**BIV en PIA indiensttreding**

**IBPDOC16**

**Verantwoording**

**Productie**

Kennisnet / saMBO-ICT

**Auteurs**

Wiel Kruijntjens (ROC Leeuwenborgh)

Maurits Toet (Cerrix)

Ludo Cuijpers (Kennisnet)

Leo Bakker (Kennisnet)

Versie 1.0 juli 2016

**Sommige rechten voorbehouden**

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s) en uitgever van Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden.

**Creative commons**

[](http://www.google.nl/url?sa=i&source=images&cd=&cad=rja&uact=8&ved=0CAgQjRw&url=http://creativecommons.org/about/downloads&ei=ViUYVb6yHcbWPPKhgMAM&psig=AFQjCNFD0SQUbum02GpIZCKN9_e8blqrwQ&ust=1427732182559562)Naamsvermelding 3.0 Nederland

(CC BY 3.0)

**De gebruiker mag:**

* Het werk kopiëren, verspreiden en doorgeven
* Remixen – afgeleide werken maken

**Onder de volgende voorwaarde:**

* Naamsvermelding – De gebruiker dient bij het werk de naam van Kennisnet te vermelden (maar niet zodanig dat de indruk gewekt wordt dat zij daarmee instemt met uw werk of uw gebruik van het werk).

Inhoudsopgave

[Verantwoording 2](#_Toc456689655)

[1. Inleiding en procesbeschrijving 4](#_Toc456689656)

[1.1 Aanleiding 4](#_Toc456689657)

[1.2 Globale procesbeschrijving 4](#_Toc456689658)

[1.2.1 Proces Indiensttreding 4](#_Toc456689659)

[1.2.2 Proces Lifecycle 5](#_Toc456689660)

[1.2.3 Proces Uitdienst 5](#_Toc456689661)

[1.3 HR applicatie (HRnu) 5](#_Toc456689662)

[2. Dataset online leren 6](#_Toc456689663)

[2.1 Dataset die doorgegeven wordt aan HRnu 6](#_Toc456689664)

[3. BIV classificatie 7](#_Toc456689665)

[3.1 Beschikbaarheid 7](#_Toc456689666)

[3.2 Integriteit 8](#_Toc456689667)

[3.3 Vertrouwelijkheid 8](#_Toc456689668)

[3.4 HRnu classificatie 9](#_Toc456689669)

[4. Privacy Impact Assessment 10](#_Toc456689670)

[4.1 Inleiding 10](#_Toc456689671)

[4.2 Bevindingen 10](#_Toc456689672)

[Bijlage 1: Gedetailleerde procesbeschrijving 13](#_Toc456689673)

[De gehanteerde globale workflow als implementatie van het proces 17](#_Toc456689674)

[Dataset indiensttreding 18](#_Toc456689675)

[Bijlage 2: Framework Informatiebeveiliging en Privacy voor het MBO 20](#_Toc456689676)

# Inleiding en procesbeschrijving

## Aanleiding

Informatiebeveiliging en privacy zijn ook binnen de mbo wereld inmiddels ingeburgerde begrippen. Weliswaar nog niet zo ingeburgerd dat ze doorgedrongen zijn tot in de vezels van de organisaties maar steeds meer begint ook het onderwijs op mbo niveau doordrongen te raken van het belang van kennis, afspraken en maatregelen, kortom beleid, op deze aspecten van het gebruik van geautomatiseerde processen en administratieve organisatie, in navolging van het WO en HBO onderwijs.

Medewerkers van een mbo instelling, met name docenten, komen dagelijks in aanraking met gegevens van deelnemers die al dan niet privacy gevoelig zijn. Zij moeten zorgen dat binnen de wet- en regelgeving zorgvuldig met deze gegevens wordt omgegaan.

Uiteraard zijn de gegevens van de medewerkers van de mbo instellingen aan diezelfde wet en regelgeving onderhevig. Zij moeten ervan uit kunnen gaan dat met hun gegevens zorgvuldig wordt omgegaan en dat zij ten allen tijde weten wat met hun gegevens gedaan wordt.

Binnen een mbo instelling zijn er, doorgaans, een viertal processen die betrekking hebben op de registratie en verwerking van personeelsgegevens, te weten:

1. Basis – en salarisgegevens;
2. Management informatie betreffende personeel;
3. Zelf service (reiskosten, wijzigen persoonlijke gegevens, etc.);
4. Gesprekscyclus (verslagen van beoordelingsgesprekken, functioneringsgesprekken, scholingsafspraken, etc.)

Deze processen kunnen in een drietal fasen worden onderverdeeld:

1. Indiensttreding;
2. Life cycle;
3. Uitdiensttreding.

In dit document wordt van het proces basis- en salarisgegevens het onderdeel indiensttreding uitgewerkt. Deze uitwerking wordt aan de hand van een casus beschreven.

## Globale procesbeschrijving

De casus betreft een middelgroot mbo instelling met ongeveer 8000 studenten en 700 vaste en tijdelijke medewerkers. Daarnaast zijn er +/- 100 externen (inleners) op projectbasis verbonden aan de organisatie. De tijdelijke schil bedraagt 20% van het totaal aantal medewerkers. De organisatie kent een verloop van +/- 100 personen per schooljaar, voor het overgrote deel onderwijzend personeel.

