Aanpak ibp in het mbo

Auteur Kennisnet IBP MBO - oud -

Laatst gewijzigd 14 may 2018

Webadres https://maken.wikiwijs.nl/104332

Inhoudsopgave

Welkom bij de roadmap 'IBP IN HET MBO'

Voor vragen kun je contact opnemen met Leo Bakker
via l.bakker@kennisnet.nl of 0800-3212233

Voor wie maken we dit?

'**Informatiebeveiliging en privacy**' (ibp) staat hoog op de agenda bij mbo instellingen. In veel gevallen is er ook al een ibp functionaris (of een security- of privacy officer) aanwezig. Naast deze specialisten raken steeds meer mensen betrokken bij ibp; ook voor hen is kennis over wat ibp precies inhoudt van groot belang.

Roadmap

Deze aanpak, ook wel de roadmap voor het mbo genoemd, geeft dat inzicht en biedt je tevens een praktisch handvat om jouw taak op het gebied van ibp op een goede manier in te vullen. Met name het aspect van de privacy is actueel en behoeft nog veel aandacht. Daarom is naast de basiselementen voor informatiebeveiliging een aparte module voor privacy ontwikkeld om je daarbij te ondersteunen.

Het arrangement is in eerste instantie bedoeld voor de ibp functionaris en zijn directe collega's die aan ibp in de instelling werken. Ook voor de verantwoordelijke managers, bijvoorbeeld proceseigenaren (zoals een onderwijs manager, een HR manager en het CvB als eindverantwoordelijke) is het een nuttige handreiking om die verantwoordelijkheid op een goede manier in te vullen.

Waarom doen we dit?

Het onderwerp **ibp** is in korte tijd hoog op de agenda van het mbo gekomen. Het onderwijs houdt steeds meer gegevens bij: ook de mbo-sector realiseert zich hoe belangrijk het is om op een goede en veilige manier met deze informatie om te gaan.

Het belang van een ibp-beleid

Dit geldt zeker voor alle persoonsgegevens die een mbo-instelling beheert. Deelnemers en medewerkers mogen ervan uitgaan dat de instelling hun gegevens zorgvuldig behandelt en het geschonken vertrouwen niet beschaamt.

Daarnaast is het van belang dat het mbo zijn primaire rol op een betrouwbare en correcte wijze uitvoert. Namelijk: goed onderwijs geven en studenten diplomeren. Diploma's zijn maatschappelijk van grote waarde en mogen nooit ter discussie komen te staan. Om deze redenen is ook voor het mbo een goed ibp-beleid cruciaal. Kennisnet ondersteunt mbo-instellingen bij de realisatie hiervan.

Ibp & privacy

'*Ibp*' staat zoals gezegd voor '*informatiebeveiliging en privacy*'. Er is bewust een keuze gemaakt om deze twee aspecten in een adem te noemen en ook tezamen in een aanpak op te nemen. Geen privacy zonder informatiebeveiliging. Andersom maakt privacy weer integraal onderdeel uit van informatiebeveiliging.

Meer lezen?

In twee **Hoe?Zo!** publicaties van Kennisnet lees je alles over informatiebeveiliging en privacy. Deze publicaties zijn bedoeld voor het management van een mbo instelling. Tevens vind je hier een publicatie over de verantwoording van het programma ibp in het mbo.

Interviews

In de praktijk is het behoorlijk complex om informatiebeveiliging en privacy in te bedden in het mbo. Dat geldt zowel voor de verantwoordelijken als voor de uitvoerders. Ga er maar aan staan. Het blijkt keer op keer in het mbo dat samenwerking en uitwisseling een groot goed is. Het heeft ons zeker rondom ict ook al veel opgeleverd.

Belangrijk is om in dit verantwoordingsdocument ook de praktijk en de urgentie zoals die in de instellingen wordt gevoeld weer te geven. Daarom hebben we aan een voorzitter van een College van Bestuur als eindverantwoordelijke en aan een ibp manager als uitvoerder gevraagd hun ervaringen en

ideeën over informatiebeveiliging en privacy hier te delen.

Deze interviews zijn **hier** te lezen.

Wat levert het je op?

Deze roadmap biedt een handig stappenplan waarmee je jouw organisatie 'ibp compliant' kunt maken. Klaar voor de Europese wetgeving AVG die in mei 2018 ingaat.

Initiatief

Door deze stappen te volgen laat je als instelling zien dat je ibp serieus neemt en dat je er alles aan gedaan hebt om de risico's die je altijd loopt zo klein mogelijk te maken. En daar gaat het bij een mogelijke controle vooral om: kunnen aantonen dat je 'voldoende' initiatief genomen hebt om ibp-beleid te ontwikkelen en uit te voeren.

Resultaat

Na afloop van deze roadmap heb je gegarandeerd:

- *het informatiebeveiligingsbeleid goed in de steigers gezet;*
- *de instelling AVG compliant gemaakt;*
- *volgens de algemeen geaccepteerde onderwijsstandaarden voor ibp gewerkt;*
- *samen met andere mbo instellingen de sector een stap veiliger en robuuster gemaakt.*

Zo werkt deze roadmap

Deze 'Roadmap 2' is een uitbreiding op de eerste versie van de Roadmap in het Framework, de '**Roadmap informatiebeveiliging en privacy in het mbo**'. In die eerste versie is het traject geschetst dat je de eerste maanden als instelling doorloopt indien er nog niks aan ibp is gedaan.

Maar dan? Er was behoefte aan een vervolgstap, hoe maak je de organisatie nu ibp compliant. In deze Roadmap 2 wordt geschetst welke zaken je allemaal op orde moet brengen om ibp compliant te worden.

De roadmap bestaat uit twee delen: indien je ze stap voor stap doorloopt weet je zeker dat je geen belangrijke ibp-onderdelen overslaat.

Module 'Roadmap Informatiebeveiliging':
Hierin beschrijven we de maatregelen om te treffen met name op het gebied van informatiebeveiligingsbeleid, bewustwording en security architectuur.

Module 'Roadmap Privacy':
Hierin beschrijven we de tien stappen die nodig zijn om voldoende privacy-bestendigheid binnen de organisatie te realiseren. Deze tien stappen zijn geheel gebaseerd op het **10-stappen plan** dat de Autoriteit Persoonsgegevens heeft ontwikkeld.

Netwerk, regiegroep en platform

Samenwerking is van groot belang. Het thema is voor veel instellingen te complex om helemaal zelf aan te pakken. Daarom is het cruciaal om samen te werken aan modellen, overeenkomsten en afsprakenkaders, zodat de sector in de hele informatie-keten als goede partner effectief en efficiënt kan functioneren.

Netwerk en Regiegroep

Hiervoor is het '**Netwerk ibp in het mbo**' in het leven geroepen, onder de vlag van saMBO-ICT, om kennis te ontwikkelen en ervaringen te delen. Een regiegroep stuurt het netwerk aan en bepaalt de agenda rond ibp in het mbo. Kennisnet en SURF maken deel uit van de regiegroep en ondersteunen en faciliteren de regiegroep en het netwerk met inzet van middelen en expertise.

Platform netwerk

Het netwerk 'ibp in het mbo' heeft ook een eigen platform. Dit is een besloten groep voor leden van het netwerk in de groepsomgeving van saMBO-ICT. De leden vinden daar bijvoorbeeld alle verslagen en presentaties die bij de netwerkbijeenkomsten aan de orde zijn. Ook zijn alle Word-documenten van het 'Framework ibp in het mbo' te downloaden zodat je daar zelf mee aan de slag kunt gaan.

Je kunt je bij het netwerk aanmelden met een mailtje naar Leo Bakker (**l.bakker@kennisnet.nl**). Dan krijg je ook toegang tot de besloten groepsomgeving van saMBO-ICT.

Verhoudingen

Om de verhoudingen tussen de verschillende spelers weer te geven is onderstaande illustratie gemaakt. Onderdeel van de saMBO-ICT organisatie is de ibp regiegroep (gebruikersgroep). Deze groep bepaalt de agenda voor ibp in het mbo en heeft het netwerk 'ibp in het mbo' onder haar hoede.

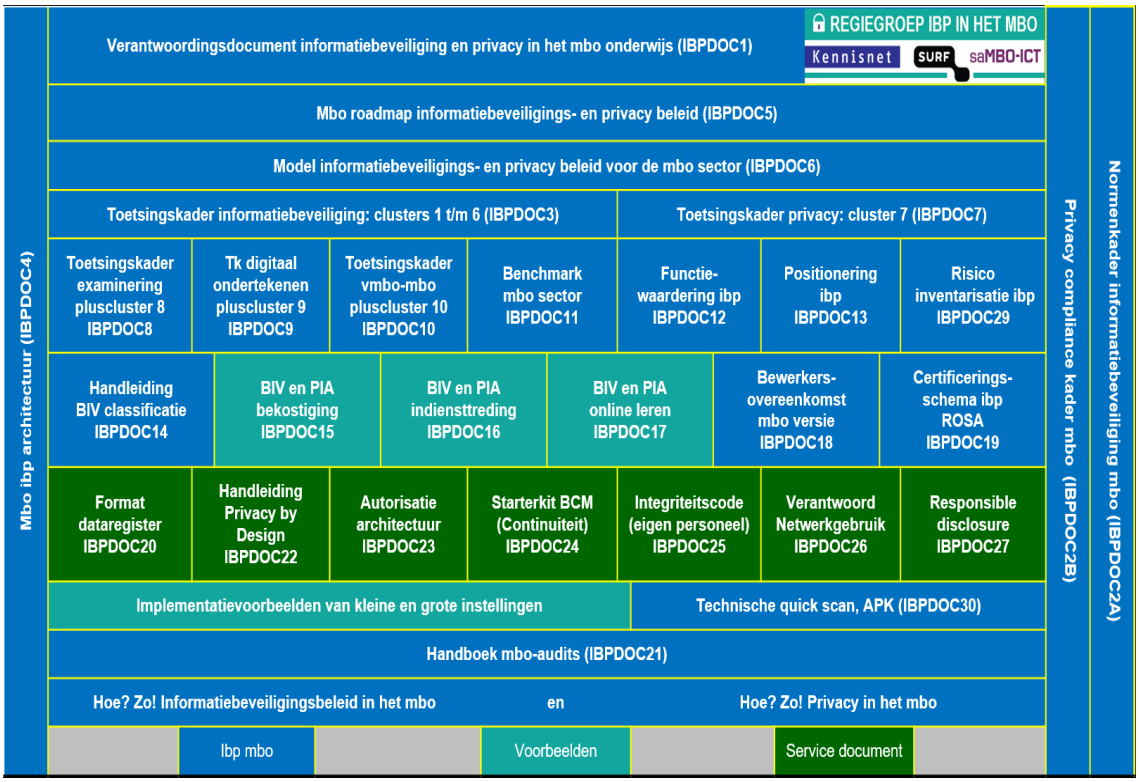
De ondersteuningsorganisaties Kennisnet en SURF maken hier ook deel van uit en kunnen op verzoek van de regiegroep inhoudelijke bijdragen leveren op verschillende functionele issues rond ibp. De saMBO-ICT organisatie draagt zorg voor de bestuurlijke verankering van ibp bij de MBO Raad en OCW.

