Kennisnet

Aanpak ibp voor het po en vo

Auteur	Aanpak IBP

Laatst gewijzigd	23 april 2018

Webadres	https://maken.wikiwijs.nl/81891

Inhoudsopgave

Welkom

Welkom bij de online 'aanpak informatiebeveiliging en privacy'!

Deze aanpak is ontwikkeld voor scholen in het primair en voortgezet onderwijs, zodat mensen zonder achtergrondkennis over deze onderwerpen hier toch invulling aan kunnen geven. Wij hebben de nodige kennis en expertise vertaald naar het onderwijs.

Deze aanpak wordt pas écht van het onderwijs als wij van jou te horen krijgen wat je ervan vindt en waar je aanvullend behoefte aan hebt. Samen maken we het onderwijs dan een stuk veiliger.

Voor vragen, opmerkingen of ideeën kun je contact opnemen met de IBP-helpdesk via ibp@kennisnet.nl of 0800-3212233

IBP?

Scholen maken steeds beter en meer gebruik van ict. Daardoor neemt niet alleen het aantal persoonsgegevens dat scholen gebruiken toe. Ook brengt de afhankelijkheid van ict nieuwe risico's met zich mee, zoals cybercrime en datalekken. Het beschermen van de persoonsgegevens van leerlingen en medewerkers en daarmee het waarborgen van de privacy, wordt dan ook steeds belangrijker. Schoolbestuurders zijn volgens de wet verplicht om privacy goed te regelen.

Wetgeving bepaalt niet alleen onder welke voorwaarden persoonsgegevens gebruikt mogen worden, maar geeft ook aan dat er passende technische en organisatorische maatregelen genomen moeten worden om de persoonsgegevens te beschermen. Informatiebeveiliging is een belangrijke voorwaarde voor privacy, terwijl omgekeerd het zorgvuldig omgaan met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Beide begrippen staan naast elkaar, en zijn van elkaar afhankelijk.

Om makkelijk over informatiebeveiliging en privacy te kunnen praten korten we het af tot **IBP**.

Job Vos, privacy-expert bij Kennisnet, legt uit waarom het regelen van een IBP-beleid zo belangrijk is voor iedere school:

https://youtu.be/BB2owgG_vWE

De rol van Kennisnet

Iedere school is uniek. Maar daarmee is niet iedere aanpak voor informatiebeveiliging en privacy uniek. Er zijn nu eenmaal zaken die je op elke school geregeld moet hebben. IBP zijn randvoorwaarden voor eigentijds, veilig en persoonlijk onderwijs. Hoe is dat op kouw school geregeld? Voldoet jouw school aan de AVG-wetgeving?

Meer weten? Lees dan 'Alles wat je moet weten over informatiebeveiliging en privacy (IBP)'.

IBP goed regelen is aardig wat werk, maar je kan het stap voor stap oppakken.

Het is dan ook het uitgangspunt geweest voor de PO-Raad, VO-raad en Kennisnet om een aanpak te ontwikkelen die scholen helpt met het op eenvoudige en praktische wijze organiseren van informatiebeveiliging en privacy (IBP). Deze aanpak draagt eraan bij dat de privacy van leerlingen en medewerkers is gegarandeerd, terwijl de continuïteit van het onderwijs geregeld is. Scholen zijn daarmee in staat om in de toekomst eigentijds, veilig en persoonlijk onderwijs te blijven geven met behulp van ict.

Zo werkt de Aanpak IBP

Deze online aanpak is ontwikkeld voor jou als bestuurder, docent, ict-coördinator of communicatiemedewerker bij een onderwijsinstelling. Vaak is IBP maar één van de onderwerpen waar je mee bezig bent en kun je er niet je volle werkweek aan besteden. De Aanpak helpt je IBP goed te regelen met voorbeelddocumenten, handreikingen, uitleg en praktische tips in drie eenvoudige stappen:

organiseren, realiseren en communiceren.

Organiseren

In de eerste stap 'organiseren' gaat het om het opstellen van een IBP-beleid. Dit wordt de kapstok om afspraken, richtlijnen en procedures rondom IBP goed te regelen. We helpen je met tips en voorbeeldteksten om eenvoudig een eerste opzet te maken. We noemen een aantal aandachtspunten en stellen een document beschikbaar waarin we de onderdelen toelichten. Je kan gebruik maken van het voorbeeldbeleid of het eigen beleid aanscherpen op basis van de informatie.

Realiseren

Het beleid is pas de kapstok. Het gaat er nu om wat daar in de dagelijkse praktijk aan komt te hangen. In de tweede stap wordt het beleid uitgewerkt door de nodige technische en organisatorische maatregelen vast te leggen. Denk hierbij aan het opstellen van procedures en het maken van afspraken; kortom aan het nemen van maatregelen om de continuïteit van het onderwijs en de bedrijfsvoering te waarborgen en de privacy van leerlingen en medewerkers te garanderen. We helpen je hierbij met uitleg, voorbeelden, checklists en handige bronnen.