De organisatie maakt veelal gebruik van standaard software en heeft de laatste jaren enkele bedrijf kritische pakketten vervangen. Onder andere de HR en financiële software is vervangen door SaaS oplossingen.

Eigenaar van het traject ‘Indienst – LifeCycle – Uitdienst’ is de afdeling Human Resources. Deze afdeling is een afdeling met een eigen directeur die verantwoording aflegt aan het College van Bestuur. De afdeling maakt gebruik van een HR applicatie voor personeels- en salarisadministratie.

* + 1. **Proces Indiensttreding**

Het proces ‘Indienst’ volgt op het (afgeronde) proces ’Werving en selectie’. De output van dat proces is de input en trigger voor ‘Indienst’. Het proces wordt geïnitieerd door HR en wordt door diverse afdelingen binnen de casusorganisatie uitgevoerd. Het proces ‘Indienst’ is uitvoerig beschreven in bijlage 1. In dit proces worden faciliteiten (emolumenten) en rechten uitgegeven aan nieuw in dienst tredende medewerkers. Ter ondersteuning is een workflow beschreven en in uitvoering genomen.

* + 1. **Proces Lifecycle**

Het proces ‘Lifecycle’ volgt op het proces ‘Indienst’ en behelst de wijzigingen m.b.t. rechten en faciliteiten die gedurende de actieve loopbaan van een medewerker optreden. Deze wijzigingen treden op als de functie of de rol van een medewerker wijzigt. Dit proces is binnen de casusorganisatie niet beschreven. ‘Lifecycle’ wordt deels uitgevoerd op basis van ad hoc activiteiten van betrokken uitvoeringsmedewerkers.

* + 1. **Proces Uitdienst**

Het proces ‘Uitdienst’ volgt op het proces ‘Lifecycle’. Dit proces wordt geïnitieerd op basis van een vooraf vastgestelde uitdienst datum (tijdelijke contracten), een wettelijk einde dienstverband (denk aan het bereiken van de pensioengerechtigde leeftijd) of ontslag (bijvoorbeeld op eigen verzoek).

Het proces ‘Uitdienst’ is (deels) beschreven maar niet vastgesteld. Er is geen workflow die het proces ondersteunt. Het verloop en de uitvoering van het proces zit met name ‘in de hoofden’ van betrokken uitvoeringsmedewerkers.

* 1. **HR applicatie (HRnu[[1]](#footnote-1))**

HRnu is de tool waarmee binnen de organisatie de personeels- en salarisadministratie wordt uitgevoerd. HRnu wordt als SaaS oplossing afgenomen (HRnu Online). Medewerkers en managers beschikken over HRnu Insite waarmee onder andere workflows zoals de Gesprekscyclus beschikbaar worden gesteld.

**Topdesk**

Topdesk is de tool die door door veel mbo instellingen wordt gebruikt ter ondersteuning van de ITIL processen. In het kader van dit document is daarbij met name *Wijzigingsbeheer* (Change management) van belang omdat daarin de workflow ‘Provisioning’ voor het proces Indiensttreding is vastgelegd. Deze workflow is eigendom van de dienst HR. HR initieert de workflow, monitort deze en neemt initiatief om deze bij wijzigingen in het proces aan te passen. Het functioneel- en technisch beheer van Topdesk ligt bij de afdeling ict.

**Koppelingen**

***Technische toelichting:*** *Het bronsysteem is HRnu. Dit bronsysteem wordt gevuld door handmatige input op basis van formulieren die door de afdeling HR bij indiensttreding worden opgemaakt. Deze formulieren bevatten enerzijds de persoonlijke gegevens van betrokken medewerker of inlener, anderzijds een aantal gegevens die door de organisatie worden gebruikt.*

*Het bronsysteem heeft nog geen koppeling met de Active Directory (AD). Accounts worden handmatig, met behulp van middleware (Forefront Identity Manager, FIM), in de AD aangemaakt. De gegevens die hier bij gebruikt zijn afkomstig van de eerder genoemde HR formulieren (deze ‘lopen’ mee in de workflow).*

*FIM synct 2 maal daags met de AD om de accounts in het systeem actief te maken.*

*Vanuit de AD zijn er diverse koppelingen naar afnemende systemen om accounts aan te maken. Zo worden er bijvoorbeeld in Topdesk medewerkerskaarten aangemaakt. Een ander afnemende systemen is Equitrac (printsysteem). De AD synct door middel van Dir sync met de AD in Microsoft Azure ten behoeve van de aanmaak van de Office 365 licenties en accounts voor medewerkers.*

*Binnen de casusorganisatie wordt momenteel nagedacht over de invoering van role based Identity management. In het kader daarvan zullen de in gebruik zijnde middleware en de koppelingen tussen de verschillende systemen opnieuw bekeken worden met als doel verdere automatisering en het vermijden van handmatige werkzaamheden in het proces.*