Framework ibp in het mbo

Het **Framework ibp in het mbo** bevat alle documentatie voor een goede implementatie van ibp in een mbo-instelling. De gegeven kaders in deze documenten zijn relatief vast; de handreikingen, voorbeelden en modellen zijn hierin dynamischer van aard.

Framework

Deze roadmap is geheel gebaseerd op de onderdelen uit onderstaand **Framework ibp in het mbo**; door de stappen in deze roadmap te doorlopen kom je alle onderdelen uit dit framework vanzelf tegen. Eigenlijk is deze aanpak een gebruiksvriendelijke benadering van het Framework. Klik **hier** als je direct naar de website van het framework wilt gaan.



Het framework is eind 2016 ook fysiek gepubliceerd in de vorm van een toolbox. Deze is intussen aan alle CvB's van de mbo instellingen persoonlijk aangeboden.

Toetsingskaders

Kern van het framework zijn de toetsingskaders voor het mbo. Deze kaders zijn afgeleid van de normenkaders die we binnen het onderwijs hanteren. Afspraak is om binnen het onderwijs één normenkader te hanteren dat gebaseerd is op de ISO norm 27001/27002 voor informatiebeveiliging.

Dit levert voor het mbo het **Normenkader informatiebeveiliging mbo** op, zoals er ook een variant voor het hoger onderwijs is. Zowel de normen- en toetsingskaders zijn inhoudelijk gelijk, alleen de lay-out en grafische vormgeving wijkt af. Het toetsingskader is ten opzichte van het normenkader verrijkt met de bewijsvoering op 5 niveaus, te beginnen bij **ad hoc** (niveau 1) tot en met **state of the art** (niveau 5).

Roadmap Informatiebeveiliging

Onderstaand overzicht toont je het basismodel van deze aanpak.

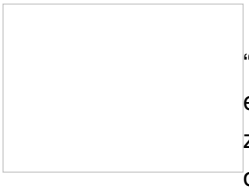
Het startpunt zijn de risico's die je als instelling loopt op het gebied van informatiebeveiliging en privacy. Daarop volgt een aanpak die bestaat uit drie cruciale pijlers, allen even belangrijk: het beleid, de mens en de architectuur.

Op alle drie de pijlers worden maatregelen getroffen: maatregelen die concreet en ook meetbaar zijn. Daarvoor is het toetsingskader mbo ontwikkeld. Aan de hand van een inventarisatie (een scan, een audit) kun je kijken of de maatregelen ook effect hebben. Om het geheel te onderhouden, verder te ontwikkelen en te verbeteren is er een ibp beheer organisatie nodig.

We gaan in deze module stap voor stap deze pijlers uitwerken, waarmee je een gezonde basis voor een adequaat informatiebeveiligingsbeleid in je instelling legt.

Succes!

0. Inventarisatie risico's IB



"*Breng nu eerst maar eens de risico's voor onze instelling in kaart.*" Dit is de eerste opmerking die menig ibp-functionaris hoort. Begrijpelijk natuurlijk, want het zijn de risico's tenslotte die de urgentie van je programma bepalen (zie hiervoor ook het **Verantwoordingsdocument**).

Risico inventarisatie

Gelukkig is er op het gebied van risico-inventarisatie al veel werk verricht door diverse mbo's. Dat heeft geresulteerd in een zeer complete inventarisatie; de **Handleiding Risico management**. Als eerste stap in het proces kun je de in deze inventarisatie beschreven risico's ook als uitgangspunt voor jouw organisatie nemen.

Ervaringen

Als je kijkt naar ervaringen vanuit het mbo veld dan zijn de grootste risico's als volgt te benoemen:

- **toetsing en examinering;**
- **zorgdossier studenten;**
- **gesprekscyclus medewerkers;**
- **continuering bedrijfsproces.**

Uiteraard staat de examinering bovenaan; de belangrijkste waardepapieren van een onderwijsinstelling zijn tenslotte de diploma's. Direct daarna is het van belang om alle gegevens die een onderwijsinstelling heeft van studenten en medewerkers zo goed mogelijk te beschermen. Tot slot is er een continue toename van hacks en DDoS aanvallen waarmee kwaadwillenden proberen het werken van de instelling onmogelijk te maken. Via **deze link** kun je lezen hoe je hier als school mee om kunt gaan.

Het Cyberdreigingsbeeld (SURF, 2016) voor de sector onderwijs en onderzoek geeft een prima overzicht van de dreiging voor het onderwijsproces. Kennisnet heeft meegewerkt aan dit rapport.

Stap 0: Nul-meting

Maar hoe ga je hier nu mee aan de slag? Als handvat kiest Kennisnet ervoor om gebruik te maken van de 'mbo audit methode' gebaseerd op het **mbo toetsingskader**, als afgeleide van de betreffende ISO normering voor informatiebeveiliging en privacy (ISO 27001/27002). Aan de hand van deze 'mbo audit' kun je een quick scan uitvoeren die jullie zwakke plekken ten aanzien van de informatiebeveiliging in beeld brengt; dat zijn tenslotte ook je directe risico's.

Je doet de nul-meting om een eerste beeld te krijgen van de ibp situatie in je instelling. Dat geeft helder de risico's weer en je hebt ook meteen je prioriteiten helder.

Maturity levels

Deze nul-meting levert je niet alleen een prioritering op; het toetsingskader voorziet ook in een set van maatregelen met bijbehorende 'maturity levels' van niveau 1 tot en met 5. Deze levels geven aan tot op welk niveau je de betreffende maatregel kunt implementeren om het risico te verminderen. Want niet alles hoeft in één keer; risicomanagement gaat in stappen. Zie het hoofdstuk 'Audit' in het **Toetsingskader** voor verdere verdieping. Het **handboek Mbo Audit** geeft daarnaast alle statements en maatregelen overzichtelijk weer.

1. Beleidsplan IB

De volgende stap in het proces is het op orde brengen van de beleidsmatige zaken. Het doel is om een algemeen deel van het beleidsplan op te stellen waarmee de instelling zich verantwoordt op de aanpak van ibp. Dit is zeker geen uitputtend verhaal over ibp, maar een set van basisafspraken rondom de omgang met ibp.

Stap 1: Beleid op orde

Het algemene deel van het beleidsplan is aan de hand van het 'model beleidsplan voor ibp in het mbo' vrij eenvoudig op te stellen. Je kunt hiervoor onderstaande stappen doorlopen:

1. *download het model beleidsplan in **Word-formaat**;*
2. *vul waar nodig de naam van de eigen mbo-instelling in;*
3. *vul in de met rood gearceerde delen de specifieke situatie voor de eigen instelling in.*

Je hebt nu een beleidsplan voor de omgang met ibp binnen jouw instelling! **LET OP**: Het College van Bestuur is eindverantwoordelijk voor het beleidsplan en moet het dan ook formeel vaststellen en in de organisatie beleggen. Het beleidsplan ibp biedt vervolgens de kaders en een houvast voor de ibp manager.

Toelichting op het model beleidsplan

Een beleidsplan ibp bevat minimaal de volgende onderdelen:

- **Algemene verantwoording;**
- **Governance (IBP manager);**
- **Compliance (AVG, WEB, etc.);**
- **Classificatie schema;**
- **IB crisisgroep benoemd.**

In het model beleidsplan komen deze onderdelen ook aan de orde. Onderstaand vind je voor enkele onderdelen een korte toelichting. Lees deze goed door voordat je het model zelf gaat invullen:

- Governance

Belangrijk onderdeel van het beleidsplan is de 'governance'; hoe heb je ibp binnen de instelling geregeld, wie heeft welke verantwoordelijkheid en welke rollen en functies heb je op welke manier ingevuld? Het is goed om dit al zoveel mogelijk in het beleidsplan op te nemen. Belangrijk is om in samenwerking met de proceseigenaren goed weer te geven op welke wijze je de dataregistratie vormgeeft.

Als ondersteuning voor deze aspecten zijn er twee documenten opgesteld:

- het document **Positionering ibp** geeft weer hoe de verschillende mbo instellingen de Governance geregeld hebben. De onderliggende enquête dateert van medio 2016;
- in het document **Competenties ibp** zijn enkele functiebeschrijvingen rond ibp weergegeven die kunnen helpen bij het inschalen en positioneren van personen op deze functies.

- Compliance

Het begrip 'compliance' heeft betrekking op de manier waarop de instelling 'compliant' wil worden tot de wetgeving op het gebied van ibp. Ook hier is het van belang om het beschreven beleid in eerste instantie algemeen te houden; de details komen later wel. Met het oog op de aankomende verplichting

om te voldoen aan de AVG (vanaf mei 2018) is het relevant om dit in het beleidsplan op te nemen. Dat geldt zowel voor de inleidende tekst die moet verwijzen naar de AVG, als voor de diverse andere hoofdstukken.

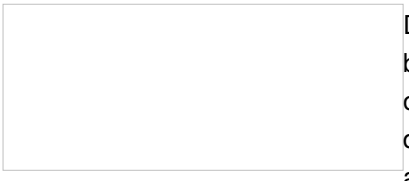
- Classificatie

De kern van het informatiebeveiligingsbeleid is het classificeren van de data; welke mate van beveiliging is nodig voor welk type data? In het beleidsplan vind je een aanzet om tot een zogenaamde BIV classificatie te komen (betrouwbaarheid, integriteit en vertrouwelijkheid). Dit is de basis voor de te treffen maatregelen rondom informatiebeveiliging. Zeker in het kader van de AVG is het belangrijk om deze classificatie serieus op te nemen. In het beleidsplan is het tevens van belang om aan te geven welke classificatie waarop van toepassing is en welke beheersmaatregelen je hiervoor gaat nemen.

- Incidenten

Tot slot moet je in het beleidsplan aangeven op welke wijze de instelling omgaat met incidenten en hoe je de organisatie daarvan in de vorm van een IB-crisisgroep (ook wel 'incident response team' genoemd) aanpakt. In het hoofdstuk over dergelijke incidenten moet je in het kader van de AVG ook aandacht besteden aan het beleid rondom datalekken.

