is een best practice die bruikbaar is voor de mbo sector. In dit beleidsplan worden afspraken gemaakt betreffende governance, compliance, incidenten registratie, etc. maar ook afspraken op het gebied van classificatie van informatie. Deze classificatie komt, uiteraard, terug in de roadmap ibp.

In de ibp roadmap[1] worden 5 fasen benoemd om te komen tot een gedragen informatiebeveiliging en privacy beleid. Fase 1 (Aanleiding) en fase 2 (Opdracht) is het College van Bestuur en de ibp manager aan zet. In fase 3 (Inventarisatie) zijn de proceseigenaren en de ICT ondersteuners aan het woord. De proceseigenaren bepalen classificatie van de informatie waar zij verantwoordelijk voor zijn.

1. Aanleiding

- Beschrijving urgentie informatiebeveiliging en privacy met als logische vervolgstap het opzetten van Informatiebeveiliging en privacy beleid binnen de MBO instelling.

2. Opdracht

- Formulering van de opdracht voor de kwartiermaker.
- Benoemen van de faciliteiten.
- Vastleggen van de kaders (bijvoorbeeld normenkader ISO 27001-2).

3. Inventarisatie

- Inventarisaties architecturen (proces, data, applicatie en netwerk).
- Gesprekken met medewerkers binnen MBO instelling.
- Eerste globale BIV classificatie en ranking van IT voorzieningen.

Dit document is een handleiding om te komen tot een classificatie per proces. Als uitgangspunt voor deze classificatie zal de enterprise architectuur van de instellingen kunnen dienen. Hierover is in het document IBPDOC4, Mbo ibp architectuur uitgebreid geschreven.
De classificatie wordt toegevoegd aan het proceslandschap. Uiteindelijk zal dit leiden tot een ibp (security) architectuur die een ibp manager wil en moet opstellen. Dit document ondersteunt de ontwikkeling van de ibp (security) architectuur.

[1] IBPDOC5 Roadmap informatiebeveiligings- en privacy beleid

1.2 Stappenplan BIV/PIA

De ibp (security) architectuur is gebaseerd op processen en classificaties. De BIV-classificatie[2] en de (het) PIA[3] beoordeling zijn stappen om te komen tot de genoemde architectuur. De 6 stappen schematisch weergegeven:

	#	Stappen	Gehanteerde bron	Bron	
BIV classificatie	1	Voeg aan alle processen uit het (gekozen) procesplaatje een nummer en een proces-eigenaar toe.	Proces architectuur	Triple A en HORA	Proceseigenaren
	2	Koppel het proces aan een applicatie en benoem de data uitwisseling (globaal)	Applicatie en data architectuur	Best practices mbo sector, IBPDOC4	
	3	Voer de BIV classificatie uit op het proces samen met de proces eigenaar.	• SCIPR: Leidraad Classificatiemode (versie 2.0) • aanvullingen in dit documenten	SCIPR en IBPDOC14	
PIA en privacy	4	Maak een PIA voor de gehanteerde applicatie, die het proces ondersteund, zodat de privacy risico's in kaart worden gebracht.	Privacy Impact Assessment (versie 2.0)	Integrale Veiligheid Hoger Onderwijs, PIA tool 3.0	Leveranciers
	5	Overleg een bewerkersovereenkomst, incl. datalekken.	Bewerkersovereenkomst: • model Kennisnet • model SURF • model leverancier	Kennisnet, SURF , IBPDOC28	
	6	Geef een oordeel van het ibp beleid van de externe leverancier van de applicatie.	Certificeringsschema.	Kennisnet	

1.3 Verwijzing voor de stappen 1, 2, 5 en 6

De stappen 3 en 4 worden in dit document gedetailleerd uitgewerkt. De overige stappen 1, 2, 5 en 6 worden in andere documenten uitgewerkt. Hieronder volgt een overzicht hiervan:

1.3.1 Procesbeschrijving (stap 1)

IBPDOC4 Mbo ibp architectuur is in juli 2016 opgeleverd. In dit document hebben een aantal informatiemanagers uit de mbo sector een aantal processen geselecteerd die bij voorkeur geclassificeerd kunnen worden Er wordt geen standaard procesbeschrijving aangeboden omdat dit binnen alle mbo instellingen al volop beschikbaar is.

1.3.2 Gehanteerde dataset (stap 2)

IBPDOC4 Mbo ibp architectuur geeft ook een aantal voorbeelden van applicatie, data en informatie architecturen. Voor ibp architectuur is dit cruciale input, immers koppelingen tussen applicaties leiden tot uitwisseling van data. Met name vanuit het oogpunt van privacy is dit van belang.

1.3.3 Bewerkersovereenkomst, incl. datalekken (stap 5)

IBPDOC28 Bewerkersovereenkomst mbo versie presenteert een format voor een bewerkersovereenkomst. Dit document is vanaf medio 2016 beschikbaar.

[2] BIV: **B**eschikbaarheid, **I**ntegriteit, **V**ertrouwelijkheid

[3] PIA: **P**rivacy **I**mpact **A**ssessment

1.3.4 Toelichting ibp beleid externe leveranciers (stap 6)

Medio 2016 is er ook een certificeringsschema beschikbaar met vragen die leiden tot de beoordeling van externe leveranciers.

1.4 BIV classificatie (stap 3) en PIA (stap 4)

In hoofdstuk 2 zal de BIV classificatie worden toegelicht en in hoofdstuk 3 zal een voorbeeld van een BIV classificatie worden gegeven. Beschikbaarheid (**B**IV), integriteit (B**I**V) en vertrouwelijkheid worden globaal beschreven (BI**V**). De mbo sector heeft besloten om alleen de processen te classificeren en niet de systemen (applicaties) en data omdat deze een voortvloeisel zijn uit de processen. Zoals in de tabel weergegeven is de proceseigenaar leidend. Als bijlage is een voorbeeldovereenkomst opgenomen voor de vastlegging van de BIV classificatie tussen de proceseigenaar en de mbo instelling (ibp manager).
In hoofdstuk 4 wordt de achtergrond van de PIA beschreven. Er wordt verwezen naar het format voor het uitvoeren van een PIA.
In hoofdstuk 5 wordt een voorbeeld gegeven van een ibp architectuur op basis van de uitleg van de BIV classificatie en de PIA, alsmede de input van geraadpleegde mbo-informatiemanagers en documenten van Kennisnet en SURF.

1.5 Vervolg

Voor enkele concrete processen is de BIV classificatie en de opstelling van de PIA verder uitgewerkt. Het gaat om de processen rond bekostiging (deelnemersadministratie), indiensttreding (personeel) en online leren (gebruik educatieve software). De volgende documenten zijn hierbij beschikbaar:

- IBPDOC15 BIV PIA bekostiging,
- IBPDOC16 BIV PIA indiensttreding
- IBPDOC17 BIV PIA online leren

2. BIV classificatie processen mbo instellingen

2.1 Inleiding

Iedere mbo instelling streeft naar een goede balans tussen het optimaal gebruik van ict-middelen enerzijds en het borgen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie anderzijds. Deze doelstellingen kunnen enkel bereikt worden met een gedegen uitgevoerde classificatie – en beleid – op functioneel, technisch en organisatorisch vlak.
Classificatie helpt bij::

- een veilige leer- en werkomgeving;
- een goed imago;
- naleving van wetgeving, zoals Algemene Verordening Gegevensbescherming (AVG).

Classificatie van informatie helpt bij:

- het selecteren van maatregelen die genomen moeten worden om informatie adequaat te beschermen, de integriteit te waarborgen en de beschikbaarheid te optimaliseren;
- het vergroten van de alertheid van de organisatie met betrekking tot de waarde van informatie en beveiligingsrisico's.

Informatie betekent in dit verband alle data en gegevens, ongeacht het medium (bijvoorbeeld ook papieren documenten) waarop deze opgeslagen worden en ongeacht de presentatie daarvan. Informatie wordt in de praktijk verwerkt binnen één of meerdere onderwijs- en bedrijfsprocessen en op één of meer systemen/applicaties. Deze context wordt dan ook bij de classificatie betrokken. Gekozen is voor het begrip "classificatie van informatie", in lijn met de naam van het vakgebied: "informatiebeveiliging".

2.1.1 Classificatie-aspecten: BIV

Het beschermingsniveau van informatie wordt getoetst aan de kwaliteitscriteria Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV).
Beschikbaarheid: de mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ict-dienstverlening waarborgen.
Deelaspecten hiervan zijn:

- Continuïteit: de mate waarin de beschikbaarheid van de ict-dienstverlening gewaarborgd is;
- Portabiliteit: de mate waarin de overdraagbaarheid van het informatiesysteem naar andere gelijksoortige technische infrastructuren gewaarborgd is;
- Herstelbaarheid: de mate waarin de informatievoorziening tijdig en volledig hersteld kan worden.

Integriteit: de mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de IT-dienstverlening waarborgen.
Deelaspecten hiervan zijn:

- Juistheid: de mate waarin overeenstemming van de presentatie van gegevens/informatie in IT-systemen ten opzichte van de werkelijkheid is gewaarborgd;
- Volledigheid: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is;
- Waarborging: de mate waarin de correcte werking van de IT-processen is gewaarborgd.

Vertrouwelijkheid: de mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.
Deelaspecten hiervan zijn:

- Autorisatie: de mate waarin de adequate inrichting van bevoegdheden gewaarborgd is;
- Authenticiteit: de mate waarin de adequate verificatie van geïdentificeerde personen of apparatuur gewaarborgd is;
- Identificatie: de mate waarin de mechanismen ter herkenning van personen of apparatuur gewaarborgd zijn;

- Periodieke controle op de bestaande bevoegdheden. Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.