# Dataset online leren

## Dataset die doorgegeven wordt aan HRnu

|  |  |  |  |
| --- | --- | --- | --- |
| **De volgende dataelementen kunnen worden geïdentificeerd:** | |  | **Deze gegevens of onderdelen hiervan worden verstrekt aan de volgende partijen:** |
| 1. *Naam* 2. *Voorvoegsel* 3. *Voornamen* 4. *Roepnaam* 5. *Geslacht* 6. *Burgerlijke staat* 7. *Naam partner* 8. *Voorvoegsel partner* 9. *Geboortedatum* 10. *Geboorteplaats* 11. *Nationaliteit* 12. *Adres* 13. *Postcode* 14. *Woonplaats* 15. *Telefoon* 16. *GSM-nummer* 17. *Prive e-mailadres* 18. *IBAN-Bank-/gironummer* 19. *Aanstellingsperiode* 20. *Stagevergoeding* 21. *Werkgever* 22. *Vacature* 23. *Functie* 24. *Bevoegd* | 1. *Reden aanstelling* 2. *Stap Flexwet* 3. *Werktijdfactor* 4. *Werkdagen* 5. *Sector/ portaal / dienst* 6. *Afdeling/team* 7. *Leidinggevende* 8. *Standplaats* 9. *1e en 2e Vestiging* 10. *Ruimte* 11. *Kostendrager* 12. *Unieke code* 13. *E-mail adres* 14. *UPN* 15. *VoIP nummer* 16. *Mobiel nummer* 17. *AD groepslidmaatschappen* 18. *Rechten op applicaties* 19. *Merk en type notebook* 20. *Extra software* 21. *Niet-standaard sleutels* 22. *VPN account (token)* |  | 1. *HRnu* 2. *SIS* 3. *Belastingdienst* 4. *Pensioenfonds* 5. *Externe beheerders* 6. *Ict* 7. *Facilitair* 8. *Postkamer* |

# BIV classificatie

De BIV classificatie bestaat uit drie onderdelen te weten beschikbaarheid, integriteit en vertrouwelijkheid. Het document Handboek BIV classificatie (IBPDOC14) is onderdeel van het mbo framework en daarin worden de naast de definities van beschikbaarheid, integriteit en vertrouwelijkheid ook de classificatie indelingen in drie klassen weergegeven: laag, midden en hoog. Het is van belang deze klassenindeling met bijbehorende beschrijving en beheersmaatregelen voor alle processen toe te passen zodat er van uniformiteit gesproken kan worden. Deze indeling komt ook weer terug in de afspraken kaders die met leveranciers worden gehanteerd. Het staat de instelling uiteraard altijd vrij om daar een eigen invulling aan te geven.

## Beschikbaarheid

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 is Laag, Midden en Hoog zoals uitgewerkt in de volgende tabel:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **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[[2]](#footnote-2)** 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 |

## 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.

In de onderstaande tabel is per classificatie indeling het classificatiegevolg beschreven met de daarbij behoren beheersmaatregel.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Classificatie**  **indeling** | **Classificatie gevolg** | **Beheersmaatregel** |
| **Integriteit** | Integriteit  **Laag** | Het bedrijfsproces staat **enkele** integriteitsfouten toe. | * Application controls + business rules |
| 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 |

## 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 mechanismen ter herkenning van personen/apparatuur gewaarborgd zijn.
* Periodieke controle op de bestaande bevoegdheden. Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **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[[3]](#footnote-3) en/of encryptie[[4]](#footnote-4) |

## HRnu classificatie

Uitgaande van deze generieke beschrijvingen vanuit het handboek BIV classificatie is het zaak om dit toe te passen op het proces indiensttreding.

Beschikbaarheid: als uitgangspunt voor de processen rondom medewerkersgegevens wordt voor beschikbaarheid de klasse **MIDDEN** gekozen. Dit lijkt voor het gebruik voor de organisatie en medewerkers een voldoende garantie om te kunnen werken en het is voor mbo instelling en leverancier ook een haalbaar criterium. Dit is ook met de leveranciers afgestemd.

Integriteit: de juistheid, tijdigheid en volledigheid van de gegevens worden voor de HR processen geclassificeerd als **HOOG**. De data moet kloppen omdat er gegevens worden gedeeld met de belastingdienst, het pensioenfonds, OCW, etc.

Vertrouwelijkheid: alleen aangewezen personen hebben toegang tot de informatie van de medewerkers. Vandaar dat gekozen is voor de classificatie **MIDDEN**. Medewerkers krijgen op basis van hun rol (functie) toegang tot de gegevens van collega medewerkers. Uiteraard krijgen medewerkers toegang tot hun eigen gegevens.