Communiceren

Een belangrijk onderdeel van IBP is het duidelijk communiceren naar alle belanghebbenden. Dat zijn niet alleen de leerlingen en medewerkers, maar ook de ouders. In de laatste stap staan handreikingen over hoe je dit voor elke doelgroep kunt aanpakken.

Doorloop je de aanpak stap voor stap, dan kom je alles tegen wat er rondom IBP geregeld moet worden. Je kan niet alles in één keer realiseren. Daarom geven we ook duidelijk aan wat je op korte termijn moet doen en wat je later kan oppakken. We raden aan om eerst de hele aanpak te bekijken. Dan heb je een goed en compleet beeld. Is alles nieuw? Begin dan gewoon met 'Organiseren'. Is IBP geen onbekend onderwerp meer en zoek je specifieke informatie? Kies dan links eenvoudig zelf het gewenste onderwerp.

Ben je op zoek naar een overzicht van de documenten in de Aanpak klik dan op het onderstaande document. (let op dit document is een moment opname, het is mogelijk dat er inmiddels documenten en of verwijzingen zijn bijgekomen)

Overzicht documenten uit de Aanpak per onderwerp
kn.nu/ww.03d4f49 (pdf, maken.wikiwijs.nl)

Vragen en opmerkingen over de Aanpak kun je altijd kwijt via ibp@kennisnet.nl of 0800-3212233.

Basisbegrippen IBP

De privacy van leerlingen en medewerkers moet goed geregeld zijn. Om hiervoor de juiste maatregelen te kunnen nemen, is het nodig dat je weet waar privacy over gaat en dat je de belangrijkste begrippen en uitgangspunten van privacy kent.

Basisregels privacywetgeving

Het is vanuit de privacywetgeving belangrijk om een aantal basisregels te kennen over het gebruik van persoonsgegevens, zodat je weet waar je je aan moet houden als je te maken krijgt met persoonsgegevens. Deze basisregels komen voort uit de Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018) **en** de Algemene verordening gegevensbescherming (AVG; na 25 mei 2018).

Kennisnet heeft de belangrijkste uitgangspunten voor het gebruik van persoonsgegevens in vijf vuistregels samengevat..

5 vuistregels 2.0

Naast deze vijf vuistregels voor het gebruik van persoonsgegevens zijn er een aantal begrippen die je moet kennen als je IBP op school goed wilt regelen. Deze zijn in het onderstaande document '*privacy - dit moet je weten over de wet*' uitgewerkt en aangevuld met een uitleg over de vijf vuistregels.

Privacy - dit moet je weten over de wet
kn.nu/ww.369510a (pdf, maken.wikiwijs.nl)

Vanaf 25 mei 2018 is er nog maar één privacywet voor de hele Europese Unie. De **Algemene verordening gegevensbescherming**. Hoewel de AVG op veel punten gelijk is aan de Wbp bevat de AVG ook een aantal belangrijke wijzigingen en aanvullingen.

De belangrijkste wijzigingen en uitbreidingen zijn onder 'Aandachtspunten AVG mei 2018' op een rij gezet.

Aandachtspunten AVG mei 2018

Het Europees Parlement stemde in 2016 in met de **Algemene verordening gegevensbescherming** (AVG). Deze nieuwe wetgeving sluit aan op technologische ontwikkelingen en globalisering. Door de AVG zijn persoonsgegevens van alle EU-inwoners straks op dezelfde wijze beschermd, ongeacht of hun gegevens zijn opgeslagen in Europa of bijvoorbeeld de Verenigde Staten.

Dat betekent dat er vanaf 25 mei 2018 nog maar één privacywet geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer. De AVG is een verordening, dit houdt in dat er rechtstreeks verplichtingen worden opgelegd aan

organisaties die persoonsgegevens verwerken en rechten worden toegekend aan betrokkenen (degenen van wie persoonsgegevens verwerkt worden). Ook Nederlandse scholen moeten vanaf 25 mei 2018 voldoen aan de nieuwe wetgeving. Dat betekent huiswerk voor scholen die privacy nog niet goed hebben geregeld.

Als de AVG van toepassing is, hebben organisaties die persoonsgegevens verwerken meer verplichtingen. Er wordt in de AVG meer nadruk gelegd op de verantwoordelijkheid van organisaties (scholen) zelf. Scholen moeten niet alleen de **wet naleven**, zij moeten kunnen **aantonen** dat zij zich aan de wet houden.

De volgende tien onderwerpen laten niet alleen de uitbreidingen en aanpassingen van de huidige regels van de Wbp zien, maar bevatten ook de nieuwe elementen die zijn toegevoegd in de AVG.