2.1.2 Doelstelling classificatieproces: classificatie en maatregelen

Classificatie geeft een inschatting van de gevoeligheid en het belang van informatie om tot een juiste mate van beveiliging te komen. Niet alle informatie is even vertrouwelijk of hoeft bij een incident even snel weer beschikbaar te zijn. Het is niet erg efficiënt of gebruiksvriendelijk om niet vertrouwelijke informatie op dezelfde manier te beschermen als vertrouwelijke informatie.
Informatieclassificatie hoort in elk project thuis waar informatie een rol speelt, maar zal ook op nieuwe toepassingen en bestaande omgevingen moeten worden uitgevoerd. Zo kan door veranderende processen de waarde van informatie in de loop van de tijd veranderen. Ook het niveau van dreiging kan veranderen. Daardoor kunnen de benodigde beschermingsmaatregelen veranderen.

2.2 Classificeren van informatie

Deze paragraaf beschrijft uitgangspunten, verantwoordelijkheden en classificatie niveaus.

2.2.1 Uitgangspunten

- Alle processen hebben een eigenaar.
- De (gemandateerd) proceseigenaar bepaalt de classificatie (het vereiste beschermingsniveau) en welke restrisico's aanvaardbaar zijn.[4]
- De ibp manager controleert of classificatie in overeenstemming is met de geldende wet en regelgeving. De proceseigenaar is en blijft eindverantwoordelijk voor de classificatie.
- De ibp-manager, in afstemming met proceseigenaren, applicatiebeheerders en ICT, bepaalt wat bij het beschermingsniveau passende beveiligingsmaatregelen zijn.
- Er wordt gestreefd naar een verantwoord, maar zo 'laag' mogelijk classificatieniveau; overbodig hoge classificatie leidt tot onnodige drempels en kosten.
- De ibp-manager beheert het register van alle classificatierapporten en initieert de periodieke review door de proceseigenaar (zie bijlage 3, BIV overeenkomst).

2.2.2 Verantwoordelijkheden en Werkwijze Classificatie

1. De proceseigenaar heeft de eindverantwoordelijkheid voor de uitvoering en het resultaat van de classificatie. De proceseigenaar beslist over (wijzigingen in) functionaliteit, voert op basis daarvan de informatieclassificatie uit en draagt de kosten die verband houden met informatiebeveiliging. De proceseigenaar is verantwoordelijk voor de implementatie en opvolging van de afgesproken beveiligingsmaatregelen.
2. De ibp manager is verantwoordelijk voor beleid, kaders en richtlijnen op het gebied van informatiemanagement en informatiebeveiliging, bepaalt de methode van de informatieclassificatie en risicoanalyse en levert een bijdrage aan het bepalen van de informatieclassificatie in overleg met de functioneel beheerders van de informatie en/of it-voorziening.

De classificatie zal in groepsverband worden uitgevoerd met een aantal betrokkenen, minimaal de proceseigenaar, de ibp manager en een functioneel beheerder. Dit zorgt voor een lerend effect, geeft commitment binnen de groep, zorgt voor samenwerken en vooral voor een goed afgewogen gemiddelde. De ibp manager stelt vervolgens maatregelen voor in overleg met betrokkenen, in ieder geval functioneel beheer, soms ook de (interne/externe) ict-leverancier in verband met de technische mogelijkheden.
De BIV-scores, de (mogelijk) ingevulde vragenlijsten, een samenvatting, de afspraken over te nemen maatregelen en een eventueel vastgesteld restrisico worden door de ibp manager verwerkt in een classificatierapport dat uiteindelijk door de eigenaar formeel wordt vastgesteld (zie bijlage 3, BIV overeenkomst).
In het kader van reproduceerbaarheid en voor bijvoorbeeld audits of om vergelijkingen te kunnen maken bij toekomstige her-classificaties, worden deze classificatierapporten gearchiveerd door de ibp manager.

[4] Afwijkend van SCIPR

2.3 De fasen in het classificatieproces

De drie fasen van de classificatie zijn als volgt:

2.3.1 Inventarisatie (Wat is er?)

De informatieclassificatie start met vaststellen van welke onderwijs- en bedrijfsprocessen gehanteerd worden en welke wet- en regelgeving mogelijke eisen stelt aan het gebruik, distributie en opslag. Denk bijvoorbeeld aan bewaartermijnen en de Algemene Verordening Gegevensbescherming (AVG)., maar ook aan proces-, applicatie, data en technische architectuur documenten.

2.3.2 Niveaubepaling (Wat wil je?)

Aansluitend op de inventarisatie wordt bepaald hoe groot de kans op en de impact van inbreuken is op de BIV kwaliteitscriteria. Deze inschatting leidt tot de eindclassificatie voor beschikbaarheid, integriteit en vertrouwelijkheid. Deze eindklasse is bepalend voor de bijpassende maatregelen.
Vertaald naar stappen in het proces zijn dit:

1. De proceseigenaar bepaalt het niveau van de afzonderlijke BIV kwaliteitscriteria.
2. De ibp manager bestudeert de uitkomst en vormt zich een mening.
3. Proceseigenaar en ibp manager bepalen de uiteindelijke score van de BIV-classificatie
4. De te treffen maatregelen worden overgenomen vanuit de beheersmaatregelen set.

2.3.3 Toetsing van de BIV classificatie (Hoe controleer je dat?)

In deze stap wordt regelmatig bekeken of de beheersmaatregelen ook daadwerkelijk worden toegepast en uitgevoerd. De beheersmaatregelen set bevat ook de audit frequentie en controle op basis van het mbo toetsingskader.

3. Model BIV classificatie

3.1 Toelichting

In de volgende paragrafen worden de onderdelen van de BIV classificatie verder uitgewerkt. De beschikbaarheid zal uitvoerig worden besproken omdat doorgaans de risico's niet of onvoldoende door mbo instellingen worden onderkend. De risico's op het gebied van Integriteit en vertrouwelijkheid zijn voor mbo instellingen inzichtelijk door accountscontroles.
De BIV classificatie en labelling is onderdeel van het Mbo toetsingskader informatiebeveiliging. Met name cluster 1 (beleid en organisatie) bevat een aantal statements die rechtstreeks gekoppeld (geplot) kunnen worden aan dit onderwerp.

3.2 Beschikbaarheid

Als een mbo instelling een beschikbaarheid (herstelbaarheid) van 48 uur afgeeft dan is dat maar voor een klein gedeelte door de instelling zelf te regelen. Voor een groot deel van de keten is de instelling afhankelijk van externe partners.
Onderstaand overzicht laat als voorbeeld zien hoeveel elementen in die keten van belang en dus van invloed zijn op de beschikbaarheid:

Stappen in de technische keten die het mogelijk maken voor een student om in te loggen in SIS (Studenten Informatie Systeem):

	Stap	IT onderdeel	Risico	Kans	Impact	Beheersmaatregel
1	Student logt in met notebook in SIS (student en notebook zijn bekend)	Notebook	Notebook defect	M	K	Helpdesk lost probleem op
2	Access point ontvang signaal	WAP	WAP defect	M	K	Reserve WAP of aanliggende WAP's nemen signaal op
3	Verbinding WAP naar SER	Glasvezel mbo instelling	Breuk	K	K	Verbinding dubbel uitgevoerd of kabel wordt vervangen
4	SER	Switch	Switchdefect SER defect	M K	K H	Reserve switches of NEXT DAY contract
5	Verbinding SER naar MER	Glasvezel mbo instelling	Breuk	K	K	Verbinding dubbel uitgevoerd of kabel wordt vervangen
6	MER	Catalyst 6509	Catalyst defect of MER defect	K K	H H	Reserve Catalyst of NEXT DAY contract
7	Verbinding MER naar Knooppunt (datacenter 1)	Glasvezel extern	Breuk	K	K	Redundante verbinding
8	Knooppunt (datacenter 1)	Catalyst	Defect	K	H	Reserve Catalyst of NEXT DAY contract
9	Verbinding Provider naar aansluitpunt SURFnet	Glasvezel SURFnet	Breuk	K	K	Redundante verbinding
10	SURFnet aansluitpunt bij het ICT-servicecentrum externe instelling	SURFnet hardware	Defect	K	K	Reserve onderdelen
11	Van ICT servicecentrum via de SURFnet backbone kan het verkeer dan via meerdere routes	Glasvezel SURFnet (lichtpad)	Breuk	K	K	Redundante verbinding

	bij 2 backbone-locaties terecht komen					
12	Vancis datacenter 2 in Amsterdam	Datacenter 2 hardware	Calamiteit	K	G	Uitwijk Datacenter 2
13	Via 1 van deze 2 locaties loopt het verkeer dan via verschillende mogelijke SURFnet-routes naar onze PoP op locatie					
14	Vanuit de SURF PoP op locatie loopt het verkeer dan via een verbinding van provider naar het datacentrum van provider in Hengelo alwaar de hard- en software van SIS voor mbo instelling staat.					

Het is niet de bedoeling dat een dergelijk overzicht door een ibp manager wordt gemaakt. Wellicht zijn de basisgegevens beschikbaar in een technisch architectuur plaatje zodat vervolgens een dergelijk overzicht kan helpen om de beschikbaarheid te garanderen onder bepaalde voorwaarden (bijvoorbeeld uitsluiting van calamiteiten). (Zie IBPDOC4, Mbo ibp architectuur).

Beschikbaarheid is een kwaliteitscriterium dat als volgt wordt gedefinieerd:
De mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ict-dienstverlening waarborgen.
Deelaspecten hiervan zijn:

- Continuïteit: de mate waarin de beschikbaarheid van de ict-dienstverlening gewaarborgd is.
- Portabiliteit: de mate waarin de overdraagbaarheid van het informatiesysteem naar andere gelijksoortige technische infrastructuren gewaarborgd is.
- Herstelbaarheid: de mate waarin de informatievoorziening tijdig en volledig hersteld kan worden.