2. Mens



De menselijke factor is van groot belang bij de implementatie van beleid rondom ibp. Je kan nog zulk goed beleid hebben ontwikkeld of nog zulke goede technische maatregelen hebben getroffen, als de mensen in de instelling de 'deur' open laten staan dan helpt dat allemaal niks. Daarom is bewustwording rond ibp van cruciaal belang.

De menselijke factor

Ook zonder kwade bedoelingen kan er rondom ibp een hoop misgaan. Gewoon in de simpele dagelijkse handelingen die wij als mens en als medewerker doen:

- wachtwoorden opschrijven op die handige gele memootjes en op je toetsenbord plakken;
- even koffie halen en je laptop open laten staan waar studenten er eventueel bij kunnen;
- de intaker van een andere instelling even via e-mail wat persoonlijke gegevens van een student sturen;
- per ongeluk een lijstje met wachtwoorden van de studenten voor je onderwijsapplicatie op de beamer tonen;
- enzovoort…

En zeker, dat gebeurde jaren terug ook al. Iedereen kent wel een collega die informatiegevoelige papieren op een bureau liet slingeren of het originele proefwerk onder het kopieerapparaat vergat. In onze steeds digitalere wereld zijn de risico's voor een snelle verspreiding alleen exponentieel toegenomen. Daarom is 'awareness' rondom ibp in het onderwijs misschien wel **het belangrijkste aandachtspunt**.

Medewerkers van een onderwijsinstellingen moeten een gevoeligheid ontwikkelen voor de problematiek en het antwoord weten op vragen als:

- wat zijn de risico's rond ibp?
- wat is het beleid, welke afspraken en regels zijn er?
- waar kan ik terecht voor ondersteuning of bij vragen?

Stap 2: Start een 'Awareness' campagne

In het toetsingskader zijn onder cluster 2 (Personeel, Studenten en Gasten) maatregelen opgenomen die de risico's op dit gebied aanpakken. Deze maatregelen kunnen de basis vormen van een 'awareness campagne', een zichtbaar offensief binnen de instelling om meer bewustzijn te creëren op het gebied van ibp. Je kunt hiervoor onderstaande stappen doorlopen:

1. lees de mogelijke maatregelen in **cluster 2 van het toetsingskader**;
2. zorg voor heldere protocollen, bijvoorbeeld ten aanzien van:
    - verantwoord internetgebruik (**Verantwoord netwerkgebruik mbo versie**);
    - melden van mogelijke lekken (**Responsible disclosure mbo versie**);
    - geheimhoudingsplicht voor specifieke functies (**Intergriteitscode, mbo versie**);
3. ontwikkel, mogelijk in samenwerking met de communicatie-afdeling, een interne campagne over bewustwording rondom ibp;
4. monitor de voortgang en zorg voor een cultuur waarbij men elkaar op dit onderwerp durft aan te spreken.

Hulpmiddelen

Onderstaand vind je enkele hulpmiddelen die je kunnen helpen bij het ontwikkelen van een 'awareness campagne':

- materialen zoals **posters, flyers en podcasts** (alleen toegankelijk voor leden van het netwerk);
- het spelen van een quiz of een game met elkaar, bijvoorbeeld deelname aan de **MBOAlert! game** is een goede mogelijkheid voor alle mbo instellingen (alleen toegankelijk voor leden van het netwerk);
- de toolbox **Cybersafe Yourself** van SURF kan je op allerlei nieuwe ideeën en initiatieven komen.

3. Architectuur

De derde pijler van het model is de 'architectuur'. Architectuur is een breed begrip, waarbij wel eens verwarring is waar het dan over gaat. Architectuur gaat feitelijk over uitgangspunten en principes die je wilt hanteren en de afspraken die je aan de hand daarvan maakt.

Ingewikkeld?

Op basis van uitgangspunten en principes volgt veelal een concept of ontwerp; vandaar dat men bij architectuur vaak aan ingewikkelde schema's denkt, wat niet geheel onterecht is. Ook denkt men bij 'architectuur' vaak aan het technische deel en ook daarvoor is iets te zeggen. De uitgangspunten en afspraken hebben zeker veelal technische consequenties.

Drie hoofdaspecten

In deze roadmap bakenen we architectuur af tot drie hoofdaspecten:

3a. BIV classificatie

Het classificeren, dus het neerleggen van uitgangspunten en het maken van afspraken over het belang van verschillende informatiestromen en systemen. Dit doen we aan de hand van drie aspecten, te weten beschikbaarheid (van systemen), integriteit (kloppen de gegevens?) en vertrouwelijkheid (wie mag waar bij?).

3b. Proceseigenaren

Het koppelen van processen en systemen aan proceseigenaren en het maken van afspraken met hen over de gewenste/noodzakelijke niveau's van beveiliging.

3c. Techniek

De onderliggende technische aspecten; voldoet de organisatie wel aan de technische afspraken die er zijn om de beveiliging adequaat te regelen?

In de volgende drie pagina's gaan we dieper op deze drie hoofdaspecten in.

- 3a Architectuur: BIV classificatie

De 'architectuur' is de derde pijler waarop het programma ibp is gebaseerd. Schrik niet, we hebben het dan gewoon over de kaders en afspraken die er liggen en de principes van waaruit gewerkt wordt, niet zoals gezed over ingewikkelde ICT…

BIV classificatie

Het doel van deze stap is om de processen en bijbehorende applicaties binnen je instelling goed in beeld te krijgen. Hiermee weet je welke gegevens jouw instelling verwerkt zodat je aan de hand daarvan kunt bepalen welke mate van beveiligingseisen je moet stellen. Dat proces heet de 'BIV classificatie'. BIV staat voor:

- **Beschikbaarheid;**
- **Integriteit;**
- **Vertrouwelijkheid.**

In het kort komt het erop neer dan je kijkt naar de mate van beschikbaarheid die nodig is voor een applicatie die een proces ondersteunt; dat is het infrastructurele kenmerk. Klik op de afbeelding rechts om de verschillende classificatieniveau's te zien:

Stap 3a: jouw BIV classificatie opstellen

Een BIV classificatie voor jouw instelling stel je in drie stappen op:

1. Beschikbaarheid

De eerste prioriteit is het in beeld brengen van alle processen en de bijbehorende applicaties. We raden je sterk aan gebruik te maken van een referentie architectuur, zodat je niet het wiel opnieuw hoeft uit te vinden… Welke referentie je daarbij gebruikt is minder relevant; kies bijvoorbeeld uit een van onderstaande referenties:

- **De ROSA (referentiearchitectuur onderwijs)**
- **De HORA (hoger onderwijs referentie architectuur)**
- **De Triple A (mbo sectorspecifieke onderwijs procesarchitectuur)**

De basis voor de referentiearchitectuur is weergegeven in het document **Mbo ibp architectuur**. De beschikbaarheid zet je standaard op 'midden' (hersteltijd 48 uur).

2. Integriteit

Vervolgens kijk je naar de mate van accuratesse die nodig is; de integriteit. Dit geeft het belang van de volledigheid, juistheid en tijdigheid van de gegevens aan. Voor integriteit is bepalend in welke mate gegevens correct moeten zijn (volledigheid, tijdigheid en juistheid). Dit bepaalt ook de maatregelen die je moet nemen (zelfcontrole, automatische controle door de applicatie, persoonlijke controle of dubbele

persoonlijke controle: het ‘vier ogen principe’).

3. Vertrouwelijkheid

Tot slot gaat het om de vertrouwelijkheid; wie heeft toegang tot welke gegevens? Dit moet voor alle relevante applicaties in de instelling geregeld zijn. Wat betreft vertrouwelijkheid moet bij het verwerken van persoonsgegevens de toegang tot die gegevens extra aandacht krijgen. Vertrouwelijkheid is dan ook altijd ‘midden’ of ‘hoog’, waarbij een autorisatiematrix (midden) of strikt persoonlijke toegangsrechten (hoog) worden gehanteerd. Met de vertrouwelijkheid komt dus vooral de menselijke kant in beeld.

- 3b Architectuur: proceseigenaren

De proceseigenaren bepalen welke classificatie ieder proces krijgt. De BIV classificatie stel je dan ook samen met hen op. De ibp-functionaris heeft hierbij een faciliterende rol, met als uitdaging om de proceseigenaren hierbij echt te betrekken.

Persoonsgegevens

De proceseigenaren bepalen de BIV classificatie omdat zij eigenaar zijn van de processen, systemen (applicaties) en data. Maar zij zijn geen eigenaar van de persoonsgegevens van de medewerkers, studenten en andere betrokkenen. Een mbo instelling heeft namelijk de (reguliere en bijzondere) persoonsgegevens slechts in bruikleen. Het College van Bestuur (CvB) is verwerkingsverantwoordelijke en mandateert hun directeur(en) om er op toe te zien dat dit zorgvuldig gebeurt.

Een CvB kan er voor kiezen de directeur HR verantwoordelijk te maken voor de persoonsgegeven van het personeel en de directeur Onderwijs voor de persoonsgegevens van de studenten. Ondersteund door de functionaris(sen) ibp toetsen zij of men persoonsgegevens mag delen met Externe Verwerkingsverantwoordelijken (Belastingdienst, DUO, etc..). Worden persoonsgegevens verwerkt in cloud-applicaties, dan zorgen zij dat er een Bewerkersovereenkomst aanwezig is.

In de **Handleiding BIV classificatie** is uitgebreid beschreven hoe je deze aanpak kunt uitvoeren. In een set van voorbeelden voor enkele specifieke processen zoals bekostiging, indiensttreding en online leren zijn deze BIV classificaties voor deze processen ook als voorbeeld helemaal uitgewerkt:

- **BIV en PIA bekostiging**;
- **BIV en PIA indiensttreding**;
- **BIV en PIA online leren**.

Klik op de figuur rechts om de verschillende koppelingen te zien waar je in het mbo mee te maken hebt. Wees bij iedere koppeling dus alert op mogelijke uitwisseling van persoonsgegevens die onder de strikte normen van ibp vallen.

Stap 3b: Maak goede afspraken met de proceseigenaren

Het is belangrijk om de juiste proceseigenaren te identificeren of te benoemen en om vervolgens met hen afspraken te maken in het kader van informatiebeveiliging en privacy. Het gaat dan om de data waar de proceseigenaren verantwoordelijk voor zijn te classificeren en de juiste maatregelen te treffen.