- Uitgangspunten privacy (5 vuistregels2.0)
- Privacy by design / by default
- Verplichte risicoanalyse
- Documentatieplicht
- Bewustzijn creëren en voorlichten
- Gebruik digitale diensten onder de 16 jaar
- Verwerkersovereenkomsten
- Meldplicht datalekken
- Functionaris voor gegevensbescherming
- Technische en organisatorische maatregelen

Maar wat betekent dit voor mijn school, mijn organisatie? Lees hierover meer in het volgende document:

Aandachtspunten AVG
kn.nu/ww.d254686 (pdf, maken.wikiwijs.nl)

1. Organiseren

Waarom heb ik een beleidsplan nodig?

We hebben gezien dat wetgeving niet alleen bepaalt onder welke voorwaarden persoonsgegevens gebruikt mogen worden, maar ook aangeeft dat er passende technische en organisatorische maatregelen genomen moeten worden om de persoonsgegevens te beschermen.

Om hieraan te voldoen zal een school moeten vastleggen wat er wel en niet met persoonsgegevens gedaan mag worden. Als school moet je weten waar de risico's liggen en wat je eraan kan doen.

Het gaat in eerste instantie niet om die technische maatregelen, niet om ict, maar om gedrag, cultuur en bewustwording. IBP is een constant bewustzijn van de risico's die een school loopt; niet alleen risico's waardoor de continuïteit in zowel het onderwijs als de bedrijfsvoering in gevaar kan komen, maar ook risico's rondom het beschermen van de privacy van leerlingen en medewerkers. Het IBP-beleid, met de onderliggende afspraken, procedures en verantwoordelijkheden moet school-breed geïmplementeerd zijn, dan pas is ict aan zet bij de technische uitvoering en monitoring.

Het schoolbestuur is verantwoordelijk om informatiebeveiliging en privacy(IBP) te regelen. Het regelen van IBP begint dan ook met een goedgekeurd en bij iedereen bekend gemaakt IBP-beleid. Dat is de basis, de kapstok, om processen, richtlijnen en procedures rondom IBP uit te werken.

Maar wat moet je nu als bestuurder zelf doen en wat kan je bij anderen neerleggen?

- Van belang is dat je als bestuurder de organisatie rondom IBP goed inricht (hier wordt bij 'wie doet wat' verder op ingegaan).
- D e basisbegrippen IBP en de aandachtspunten AVG geven een bestuurder belangrijke informatie om IBP goed te regelen.
- Als bestuurder laat je IBP ook regelmatig op de agenda terugkomen. Het is belangrijk om op basis van rapportages en nieuwe ontwikkelingen IBP te evalueren.

Hoe maak je een beleidsplan

Het goed regelen van IBP begint met een goedgekeurd en bij iedereen bekend gemaakt IBP-beleid. Het beleid is de basis, de kapstok, om processen, richtlijnen en procedures rondom IBP en de communicatie erover verder uit te werken en vast te leggen.

Het is belangrijk om te beseffen dat je eerste IBP-beleid een vertrekpunt is. Het kan goed zijn dat in de loop van de tijd veranderingen in de techniek, de situatie op school of wijzigingen in wet- en regelgeving vragen om aanpassing van het beleid.

Dit is de aanleiding geweest om het format IBP-beleid aan te passen aan de AVG. In het nieuwe format is rekening gehouden met o.a. rechten van betrokkenen, de verplichting om vast te leggen welke persoonsgegevens verwerkt worden (dataregister), de (D)PIA, privacy by design en privacy by default, de functionaris voor gegevensbescherming en meer.

Let op: *Vanuit de AVG gaat het er niet alleen om dat scholen de wet* ***naleven;*** *zij moeten ook kunnen* ***aantonen*** *dat zij zich aan de wet houden. Dit is van belang als je het beleid verder gaat uitwerken en erover gaat communiceren.*

Het IBP-beleid is voorzien van een extra document met een toelichting in een kolom naast de tekst. Deze toelichting bevat verdere uitleg en verwijzigingen naar onderliggende documenten, afspraken en procedures. Hiermee wordt de 'kapstokfunctie' van het beleid inzichtelijker. Het laat enerzijds zien wat de achterliggende gedachte is van bepaalde afspraken, maatregelen en procedures en anderzijds geeft het je de mogelijkheid om aantoonbaar te maken dat je aan bepaalde eisen vanuit de AVG voldoet.