De classificatie indeling Laag, Midden en Hoog kan als volgt worden vastgesteld zoals verwoord in de onderstaande tabel. Nogmaals voor de volledigheid: dit is een voorstel waar een mbo instelling van kan afwijken.

	Classificatie indeling	**Classificatie gevolg**	**Beheersmaatregel**
Beschikbaarheid	Beschikbaarheid **Laag**	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan **1 week** brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.	• Beschikbaarheid netwerk standaard. • Standaard back up en restore test
	Beschikbaarheid **Midden**	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan **48 uur**[5] brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.	• Beschikbaarheid netwerk standaard. • Regelmatig back up en restore test • Risico analyse op de keten uitgevoerd (zie voorbeeld) • Reserve onderdelen voor MER en SER aanwezig
	Beschikbaarheid **Hoog**	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan **4 uur** brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.	• Standaard netwerk plus extern netwerk • Regelmatig back up en restore test • Extern netwerk beschikbaar

Toelichting: De meeste processen kunnen geclassificeerd worden op het niveau Midden. Met andere woorden een herstel periode van 2 dagen wordt gegarandeerd, dit geldt echter niet als er sprake is van een

[5] HO: 24 uur

calamiteit (brand, explosie, overstroming, aardbeving, etc.). Voor sommige processen kan een beschikbaarheid Hoog worden afgesproken. Zelfs bij calamiteiten kan dan worden teruggevallen op een extern netwerk. Voorbeeld is het proces communicatie (e-mail en website) dat binnen 4 uur weer op devices beschikbaar is, weliswaar niet op het eigen netwerk maar wel op de netwerken van externe providers (KPN, Vodafone, etc.).
Op een kleine locatie, die niet redundant is verbonden, kan mogelijkerwijs alleen een beschikbaarheid Laag worden afgegeven op basis van kostenoverwegingen.

Audit: Het cluster 4 (Continuïteit) bevat een aantal statements dat betrekking heeft op het kwaliteitscriterium beschikbaarheid. Met name statement 4.15,[6] Beschikbaarheid van informatie verwerkende systemen, sluit hier bij aan. Het is wenselijk om ten minste 1 maal per jaar dit te auditen.

3.3 Integriteit

Integriteit is een kwaliteitscriterium dat als volgt wordt gedefinieerd:
De mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de IT-dienstverlening waarborgen.
Deelaspecten hiervan zijn:

- Juistheid: de mate waarin overeenstemming van de presentatie van gegevens/informatie in IT-systemen ten opzichte van de werkelijkheid is gewaarborgd.
- Volledigheid: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is.
- Waarborging: de mate waarin de correcte werking van de IT-processen is gewaarborgd.

De integriteit van informatie wordt voortdurend gecontroleerd door verschillende in- en externe functionarissen binnen een mbo instelling. Denk aan:

- Bekostigingscontrole door de accountant;
- Jaarrekeningcontrole door de accountant,
- Staat van de Instelling door de Inspectie,
- Etc.,

De proceseigenaren en ibp manager maken dan ook dankbaar gebruik van deze goedkeurende verklaringen van deze externe accountants en inspectie. Een aanvullende controle is dan ook niet noodzakelijk.

Een belangrijk aandachtspunt voor de ibp manager samen met de verantwoordelijke voor technisch en functioneel beheer is toezien op de integriteit van de identiteit en de rol van medewerkers van de organisatie. Dit is van groot belang voor een correcte toegangscontrole op applicaties en netwerken. De afdeling personeelszaken speelt een belangrijke rol in het aanleveren van informatie voor een correcte inregeling van de betreffende toegangsrechten. Immers de rol of functie is, mede, bepalend voor het toekennen van deze rechten. En omdat deze nog wel eens wijzigen tijdens de carrière van een medewerker is een adequate check op de integriteit hiervan cruciaal.
Applicaties hebben vaak ook toegang tot informatie op basis van slimme koppelingen, uiteraard moet deze toegang ook regelmatig worden gecontroleerd.

In de onderstaande tabel is per classificatie indeling een classificatiegevolg beschreven met de daarbij behoren beheersmaatregel. Dit is wederom een voorstel waar een mbo instelling van kan afwijken.

[6] Zie: Toetsingskader ib: clusters 1 t/m 6 (IBPDOC3)

	Classificatie indeling	Classificatie gevolg	Beheersmaatregel
Integriteit	Integriteit **Laag**	Het bedrijfsproces staat **enkele** integriteitsfouten toe.	• Application controls + business rules Zie toelichting
	Integriteit **Midden**	Het bedrijfsproces staat **zeer weinig** integriteitsfouten toe. Bescherming van integriteit is absoluut noodzakelijk.	• Application controls + business rules • Manual controls
	Integriteit **Hoog**	Het bedrijfsproces staat **geen** integriteitsfouten toe.	• Application controls + business rules • Manual controls • 4 ogen principe

Toelichting: Application controls + business rules zijn beheersmaatregelen die door de applicatie (-instelling) worden opgelegd. Bijvoorbeeld bij het veld postcode kunnen alleen 4 cijfers en 2 letters worden ingevoerd (application control) al dan niet voorzien van een spatie tussen de cijfers en letters (business rule).
Manual controls zijn handmatige controles door medewerkers van de mbo instelling. Bijvoorbeeld medewerkers controleren aan de hand van een paspoort of id kaart de juistheid van de gegevens van de studenten. Zij noteren, bijvoorbeeld, het bsn van de student omdat kopiëren van een paspoort of ID verboden is.

Audit: Het cluster 5 (Toegangsbeveiliging en integriteit) bevat een aantal statements (5.4 en 5.5) die betrekking hebben op het kwaliteitscriterium integriteit. Het is noodzakelijk om aan te sluiten bij de audits van de accountant en de kwaliteitszorgmedewerker en een eigen audit uit te voeren op de juistheid van de identiteit van de medewerkers met de bijbehorende rollen.

3.4 Vertrouwelijkheid

Vertrouwelijkheid is een kwaliteitscriterium dat als volgt wordt gedefinieerd:
De mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.
Deelaspecten hiervan zijn:

- Autorisatie: de mate waarin de adequate inrichting van bevoegdheden gewaarborgd is.
- Authenticiteit: de mate waarin de adequate verificatie van geïdentificeerde personen of apparatuur gewaarborgd is.
- Identificatie: de mate waarin de mechanismen ter herkenning van personen of apparatuur gewaarborgd zijn.
- Periodieke controle op de bestaande bevoegdheden. Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.

Een lage vertrouwelijkheid betekent dat externen toegang hebben tot openbare informatie zoals bijvoorbeeld de informatie die te vinden is op een website van een mbo instelling. Voor medewerkers of studenten is dit de interne informatie die voor alle medewerkers en studenten beschikbaar is.
Vertrouwelijkheid Midden duidt op de informatie die gekoppeld is aan een rol van een medewerker of de opleiding van een student. Hier valt ook de informatie onder die persoonsgebonden is, zoals e-mail. Apart inloggen is noodzakelijk. Uiteraard kan dit vereenvoudigd zijn doordat er gebruik gemaakt wordt van een Single Sign On methodiek.
Vertrouwelijkheid hoog is vereist bij de verwerking van zeer gevoelige informatie. Te denken valt aan Zorgdossiers, examenconstructie, examenresultaten registratie, loonbeslag bij medewerkers, gesprekscyclus, reorganisatieplannen, etc. Informatie die geclassificeerd wordt met Vertrouwelijkheid Hoog is doorgaans ook privacy gevoelig, omgekeerd is dat echter niet altijd het geval. Een reorganisatie die leidt tot het ontslag van 40% van de medewerkers is niet privacy gevoelig ervan uitgaande de namen van de collega's die moeten afvloeien nog niet zijn ingevuld.

Zoals bij integriteit al is aangegeven is het van groot belang dat op basis van rol en functie de juiste rechten worden toegekend aan een medewerker.
Nieuwe medewerkers (joiners) krijgen rechten die bij hun functie horen. Als een medewerker vertrekt (leavers) worden deze rechten ingetrokken. Het grote probleem zit bij collega's die een nieuwe functie en/of een nieuwe rol krijgen of waarbij een rol wordt ingetrokken. Deze "changers" behouden vaak rechten die behoren bij een eerdere rol of functie, hetgeen kan leiden tot een informatiebeveiliging of privacy risico.

Een sluitende procedure voor het toekennen en intrekken van rechten plus een regelmatige controle van de autorisatiematrix is dan ook noodzakelijk.

In de onderstaande tabel is per classificatie indeling een classificatiegevolg beschreven met de daarbij behoren beheersmaatregel. Dit is wederom een voorstel waar een mbo instelling van kan afwijken.

	Classificatie indeling	**Classificatie gevolg**	**Beheersmaatregel**
Vertrouwelijkheid	Vertrouwelijkheid **Laag**	Informatie die toegankelijk mag of moet zijn voor **alle of grote groepen** medewerkers of studenten. Vertrouwelijkheid is gering.	• Generieke toegangsbeveiliging
	Vertrouwelijkheid **Midden**	Informatie die alleen toegankelijk mag zijn voor een **beperkte groep** gebruikers. De informatie is vertrouwelijk.	• Autorisatiematrix
	Vertrouwelijkheid **Hoog**	Dit betreft zeer vertrouwelijke informatie, alleen bedoeld voor **specifiek benoemde personen**, waarbij onbedoeld bekend worden buiten deze groep grote schade kan toe brengen.	• Autorisatiematrix • Eventueel aanvullende maatregelen zoals 2-weg authenticatie[7] en/of encryptie[8]

Toelichting: Generieke toegangsbeveiliging houdt in dat iedere student of medewerkers die ingeschreven is of een arbeidsovereenkomst heeft toegang heeft tot het netwerk.
Autorisatiematrix is gebaseerd op de arbeidsovereenkomst (functie en rollen) of de onderwijs overeenkomst.
2-weg authenticatie betekent dat niet alleen een wachtwoord vereist maar, bijvoorbeeld, een cijfercode die op verzoek wordt toegezonden per sms (vergelijk dit meteen digitale betaling via een bank account).