Voer een PIA uit

Een nog onbekend aspect hierbij is de eventuele noodzaak om een ‘PIA’ uit te voeren. PIA staat voor

‘privacy impact assessment’; In goed Nederlands een gegevensbeschermings-effect-beoordeling (GEB) genoemd. In de nieuwe wetgeving moet je een PIA uitvoeren op het moment dat je denkt dat een applicatie gegevens verwerkt waarbij, gelet op de aard, de omvang, de context en de doeleinden van de applicatie, het waarschijnlijk is dat die een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

In hoofdstuk 3.4 gaan we verder in op de PIA. Aan de hand van de PIA kun je vervolgens bepalen of je een zogeheten bewerkersovereenkomst moet afsluiten met de leverancier van de applicatie. De bewerkersovereenkomsten behandelen we in hoofdstuk 3.8.

Bewerkersovereenkomst

Een belangrijk punt uit de bewerkersovereenkomst is de vraag of een leverancier zich aan de overeenkomst houdt. Dat kan doordat de leverancier een verklaring afgeeft die door een externe partij is opgesteld (een third party memorandum) of doordat ze voldoen aan een specifieke normering (ISO certificering).

Een ontwikkeling hierbij is het certificerings-schema; een checklist met beveiligings- en privacymaatregelen die in samenwerking tussen onderwijsraden, instellingen en leveranciers onder leiding van Kennisnet is vastgesteld. Aan de hand hiervan kun je aangeven in welke mate een leverancier voldoet aan de vereisten. Dit geeft instellingen en leveranciers een handvat om te beoordelen of de overeengekomen afspraken hard te maken zijn.

Security-architectuur

Als al deze checks zijn gedaan, dan is voor het betreffende proces de BIV classificatie en eventueel de vereiste van een PIA afgerond. Het aan één rijgen van alle processen binnen de onderwijsinstelling levert uiteindelijk een compleet schema op dat je ook de ‘security-architectuur’ van de instelling kunt noemen. Klik op de figuur rechts om een voorbeeld van een dergelijk schema te zien.

Meer informatie over de security-architectuur is opgenomen in de **Handleiding BIV classificatie**.

- 3c Architectuur: techniek

In het verleden was het ibp-beleid vooral een technische aangelegenheid. Tegenwoordig gaat het bij de aanpak van ibp in het mbo veel meer over goede afspraken en menselijke aspecten.

Benchmarks

Toch is ook de techniek nog steeds een belangrijk aspect bij ibp. Uit de benchmarks blijkt gelukkig dat de techniek in het mbo vaak goed geregeld is; de clusters 3 en 4 scoren bij de meeste instellingen boven maturity level 2. Zou ook nog de documentatie rondom de techniek verbeteren, dan zou de werkelijke score nog hoger liggen.

Stap 3c: doe een Quick scan

Niettemin moet de ibp functionaris ook met de ict afdeling aan de slag om hier kritisch op te blijven. In het kader van het ibp programma is er een ‘Quick scan APK’ ontwikkeld om de belangrijkste technische aspecten in beeld te brengen. Ook voor de niet technisch onderlegde ibp-functionaris is dit een goed werkbaar schema (**Quick scan APK**).

Mocht dit toch te ingewikkeld blijken, dan zijn er intussen diverse marktpartijen die de Quick scan goed uit kunnen voeren. Het verdient overigens aanbeveling om het daar niet bij te laten, maar bijvoorbeeld ook een 'PEN test' te laten uitvoeren. Deze test bekijkt in welke mate de infrastructuur gevoelig is voor externe hacks.

Ondersteuning

Voor de meer technische kant biedt het Framework ibp in het mbo nog een set van handige service documenten die deels ook uit het hoger onderwijs zijn overgenomen:

- **Autorisatie Architectuur mbo versie**;
- **Starterkit business continuity management mbo versie**.

4. Audit IBP

Het doel van de in deze cursus beschreven aanpak is dat de gepleegde interventies tot meetbare resultaten leiden. Hiermee maak je de voortgang en de nog te zetten stappen inzichtelijk. Door het werken met een concreet toetsingskader meet je waar je staat, waar je zou moeten staan en waar je zou willen staan. Dat gebeurt aan de hand van een 'audit'.

Audit

De audit kent diverse gradaties. In deze aanpak is een in zwaarte oplopend schema van vijf type audits opgenomen waarmee je de status van ibp in jouw instelling kunt toetsen:

- **Self-assessment (quick scan)**;
  Een interne audit, uitgevoerd door de ibp-functionaris zelf
- **Benchmark ibp in het mbo**;
  Een intensievere check van alle statements binnen de organisatie
- **Peer review**;
  Een collega-instelling beoordeelt de scores die jij jezelf hebt gegeven
- **Peer audit**;
  Een collega-instelling voert een audit bij jouw instelling uit en vice versa
- **Externe audit.**
  Een extern bureau gespecialiseerd in audits voert de audit uit

In **dit document** vind je meer informatie over de inhoud van ieder type audit.

Stap 4: Neem deel aan de benchmark!

De **Benchmark ibp in het mbo** is in 2015 voor de eerste keer gehouden. Deze benchmark gaf een eerste voorzichtig beeld van de stand van zaken in de mbo sector. In 2016 is de benchmark herhaald, waarbij tot nu toe in totaal 30 instellingen aan de benchmark deelnamen. De drie gehouden benchmarks zijn onderstaand te vinden:

- **Benchmark versie 1.0**;
- **Benchmark 2015**;
- **Benchmark 2016**.

In 2017 is de ambitie dat de meeste mbo-instellingen gaan deelnemen, om:

- een zo breed mogelijk beeld van de sector te verkrijgen, dat is immers alleen mogelijk als

zoveel mogelijk instellingen deelnemen;
- te bewerkstelligen dat zoveel mogelijk instellingen in samenwerking met ibp bezig zijn, al dan niet in sectorverband.

Alleen op deze manier nemen we als sector onze verantwoordelijkheid en maken we ook daadwerkelijk stappen om de risico's zoveel mogelijk te beperken.

Training

In 2016 is een eerste groep ibp functionarissen uit het mbo getraind in het doen van peer reviews. Naast een inhoudelijk training met betrekking tot auditing wordt ook in de praktijk geoefend door bij elkaar in de keuken te gaan kijken. In 2017 wordt een tweede ronde georganiseerd. Doelstelling is om wat meer mensen in de mbo sector deze deskundigheid te laten verkrijgen zodat men wellicht op termijn een systeem van peer reviews in het mbo kan introduceren.

5. Beheersorganisatie IBP

Informatiebeveiliging en privacy is geen eenmalig actie, geen project dat ooit klaar is. Het is een continu en cyclisch proces dat borging heeft in de dagelijkse gang van zaken. Dit vereist een beheerorganisatie die constant nadenkt over aanpassingen en verbeteringen, zodat ibp stapsgewijs in het DNA van de instelling komt te zitten.

Continue ontwikkeling

Een goed ibp beleid vergt een continue ontwikkeling, hoe klein de stapjes die je kunt zetten misschien ook zijn. Uiteindelijk moet het in iedere mbo-instelling, groot en klein, onderdeel van de dagelijkse praktijk worden. In de arbeidscontracten en de gesprekscyclus van het personeel, in de onderwijs- en praktijkovereenkomsten met studenten, in de afspraken en contracten met leveranciers en bij de uitwisseling van gegevens met anders onderwijs gerelateerde instellingen.

Stap 5: Breng de governance op orde

Met een mooi woord geven we aan dat de 'governance' dan goed geregeld is. Dat betekent dat de verantwoordelijkheden belegd zijn, dat er functionarissen benoemd zijn en dat er functies, rollen en taken zijn belegd in de organisatie.

1. College van Bestuur

De governance begint bij het CvB die direct verantwoordelijk is voor ibp in de organisatie. Daarom is het ook zo van belang dat er voldoende draagvlak is bij het CvB om dit aan te pakken.

2. Functionaris

De tweede stap is het aanstellen van een ibp functionaris (ook wel security officer, privacy officer of ibp manager genoemd). Deze persoon moet het mandaat hebben om ibp vorm te geven en in nauwe samenspraak met de proceseigenaren het beleid uitrollen. Voorwaarde hierbij is dat deze proceseigenaren ook expliciet bekend en benoemd zijn.

3. Beheerorganisatie

De uiteindelijke beheerorganisatie kan op meerdere manieren vorm krijgen. In het document **Positionering ibp** is op basis van een enquête een overzicht gegeven hoe dit in mbo instellingen is aangepakt. Gebruik dit document om voor jouw instelling een beeld te vormen hoe jullie de beheerorganisatie vorm kunnen geven. Bij kleinere instellingen, waar minder personeel beschikbaar is, zal het dan veelal gaan om combifuncties.

4. Verplichting

Per 25 mei 2018 is elke onderwijsinstelling verplicht om een zogenaamde FG, een Functionaris voor de Gegevensbescherming, te hebben. Deze persoon is expliciet in de functie van FG voor de instelling benoemd. Dat kan in de vorm van een deelfunctie binnen de instelling, maar ook in een samenwerking met andere instellingen of zelfs als dienst (FG as a service) vanuit een externe partij.

In hoofdstuk 3 van deze roadmap, waar het expliciet gaat over privacy en het compliant worden aan de Europese verordening in deze (de AVG), gaan we hier dieper op in.

Roadmap Privacy

Deze Roadmap-2 helpt je om op 25 mei 2018 op hoofdlijnen te voldoen aan de AVG (Algemene Verordening Gegevensbescherming). De belangrijkste punten hieruit zijn door de Autoriteit Persoonsgegevens in een tiental stappen weergegeven. Op basis hiervan is dit tien stappen model gemaakt voor het mbo, dit maakt de implementatie van de AVG concreet en hanteerbaar.

Hiernaast vind je een begrippenlijst voor de privacy module. Begrippenlijst

De volgende 10 stappen komen aan de orde. Tussen haakjes is aangegeven welke ondersteuning Kennisnet naast deze roadmap aanbiedt.

Stap 1: **Bewustwording** (scholing en awareness);

Stap 2: **Rechten van de betrokkenen** (nieuw privacy reglement);

Stap 3: **Overzicht verwerkingen** (data registers);

Stap 4: **Privacy impact assessment** (3 methoden plus voorbeelden);

Stap 5: **Privacy by design en Privacy by default** (voorbeeld vanuit CIP);

Stap 6: **Functionaris voor de gegevensbescherming** (functiebeschrijving, scholing en netwerk);

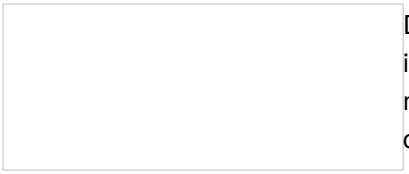
Stap 7: **Meldplicht datalekken** (best practices);

Stap 8: **Bewerkersovereenkomsten** (vastgestelde bewerkersovereenkomsten);

Stap 9: **Leidende toezichthouder** (Nederland en België).