Template IBP beleid 2.0
kn.nu/ww.f0343b5 (docx, maken.wikiwijs.nl)

Toelichting template IBP beleid 2.0
kn.nu/ww.55bd5dd (pdf, maken.wikiwijs.nl)

Als je een vliegende start wilt maken, hoef je alleen de 'gele' velden in te vullen zodanig dat deze voor jouw schoolorganisatie passend zijn. Daarmee heb je de eerste versie van het IBP-beleid om intern te bespreken en goed te (laten) keuren. Begin je liever met een schone lei, of heb je al een IBP-beleid? Ook goed! Zorg dan in ieder geval dat alle onderwerpen die in het template staan ook in je eigen IBP-beleid terugkomen.

We hebben gemerkt dat het onderdeel **Organisatie** uit het beleid een lastig stuk is. De vraag ‘wie doet wat’ invullen en dus de verantwoordelijkheden goed beleggen is niet voor alle scholen zo eenvoudig. Daarom komt dat in het volgende blok als apart onderwerp terug.

Wie doet wat?

Ondanks dat iedere school anders georganiseerd is, kom je veelal dezelfde functies, rollen en taken tegen. Dat geldt ook voor het organiseren van IBP. In dit onderdeel helpen we je om de juiste rol- en taakverdeling voor IBP in je beleid op te nemen.

Bedenk hierbij vooral:

- *Wie gaat er verantwoordelijk zijn voor een bepaalde taak?*
- *Waar gaat het precies over? Denk hierbij aan afspraken, processen en dagelijks werk.*
- *Welke documenten (of andere manieren van vastlegging) ondersteunen dit?*

Probeer rollen en taken zo specifiek mogelijk te omschrijven. Dit maakt de afspraken binnen de school duidelijk voor iedereen. In de tabel IBP rollen en taken hebben we vast een opzet gemaakt.

De kolom **‘wie’** geeft aan wie op welk niveau een rol speelt.

- Op **strategisch niveau** is de bestuurder verantwoordelijk om IBP goed te regelen en daarmee ook om de IBP-organisatie goed in te richten. Kies de benaming die het best bij de organisatie

past.

- Een **manager informatiebeveiliging en privacy** (afgekort als manager IBP) is een rol op strategisch, tactisch en operationeel niveau. Hij/zij adviseert o.a. de bestuurder. De manager IBP bewaakt de uniformiteit op het gebied van IBP binnen de instelling. Het kan een fulltime rol zijn of een rol die iemand erbij krijgt, dat hangt af van de grootte van de organisatie. Het gaat er niet om dat er extra rollen en/of functies gemaakt moeten worden, maar dat gekeken wordt wie op jouw school die taken kan vervullen. Ook kan één persoon prima meerdere rollen vervullen. Let daarbij wel op dat de rollen niet conflicteren met andere verantwoordelijkheden. Kies ook hier de benaming die het best bij de organisatie past.
- Een **proceseigenaar** is iemand die verantwoordelijk is voor één van de primaire of ondersteunende processen, zoals HRM/P&O, administratie, financiën of onderwijs.

In de kolom **'hoe'** staat aangegeven welke verantwoordelijkheden en taken er minimaal belegd moeten worden. Kijk hierbij goed naar de inhoud van de taken en de werkzaamheden die daarbij horen. Zijn dat éénmalige activiteiten of komen ze zeer regelmatig terug. Een rol als manager IBP kun je niet 'zomaar even tussendoor' doen. De tijd die het vraagt is mede afhankelijk van de grootte van je organisatie.

De kolom **'wat'** geeft de praktische uitwerking van het beleid op elk niveau weer. Welke processen worden er door wie beschreven, wie legt welke afspraken vast, wie keurt deze goed en hoe wordt er gecommuniceerd.

Een schematische weergave kan helpen de juiste verdeling te maken op strategisch, tactisch en operationeel niveau. Klik op de afbeelding om het schema te vergroten.

Extra aandacht vragen de volgende punten:

· **Toegang en toegangsbeleid**

Het is voor informatiebeveiliging en privacy héél belangrijk om te weten wie waar bij mag en wie daarover uiteindelijk de beslissingen neemt. Daarom is het goed om iemand specifiek hiervoor verantwoordelijk te maken.

· **Individuele medewerkers**

Degenen die het meest in aanraking komen met persoonsgegevens, zijn de medewerkers. Docenten leggen veel gegevens van leerlingen vast om ze op de juiste manier te kunnen begeleiden en ook administraties verwerken veel persoonsgegevens. Het is daarom belangrijk dat alle medewerkers het belang van informatiebeveiliging en privacy inzien en erkennen. Betrek hen dan ook zoveel mogelijk bij het hele proces.

Van plan naar uitvoering

Het goedgekeurde IBP-beleid is er.... Maar hoe nu verder? Het is belangrijk dat dit geen papieren tijger wordt of stof gaat staan vangen in de kast. De bedoeling is dat dit beleid in het DNA van alle medewerkers komt te zitten en dat het geheel regelmatig geëvalueerd en zo nodig aangepast wordt.