Audit: Het cluster 5 (Toegangsbeveiliging en integriteit) bevat een aantal statements die betrekking hebben op het kwaliteitscriterium vertrouwelijkheid. Maar ook cluster 6 (Controle en logging) bevat een aantal statements die de controle op vertrouwelijkheid mogelijk maken.[9]

[7] 2-weg authenticatie: medewerkers kunnen alleen inloggen nadat ze twee handelingen hebben uitgevoerd. Bijvoorbeeld nadat ze zijn ingelogd moet er ook nog een code worden ingevoerd die per sms is toegezonden.
[8] Encryptie: informatie is versleuteld en kan alleen door een aangewezen ontvanger worden gelezen.
[9] Zie: Toetsingskader ib: clusters 1 t/m 6 (IBPDOC3)

4. PIA en privacy

4.1 Risico's bij niet voldoen aan de AVG

Het niet-voldoen aan de AVG leidt tot schending van de informationele privacy van degene op wie de gegevens betrekking hebben. Dit kan verregaande (negatieve) consequenties hebben: niet alleen voor de persoon in kwestie, maar ook voor de betreffende organisatie. Zo kan het niet-voldoen aan de AVG (of zelfs de schijn daarvan) leiden tot negatieve publiciteit en imagoschade voor de organisatie. En niet te vergeten: het niet-voldoen aan de AVG kan leiden tot juridische consequenties, waaronder:

- Een door de rechter opgelegd verbod op het handelen van de organisatie en de verplichting tot het treffen van herstelmaatregelen bij (dreiging van) schade;
- Vergoeding van de schade die de betrokkene heeft geleden;
- Een bestuurlijke boete, opgelegd door de AP;
- Een last onder bestuursdwang of dwangsom door de AP.
    - Een last onder bestuursdwang houdt in dat de AP kan eisen de overtreding te beëindigen en bij het uitblijven daarvan dit 'persoonlijk' kan komen doen;
    - een last onder dwangsom houdt in dat de organisatie nog tijd heeft om de overtreding (gedeeltelijk) te herstellen, en de dwangsom wordt opgelegd bij het uitblijven van het (gedeeltelijk) herstel.
- Strafrechtelijke vervolging door het Openbaar Ministerie.

4.2 Meldplicht Datalekken

Op 1 januari 2016 is de privacy wet gewijzigd. Naast de naamswijziging van het CBP (college bescherming persoonsgegevens) in AP (autoriteit persoonsgegevens) is de boetebevoegdheid uitgebreid. Sinds 1 januari 2016 kan de AP bij schending van meer algemene verplichtingen van de AVG boetes opleggen, bijvoorbeeld als persoonsgegevens niet op een behoorlijke en zorgvuldige manier zijn verwerkt of langer worden bewaard dan noodzakelijk. De bedragen van de boetes komen ook aanzienlijk hoger te liggen en kunnen oplopen tot maximaal €820.000 of, als de omzet hoger is, 10% van de wereldwijde omzet van de organisatie.

Met de wetswijziging zijn organisaties verplicht om een datalek te melden bij de AP en op te nemen in de bewerkersovereenkomst. Onder de AVG moeten organisaties allang passende technische en organisatorische maatregelen getroffen hebben om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking (en/of deze opgenomen hebben in de bewerkersovereenkomsten). Met de komst van de Meldplicht datalekken wordt elke inbreuk die leidt tot (de aanzienlijke kans dat) ernstige nadelige gevolgen voor de bescherming van persoonsgegeven intreden, aangemerkt als een datalek dat gemeld moet worden aan in ieder geval de AP en in sommige gevallen ook aan de betrokkene. Met andere woorden: elk beveiligings-incident waarbij persoonsgegevens misbruikt zouden kunnen (gaan) worden, is dus een datalek dat 'onverwijld' gemeld moet worden. Hierbij kun je denken aan bijvoorbeeld hacking of verlies van een usb-stick of laptop, of een smartphone met werk mail. Hoewel er in de AVG al eisen staan opgenomen met betrekking tot de kennisgeving van de datalek, kunnen bij Algemene maatregel van bestuur hierover nadere regels gesteld worden.
Een datalek zoals hierboven bedoeld moet onverwijld gemeld worden bij de AP en aan een aantal inhoudelijke voorwaarden voldoen. Volgens de richtsnoeren van de AP wordt met 'onverwijld' drie dagen bedoeld. Deze voorwaarden zijn zodanig dat het uitermate raadzaam is de organisatie tijdig op orde te brengen en goed in te richten op het ontdekken, beoordelen en vastleggen van inbreuken. Niet de inbreuk immers wordt bestraft, wel het niet (correct) melden ervan (zie bijlage 5: AP publiceert definitieve beleidsregels meldplicht datalekken).

Heeft een inbreuk waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkenen, dan moeten ook zij een gespecificeerde kennisgeving en een advies ontvangen. Dat advies moet gaan over wat de betrokkene zelf eventueel nog kan doen om schade te beperken. Het bijzondere is hier dat de verantwoordelijke dus zelf een inschatting moet maken van de kans op ongunstige gevolgen voor betrokkenen; en deze inschatting moet kunnen verantwoorden aan de AP, wanneer wordt besloten niet te melden.

4.3 Privacy Impact Assessment

Definitie PIA

Een Privacy Impact Assessment (PIA) is een toets waarmee op een gestructureerde en heldere manier in beeld brengen privacy risico's in beeld kunnen worden gebracht. Het daarbij om te onderzoeken wat impact is van het gebruik van persoonsgegevens op de privacy van de betrokkenen, wat de risico's zijn voor de organisatie en of er alternatieven zijn die minder impact hebben. Doorgaans is de PIA een model in de vorm van vragenlijsten die de privacy risico's van een specifieke verzameling alsmede de (verdere) verwerking en bewaring van persoonsgegevens op systematische wijze identificeert en lokaliseert. Onder risico wordt verstaan: de kans dat een incident zich voordoet, vermenigvuldigd met de impact die dit incident heeft. Overigens is risico = kans x impact wel een erg theoretische definitie; in praktijk zal het vaak gaan om 'de kans dat een incident zich voordoet in relatie met de potentiele impact die dit incident heeft'. Sommige incidenten hebben een grote impact, maar als de kans verwaarloosbaar is dat dit voorkomt dan is dit niet zo'n groot risico (en andersom: als de kans heel groot is maar de impact is gering, dan is het risico niet zo heel groot).

Juridische betekenis PIA

Momenteel is het uitvoeren van een PIA alleen nog verplicht voor de rijksoverheid bij de ontwikkeling van nieuwe beleid en wetgeving waarbij de bouw van nieuwe ict-systemen of de aanleg van grote databestanden wordt voorzien[10]. Vanaf 25 mei 2018 wordt het verplicht volgens artikel 35 van de AVG om te beoordelen wat het effect van het beoogde gebruik van persoonsgegevens is op de bescherming van persoonsgegevens. In de Nederlandse vertaling van de AVG wordt deze PIA een 'gegevensbeschermingseffectbeoordeling' (gbeb) genoemd. Deze beoordeling wordt uitgevoerd wanneer er persoonsgegevens worden gebruikt die waarbij er nieuwe technologieën worden gebruikt, of als het gebruik van de persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen (rekening houdend met de aard, de omvang, de context en het doel van het gebruik van de persoonsgegevens). Een gegevensbeschermingseffectbeoordeling is vanaf 25 mei 2018 in ieder geval verplicht in geval van:

- Geautomatiseerde besluitvorming: als ict-systemen automatisch beslissingen nemen op basis van een profiel dat over een betrokkene is samengesteld.
- Als er op grote schaal bijzondere persoonsgegevens worden gebruikt (zoals gezondheid, religie).
- Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

Een gbeb bevat ten minste de volgende onderdelen:

1. Een systematische beschrijving van de beoogde gebruik van de persoonsgegevens, en het beoogd doel daarvan;
2. Een beoordeling van de noodzaak en de evenredigheid van het gebruik in relatie tot het doel;
3. Een beoordeling van de risico's voor de privacy van de betrokkenen;
4. Een beoordeling van de te nemen maatregelen om de risico's te beperken (zoals veiligheidsmaatregelen, dataminimalisatie, privacy-enhancing-technologies zoals pseudonimisering).

Als er binnen de instelling een FG is aangesteld, is deze betrokken bij de PIA of gbeb.

Het gebruik van de uitkomsten van de PIA.

Een organisatie kan de uitkomsten van een PIA gebruiken om te bepalen welke (technische en/of organisatorische) maatregelen passend en nodig zijn om de betreffende risico's te verminderen of weg te nemen. Uit een PIA zelf blijkt niet welke concrete maatregelen er genomen moeten worden. Maar door de risico's van een gegevensverwerking in kaart te brengen kan een organisatie op basis daarvan bepalen welke maatregelen nodig en passend zijn.

Het is raadzaam om een PIA in een zo vroeg mogelijk stadium uit te voeren, zodat een organisatie maatregelen kan nemen voordat het risico's zich daadwerkelijk manifesteren en er schade ontstaat voor de organisatie en/of betrokkene. Op deze manier kunnen ook kosten bespaard worden: het tijdig aanpassen van een verwerking is immers goedkoper dan de kosten van het achteraf aanpassen van een afgeronde gegevensverwerking en een eventueel daarmee gepaard gaande schadevergoeding.