Op basis van de wensen, de financiële mogelijkheden en bovenstaande argumentatie wordt “Indiensttreding” gelabeld, op basis van de vastgestelde BIV classificatie, met **M-H-M**. Schematisch als volgt weergegeven.

|  |  |  |
| --- | --- | --- |
| *Proces:* **HRM**  **Indiensttreding** | | **24a** |
| *Proceseigenaar:* **Directeur HR** | | |
| *BIV classificatie*  **M – H – M** | *Privacy (PIA-BO-PB)* | |

# Privacy Impact Assessment

## Inleiding

Tweede stap in de procesbenadering is het doen van een privacy impact assessment (PIA). In goed Nederlands is dat een gegevensbeschermingseffectbeoordeling (GEB). In het toetsingskader privacy in het mbo (IBPDOC7) is dit bij statement P21 uitvoerig weergegeven:

|  |
| --- |
| **P21 MBO controledoelstelling: gegevensbeschermingseffectbeoordeling (GEB)**   * De instelling voert een (tweejaarlijks terugkerende) evaluatie uit van de mogelijke effecten van de verschillende gegevensverwerking op de rechten en vrijheden van de betrokkenen. Deze evaluatie vindt eveneens plaats in geval van een wijziging in de verwerking van persoonsgegevens die specifiek de risico’s wijzigt voor de privacy van de betrokken deelnemers en medewerkers. * De instelling voert naar aanleiding van de evaluatie een volledige GEB uit in geval de verwerking van de persoonsgegevens:   + in geval van een systematische en uitgebreide beoordeling van persoonlijke aspecten van betrokkenen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;   + Bijzondere persoonsgegevens (ras, gezondheid) worden verwerkt;   + Geautomatiseerde bewaking van publiek toegankelijke ruimtes. * De beoordeling heeft betrekking op de gehele levenscyclus van persoonsgegevens van verzameling van verwerking tot verwijdering. * In geval van herziening van of nieuwe verwerkingen van grote hoeveelheden persoonsgegevens, wordt vooraf bepaald wat de impact is van deze (gewijzigde) verwerking op de privacy van de deelnemers. * Bij de GEB is altijd de FG betrokken. |

In de toelichting hierbij staat dat informatiebeveiliging behoort te worden geïntegreerd in de projectbeheermethode(n) van de organisatie om ervoor te zorgen dat informatiebeveiligingsrisico’s worden geïdentificeerd en aangepakt als deel van een project. Dit geldt in het algemeen voor elk project ongeacht het karakter, bijv. een project voor een proces voor kernactiviteiten, IT, ‘facility management’ en andere ondersteunende processen.

Indien uit een PIA blijkt dat de gegevensverwerking een hoog risico zou opleveren, dan moeten er maatregelen worden genomen om dat risico te mitigeren. Indien dat niet mogelijk is, is vanaf mei 2018 voorafgaand overleg met de AP noodzakelijk.

Een instelling moet dus vertrouwd raken met het uitvoeren van een PIA. Dit document laat voor een specifiek proces, namelijk dat van het gebruik van digitaal educatief leermateriaal (online leren) zien hoe je dat kunt aanpakken.

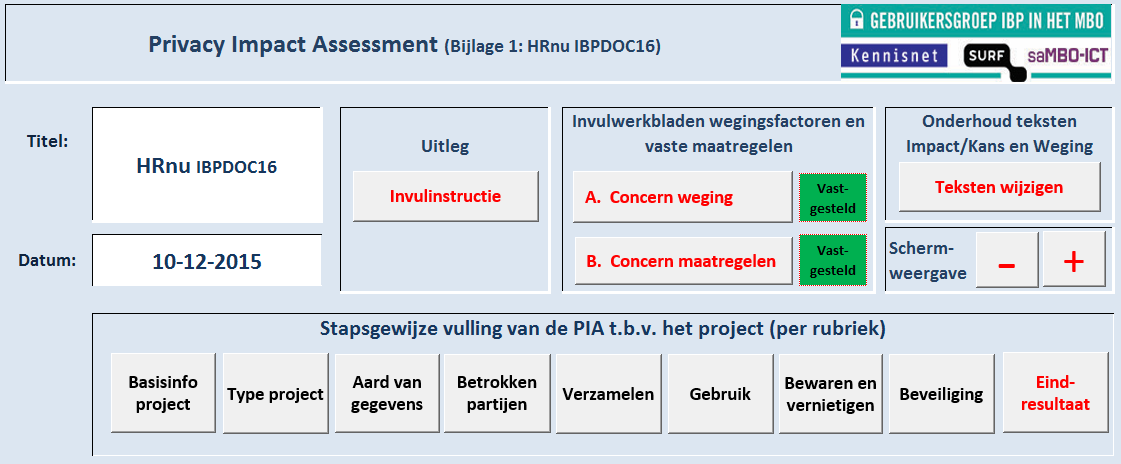
## Bevindingen

Voor het uitvoeren van een PIA kun je een zelf een methode ontwikkelen maar je kan ook gebruik maken van een al ontwikkelde methodiek. Voor het mbo is gekozen om gebruik te maken van de PIA tool die ook door het hoger onderwijs wordt benut. Deze tool is vrij verkrijgbaar voor het mbo (saMBO-ICT site, groep ibp).