Communicatie: Zorg dat iedereen bekend is met het IBP-beleid

· het lezen formaliseren

Het is belangrijk dat iedereen die bij de school komt werken ook weet wat de huisregels zijn. Dit kan een reden zijn om het lezen van het IBP-beleid en de onderliggende afspraken onderdeel te maken van de arbeidsvoorwaarden. Tekent een nieuwe medewerker voor de arbeidsvoorwaarden, dan geeft dat aan dat deze het IBP-beleid, en de onderliggende afspraken heeft gelezen en de consequenties ervan begrepen heeft. Voor externen kan het op dezelfde manier geregeld worden, door het in de contractvoorwaarden op te nemen.

· het lezen stimuleren

Maar je hebt natuurlijk ook bestaande medewerkers, hoe bereik je die? Enkele tips hiervoor zijn:

- Creëer urgentie door op de volgende teamvergadering voorbeelden te tonen van wat er fout kan gaan als je IBP niet goed regelt. Voorbeelden hiervan zijn datalekken die nu (te) vaak in het nieuws komen.
- Gebruik de kracht van de herhaling. Het eenmalig in een vergadering noemen van de term IBP is voor de meeste mensen te weinig. Benoem het belang van IBP in nieuwsbrieven, breng het regelmatig ter sprake tijdens bijeenkomsten.

· extra aandacht besteden aan bewustwording

Hiervoor verwijzen we vast naar de module communiceren medewerkers waar twee mogelijkheden gegeven worden om bewustwording binnen je school onder de aandacht te brengen.

Evalueer regelmatig; IBP is een continu proces

Als je wilt kunnen zeggen dat je IBP onder controle hebt, dan moet je dat kunnen aantonen. Maar hoe weet je of je het onder controle hebt? Door regelmatig te evalueren komen de punten naar voren, die verbetering en/of aanpassing vragen. Nieuwe ontwikkelingen zoals nieuwe processen of nieuwe systemen, maar ook nieuwe wet- en regelgeving kunnen om aanpassingen vragen.

Ga naar het onderdeel continu verbeteren om te zien hoe je dat kunt regelen.

2. Realiseren

Start

Nu het beleid op papier staat, moeten we zorgen dat er verdere invulling aan gegeven wordt. In deze module maken we daar een start mee. We gaan **maatregelen** nemen, procedures uitwerken en nog veel meer. Hiervoor is het belangrijk dat we weten op welke **gebieden** IBP een rolt speelt en waar de risico's liggen.

Achtergrond van de maatregelen

De maatregelen die we kunnen en soms moeten nemen zijn gebaseerd op:

- **De code voor informatiebeveiliging (ISO 27001 / 27002);** deze beschrijft welke beveiligingsmaatregelen van een instelling (mogen) worden verwacht om informatie goed te beveiligen;
- het daarvan afgeleide **normenkader voor hbo en mbo,** dat ook voor het po en vo op veel punten bruikbaar is*;
- richtlijnen en uitgangspunten die zijn gebaseerd op de huidige **relevante wet- en regelgeving**, waaronder de Algemene verordening gegevensbescherming (AVG) en de meldplicht datalekken;
- de in het onderwijs **toegepaste standaarden** (waaronder 'ROSA katern IBP').

Al deze normen en standaarden geven aan welke maatregelen van een school worden verwacht op het gebied van informatiebeveiliging en privacy. Als je ze allemaal moet lezen, begrijpen en toepassen in jouw school dan is dat veel werk. Daarom is in deze aanpak IBP de essentie er voor je uit gehaald.

**Bij het Normenkader informatiebeveiliging mbo hoort een toetsingskader. In dit toetsingskader staat in detail beschreven wat een school geregeld moet hebben om aan bepaalde normen te voldoen. Hierbij komt ook het gewenste niveau van beveiliging aan de orde. Dit is een groot document, waarvan op dit moment niet alles voor het po en vo even belangrijk is. Wel wordt er vanuit de Autoriteit Persoonsgevens steeds meer gekeken of scholen hun informatiebeveiliging op orde hebben en zij verwijst dan naar de ISO-maatregelen. De maatregelen vanuit het normen- en toetsingskader zullen dan ook in de volgende stappen een rol op de achtergrond spelen.*

Welke gebieden hebben te maken met IBP?

Iedere organisatie, dus ook jouw school, bestaat uit meerdere onderdelen, zoals mensen, apparatuur, programmatuur en gegevens, maar ook de organisatie zelf, de omgeving en leveranciers. IBP raakt in elke organisatie ook al deze onderdelen. Om de maatregelen te groeperen zijn er **zes clusters** gemaakt. Deze clusters komen vanuit het eerder genoemde normenkader van het mbo. Het uitwerken en toepassen van maatregelen op basis van deze zes clusters wordt zo relatief eenvoudig.