Een PIA maakt echter niet duidelijk wat een organisatie allemaal concreet waar moet regelen om volledig aan de AVG te voldoen: de PIA brengt 'slechts' risico's in kaart en hoewel dit zeer nuttig is, wordt hiermee niet volledig aan de AVG voldaan, omdat de AVG meer eist dan alleen risicobeheersing.

10 Toetsmodel PIA Rijksoverheid: http://www.rijksoverheid.nl/documenten-en-publicaties/publicaties/2013/06/24/toetsmodel-privacy-impact-assessment-pia-rijksdienst.html

4.4 Aanpak mbo sector

Voor de mbo sector is een mbo-PIA tool beschikbaar die door Kennisnet en SURF ontwikkeld is. Voor een drietal[11] applicaties is reeds een PIA uitgevoerd.
Medio 2016 is er een format bewerkersovereenkomst beschikbaar voor de mbo sector. Onderdeel hiervan is de "Meldplicht datalekken". In bijlage 5, AP publiceert definitieve beleidsregels meldplicht datalekken, is een en ander na te lezen.

De stappen 4 t/m 6 van de ibp (security) architectuur gaan hier dieper op in. Stap 4 geeft aan of er wel of niet een PIA is uitgevoerd, en als dit het geval is dan kan er worden bepaald of het systeem (applicatie) privacy gevoelige informatie verwerkt.
Indien dit het geval is dan zal de leverancier van het systeem een bewerkersovereenkomst moeten kunnen overleggen (dit is toch alleen zo als de leverancier ook als bewerker fungeert, dat is niet bij elke leverancier toch zo). en als de leverancier geen eigen bewerkersovereenkomst heeft dan kan gebruik worden gemaakt van het format van Kennisnet of SURF. Daarmee is stap 5 dan afgerond.
Stap 6 toetst vervolgens of de leverancier de bewerkersovereenkomst ook daadwerkelijk toepast. Deze toetsing vindt nu plaats op basis van een globale vragenlijst of certificatieschema. In de toekomst zal deze mogelijk vervangen worden door internationaal erkende normenkaders (ISO 27002 en ISAE3402).

5. Voorbeeld ibp (security) architectuur

5.1 Inleiding

In hoofdstuk 1 is aangegeven hoe we komen tot de ibp architectuur, die ook wel security architectuur wordt genoemd. In de hoofdstukken 2, 3 en 4 is de BIV classificatie en de PIA toegelicht. In dit hoofdstuk wordt iedere stap, inclusief BIV en PIA, uitgewerkt om uiteindelijk te komen tot de ibp architectuur. De stappen op een rij:

	#	Stappen	Gehanteerde bron	Bron	
BIV classificatie	1	Voeg aan alle processen uit het (gekozen) procesplaatje een nummer en een proces-eigenaar toe.	Proces architectuur	Triple A en HORA	Proceseigenaren
	2	Koppel het proces aan een applicatie en benoem de data uitwisseling (globaal)	Applicatie en data architectuur	Best practices mbo sector, IBPDOC4	
	3	Voer de BIV classificatie uit op het proces samen met de proces eigenaar.	• SCIPR: Leidraad Classificatiemode (versie 2.0) • aanvullingen in dit documenten	SCIPR en IBPDOC14	
PIA en privacy	4	Maak een PIA voor de gehanteerde applicatie, die het proces ondersteund, zodat de privacy risico's in kaart worden gebracht.	Privacy Impact Assessment (versie 2.0)	Integrale Veiligheid Hoger Onderwijs, PIA tool 3.0	Leveranciers
	5	Overleg een bewerkersovereenkomst, incl. datalekken.	Bewerkersovereenkomst: • model Kennisnet • model SURF • model leverancier	Kennisnet, SURF , IBPDOC28	
	6	Geef een oordeel van het ibp beleid van de externe leverancier van de applicatie.	Certificeringsschema.	Kennisnet	

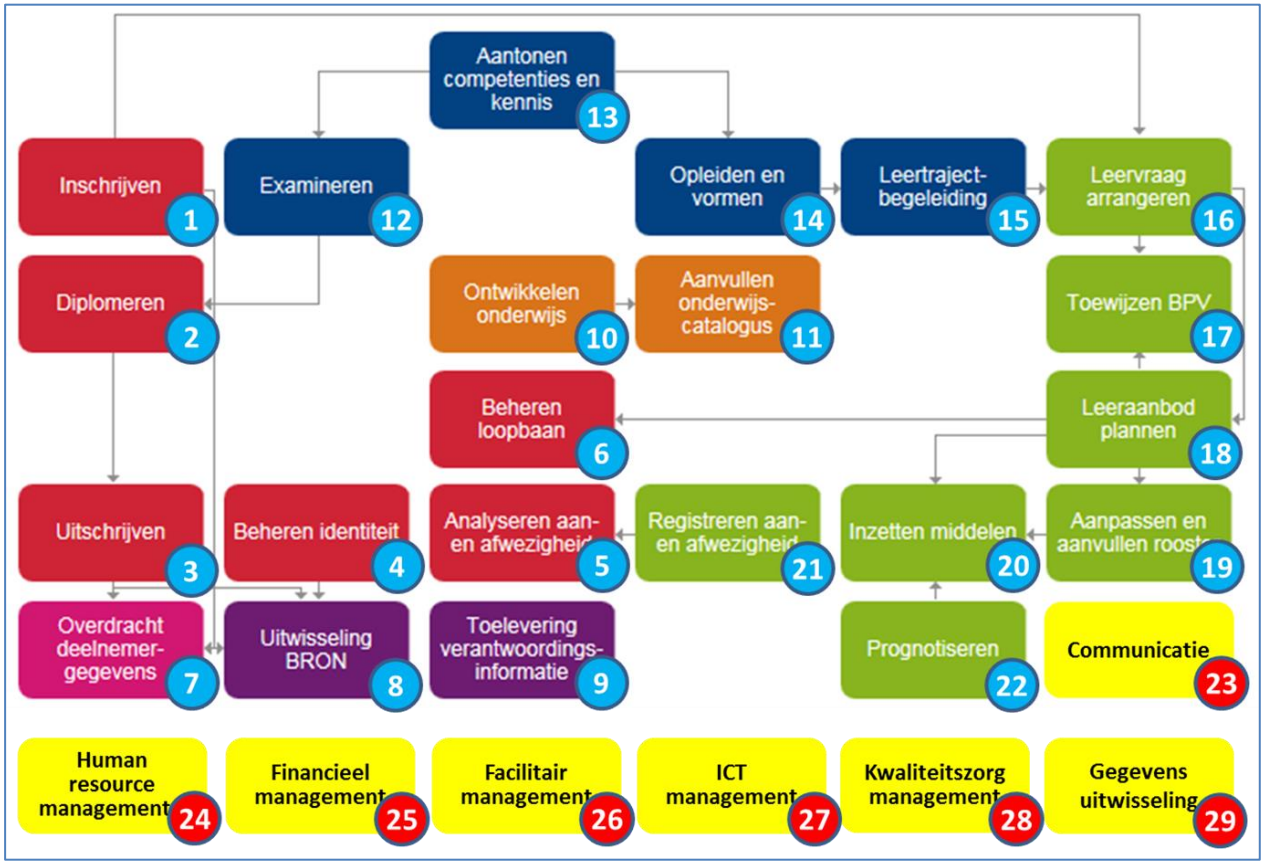
[11] Er zijn een drietal PIA uitgevoerd voor een Studenten Informatie Systeem, en HR pakket en een Online leren pakket.

In dit hoofdstuk wordt een voorbeeld uitgewerkt waarbij er voor gekozen is om geen namen van applicaties te noemen.

5.2 Stap 1: Vaststellen proceslandschap

	#	Stappen	Gehanteerde bron	Bron en auteurs	
BIV classifica-	1	Voeg aan alle processen uit het (gekozen) procesplaatje een nummer en een proces-eigenaar toe.	Proces architectuur	Triple A en HORA	Proceseigena-
	2	Koppel het proces aan een applicatie en benoem de data uitwisseling (globaal)	Applicatie en data architec-tuur	Best practices mbo sector, IBPDOC4	

In het document IBPDOC4 Mbo ibp architectuur is een voorbeeld gegeven van een proceslandschap. Uiteraard is het wenselijk dat iedere mbo instelling gebruikt maakt van de eigen procesarchitectuur. In dit document wordt de triple A procesarchitectuur gehanteerd die wordt aangevuld vanuit de HORA met een aantal bedrijfsprocessen die geel gearceerd zijn. Alle processen zijn voorzien van een procesnummer in en een licht blauw vlak voor de triple A processen en in een rood vlak voor de aanvullende processen.