De uitgevoerde PIA voor het proces online leren is als losse Excel bijlage toegevoegd en te downloaden op de saMBO-ICT site. Zie: **Bijlage 1:PIA HRnu IBPDOC16**

Op grond van de AVG (privacy wetgeving) kan geconcludeerd worden dat er sprake is van de noodzaak om een PIA te maken. Dit kan je bijvoorbeeld doen als er sprake is van een nieuwe situatie, bijvoorbeeld aanbesteding van nieuwe materialen. Het kan ook zijn dat dit een keer tussendoor wordt georganiseerd. In ieder geval moet in mei 2018 sprake zijn van een op dit proces uitgevoerde PIA.

De volgende aanbevelingen komen naar voren op basis van de uitgevoerde PIA (zie aparte Excel sheet Bijlage 1 PIA HRnu.



|  |
| --- |
| **Beheersmaatregelen gebruikers** |
| 1. Informeren van betrokkenen over gebruik van gegevens en recht op inzage/wijziging. |
| 1. Mogelijk inregelen van opt-in/opt-out. |
| 1. Betrokkene inzage geven in de eigen gegevens en een procedure voor correctie (en verwijdering) inregelen. |
| 1. Zorgen voor klachtenprocedure. |
| 1. Informeren betrokkene over herkomst en gebruik gegevens. |
| **Beheersmaatregelen data gebruik** |
| 1. Per data element doel omschrijven. |
| 1. Dataminimalisatie op basis van doelbinding. |
| 1. Zorgen voor voldoende kwaliteit van data. |
| 1. Zorgen voor een goede AO die kwaliteit van de data volgens afgesproken norm garandeert. |
| 1. Geautomatiseerde beoordeling op basis van profielen is hulpmiddel, geen grond voor besluit of handeling waarbij iemand in aanmerkelijke mate wordt geraakt (vereist). |
| 1. Onderzoekdata en persoonsgegevens die nodig zijn voor management rapportages zoveel mogelijk anonimiseren of geaggregeerd bewaren. |
| 1. Bewaar alleen dat deel van de verzamelde info over het individu dat echt noodzakelijk is (wettelijke basis of selectielijst). |
| 1. Stel vooraf duidelijke bewaar termijnen vast en handel daarna. |
| 1. Indien vernietigen niet mogelijk is beperk de toegang tot strikt noodzakelijke. |
| **Beheersmaatregelen techniek** |
| 1. Beveiligen van data tegen lekken en hacken. |
| 1. Beveiligen van communicatie kanalen m.b.v. encryptie technieken (bv https). |
| 1. Bewerkersovereenkomsten, juridisch normenkader. |
| 1. Privacy beleid en werkinstructies voor verwerkers van persoonsgegevens. |
| 1. Authenticatie en autorisatie op basis van least privileges (minimale rechten). |
| 1. Stel beveiligingseisen aan bewerkers. |

Deze 20 beheersmaatregelen 15 t/m 20 moeten dus worden gedeeld en vervolgens gerealiseerd door de bewerker (leverancier HRnu) en vastgelegd in een bewerkersovereenkomst en aangevuld met een SLA. De mbo instelling is verantwoordelijk voor de beheersmaatregelen 1 t/m 14.

Schematisch weergegeven er is een PIA uitgevoerd (**Ja**), HRnu heeft een eigen (**E**) bewerkersovereenkomst (BO) aangeboden aan de mbo instelling, bovendien blijkt uit een korte scan dat het privacy beleid (PB) van HRnu goed (**G**) te noemen is. Samengevat in onderstaand ibp architectuur deel schema:

|  |  |  |
| --- | --- | --- |
| *Proces:* **HRM**  **Indiensttreding** | | **24a** |
| *Proceseigenaar:* **Directeur HR** | | |
| *BIV classificatie*  **M – H – M** | *Privacy (PIA-BO-PB)*  **Ja – E – G** | |

Bijlage 1: Gedetailleerde procesbeschrijving

Het proces ‘Indiensttreding’ (kortweg ‘Indienst’) is binnen de casusorganisatie het meest uitgewerkte proces binnen het traject ‘Indienst – Lifecycle – Uitdienst’. In dit hoofdstuk wordt dit proces in detail toegelicht.

Hieronder volgen het formele, vastgestelde processchema met bijbehorende beschrijving en de workflow die dit proces in de praktijk ‘handen en voeten’ geeft.

Voorbeeld procesbeschrijving omdat er geen Triple A is



Processchema ‘Indiensttreding’.