De zes clusters zijn:

1. Beleid en organisatie
2. Personeel, leerlingen en derden
3. Ruimten en apparatuur
4. Continuïteit
5. Toegangsbeveiliging
6. Controle en logging

*Het is niet noodzakelijk de inhoud van de zes clusters uit je hoofd te leren; het geeft vooral inzicht en overzicht in de complexiteit. Waar nodig zullen we aangeven waar bepaalde documenten of processen betrekking op hebben. Klik **hier** voor een overzicht.*

Wat moet je wettelijk regelen?

Vanuit het IBP-beleid zijn er een aantal onderwerpen die een school op basis van de **wetgeving** op orde moet hebben. Vanaf 25 mei 2018 wordt de huidige Wet bescherming persoonsgegevens (Wbp) vervangen door de Algemene verordening gegevensbescherming (AVG). Dit brengt een aantal aandachtspunten met zich mee, die we al eerder beschreven hebben. We zetten ze nog even op een rij:

- Uitgangspunten privacy (5 vuistregels2.0)
- Privacy by design / by default

- Verplichte risicoanalyse
- Documentatieplicht
- Bewustzijn creëren en voorlichten
- Gebruik digitale diensten onder de 16 jaar
- Bewerkersovereenkomsten
- Meldplicht datalekken
- Functionaris voor gegevensbescherming
- Technische en organisatorische maatregelen

Let op: De termen 'verantwoordelijke ' en 'bewerker' uit de Wbp krijgen in de AVG een andere naam! Vanaf nu worden in alle documenten in de Aanpak de benamingen vanuit de Wbp vervangen door de benamingen vanuit de AVG.

- De '**verwerkingsverantwoordelijke**', is in de AVG de nieuwe naam voor de 'verantwoordelijke'.
- De '**verwerker**', is in de AVG de nieuwe naam voor de 'bewerker'.

Classificeren en risicoanalyse

IBP regel je onder andere om de continuïteit van het onderwijs en de bedrijfsvoering te waarborgen en de privacy van leerlingen en medewerkers te garanderen. Als school wil je de juiste maatregelen nemen om het risico op beveiligings- en privacy-incidenten en de eventuele gevolgen daarvan tot een minimum te beperken.

Maar hoeveel maatregelen moet je nemen, wat is het minimum? Op welk gebied (cluster) moet je maatregelen nemen? En hoe ver moeten die maatregelen gaan? Wat zijn de grootste risico's? Allemaal vragen die je pas kan beantwoorden als je weet hoe belangrijk bepaalde gegevens en systemen zijn en als je een risicoanalyse hebt gedaan.

De AVG doet er nog een schepje bovenop. De AVG verwacht namelijk van organisaties dat zij niet alleen jaarlijks de huidige risico's in kaart brengen. Maar dat er ook bij nieuwe ict-ontwikkelingen en gebruik van nieuwe technieken vóóraf wordt bekeken wat de mogelijke impact ervan is op de bescherming van persoonsgegevens. Dit laatste staat in de AVG beschreven als data protection impact assessment afgekort tot DPIA. In het Nederlands een gegevensbeschermingseffectbeoordeling.

Het is van belang dat we eerst inzichtelijk krijgen hoe belangrijk bepaalde informatie en/of informatiesystemen zijn. Dit kan door deze te **classificeren.** Vervolgens moeten we aandacht schenken aan het uitvoeren van een **risicoanalyse.**

Alles over de DPIA wordt op termijn (verwachting maart 2018) onder 'samen vooruit' in de Aanpak IBP beschreven.

Classificeren

Elk proces, elk systeem en alle gegevens op school zijn in bepaalde mate belangrijk. Maar hoe belangrijk, hoe essentieel zijn ze? En welke gegevens gebruiken we eigenlijk in welke systemen? Tot welke hoogte moet de informatie beveiligd worden?

Het doel van deze stap is om de processen en bijbehorende applicaties binnen de onderwijsinstelling goed in beeld te krijgen. Het is belangrijk dat je weet welke gegevens jouw instelling verwerkt, wanneer deze beschikbaar moeten zijn en hoe het zit met de integriteit en de vertrouwelijkheid van die gegevens. Dat is nu precies het terrein van de informatiebeveiliging. Informatiebeveiliging heeft te maken met drie aspecten: **Beschikbaarheid, Integriteit en Vertrouwelijkheid.**

We moeten de gegevens en/of systemen op deze drie aspecten **classificeren** om het juiste niveau van beveiliging vast te kunnen stellen. Dit wordt een BIV-classificatie genoemd. Klik hier voor een uitgebreide beschrijving van de Beschikbaarheid, Integriteit en Vertrouwelijkheid..