Stap 10: **Toestemming** (voorbeeld document)

1. Bewustwording



De factor 'mens' is en blijft van groot belang. Niet alleen bij informatiebeveiligingsaspecten, zoals we in hoofdstuk 2 zagen, maar ook bij privacy is bewustwording van alle betrokkenen cruciaal. Enkele voorbeelden:

- je stuurt een e-mail met alle gegevens van een student naar een collega;
- bij de aanmelding voor een activiteit vraag je toch maar even wat extra gegevens, altijd handig;
- leuk al die foto's van de excursie, ik zet ze even op de website.

Het lijkt zo voor de hand liggend om te doen, toch mag het in veel gevallen niet. En al helemaal niet zonder goede afspraken. Daarom is het zo van belang dat medewerkers van onderwijsinstellingen zich goed bewust zijn van de regels, de wetgeving en de afspraken die een instelling maakt met medewerkers, studenten en externe partijen.

Wat moet je doen?

Zorg ervoor dat de relevante mensen in jouw organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op de huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Bedenk dat de Authoriteit Persoonsgegevens (AP) jouw organisatie bij overtreding van de nieuwe privacywetgeving sancties kan opleggen van maximaal 20 miljoen euro of 4% van de wereldwijde omzet!

Hoe doe je dat?

Er zijn vier belangrijke veranderingen die vanaf 25 mei 2018 gaan spelen. Zorg dat alle betrokkenen in jouw organisatie zich hiervan bewust zijn:

1. Voldoen aan de AVG

De instelling moet voldoen aan een set van Europese privacyregels, vastgelegd in de **Algemene Verordening Gegevensbescherming** (AVG). Door de AVG zijn alle persoonsgegevens van alle EU-inwoners straks op dezelfde wijze beschermd, ongeacht of hun gegevens zijn opgeslagen in Europa of - bijvoorbeeld - de Verenigde Staten.

2. Dataminimalisatie

Als school ben je straks verplicht om te onderbouwen waarom je persoonsgegevens van studenten wilt gebruiken en hoe lang je die gegevens bewaart. Uitgangspunt daarbij is *dataminimalisatie*: je mag niet meer gegevens vragen dan strikt noodzakelijk. Na beëindiging van het gebruik van persoonsgegevens hebben ook studenten het 'recht om vergeten te worden'; zij kunnen hierom vragen.

3. Toestemming

Je moet toestemming voor het gebruik van persoonsgegevens regelen. Voor dat gebruik heb je soms toestemming nodig van studenten, bijvoorbeeld bij het gebruik van foto's. Je mag niet meer uitgaan van toestemming; er is een actieve handeling van studenten nodig, zoals een handtekening. Ook moet je studenten informeren waar ze precies mee instemmen en je moet kunnen bewijzen dat je toestemming hebt verkregen. En begin op tijd met het vastleggen van toestemming. Bijvoorbeeld als je je producten zoals leermiddelen in het onderwijs wilt gebruiken waar toestemming van studenten voor nodig is.

4. Bewuste omgang

De AVG stimuleert organisaties tot een bewustere omgang met privacy; op centraal niveau betekent

dat het uitvoeren van risicoanalyses, bijvoorbeeld om de aanschaf van een administratiesysteem te onderbouwen. Voor medewerkers betekent dit terughoudendheid bij het uitwisselen van persoonsgegevens, het maken van goede afspraken met studenten hierover en het kritisch bekijken welke informatie je publiceert of distribueert.

Vijf vuistregels

Bovenstaande veranderingen kun je samenvatten in een vijftal vuistregels; klik op de afbeelding rechts om ze te bekijken. Op grond hiervan kunnen medewerkers een inschatting maken van wat de impact van de AVG is op hun huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen.

Houd er rekening mee dat de implementatie van de AVG veel kan vragen van de beschikbare menskracht en middelen en dat zij vanaf 25 mei 2018 dus operationeel moet zijn!

Welke ondersteuning is beschikbaar?

In hoofdstuk 2 zijn al de verschillende hulpmiddelen genoemd, zoals:

- de game MBO Alert!, inclusief een medewerkersflyer, een presentatie en een Kahoot versie;
- de ideeën- en materialenbank Cybersafe Yourself;
- het platform van het netwerk ibp in het mbo waar de diverse materialen en ideeën vanuit mbo instellingen worden gedeeld.

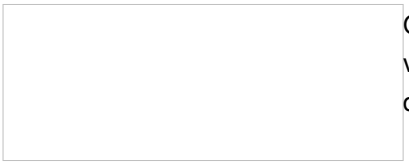
In het najaar van 2017 wordt in het mbo een Awareness Campagne Award uitgereikt. Instellingen worden opgeroepen om hun awareness campagnes te delen en de leuksten zullen uitgekozen en met een Award beloond worden. Meer info staat op het netwerk ibp in het mbo.

Tot slot is er een arrangement gemaakt speciaal voor medewerkers in het mbo. Dit kan je goed gebruiken om jij je collega's in te zettenom de bewustwording op een hoger peil te brengen. Er is ook een presentatie bij gemaakt die je in workshops met groepen collega's kunt gebruiken.

Bewustwording IBP voor medewerkers in het mbo

Presentatie bewustwording IBP voor medewerkers in het mbo

2. Rechten van betrokkenen



Onder de AVG krijgen de mensen van wie je persoonsgegevens verwerkt meer en verbeterde privacy rechten. Zorg er daarom voor dat zij hun privacy rechten goed kunnen uitoefenen.

Denk daarbij aan bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering. Maar houd ook alvast rekening met nieuwe rechten, zoals het recht op dataportabiliteit. Bij dit recht moet je ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen. Ook kunnen mensen bij de AP klachten indienen over de manier waarop je met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

Wat moet je doen?

Binnen de AVG moet je rondom de rechten van betrokkenen drie zaken regelen:

1. zorg dat er een **locatie** is (online en/of fysiek) waar betrokkenen verzoeken kunnen indienen;
2. zorg voor duidelijke **procedures** bij de behandeling van deze verzoeken;
3. zorg voor een **controlemechanisme** op de procedures.

Heb je deze drie zaken geregeld, dan ben je wat betreft de rechten van betrokkenen 'AVG compliant'!

Hoe doe je dat?

Iedere onderwijsinstelling is vrij om een vorm te kiezen waarin je bovenstaande zaken regelt. Als het maar op 25 mei 2018 geregeld is. Belangrijk hierbij is om goed op de hoogte te zijn om welke rechten het gaat en welke maatregelen je daarvoor moet nemen. Via onderstaande knop kun je het overzicht van 'Rechten van betrokkenen' downloaden en inzien:

Rechten van betrokkenen

Dit is tekstueel een lastig leesbaar document, vooral als je deze rechten intern of extern wilt communiceren. Als voorbeeld vind je onder de kop 'Welke ondersteuning is beschikbaar?' een versie van het Deltion College uit Zwolle, die de tekst zelf herschreven hebben. Die vrijheid mag je dus nemen, zolang de inhoud maar overeind blijft.

En wil je precies weten in welke artikelen je de rechten van betrokkenen binnen de **AVG** kunt terugvinden, dan vind je daar een overzicht van in onderstaand document:

Artikelen in AVG

Flyer

Rechts is een voorbeeld weergegeven van een flyer die je voor privacy zou kunnen gebruiken om de rechten van betrokkenen helder te maken. Klik op de afbeelding om de flyer te downloaden:

Welke ondersteuning is beschikbaar?

Ter ondersteuning vind je onderstaand twee voorbeelden van privacyverklaringen voor medewerkers en studenten van het Deltion College. Deze documenten kun je als eigen voorbeeld gebruiken en aanpassen voor jouw specifieke situatie:

Privacyverklaring medewerkers

Privacyverklaring studenten

3. Overzicht bewerkingen

Onder de AVG bestaat er een documentatieplicht, wat inhoudt dat je moet kunnen aantonen dat jouw organisatie in overeenstemming met de AVG handelt. Om hieraan te kunnen voldoen moet je alle verwerkingen van gegevens goed in kaart hebben gebracht.

Het overzicht van gegevensverwerkingen kun je ook nodig hebben als betrokkenen hun privacy rechten uitoefenen. Als zij jouw school vragen hun gegevens te corrigeren of te verwijderen, moet je dit doorgeven aan de organisaties waarmee je hun gegevens hebt gedeeld.

Wat moet je doen?

Om 'AVG compliant' te zijn met betrekking tot de verwerking van gegevens zul je aan vier criteria moeten voldoen:

- je moet een overzicht hebben **welke** persoonsgegevens er van betrokkenen verwerkt worden;
- je moet een overzicht hebben **wat** er bij die verwerkingen met de gegevens gebeurt;
- je moet van alle verwerkingen inzichtelijk hebben wat de **grondslag** van de verwerking is;
- je moet in staat zijn deze informatie aan de Authoriteit Persoonsgegevens te kunnen **overhandigen**.

Zowel de Verwerkingsverantwoordelijke als de Verwerker hebben hierbij een specifieke documentatieplicht. Via onderstaande knop vind je een overzicht wat deze documentatieplicht voor beide rollen precies inhoudt:

Overzicht documentatieplicht

De Verwerkingsverantwoordelijke is de voorzitter van het College van Bestuur. Hij/zij draagt deze taak over aan de directeur HRM. De instelling benoemt een ibp manager die er op toe ziet dat voldaan wordt aan de AVG.

Als persoonsgegevens met derden buiten een mbo instelling of met cloud applicaties worden gedeeld dan moet de medewerker daarvan **op de hoogte zijn** en doorgaans zal de medewerker **toestemming moeten geven**.

Dit is een van de kernpunten. Een onderwijsafdeling of dienst die persoonsgegevens wil delen met anderen of een cloud-applicatie wil aanschaffen, zal dit allereerst moeten voorleggen aan de IBP manager. *Klik rechts op de afbeelding om dit in een schematisch overzicht te zien.*

De gemandateerde Verwerkingsverantwoordelijke beheert de persoonsgegevens van de medewerkers, in dit geval de directeur HRM. Samen met de FG (Functionaris voor de Gegevensbescherming) en de IBP manager ziet deze persoon erop toe dat aan alle eisen van de AVG wordt voldaan.