| *Procesbeschrijving ‘Indiensttreding’* | | |
| --- | --- | --- |
| **Onderwerp naam** | **Wie** | **Omschrijving** |
| *Invullen formulier* | Leidinggevende | Invullen van het akkoordformulier.  Formulier kan via Fronter (ELO en intranet) gedownload worden. |
| *Verzenden akkoordformulier* | Leidinggevende | Verzenden van het Provisioning akkoordformulier. |
| *Akkoordformulier volledig?* | HR | Controle van het ingevulde formulier |
| *WG-relatie?* | HR | Is er sprake van een werkgeversrelatie. |
| *BSN-formulier versturen* | HR | Versturen van het BSN-formulier |
| *Invullen BSN-formulier* | Leidinggevende | Invullen van het BSN-formulier |
| *Retour zenden BSN-formulier* | Leidinggevende | Retour zenden van het BSN-formulier naar HR. |
| *Uitnodigen nieuwe medewerker* | [HR](#Appendix542) | Nieuwe medewerker uitnodigen voor een intakegesprek. Tevens aangeven welke documenten de medewerker mee moet nemen voor het gesprek. |
| *Intakegesprek* | [HR](#Appendix542) | Voeren van een intakegesprek.  Tijdens het intakegesprek wordt het [Provisioning akkoordformulier](#Appendix478) en het [BSN-formulier](#Appendix479) ingevuld.  Tijdens de intake wordt de medewerker begeleidt naar de servicedesk, alwaar het paspoort gescand wordt of een foto gemaakt wordt van de medewerker. *(Na september 2015 wordt alleen een foto gemaakt.)* |
| *Melding via topdesk* | [HR](#Appendix542) | Een wijzigingsaanvraag aanmaken Topdesk, inclusief het [BSN-formulier](#Appendix479) en het [Provisioning akkoordformulier](#Appendix478). |
| *Aanmaken unieke code* | [Ict](#Appendix540) | Aanmaken van een (vierletter)code voor de medewerker/inlener. |
| *Invoeren in HRM-pakket* | PSA | Invoeren van medewerker/inlener in HRM-pakket en DVS-systeem.  Voor inleners geldt dat deze in HRM-pakket worden ingevoerd met de code 3.  Via het HRM-pakket wordt DVS gevuld.  Op basis van werklocatie (Maastricht) en de woon-werkafstand (meer dan 10 km) wordt aangegeven of medewerker/inlener de basispas of de pas-plus ontvangt. Indien de medewerker/inlener recht heeft op de pas-plus wordt tevens een vinkje gezet in het veld **pluspas.**  Daarnaast wordt op het akkoordformulier een aantekening gemaakt in de zin van pas+, zodat de servicedesk weet dat de pas+ dient te worden uitgereikt aan de medewerker/inlener. |
| *Inbrengen in FIM* | [Ict](#Appendix540) | Handmatig invoeren van gegevens in FIM.  Via FIM wordt automatisch:  AD- account  E-mail adres  Top-desk account  Equitrac account aangemaakt  Op het akkoordformulier het e-mail adres invullen. |
| *Notebook imagen* | [Ict](#Appendix540) | Gereed maken van de laptop voor de medewerker/inlener. Op basis van functie en afdelingen wordt bepaald welk soort laptop. De te installeren (extra) software wordt eveneens bepaald door de functie en afdeling en het ingevulde veld “extra software”. |
| *Toewijzen VoIP nummer* | [Ict](#Appendix540) | Toekennen van een VoIP-nummer.  Op akkoordformulier het VoIP-nummer invullen. |
| *Call manager account* | [Ict](#Appendix540) | Vastleggen van VoIP-nummer in de call-manager. Invullen van het VoIP-nummer op formulier. |
| *Aanmaken Topdesk account* | [Ict](#Appendix540) | Aanmaken van een account in Topdesk. |
| *Aanmaken Slim account* | [Ict](#Appendix540) | Aanmaken van een account bij Slim. |
| *Aanmaken Fronter account* | [FB](#Appendix545) | Aanmaken van een account bij Fronter. |
| *Autorisatie FB* | FB | Aanpassen van de autorisatie in de verschillende standaard applicatie (DVS/HRM/Fin) op basis van de functie en afdeling/team. |
| *Token* | [Ict](#Appendix540) | Heeft de medewerker recht op een token?  Zie [servicecatalogus](#Appendix471) |
| *Aanmaken VPN account* | [Ict](#Appendix540) | Aanmaken van een VPN account.  Regelen van de token.  Op akkoordformulier VPN-accountnr. invullen. |
| *ID-scan/Foto uploaden* | [Ict](#Appendix540) | Foto uploaden naar de fileserver. |
| *Aanmaken pasje* | Extern  Servicedesk | Aanmaken van het pasje voor de medewerker.  *Vanaf september 2015 worden de pasjes niet meer aangemaakt door extern maar worden deze op de servicedesk uitgereikt aan de medewerkers/inlener. Afhankelijk van de extra toegevoegde opmerking wordt het basispasje of het pasje-plus uitgereikt.*  *Het pasnummer wordt geregistreerd en eveneens op het akkoordformulier weergegeven.* |
| *Aanmaken postvak* | BD | Aanmaken van een postvak.  De locatie waar het postvak aangemaakt moet worden is afhankelijk van de "Vestiging" van de medewerker.  De sleutel van het postvak wordt doorgestuurd naar de servicedesk.  zie [Provisioning akkoordformulier](#Appendix478) |
| *Softphone?* | [Ict](#Appendix540) | Dient de laptop uitgerust te worden met een softphone? |
| *Softfone en Headset* | [Ict](#Appendix540) | Installeren van softphone en inpakken van headset. |
| *Plaatsen fysiek toestel* | [Ict](#Appendix540) | Plaatsen van een toestel (incl. een handleiding) op de kamer van de nieuwe medewerker. |
| *GSM?* | [Ict](#Appendix540) | Heeft de medewerker recht op een GSM?  Zie S[ervicecatalogus](#Appendix471) |
| *Voucher toewijzen* | [Ict](#Appendix540) | Toewijzen van een voucher.  Op akkoordformulier mobielnummer invullen. |
| *Pas* | BD Postkamer | De ontvangen pas voor in het buitenland woonachtige medewerkers wordt doorgestuurd naar de servicedesk.  *Dit punt vervalt vanaf september 2015. De pas wordt dan via de servicedesk uitgereikt.* |
| *Doorgeven aan servicedesk.* | Ict | Terugkoppeling van alle benodigde documenten en emolumenten. |
| *Afhalen bij Servicedesk* | [Medewerker](#Appendix547) | De nieuwe medewerker kan alle emolumenten afhalen bij de servicedesk. De medewerker ontvangt een schrijven met daarop alle voor hem relevante informatie.  Daarnaast dient hij/zij voor ontvangst van deze emolumenten te tekenen. |
| *Bevestiging afhandeling* | [Ict](#Appendix540) | Informeren van HR dat alle afgesproken acties uitgevoerd zijn. (via mail). |
| *Informeren leidinggevende* | [HR](#Appendix542) | Informeren leidinggevende dat medewerker alle actie t.a.v proces "in dienst" zijn uitgevoerd en medewerker zijn emolumenten heeft afgehaald bij de servicedesk.  *De ontbrekende informatie (zoals pasnummer) wordt alsnog ingevoerd bij de medewerker/inlener.* |