Classificeren geeft antwoord op vragen als: Hoe vertrouwelijk is de informatie in mijn leerlingvolgsysteem? Hoe erg is het als de website een dag niet beschikbaar is?

Alle beveiligingsmaatregelen brengen kosten en afspraken met zich mee. Alles op het hoogste niveau beveiligen is niet reëel en soms zelfs onwerkbaar. Hoeveel en welke beveiligingsmaatregelen je neemt is afhankelijk van de classificatie van je informatie en informatiesystemen. Hiermee krijg je inzicht in de risico's die je loopt bij de verwerking van persoonsgegevens en in de maatregelen die je moet nemen om de risico's zo klein mogelijk te maken.

Proceseigenaren (zie schema IBP rollen en taken) geven aan hoe gegevens, die zij verwerken bij hun processen, geclassificeerd kunnen worden. Loop met hen de vragen door uit het document BIV-classificatie. De meest actuele versie van deze classificatievragen (in de vorm van een invulbare spreadsheet) kun je vinden op de website van het certificeringsschema.

Tijdens de classificatie kunnen zij ook aangeven welke risico's aanvaardbaar zijn en welke verkleind moeten worden. Onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de uitvoering van onderwijs en bij de bedrijfsvoering van de school. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies. Teveel maatregelen daarentegen kunnen de kosten onnodig laten stijgen.

In de volgende module gaan we verder in op die risico's.

Verplichte risicoanalyse

De AVG eist van organisaties dat zij bewust omgaan met privacy. Hierbij hoort het in kaart brengen van de huidige situatie rondom IBP. Scholen moeten zich daarbij niet alleen aan de wet houden, maar ook kunnen aantonen dat zij dat doen.

Huidige situatie

Waar liggen op dit moment de grootste risico's? Dit kunnen we in beeld krijgen door een risicoanalyse uit te voeren. Hiermee bepaal je eerst wat de (grootste) risico's zijn. Daarna kijk je welke maatregelen nodig zijn om die risico's tot een minimum te beperken. Deze maatregelen kun je vervolgens samen met de wettelijke verplichtingen inplannen voor de komende tijd.

De risicoanalyse kan bijvoorbeeld antwoord geven op de vragen:

- Wat zijn de grootste risico's bij gebruik van het leerlingadministratiesysteem? En welke maatregelen zijn nodig om deze risico's te beperken?
- Wat zijn de risico's bij het inzetten van sociale media in de klas? Welke maatregelen moeten we nemen om dat goed te regelen?

Een risicoanalyse zal niet alleen de grootste risico's aan het licht brengen, zodat je als school weet waar je als eerste in moet investeren. Het is ook een middel om te zorgen dat iedereen hetzelfde beeld krijgt over risico's en de nadelige gevolgen voor de school. Denk bij nadelige gevolgen aan:

1. **Reputatieschade**: Door incidenten die gemeld worden in de media, bijvoorbeeld examenfraude, wachtwoorden op straat, gestolen examens.

2. **Financiële schade**: Als leerlinggegevens niet juist zijn kan de bekostiging van deze leerlingen in gevaar komen; je niet houden aan de privacywetgeving kan financiële consequenties hebben, zoals het niet melden van een datalek.

3. **Continuïteit** van het onderwijs: Cybercrime en DDos-aanvallen kunnen het onderwijs enorm verstoren.

4. **Wet- en regelgeving**: Er moet aantoonbaar voldaan worden aan de AVG.

5. Risico's in de **cloud**: Toepassingen in de cloud leveren specifieke aandachtspunten op zoals eigenaarschap, toegang, privacy en continuïteit van de dienstverlening van externe partijen.

6. Te beperkt **kennisniveau**: Ontwikkelingen gaan snel, de eisen om te voldoen aan wet- en regelgeving worden strenger en de risico's groter. Onvoldoende kennis kan tot gevolg hebben dat er onjuiste beslissingen worden genomen ten aanzien van informatiebeveiliging en privacy met alle gevolgen van dien.

Een risicoanalyse lijkt een moeilijke bezigheid, maar met wat handreikingen kun je zelf op school een eerste risicoanalyse uitvoeren. Het is misschien niet zo diepgaand als de experts het doen, maar voor een eerste risicoanalyse is het prima.

Lees hier verder.

Risicoanalyse - uitvoering

Het doel van de jaarlijkse risicoanalyse is het school-breed bepalen wat de grootste risico's zijn op het gebied van informatiebeveiliging en privacy. Het is belangrijk dat de uitkomst van de risicoanalyse weergeeft hoe de hele school erover denkt.