Figuur 3:Proceslandschap Triple A plus secundaire processen (zie IBPDOC4 Mbo referentie architectuur)

De procesarchitectuur vormt de kern voor de ibp architectuur en wordt aangevuld met:

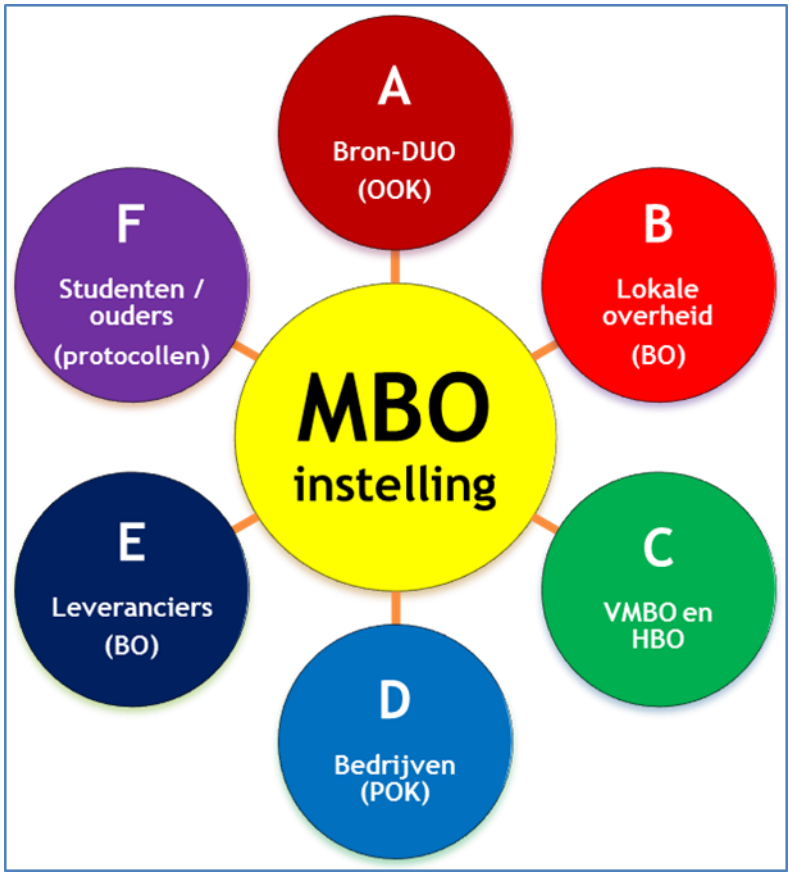
1. De naam en nummer van het proces (bijvoorbeeld *Proces:* **Inschrijven**).
2. De proceseigenaar. In dit schema wordt niet de naam van de proceseigenaar gehanteerd maar de functie. Uiteraard kan een onderwijsinstelling daarvan afwijken (bijvoorbeeld *Proceseigenaar:* **Directeur Onderwijs**).

Proces: **Inschrijven**	**1**
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie	*Privacy (PIA-BO-PB)*

5.3 Stap 2: Koppelen systeem (applicatie) aan proces

Zoals in het schema is weergegeven kan de data benoemd worden op basis van de applicatie en data architectuur.

	#	Stappen	Gehanteerde bron	Bron en auteurs	
BIV classificatie	1	Voeg aan alle processen uit het (gekozen) procesplaatje een nummer en een proces-eigenaar toe.	Proces architectuur	Triple A en HORA	Proceseigenaren
	2	Koppel het proces aan een applicatie en benoem de data uitwisseling (globaal)	Applicatie en data architectuur	Best practices mbo sector, IBPDOC4	
	3	Pas de BIV classificatie toe op het proces.	• SCIPR: Leidraad Classificatiemode (versie 2.0) • aanvullingen werkgroep	SCIPR en IBPDOC14	



Figuur 4: Schematische weergave van data uitwisseling met externe partners.

Tijdens stap 2 wordt de procesarchitectuur gekoppeld aan de applicatiearchitectuur. Een proces kan door meerdere applicaties worden ondersteund. In dit voorbeeld is gekozen om slechts één applicatie toe te wijzen aan een proces. Een applicatie kan overigens wel meerdere processen ondersteunen. In het voorbeeld ondersteunt Student Informatie Systeem meerdere processen.

Aan de hand van het schema zoals beschreven in de het document Mbo ibp architectuur IBPDOC4 wordt heel globaal beschreven welke uitwisseling plaats vindt naar externe partners.

	Studenten Informatie				Personeel informatie		
	Studenten informatie Naw Groepsdeel-name Opleidingen	**Studenten informatie** Resultaten incl. diploma en resultaten-lijst	**Studenten informatie** Presentie Overeenkom-sten	**Opleidings-informatie** Crebo's en keu-zedelen uit BRON Resultaatstruc-turen	**Basis gege-vens** Naw Bevoegdheid VOG	**Salarisgege-vens** Salarisschaal Gewerkte uren Declaraties Ziekteverzuim	**Gespreks-cyclus** Beoordeling Functioneren Carrière
A: Bron/DUO	DUO	DUO	DUO	DUO	Leraren re-gister		
B: Lokale overheid	Gemeen-ten		Gemeen-ten				
C: VMBO en HBO	VMBO en HBO	HBO		HBO			
D: Bedrij-ven	BPV bedrij-ven		BPV bedrij-ven	BPV bedrij-ven	Belasting-dienst ABP	Belasting-dienst ABP	
E: Leve-ranciers	SIS leverancier	SIS leverancier	SIS leverancier	SIS leverancier	HR-pakket leverancier	HR-pakket leverancier	HR-pakket leverancier

De applicatiearchitectuur koppelt nu de processen aan de applicaties. De naam van de applicatie wordt nu op-genomen in de ibp architectuur (SIS).

Proces: **Inschrijven** (SIS)	**1**
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie	*Privacy (PIA-BO-PB)*

5.4 Stap 3: Vaststellen BIV classificatie

Tijdens de derde stap wordt de BIV classificatie gemaakt door de proceseigenaar, de functioneel beheerder en de informatiemanager. Dit is toegelicht in de hoofdstukken 2 en 3.

	#	Stappen	Gehanteerde bron	Bron	
BIV classifi-	2	Koppel het proces aan een applicatie en benoem de data uitwisseling (globaal)	Applicatie en data architec-tuur	Best practices mbo sector, IBPDOC4	**Proceseigen.**
	3	Pas de BIV classificatie toe op het proces.	• SCIPR: Leidraad Classifi-catiemode (versie 2.0) • aanvullingen werkgroep	SCIPR en IBPDOC14	
PIA en	4	Maak een PIA voor de gehan-teerde applicatie, die het proces ondersteund, zodat de privacy risico's in kaart worden gebracht.	Privacy Impact Assessment (versie 2.0)	Integrale Veiligheid Hoger On-derwijs, PIA tool 3.0	**Leveranc.**

Uitkomst is een classificatie op:

1. Beschikbaarheid (Hoog, Midden of Laag)
2. Integriteit (Hoog, Midden of Laag)
3. Vertrouwelijkheid (Hoog, Midden of Laag)

Aan de ibp-architectuur wordt de classificatie toegevoegd (bijvoorbeeld *BIV classificatie* **M – M – M**):
Dit is uiteraard een voorbeeld classificatie.

Proces: **Inschrijven** (SIS)	**1**
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie **M – M – M**	*Privacy (PIA-BO-PB)*

5.5 Stap 4: Uitvoeren PIA

	#	Stappen	Gehanteerde bron	Bron en auteurs	
	3	Pas de BIV classificatie toe op het proces.	• SCIPR: Leidraad Classificatiemode (versie 2.0) • aanvullingen werkgroep	SCIPR en IBPDOC14	
PIA en privacy	4	Maak een PIA voor de gehanteerde applicatie, die het proces ondersteund, zodat de privacy risico's in kaart worden gebracht.	Privacy Impact Assessment (versie 2.0)	Integrale Veiligheid Hoger Onderwijs, PIA tool 3.0	**Leveranciers**
	5	Overleg een bewerkersovereenkomst, incl. datalekken.	Bewerkersovereenkomst: • model Kennisnet • model SURF • model leverancier	Kennisnet, SURF , IBPDOC28	

Tijdens de vierde stap wordt een Privacy Impact Assessment uitgevoerd door de ibp manager en een jurist (bedrijfsjurist of Functionaris Gegevensbescherming of Privacy Officer of …). De uitkomst wordt gedeeld met de proceseigenaar. De uitkomst kan ertoe leiden dat het niveau van de vertrouwelijkheid moet worden verhoogd. Als de privacy wetgeving van toepassing is dan dit weergegeven met **Ja** indien dit niet het geval is dan wordt **Nee** vermeld (bijvoorbeeld *Privacy (PIA-BO-PB)* **Ja**).

Proces: **Inschrijven** (SIS)	**1**
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie **M – M – M**	*Privacy (PIA-BO-PB)* **Ja**

5.6 Stap 5: Toetsen bewerkersovereenkomsten (incl. datalekken)

Deze stap bepaalt of en zo ja welke bewerkersovereenkomst door de leverancier moet worden overlegd en moet worden ondertekend door de verantwoordelijke medewerker binnen de onderwijsinstelling.

	#	Stappen	Gehanteerde bron	Bron	
PIA en privacy	4	Maak een PIA voor de gehanteerde applicatie, die het proces ondersteund, zodat de privacy risico's in kaart worden gebracht.	Privacy Impact Assessment (versie 2.0)	Integrale Veiligheid Hoger Onderwijs, PIA tool 3.0	Leveranciers
	5	Overleg een bewerkersovereenkomst, incl. datalekken.	Bewerkersovereenkomst: • model Kennisnet • model SURF • model Leverancier	Kennisnet, SURF , IBPDOC28	
	6	Geef een oordeel van het ibp beleid van de externe leverancier van de applicatie.	Certificeringsschema.	Kennisnet	

Om te onderzoeken of een bewerkersovereenkomst verplicht is moeten de externe koppelingen bekend zijn. De tabel uit stap 2 biedt hier voldoende houvast. Indien een bewerkersovereenkomst noodzakelijk is vanuit AVG dan wordt dat in de tabel weergegeven met een geel gearceerd veld.