De gehanteerde globale workflow als implementatie van het proces

De hierboven beschreven procesgang van het proces ‘Indienst’ wordt ondersteund en uitgevoerd door de verschillende betrokken afdelingen en functionarissen met behulp van de workflow ‘*Provisioning nieuwe medewerker*’. Deze workflow is gemaakt in Topdesk als *wijzigingssjabloon* (die telkens opnieuw wordt gebruikt) met daarin diverse herbruikbare activiteitssjablonen.

De workflow bestaat uit 3 fasen: aanvraag, uitvoering en evaluatie. De workflow start op het moment van de processtap ‘*Intakegesprek’* en dient binnen 3 werkdagen afgerond te zijn. De processtappen vòòr ‘Intakegesprek’ zijn interne HR werkzaamheden als voorbereiding op de workflow.

De fase aanvraag is bedoeld om de workflow te starten. In deze fase zet een medewerker van HR de workflow in gang door de sjabloon in te vullen (voor een specifieke nieuwe medewerker) en daarmee formeel goedkeuring te geven aan het toekennen van rechten en faciliteiten aan de nieuwe medewerker. Hij voegt de formulieren zoals in de processtap ‘*Melding maken in Topdesk’* aangegeven, toe aan de workflow.  
De HR medewerker geeft in het sjabloon verder ook aan welke (uitvoerings)activiteiten niet uitgevoerd hoeven worden bijvoorbeeld omdat gezien de functie of rol van de nieuwe medewerker deze geen recht heeft op een bepaalde faciliteit. Dit doet hij op basis van de servicecatalogus.

Na de fase aanvraag volgt de fase uitvoering. In deze fase worden de diverse activiteiten die nodig zijn om de nieuwe medewerker te voorzien van de juiste rechten en faciliteiten uitgevoerd door de betrokken afdelingen. Voor elke uitvoeringsactiviteit is een doorlooptijd bepaald. De activiteiten zijn beschreven en voorzien van een werkinstructie voor de betrokken medewerker (behandelaar).  
Op het moment dat de voorgaande activiteit is uitgevoerd en gereed gemeld, krijgt een behandelaar zijn uit te voeren (daarvan afhankelijke) activiteit pas te zien in zijn takenbord in Topdesk.

De uitvoeringsactiviteiten zijn deels *afhankelijk* van elkaar (kop- en staartactiviteit) omdat de ene activiteit noodzakelijkerwijs moet volgen op de andere. Zo dient eerst de activiteit ‘*Unieke code aanmaken’* uitgevoerd te worden voordat de activiteit ‘*Inbrengen in FIM’* kan worden uitgevoerd omdat accounts die middels FIM worden aangemaakt, gemaakt worden op basis van een unieke code.

Nadat alle uitvoeringsactiviteiten zijn uitgevoerd wordt de nieuwe medewerker en de leidinggevende geïnformeerd middels een geautomatiseerd bericht. De nieuwe medewerker kan dan zijn faciliteiten afhalen bij de servicedesk. De benodigde rechten zijn toegewezen. De nieuwe medewerker kan aan de slag.

De fase evaluatie is voor intern gebruik en bedoeld om (steekproefsgewijs) controles uit te voeren op het verloop van het proces. Deze fase sluit formeel de workflow af door middel van goedkeuring door de verantwoordelijke behandelaar.  
  
Gedurende alle fasen wordt het proces gemonitord door een coördinator van HR. Hij kan ingrijpen als doorlooptijden van de verschillende activiteiten (dreigen) overschreden (te) worden.