De IBP manager is verantwoordelijk voor de “dagelijkse” gang van zaken. Hij/zij toetst of je persoonsgegevens met externen mag delen. De onderwijsafdelingen en diensten mogen binnen de muren van een mbo instelling vrijelijk de persoonsgegevens van de medewerkers gebruiken. Als zij persoonsgegevens willen delen met derden of toevertrouwen aan applicaties dan moet de IBP manager toestemming geven.

Hoe doe je dat?

Om je met de documentatieplicht goed op weg te helpen stelt Kennisnet het schema 'Dataregister' ter beschikking. In dit schema leg je per persoonscategorie (medewerker, student, etc.) alle relevante zaken rondom ibp vast. Je kunt via ***de afbeelding rechts een leeg dataregister als template downloaden*** en eenvoudig aanpassen voor jouw situatie; dit kan je veel tijd besparen. Dit is het dataregister voorbeeld voor medewerkers in loondienst. Er worden ook andere dataregisters ontwikkeld, zo is intussen ook het dataregister voor studenten beschikbaar. In het document **IBPDOC20 Dataregisters in het mbo** staan de beschikbare dataregisters bij elkaar.

De onderdelen in het dataregister hebben allen een kleur en verwijzen naar artikel 30 van de AVG. Via **deze link** zie je wat iedere kleur betekent. Tevens zijn in het dataregister de persoonsgegevens van medewerkers uitgesplitst in categorieën. **Klik hier** voor een overzicht van deze categorieën.

4. Privacy Impact Assessment

Onder de AVG kun je verplicht zijn een zogeheten *Privacy Impact Assessment* (PIA) uit te voeren. Dat is een instrument om **vooraf** de privacy risico's van een gegevensverwerking in kaart te brengen, zodat je de juiste maatregelen kunt nemen om risico's te verkleinen.

Wat is een PIA?

Een PIA maak je bij een grote verandering binnen een organisatie, denk aan de aanschaf van een nieuwe applicatie of een update. Er zijn drie aspecten van belang om over de PIA te weten:

Toetsmodel/vragenlijst

Een PIA heeft de vorm van een toetsmodel/vragenlijst. Op die lijst staan zowel feitelijke en technische vragen als vragen die zijn gebaseerd op nationale en Europese juridische vereisten. Het richt zo in een vroegtijdig stadium en op hoofdlijnen de aandacht op alle onderdelen van de beoogde verwerking van persoonsgegevens die aandacht en uitwerking behoeven.

Niet vrijblijvend

Een PIA is geen vrijblijvende enquête. In het bijzonder is de vragenlijst inhoudelijk gezien zowel richtinggevend als corrigerend bedoeld. Daarnaast moet het beantwoordingsproces als zodanig ook bewustwording stimuleren van de uiteenlopende privacy-aspecten waarmee je rekening moet houden bij de ontwikkeling van wetgeving en beleid en in dat kader te ontwikkelen ICT-systemen en databestanden.

Richtinggevend

Een PIA is richtinggevend in de zin dat de (uitputtende) vragenreeks kan wijzen op relevante privacy-risico's die in de vroege fase van beleids- of systeemontwikkeling (wellicht nog) niet zijn onderkend. Als dat het geval is, moet je de betreffende vraag zo opvatten dat het noodzakelijk is om deze aspecten alsnog in de uitwerking mee te nemen.

Beantwoording van de PIA-vragenlijst resulteert in een geschreven document waarmee je de privacy risico's van een bepaalde applicatie of proces in kaart brengt.

Wat moet je doen?

Een PIA is een hulpmiddel om bij ontwikkeling van een adequaat applicatielandschap (en de daarmee gepaard gaande aanschaf of bouw van ICT-systemen en aanleg van databestanden), privacyrisico's op gestructureerde en heldere wijze in kaart te brengen.

Je moet een PIA **altijd uitvoeren** als de beoogde gegevensverwerking waarschijnlijk een hoog privacy risico met zich meebrengt. Het is raadzaam om direct al bij **aanvang** van een project waarbij persoonsgegevens een rol spelen een PIA uit te voeren om te zorgen dat je risico beperkende maatregelen direct in het project mee kunt nemen.

Hoe doe je dat?

1. Dataregister

Een dataregister levert veel input op voor de PIA. Het is dan ook aan te raden om eerst het relevante dataregister(s) te maken en vervolgens aan de hand van het dataregister de PIA in te vullen.

2. Proces

Zorg binnen de organisatie voor een helder proces en een duidelijke taakverdeling. Het stappenplan hiervoor is in de afbeelding rechts te zien; klik op de afbeelding voor een grotere weergave.

3. Format

Het handigst is om eerste een PIA in eenvoudige vorm te maken. Hiervoor is een zogenaamde Pré PIA beschikbaar. Meestal is dat al voldoende. Deze Pré PIA is gebaseerd op het belgische model van de PIA.

Pré PIA model

In een enkel geval moet je een zwaardere PIA uitvoeren, bijvoorbeeld bij een nieuw HRM- of een studentenregistratie systeem.

Kies dan een van onderstaande formats voor de PIA en vul deze in:

1. **SURF PIA**
2. **NOREA PIA**

5. Privacy by design & by default

Vanaf mei 2018 moet privacy een grote rol in iedere organisatie spelen. Het is verstandig om daarom nu al jouw organisatie vertrouwd te maken met de onder de AVG verplichte uitgangspunten van '*privacy by design*' en '*privacy by default*'.

Wat betekent het?

Privacy by design houdt in dat je er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd.

Privacy by default houdt in dat je technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat je, **als standaard**, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat je wilt bereiken.

Wat moet je doen?

De Verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat je de verwerking in overeenstemming met deze verordening uitvoert. Daarbij houdt hij rekening met de aard, omvang, context en doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen. Die maatregelen evalueert en actualiseert hij waar nodig.

Als het in verhouding staat tot de verwerkingsactiviteiten, is één van de maatregelen een passend gegevensbeschermingsbeleid dat de verwerkingsverantwoordelijke uitvoert.

Deze verplichting geldt voor:

- de hoeveelheid verzamelde persoonsgegevens (denk aan aangepaste invulformulieren);
- de mate waarin zij worden verwerkt (doorgeven aan in- en externen);
- de termijn waarvoor zij worden opgeslagen (DSP van de MBO Raad);

- de toegankelijkheid daarvan.

Deze maatregelen moeten er met name ook voor zorgen dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk zijn.

Hoe doe je dat?

Privacy by design en privacy by default is vooral een proces van bewustwording. Bij iedere bestaande of nieuwe verwerking van persoonsgegevens moeten de verantwoordelijken vanuit het belang van de privacy werken. Het voert hier dan ook te ver om alle mogelijke verwerkingen te bespreken. Met onderstaand voorbeeld willen we duidelijk maken wat de impact van deze uitgangspunten kan zijn.

Voorbeeld privacy by design

In de praktijk kan *privacy by design* er bijvoorbeeld toe leiden dat je op basis van een BIV classificatie applicaties moet aanpassen. Klik op onderstaande afbeelding voor een grotere weergave en lees vervolgens de aansluitende tekst:

Je ziet in het schema dat “7 Gesprekscyclus” in de BIV classificatie een M-H-H (laatste kolom) classificatie heeft. De classificatie “Hoog” voor vertrouwelijkheid betekent dat er minimaal een 2-factor authenticatie verplicht is. Verdere hebben alleen de medewerker en de leidinggevende toegang tot de verslagen van beoordelings- en functioneringsgesprekken.

Het HR pakket moet dan ook die mogelijkheid bieden. Is dit niet mogelijk en hebben alle medewerkers van de afdeling HR en de applicatiebeheerders toegang tot de verslagen, dan moet je aanvullende maatregelen treffen. *Privacy by design* zou dan kunnen betekenen dat je de applicatie aanpast zodat er twee maal moet worden ingelogd op dit onderdeel waardoor alleen de leidinggevende en de betreffende medewerker toegang tot het dossier hebben.

Een andere oplossing is dat je in een tekstveld alleen meldt dat op een bepaalde datum een beoordelingsgesprek heeft plaatsgevonden tussen leidinggevende A en medewerker B, dat beiden het verslag van het gesprek akkoord hebben bevonden en beiden het verslag hebben ondertekend. Beiden hebben tevens een papieren verslag in ontvangst genomen.

Welke ondersteuning is beschikbaar?

Er is (nog) geen uitgewerkt voorbeeld voor de mbo sector beschikbaar. Dit is wel het geval voor de HO sector op basis van het CIP (Centrum informatiebeveiliging en privacy bescherming), die heeft een Handleiding Privacy by Design ontwikkeld. Er wordt gewerkt aan een mbo handleiding.

6. Functionaris gegevensbescherming

Onder de AVG zijn onderwijsinstellingen verplicht vanaf 25 mei 2018 een functionaris voor de gegevensverwerking (FG) aan te stellen. De FG-er houdt toezicht op de toepassing en op naleving van de AVG. Dit is daarmee een andere functie dan de rol die een IBP manager heeft binnen een onderwijs-instelling.

Wat moet je doen?

Dat is relatief eenvoudig; zorg dat jouw onderwijsinstelling op 25 mei 2018 een FG'er binnen de instelling heeft. Dit kan een personeelslid van de verwerkingsverantwoordelijke of de verwerker zijn, of de FG'er kan de taken op grond van een dienstverleningsovereenkomst verrichten.

Een functionaris voor de gegevensbescherming is geen ICT'er maar ook geen jurist. De FG'er moet aan 3 voorwaarden voldoen:

- Hij/zij moet de organisatie en de processen binnen de organisatie kennen;
- Hij/zij moet de AVG kennen;
- Hij/zij moet op de hoogte zijn van informatiebeveiliging.

De verwerkingsverantwoordelijke of de verwerker maakt de contactgegevens van de functionaris voor gegevensbescherming bekend en deelt die mee aan de toezichthoudende autoriteit.

Hoe doe je dat?

Voor het onderwijs zijn de volgende vijf richtlijnen na aanstelling van een FG van belang. Bedenk daarbij dat de FG met betrekking tot de uitvoering van zijn taken overeenkomstig het Unierecht of het recht tot geheimhouding of vertrouwelijkheid is gehouden.

1. Betrekken

Betrek de FG bij alle nieuwe projecten, aanbestedingen / aanschaf van applicaties, updates van applicaties en de opzet van vragenformulieren, al dan niet digitaal. De verwerkingsverantwoordelijke en de verwerker zorgen hiervoor.