	Studenten Informatie				Personeel informatie		
	Studenten informatie Naw Groepsdeelname Opleidingen	**Studenten informatie** Resultaten incl. diploma en resultatenlijst	**Studenten informatie** Presentie Overeenkomsten	**Opleidingsinformatie** Crebo's en keuzedelen uit BRON Resultaatstructuren	**Basis gegevens** Naw Bevoegdheid VOG	**Salarisgegevens** Salarisschaal Gewerkte uren Declaraties Ziekteverzuim	**Gesprekscyclus** Beoordeling Functioneren Carrière
A: Bron/DUO	DUO	DUO	DUO	DUO	Leraren register		
B: Lokale overheid	Gemeenten		Gemeenten				
C: VMBO en HBO	VMBO en HBO	HBO		HBO			
D: Bedrijven	BPV bedrijven		BPV bedrijven	BPV bedrijven	Belastingdienst ABP	Belastingdienst ABP	
E: Leveranciers	SIS leverancier	SIS leverancier	SIS leverancier	SIS leverancier	HR-pakket leverancier	HR-pakket leverancier	HR-pakket leverancier

De ibp architectuur wordt nu aangevuld met het type bewerkersovereenkomst (BO) (bijvoorbeeld *BO* **E**) :

E Eigen bewerkersovereenkomst
K Kennisnet leveranciers overeenkomst
S SURF juridisch normenkader
G Geen bewerkersovereenkomst

Proces: **Inschrijven** (SIS)	**1**
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie **M – M – M**	*Privacy (PIA-BO-PB)* **Ja – E**

5.7 Stap 6: Beoordelen leverancier

De laatste stap staat in het teken van een globale beoordeling van de leverancier. In de bewerkersovereenkomst vermeldt de leverancier allerlei punten die de informatiebeveiliging en privacy waarborgen, maar hij zal ook moeten aantonen dat dit correct is.

	#	Stappen	Gehanteerde bron	Bron	
PIA en privacy	5	Overleg een bewerkersover-eenkomst, incl. datalekken.	Bewerkersovereenkomst: • model Kennisnet • model SURF • model leverancier	Kennisnet, SURF , IBPDOC28	**Leveranciers**
	6	Geef een oordeel van het ibp beleid van de externe le-verancier van de applicatie.	Certificeringsschema.	Kennisnet	

Partij voldoet aan Kennisnet checklist **P**rivacy **B**eoordeling (checklist niet opgenomen in dit document) (bijvoorbeeld *PB* **G**).

G Goed
O Onvoldoende
? Geen informatie ontvangen van leverancier

Proces: **Inschrijven** (SIS)	**1**
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie **M – M – M**	*Privacy (PIA-BO-PB)* **J – J – G**

5.8 Stap extra: Benoemen aanvullende risico's

Tijdens deze stap worden aanvullende risico's benoemd. Deze risico's kunnen bijvoorbeeld betrekking hebben op examineren of online leren. Voor examineren is een aanvullend toetsingskader beschikbaar[12].

Uiteindelijk leiden al deze stappen tot een overzichtelijk schema dat de ibp (security) architectuur vormt. In onderstaande plaat een voorbeeld opgenomen zoals die er uit zou kunnen zien. Nogmaals, het is aan de instelling om een eigen schema op te stellen, de waardes in het voorbeeld geven geen wenselijke of te bereiken waardes weer. Dit schema is het eindproduct van dit document IBPDOC14.

[12] Toetsingskader examinering pluscluster 8 (IBPDOC8)

Voorbeeld Informatiebeveiliging en Privacy Architectuur voor de mbo sector (ibp Architectuur)

Proces: **Inschrijven** (SIS)	1
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – H – M	**Ja – E – G**

Proces: **Examineren** (Examen pakket)	12
Proceseigenaar: **Directeur Examenbureau**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – H – H	**Ja – K – G**

Proces: **Aantonen competenties en kennis** (SIS)	13
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – H – M	**Ja – K – G**

Proces: **Opleiden en vormen** (ELO)	14
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – M – M	**Ja – E – O**

Proces: **Leertrajectbegeleiding** (ELO)	15
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – M – M	**Ja – E – O**

Proces: **Leervraag arrangeren** (ELO)	16
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – M – M	**Ja – E – O**

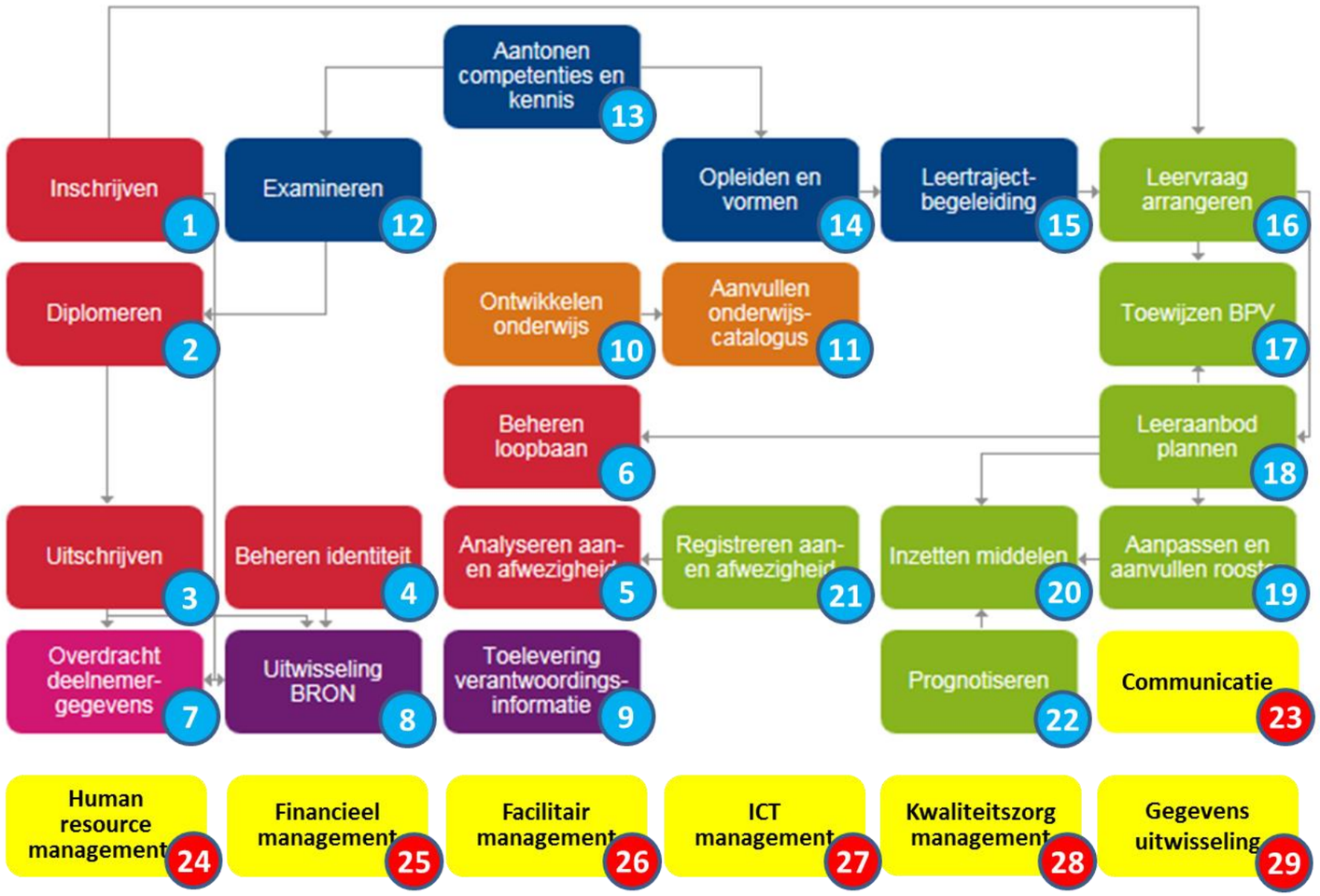
Proces: **Diplomeren** (SIS)	2
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – H – H	**Ja – E – G**

Proces: **Uitschrijven** (SIS)	3
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – H – M	**Ja – E – G**

Proces: **Beheren identiteit** (SIS)	4
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – H – M	**Ja – E – G**

Proces: **Analyseren aan- en afwezigheid** (SIS)	5
Proceseigenaar: **Directeur Marktportaal**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – M – M	**Ja – E – G**

Proces: **Beheren loopbaan** (SIS)	6
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – M – M	**Ja – E – G**



Proces: **Toewijzen BPV** (SIS)	17
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – M – M	**Ja – E – G**

Proces: **Leeraanbod plannen** (SIS)	18
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – M – M	**Ja – E – G**

Proces: **Aanvullen en aanpassen roosters** (roosterpakket)	19
Proceseigenaar: **Directeur Facilitair**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – M – M	**Ja – E – ?**

Proces: **Inzetten middelen** (Facilitair pakket)	20
Proceseigenaar: **Directeur Facilitair**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – M – L	**Nee**

Proces: **Registreren aan- en afwezigheid** (SIS)	21
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – M – M	**Ja – E – G**

Proces: **Overdracht deelnemer gegevens** (SIS)	7
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – M – M	**Ja – E – G**

Proces: **Uitwisseling BRON** (SIS)	8
Proceseigenaar: **Directeur Financiën**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – H – M	**Ja – E – G**

Proces: **Toelevering verant-woordingsinformatie** (SIS)	9
Proceseigenaar: **Directeur Financiën**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – H – M	**Ja – E – G**

Proces: **Ontwikkelen onderwijs** (ELO)	10
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – M – M	**Ja – K – O**

Proces: **Aanvullen onderwijsca-talogus** (ELO)	11
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – H – M	**Ja – K – O**

Proces: **Prognosticeren** (SIS)	22
Proceseigenaar: **Directeur Onderwijs**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – M – M	**Ja – E – G**

Proces: **Communicatie** (e-mail-pakket en website)	23
Proceseigenaar: **Directeur Communicatie**	
BIV classificatie	*Privacy (PIA-BO-PB)*
H – M – H	**Ja – S – G**

Proces: **Human resource management** (HR pakket)	24
Proceseigenaar: **Directeur HR**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – H – H	**Ja – E – G**

Proces: **Financieel management** (Financieel pakket)	25
Proceseigenaar: **Directeur Financiën**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – M – H	**Nee**

Proces: **Facilitair management** (Facilitair pakket)	26
Proceseigenaar: **Directeur Facilitair**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – M – L	**Nee**