Dataset indiensttreding

De volgende systemen en objecten kunnen worden geïdentificeerd in het proces ‘Indienst’:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Systeem of object*** | ***Detailomschrijving*** | ***Opmerking*** | ***Soort verwerking*** | ***Verantwoordelijke*** | ***Uitvoerende*** |
| *Akkoordformulier* | *Bevat werkgevers gegevens zoals functie, standplaats, kostenplaats, unieke code.* | *Beveiligd Excelformulier; formulier loopt mee in de workflow* | *Handmatig (deels) met keuzemenu’s* | *HR* | *Leidinggevende* |
| *BSN formulier* | *Bevat persoonlijke gegevens van medewerker zoals NAW, geboortedatum- plaats, bankrekeningnr., prive tel.nr., prive e-mailadres.* | *Beveiligd Excelformulier; formulier loopt mee in de workflow* | *Handmatig (deels) met keuzemenu’s* | *HR* | *Leidinggevende* |
| *Unieke code (aanmaken)* | *Vierletter code* | *Gebruikersnaam (UPN) in veel systemen; handmatig aangemaakt* | *Access bestand met formulier* | *HR* | *Ict* |
| *HR systeem* | *Aanmaken, muteren en inzage van persoonlijke en werkgeversgegevens; Workflows t.b.v. HR; Salarisspecificaties* | *Invoer op basis van akkoord- en BSN formulieren in HR pakket* | *Handmatig* | *HR* | *HR* |
| *Middleware* | *Aanmaken, muteren en inzage in een deelset persoonlijke en werkgeversgegevens bv. unieke code, e-mailadres, functie, rol, kostenplaats.* | *Invoer op basis van akkoord- en BSN formulieren in FIM* | *Handmatig met keuzemenu’s* | *HR* | *Ict* |
| *AD* | *FIM gegevens plus lidmaatschap van groepen t.b.v. toegang tot data en applicaties.*  *Koppelingen naar doelsystemen zoals Topdesk en Equitrac (printen)* | *AD synct met AD in Azure middels Dirsync* | *Geautomatiseerd* | *Ict* | *Ict* |
| *Office 365 (licentie)* | *Licentie en toegang tot O365 omgeving en software.*  *Aanmaken e-mailadres* | *Nog niet opgenomen in proces;*  *E-mailadres wordt nieuwe gebruikersnaam (UPN).* | *Script*  *Geautomatiseerd* | *Ict* | *Externe partij* |
| *Notebook* | *Medewerkersnotebook* | *Bruikleenovereenkomst van toepassing;*  *Medewerkers hebben administratorrechten op de notebook.* | *Geautomatiseerd*  *Handmatig* | *Ict* | *Ict* |
| *Token / VPN* | *VPN verbinding m.b.v. authenticatiemiddel* | *Drievoudige authenticatie; toegang tot bedrijfsdata vanaf niet-domein locatie.* | *Handmatig* | *HR* | *Ict* |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Systeem of object*** | ***Detailomschrijving*** | ***Opmerking*** | ***Soort verwerking*** | ***Verantwoordelijke*** | ***Uitvoerende*** |
| *Rechten op data* | *Groepslidmaatschappen op datamappen op het netwerk* | *Handmatige toewijzing aan groepen* | *Handmatig* | *Leidinggevende* | *Ict* |
| *Rechten op applicaties* | *Toegang en authenticatie voor specifieke applicaties* | *Fronter, AFAS Insite, Eduarte etc.* | *Deels geautomatiseerd; Handmatig* | *Leidinggevende* | *Funct. beheer voor organisatiebrede applicaties*  *Sectoren voor specifieke sectorapplicaties* |
| *Foto* |  | *Bedoeld voor pasje en applicaties* | *Handmatig* | *HR* | *Ict* |
| *Pasje (parkeerrechten)* | *Pasje t.b.v. printen en recht op toegang parkeerplaats* | *Toegang voor medewerkers met een woon-werk afstand > 10 km* | *Handmatig* | *HR* | *Ict* |
| *(Toewijzen) telefoonnummer* | *VoIP nummer of mobiel nummer* | *Stagiairs en externen geen tel. nr. of abonnement.* | *Handmatig* | *HR* | *Ict* |
| *(Toewijzen) GSM/smartphone* | *Voucher t.b.v. leverancier; uitlevering via externe partij* | *Voor specifieke functies zoals managers, consulenten* | *Handmatig* | *HR* | *Ict/Externe partij* |
| *Postvak en sleutelset* | *Postvak standplaats; sleutelset standplaats en andere locaties afh. van functie* | *Sleutels geven fysiek toegang tot ruimtes in drie gradaties.* | *Handmatig* | *HR* | *Facilitair* |

Bijlage 2: Framework informatiebeveiliging en privacy in het mbo



1. Fictieve naam [↑](#footnote-ref-1)
2. HO: 1 dag [↑](#footnote-ref-2)
3. 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. [↑](#footnote-ref-3)
4. Encryptie: informatie is versleuteld en kan alleen door een aangewezen ontvanger worden gelezen. [↑](#footnote-ref-4)