2. Toegang

De verwerkingsverantwoordelijke en de verwerker ondersteunen de FG bij de vervulling van de taken door toegang te verschaffen tot persoonsgegevens en verwerkingsactiviteiten. Ook stellen zij de door hem benodigde middelen ter beschikking, zowel voor het vervullen van zijn taken als het in stand houden van zijn deskundigheid. De FG heeft dus vergaande rechten en mag alles zien op het gebied van persoonsgegevens.

3. Ontslagbescherming

De verwerkingsverantwoordelijke en de verwerker zorgen ervoor dat de FG geen instructies ontvangt met betrekking tot de uitvoering van zijn taken. Zij kunnen hem niet ontslagen of straffen voor de uitvoering van zijn taken. De FG brengt rechtstreeks verslag uit aan de hoogste leidinggevende van de verwerkingsverantwoordelijke of de verwerker. De FG geniet dus ontslagbescherming.

4. Benaderbaar

Betrokkenen kunnen met de FG contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten uit hoofde van deze verordening. Een medewerker kan bij de FG dus een verzoek indienen dat kan leiden tot beschadiging van de mbo instelling.

5. Belangen

De FG kan ook andere taken en plichten vervullen. De verwerkingsverantwoordelijke of de verwerker zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden. Een FG kan dus geen IBP manager zijn of andersom.

Relatie FG en IBP manager

Ten aanzien van het laatste punt, 'Belangen', zetten we via de knop hieronder nog eens de

verschillende taken en verantwoordelijkheden van de ibp manager en de FG naast elkaar. Hou hier goed rekening mee bij het opstellen van het functieprofiel voor de aan te stellen FG:

Taken FG en IBP manager

Welke ondersteuning is beschikbaar?

- Ter ondersteuning bieden we hier nog het functieprofiel van de FG, zie de functiewaardering FG in het document **Competenties ibp versie 2.0, Framework ibp in het mbo**.

- Tevens vind je via **deze link** een handig artikel van de VNG over de positionering van een FG.

7. Meldplicht datalekken

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. Er zijn wel strengere eisen aan de eigen registratie van datalekken. Zo moet je alle datalekken documenteren. Hiermee moet de AP kunnen controleren of je aan de meldplicht hebt voldaan. Dit gaat verder dan de huidige Wbp-protocolplicht, die alleen gaat over gemelde datalekken.

Wat moet je doen?

Indien er sprake is van een datalek dient de FG onderstaande drie handelingen uit te voeren:

1. Melding van een datalek aan de toezichthouder

Indien een inbreuk in verband met persoonsgegevens (ook wel 'datalek' genoemd) heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk **72 uur** nadat hij er kennis van heeft genomen, aan de toezichthouder (Autoriteit Persoonsgegevens), tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Indien de melding aan de toezichthouder niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.

NB: De verwerker informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van een datalek.

2. Documentatieplicht

De verwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de toezichthouder in staat de naleving van dit artikel te controleren.

3. Melding van een datalek aan de betrokkene(n)

Wanneer het datalek een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkene het datalek onverwijld mee. De mededeling aan de betrokkene is **niet** vereist wanneer een van de volgende voorwaarden is vervuld:

- de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
- de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat

het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;
- de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

Hoe doe je dat?

Indien er mogelijk een datalek op een onderwijsinstelling heeft plaatgevonden dient er een vaste procedure te starten. De vijf stappen in deze procedure zijn rechts schematisch weergegeven. Klik op de afbeelding voor een grotere weergave:

Inhoud meldingen

De verplichte inhoud van ieder type melding is via onderstaande knop in te zien:

Verplichte inhoud meldingen

Welke ondersteuning is beschikbaar?

Onderstaand vind je best practices die kunnen dienen ter inspiratie:

- **ROC van Amsterdam (Co Klerkx)**

8. Bewerkersovereenkomsten

Een ***verwerkingsverantwoordelijke*** (een school) kan een ***verwerker*** (bjivoorbeeld een uitgeverij) inschakelen om namens hen persoonsgegevens te verwerken. De afspraken hierover moeten in mei 2018 voldoen aan de nieuwe eisen binnen de AVG.

Wat moet je doen?

De uit te voeren actie is op zich helder: er moeten 'AVG compliant' bewerkersovereenkomsten zijn met alle leveranciers die persoonsgegevens van de mbo-instelling verwerken. En de mbo-instelling is voor die overeenomsten **zelf verantwoordelijk**!

Heb je dus bepaalde gegevensverwerking uitbesteed aan een verwerker? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met de verwerkers nog steeds toereikend zijn en voldoen aan de vereisten in de AVG. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan of sluit een aparte bewerkersovereenkomst met de verwerker(s) af.

De verwerkingsverantwoordelijke mag uitsluitend een beroep doen op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.

Hoe doe je dat?

Iedere bewerkersovereenkomst moet volgens de AVG artikel 28 voldoen aan enkele vereisten. Via onderstaande knop is een overzicht van deze vereisten in te zien:

Vereisten bewerkersovereenkomsten

Mbo instellingen kunnen gebruik maken van het format zoals dat ontwikkeld is door SURF (**Model Bewerkersovereenkomst, SURF Juridisch Normenkader (Cloud)services**) voor de applicaties die door SURFmarket worden aangeboden (Microsoft, Adobe, etc.) en van het **Convenant Digitale Onderwijsmiddelen en Privacy 2.0,** waarin als bijlage de **Modelbewerkersovereenkomst versie 2.0** is opgenomen.

Dit convenant is nog niet ondertekend door de MBO Raad maar wordt wel door de werkgroep Bewerkersovereenkomsten gehanteerd. De werkgroep gaat namens de regiegroep 'ibp in het mbo' in gesprek met een aantal belangrijke leveranciers van applicaties voor het mbo om de actuele verwerkersovereenkomst van de betreffende leveranciers te bespreken.

Het eerste deel (de “artikelen”) staat dan niet ter discussie. Met name de privacy bijsluiter (bijlage A) en de technische bijsluiter (bijlage B) van de leverancier worden door de werkgroep getoetst.

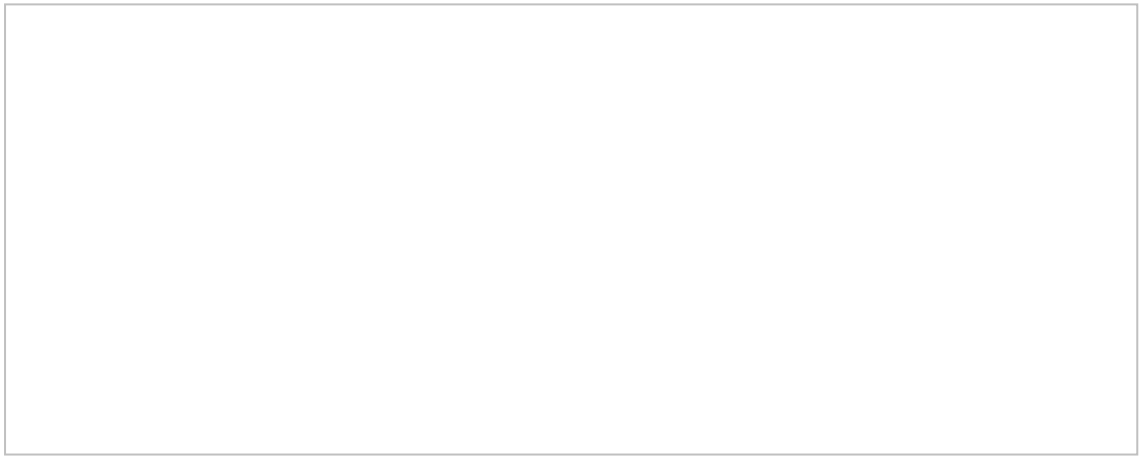
Privacy bijsluiter

De relevante onderdelen uit B (Categorieën van personen), C (Verwerkingsdoeleinden en Grondslag) en D (Categorieën van persoonsgegevens) uit het dataregister zijn onderdeel van de privacy bijsluiter. Een voorbeeld hiervan is te zien door op de afbeelding rechts te klikken.

Het Convenant is ondertekend door 150 bedrijven, is getoetst door OCW en de AP en positief beoordeeld. Ook Microsoft heeft het Convenant positief beoordeeld.

Relatie andere contracten

Om aan te geven hoe de bewerkersovereenkomst zich verhoudt tot andere contracten is onderstaande schema gemaakt. Dit laat goed zien welk onderscheid er is. Bijvoorbeeld, aansprakelijkheden werk je uit in het SLA of eventueel bij de juridische afspraken, maar niet in de bewerkersovereenkomst. Dat geldt ook voor looptijden e.d.:



Welke ondersteuning is beschikbaar?

Het uitgangspunt voor de bewerkersovereenkomsten is de **Modelbewerkersovereenkomst voor het mbo, 2.0**. Voor specifieke leveranciers zijn intussen bewerkersovereenkomsten overeengekomen tussen de betreffende leverancier en de werkgroep *Bewerkersovereenkomsten in het mbo*.

Deze verwerkersovereenkomsten worden alleen in het besloten gedeelte van het platform van het

netwerk 'ibp in het mbo' gepresenteerd. Externe dienstverleners beschouwen de verwerkersovereenkomsten als bedrijfsgeheim en willen niet dat de concurrenten hier kennis van nemen.

Tot nu toe zijn de volgende overeenkomsten beschikbaar:

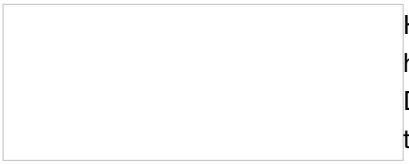
- Intergrip;
- EduArte;
- Magister.

Er wordt nog gewerkt aan de volgende overeenkomsten:

- Xedule;
- Raet;
- Trajectplanner;
- Een ELO;
- een technische applicatie voor bijvoorbeeld pasjes en dergelijke.

Tot slot wordt er in overleg met de educatieve uitgeverijen (vertegenwoordigd door de GEU), de administratieve systemen (vertegenwoordigd door de VDOD), de distributeurs (vertegenwoordigd door de KbBE) en de MBO Raad gewerkt aan een Privacy Overeenkomst inclusief een nieuw model Bewerkersovereenkomst tussen al deze leveranciers en de mbo sector.

9. Leidende toezichthouder



Heeft jouw mbo-instelling vestigingen in meerdere EU-lidstaten? Of hebben jouw gegevensverwerkingen in meerdere lidstaten impact? Dan hoef je onder de AVG nog maar met één privacy toezichthouder zaken te doen. Dit heet 'de leidende toezichthouder'. Geldt dit voor jouw organisatie, bepaal dan onder welke privacy toezichthouder je valt.