Proces: **ICT management** (ICT pakket)	27
Proceseigenaar: **Directeur ICT**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – M – M	**Ja – E – G**

Proces: **Kwaliteitszorg manage-ment** (Kwaliteitszorg pakket)	28
Proceseigenaar: **Directeur Kwaliteitszorg**	
BIV classificatie	*Privacy (PIA-BO-PB)*
M – M – H	**Ja – E – G**

Bijlage 1: Gebruikte termen

Term	Betekenis
Bedrijfsobject	Een bedrijfsobject is een passief element dat vanuit bedrijfsperspectief relevantie heeft [HORA]. De relevante bedrijfsobjecten in deze leidraad zijn gegevensobjecten. Voorbeelden van bedrijfsobjecten in de context van deze leidraad zijn alumnus, begroting en contact.
Beheerder	Een persoon die een systeem (al dan niet beroepsmatig) regelt en onderhoudt [Wikipedia]. In deze leidraad kan het beheren betrekking hebben op informatie, applicaties, databases en systemen in de rol van functioneel, technisch en/of applicatiebeheerder. Ook informatie kan een beheerder hebben.
BIA	Business Impact Analyse Een BIA wordt in het kader van het Business Continuity Management (BCM) gebruikt om de kritieke processen van de niet kritieke processen te scheiden [Wikipedia].
BIV-classificatie	Een BIV-classificatie of BIV-indeling is een indeling waarbij beschikbaarheid, (continuïteit), integriteit (betrouwbaarheid) en vertrouwelijkheid (exclusiviteit) van informatie en systemen wordt aangegeven [Wikipedia].
Beschikbaarheid ***(kwaliteitsaspect)***	De mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ict-dienstverlening waarborgen. Deelaspecten hiervan zijn: Continuïteit: de mate waarin de beschikbaarheid van de it-dienstverlening gewaarborgd is; Portabiliteit: de mate waarin de overdraagbaarheid van het informatiesysteem naar andere gelijksoortige technische infrastructuren gewaarborgd is; Herstelbaarheid: de mate waarin de informatievoorziening tijdig en volledig hersteld kan worden.
Controleerbaarheid ***(kwaliteitsaspect)***	De mogelijkheid om kennis te verkrijgen over de structurering (documentatie) en werking van de it-dienstverlening. Deelaspecten hiervan zijn: Testbaarheid: De mate waarin de integere werking van de it-dienstverlening te testen is; Meetbaarheid: Zijn er voldoende meet- en controlepunten aanwezig; Verifieerbaarheid: De mate waarin de integere werking van een it-dienstverlening te verifiëren is.
Data	Data, ofwel gegevens, zijn objectieve feiten, teksten en getallen waaraan nog geen betekenis is gekoppeld.
Eigenaar	De afdeling/dienst/persoon of rol die over een zaak (stuk grond, voorwerp, hoeveelheid geld enz.) naar eigen goeddunken kan beschikken [naar Wikipedia]. In deze leidraad wordt met de eigenaar diegene bedoeld die het beslisrecht over een proces, applicatie, systeem, gegevenselement et cetera heeft. Wanneer de formeel eigenaar (vaak het College van Bestuur) het beschikkingsrecht overdraagt (mandateert) spreken we van functioneel of gedelegeerd eigenaar. Een eigenaar kan ook bestaan voor een organisatie breed systeem en/of data in een organisatie breed systeem.
Gegevens	Gegevens zijn de objectief waarneembare neerslag of registratie van feiten op een bepaald medium, zodanig dat deze gegevens uitgewisseld en voor langere tijd bewaard kunnen worden [Wikipedia]. Aan deze objectieve feiten is nog geen betekenis gekoppeld.
Informatie	Gegevens worden informatie als de gegevens een betekenis of nieuwswaarde hebben voor de ontvanger.
Integriteit ***(kwaliteitsaspect)***	De mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de it-dienstverlening waarborgen. Deelaspecten hiervan zijn: Juistheid: de mate waarin overeenstemming van de presentatie van gegevens/informatie in it-systemen ten opzichte van de werkelijkheid is gewaarborgd;

	Volledigheid: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is; Waarborging: de mate waarin de correcte werking van de IT-processen is gewaarborgd.
PIA	Een Privacy Impact Assessment (PIA) is een tool dat helpt bij het identificeren van privacy risico's en levert de handvaten om deze risico's te verkleinen tot een acceptabel niveau [Model Privacy Impact Assessment, werkgroep SURFPIA].
Proces	Een bedrijfsproces is een ordening van het werk dat uitgevoerd dient te worden in een organisatie [Wikipedia].
Risicoanalyse	Een risicoanalyse is een methode waarbij nader benoemde risico's worden gekwantificeerd door het bepalen van de kans dat een dreiging zich voordoet en de gevolgen daarvan: Risico = Kans x Gevolg [Wikipedia].
Vertrouwelijkheid ***(kwaliteitsaspect)***	De mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen. Deelaspecten hiervan zijn: Autorisatie: de mate waarin de adequate inrichting van bevoegdheden gewaarborgd is; Authenticiteit: de mate waarin de adequate verificatie van geïdentificeerde personen of apparatuur gewaarborgd is; Identificatie: de mate waarin de mechanismen ter herkenning van personen of apparatuur gewaarborgd zijn; Periodieke controle op de bestaande bevoegdheden. Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.

Bijlage 2: BIV overeenkomst

Algemeen			
Proceseigenaar			
Functie			
Telefoonnummer			
Laatste datum invullen			
Te classificeren proces			Procesnummer:
Informatie	o.a. Studentgegevens, …		
Risico's	<algemene beschrijving risico's>		
Aanvullende risico's			
Classificatie en risicoanalyse			
	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Geadviseerd beveiligingsniveau			
Eindadvies	X voldoet in de huidige constructie WEL / NIET aan het model van informatieclassificatie, indien voldaan wordt aan de onderstaande acties		
Acties	A. B. C.		

Bijlage 3: AP publiceert definitieve beleidsregels meldplicht datalekken

De AP heeft de definitieve beleidsregels voor de meldplicht datalekken gepubliceerd. Aan de hand van deze regels kunnen organisaties vaststellen of er sprake is van een datalek en aan wie zij dit moeten melden. De meldplicht voor organisaties gaat in op 1 januari 2016.

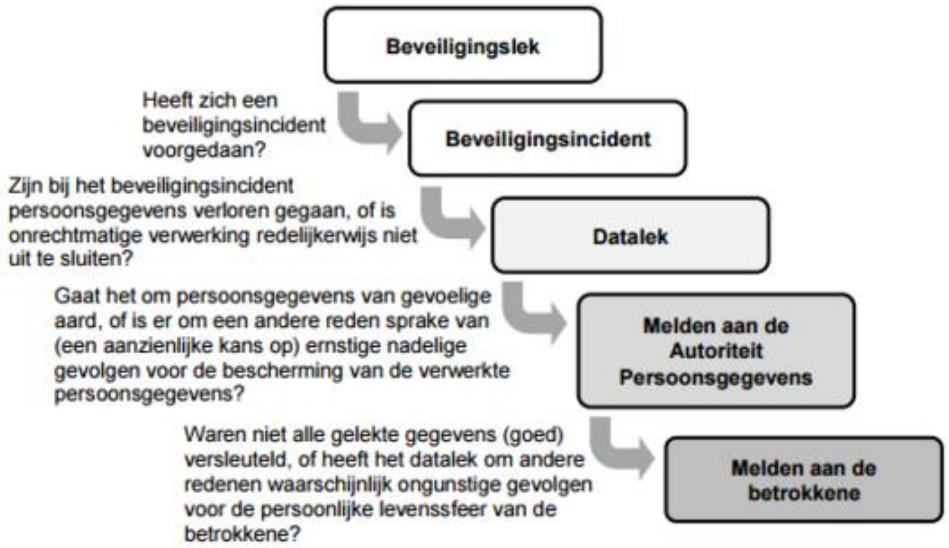
De beleidsregels zijn gepubliceerd op de site de Autoriteit Persoonsgegevens. Aan de hand van deze regels kunnen organisaties onder andere vaststellen of er sprake is van een datalek. Dit hoeft niet bij elk beveiligingsincident het geval te zijn. Het niet melden van een datalek kan een boete opleveren die kan oplopen tot 820.000 euro.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan of als dit niet kan worden uitgesloten. Ook moet er sprake zijn van een 'een inbreuk op de beveiliging', waarbij het gaat om de beveiliging die voor verwerkers van persoonsgegevens wettelijk is verplicht. Een zwakke beveiliging levert dus niet meteen een datalek op.

Vervolgens moet het lek aan de AP gemeld worden als er 'aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens' bestaat. Hierbij moet rekening worden gehouden met de aard van de gegevens. Bij gevoelige gegevens, zoals bijzondere persoonsgegevens, gebruikersnamen, wachtwoorden en gegevens over de financiële situatie van de betrokkene, zal sneller melding gemaakt moeten worden. Organisaties hebben tot 72 uur de tijd om een lek te melden.

Een datalek moet ook aan de betrokkene gemeld worden als er negatieve gevolgen zijn voor de persoonlijke levenssfeer. Met 'betrokkene' wordt de persoon bedoeld waarvan persoonsgegevens worden verwerkt. Ook hier speelt de aard van de gegevens weer een belangrijke rol. Zo zullen er bij gevoelige gegevens sneller negatieve gevolgen optreden.

De invoering van de meldplicht per 1 januari staat los van de ontwikkelingen op Europees niveau waarbij onlangs een akkoord is bereikt over een nieuwe Europese richtlijn. Deze bevat een meldplicht voor beveiligingsincidenten.



Bijlage 4: Framework informatiebeveiliging en privacy in het MBO