Leidende toezichthouder

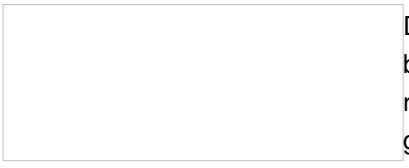
De AVG gaat uit van de zogeheten *onestopshop-regel*. Onestopshop houdt in dat organisaties die zogeheten grensoverschrijdende gegevensverwerkingen uitvoeren, nog maar met één privacy toezichthouder zaken hoeven te doen; de ‘leidende toezichthouder’ (lead supervisory authority). Voor alle Nederlandse mbo instellingen is de AP de leidende toezichthouder.

Indien een collega bijvoorbeeld een laptop in Frankrijk verliest met toegankelijke persoonsgegevens, dan wordt dit datalek gemeld aan de Nederlandse AP.

Belgische toezichthouder

Het is verfrissend om ook kennis te nemen van de documenten van de Belgische (Vlaamse) Toezichthouder. In België wordt de AP de 'Commissie voor de bescherming van de persoonlijke levenssfeer' (CBPL) genoemd. Zie **www.privacycommission.be/nl/** voor meer informatie.

10. Toestemming



De AVG stelt strengere eisen aan toestemming. Het is daarom belangrijk om de wijze waarop je toestemming vraagt, krijgt en registreert opnieuw te evalueren. Zo moet je kunnen aantonen dat je geldige toestemming hebt gekregen om persoonsgegevens te verwerken. En moet het net zo makkelijk zijn om toestemming in te

trekken als om die te geven.

Wat moet je doen?

De verwerking van persoonsgegevens is rechtmatig als er een van de grondslagen geldt:

- **Je hebt toestemming van de betrokkene;**
- **Het is noodzakelijk voor de uitvoering van de overeenkomst;**
- **Het is noodzakelijk om te voldoen aan een wettelijke verplichting;**
- **Je beschermt er een vitaal belang mee;**
- **Het is noodzakelijk voor de vervulling van een taak van algemeen belang of openbaar gezag;**
- **Er speelt een gerechtvaardigd belang.**

Speelt er niet één van de vijf laatste grondslagen, dan zul je dus expliciete toestemming van de betrokkene moeten hebben om zijn of haar gegevens te verwerken. Onderstaand lees je welke voorwaarden van toepassing zijn op het verwerken van persoonsgegevens met toestemming van betrokkenen:

- Aantonen dat de betrokkene **toestemming heeft gegeven** voor de verwerking van zijn persoonsgegevens;
- De betrokkene kan ten allen tijde zijn **toestemming intrekken**. Voordat hij zijn toestemming geeft, wordt hij daarvan in kennis gesteld. Het is even eenvoudig om toestemming in te trekken als om toestemming te geven;
- Soms geeft een betrokkene toestemming in het kader van een schriftelijke verklaring die **ook op andere aangelegenheden** betrekking heeft. Het verzoek om toestemming wordt dan in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal zodanig gepresenteerd dat een duidelijk onderscheid kan worden gemaakt met de andere aangelegenheden. Wanneer een gedeelte van een dergelijke verklaring een inbreuk vormt op deze verordening, is dit gedeelte niet bindend.

Toestemming bij kinderen

Indien verwerking plaatsvindt op grond van toestemming geldt voor een kind jonger dan **16 jaar** dat verwerking slechts rechtmatig is met toestemming of machtiging door de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt. Dit kan relevant zijn indien bijvoorbeeld een vmbo en een mbo samen in één gebouw zitten.

Hoe doe je dat?

Een veelvoorkomend voorbeeld om toestemming als grondslag voor rechtmatige verwerking te benutten is het gebruik van beeldmateriaal. Als je dit onderling goed regelt is er veel mogelijk. Hieronder vind je een voorbeeldbrief van een zorgvuldige manier van omgaan met toestemming; in dit geval van medewerkers ten aanzien van het gebruik van beeldmateriaal.

Voorbeeldbrief toestemming

Bij het omgaan met toestemming en het maken van afspraken zijn er **drie aandachtspunten** belangrijk om goed op het netvlies te hebben:

Uitzonderingen

Er is geen toestemming van medewerkers nodig voor het gebruik van foto's en video's in de klas voor onderwijskundige doeleinden. Ook is er geen toestemming nodig voor het plaatsen van een foto op een

schoolpas of voor gebruik van een foto in het administratiesysteem. Wel gelden voor het gebruik van dat beeldmateriaal de gewone privacy regels.

Specifieke beslissing

De wetgever eist dat de medewerker een goed geïnformeerde beslissing kan nemen, die ook specifiek is. Het alleen vragen van toestemming ‘voor gebruik van foto’s door de school’ is dat zeker niet. Als mbo instelling mag je het zeker ook niet zo formuleren: ‘*als je niet wilt dat we foto’s van jou gebruiken, moet je dat maar zeggen*’. Dit is een ‘opt-out’, en dat is in strijd met de wet.

Afspraken

Een school wil voor álle medewerkers een veilige omgeving zijn, en niet een plek waar men bang is steeds te worden gefotografeerd. Het maken van foto’s en video’s op een mbo instelling kun je moeilijk verbieden; het gaat vooral om het maken van goede afspraken. Bijvoorbeeld:

- spreek verwachtingen uit naar medewerkers over fotograferen tijdens een onderwijsactiviteit;
- vraag medewerkers via de nieuwsbrief terughoudend te zijn met het maken en publiceren van foto’s;
- leg regels vast voor het maken van foto’s op school in het privacyreglement of in een aparte gedragscode of protocol;
- de school kan aan het verlenen van toegang voorwaarden stellen zoals de (extreme) regel dat fotograferen van medewerkers tijdens de les of in klas alleen is toegestaan door docenten.

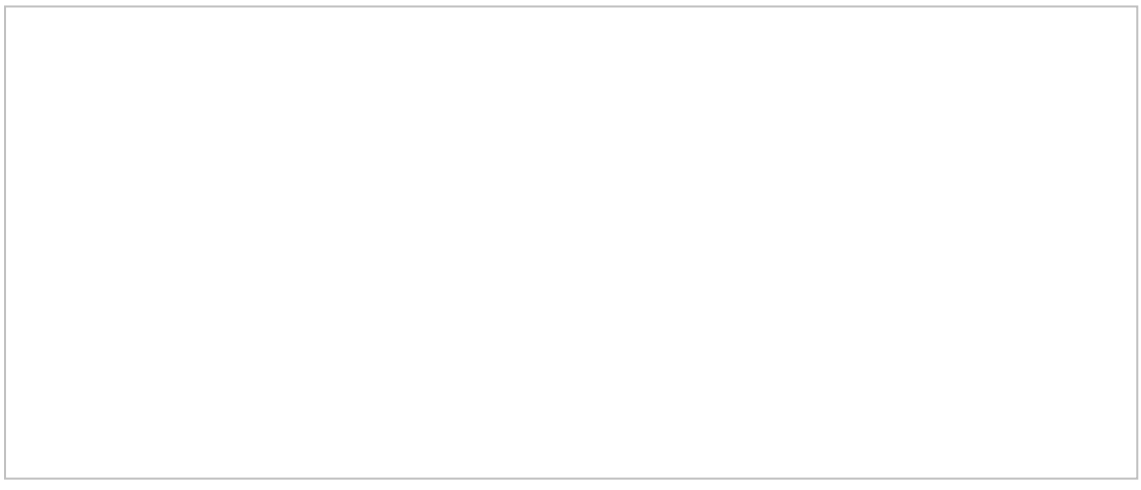
En nu?

Als je hier bent aangekomen dan heb je een megaklus geklaard. Proficiat! Maar IBP is nooit af. Het is een proces dat altijd weer vraagt om verbetering en vooral ook om continuïteit. IBP moet in de dagelijkse routine van de onderwijsprocessen zijn opgenomen, het moet in de PDCA cyclus zijn ingebakken.

Vervolgstappen

Daarom is het ook van belang dat er na al deze stappen van de aanpak een beheersorganisatie is ingericht die hier voor zorgt draagt en blijft dragen. Welke stappen moeten vooral in een continu proces worden doorgezet? Dit wordt verder beschreven in de het roadmap document van het framework ibp in het mbo (IBPDOC5).

Het gaat dan vooral om de volgende zaken:



Aanmelden?

Maar je hoeft het allemaal niet alleen te doen. Naast mogelijke collega's binnen je instelling is er een **netwerk** van ibp functionarissen in de mbo sector die allemaal met deze dingen bezig zijn. Sluit je aan en deel met hen ervaringen, kennis en ideeën. Het netwerk komt vier keer per jaar bij elkaar en kan je echt verder op deze weg helpen. Meld je aan bij Leo Bakker van Kennisnet (**l.bakker@kennisnet.nl**).

Vragen?

Heb je andere vragen, dan kun je daarvoor ook bij Leo Bakker terecht, of anders bij de servicedesk ibp van Kennisnet (**ibp@kennisnet.nl**). En tot slot is er het **framework ibp** in het mbo dat je kan helpen. Een zeer uitgebreide set van normen, kaders, handreikingen en hulpmiddelen die je kunt inzetten met je collega's om ibp in je instelling een flinke stap vooruit te brengen.

Succes!

Over dit lesmateriaal

Colofon

De productie van deze handreiking is een samenwerking tussen Kennisnet (opdrachtgever) en Flooow (e-learning productie).
Auteurs: Sander van Acht (Flooow), Leo Bakker en Ludo Cuijpers (Kennisnet)
Contactgegevens: l.bakker@kennisnet.nlen l.cuijpers@kennisnet.nl

Auteur	Kennisnet IBP MBO - oud -
Laatst gewijzigd	14 may 2018 om 15:34
Licentie	Dit lesmateriaal is gepubliceerd onder de Creative Commons Naamsvermelding-GelijkDelen 3.0 Nederland licentie. Dit houdt in dat je onder de voorwaarde van naamsvermelding en publicatie onder dezelfde licentie vrij bent om: • het werk te delen - te kopiëren, te verspreiden en door te geven via elk medium of bestandsformaat • het werk te bewerken - te remixen, te veranderen en afgeleide werken te maken • voor alle doeleinden, inclusief commerciële doeleinden. Meer informatie over de CC Naamsvermelding-GelijkDelen 3.0 Nederland licentie

Aanvullende informatie over dit lesmateriaal

Van dit lesmateriaal is de volgende aanvullende informatie beschikbaar:

Leerniveau	; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
Eindgebruiker	leraar
Moeilijkheidsgraad	gemiddeld
Trefwoorden	avg, cybersecurity, ibp, informatiebeveiliging, iso 27001, iso 27002, kennisnet, mbo, privacy, wbp