Verzamel de juiste mensen

Een risicoanalyse in de vorm van een workshop werkt prettig. Het is belangrijk dat je mensen met verschillende rollen en taken hierbij betrekt. Denk daarbij aan de bestuurder, een docent, een ict-coördinator, iemand van P&O en de administratie en misschien zelfs een stagiair. Al die mensen hebben verschillende inzichten en belangen. Wat een groot risico is voor de administratie, is misschien een klein risico voor de docent. Maak de groep niet groter dan drie tot zes personen.

Hulpmiddelen

Zorg voor flipovervellen, post-its en pennen om uitkomsten vast te leggen. Gebruik de onderstaande presentatie als extra hulpmiddel.

korte uitleg risicoanalyse
kn.nu/ww.41eeea8 (pptx, maken.wikiwijs.nl)

Spreek af hoe je een risico opschrijft.

Het moet in ieder geval een begrijpelijke omschrijving zijn, met een inschatting van de kans, en van de impact. Ook over de kans en de impact maak je afspraken. Wat is klein en wat is groot? (zie onderstaand voorbeeld) Op die manier kun je de latere discussie veel makkelijker voeren.

Een risico is een <gebeurtenis>, die leidt tot <een gevolg> door een bepaalde <oorzaak>.
Een risico wordt aangegeven door kans x impact

Kans: kans op optreden van een risico

1: Klein	kan minder dan jaarlijks voorkomen
2: Middel	kan meerdere keren per jaar voorkomen
3: Groot	kan dagelijks voorkomen

Impact: de gevolgen als een risico optreedt

1: Klein	verstoring niet-primair proces, alleen intern merkbaar
2: Middel	verstoring primair proces, extern merkbaar, snel opgelost
3: Groot	verstoring primair proces, reputatieschade, langdurig

Een risico wordt aangegeven door kans x impact

Brainstormen en discussie

Neem de eerder genoemde clusters en de bijbehorende onderwerpen als uitgangspunt en neem een uur de tijd om zoveel mogelijk risico's op te schrijven. Kijk nog eens naar de presentatie Plak deze per cluster op een flipover. Noteer de resultaten en sorteer ze. Zoek de discussie op over welk (grootste) risico bovenaan komt te staan.

Bepaal de maatregelen

De laatste stap is het bepalen van de maatregelen. Kun je zelf geen passende maatregelen bedenken, kijk dan eens op de website van Ravib. Dit is een openbaar initiatief, waarin je bij bepaalde risico's de passende maatregelen kan vinden.

Klaar?

Bijna! Het is nuttig om de resultaten samen te vatten in een memo voor de bestuurder. Beschrijf daarin kort:

- de aanpak
- de grootste risico's
- de meest belangrijke maatregelen

De bestuurder of directeur heeft dan inzicht in de uitkomst van de risicoanalyse en de onderbouwing van de te nemen maatregelen. Na een akkoord kunnen vervolgens de voorgestelde maatregelen de komende tijd opgepakt worden.

Plan acties in

Tot nu toe is gekeken naar de onderwerpen die vanuit de AVG extra aandacht vragen. Ook zijn uit de risicoanalyse de nodige maatregelen voor jouw organisatie naar voren gekomen. Maar alles in één keer realiseren is niet mogelijk; maak daarom een actieplan. Hierin geef je aan welke acties je eerst gaat uitvoeren en wat je later oppakt.

Hieronder vind je een eenvoudig voorbeeld van een activiteitenkalender. Deze kun je downloaden en er vervolgens de te nemen acties, schoolvakanties en andere belangrijke data in zetten. Als je zelf al zo'n planning hebt, maak dan gebruik van je bestaande planning.

Voorbeeld jaarkalender
kn.nu/ww.864675b (xlsx, maken.wikiwijs.nl)

Het IBP-beleid en de onderliggende documenten en procedures moeten eigenlijk regelmatig, liefst elk jaar, weer eens bekeken worden om er zeker van te zijn dat alles nog actueel is. Plan deze jaarlijkse activiteit gelijk in.

Nu de grootste risico's bekend zijn en de maatregelen gekozen zijn kunnen de bijbehorende acties ingepland worden. Hou bij het plannen van acties goed rekening met de eisen vanuit de AVG. De AVG legt immers een aantal wettelijke verplichtingen op, waarbij je als instelling moet kunnen aantonen dat hieraan wordt voldaan.

Hoe helpt de Aanpak IBP?

In deze Aanpak is vast gekeken naar wat er **wettelijk** vanuit de AVG geregeld moet worden als het gaat om IBP. Op basis daarvan is de module 'Realiseren' als volgt opgebouwd:

1. **'*Realiseren - Aan de slag*':** bevat met name de onderwerpen, die zich afspelen binnen de muren van de school.
2. **'*Realiseren - Goed op weg*':** laat zien wat je moet regelen als je te maken krijgt met de wereld buiten je school, zoals afspraken rondom sociale media, uitwisseling van leerlinggegevens/-dossiers et cetera
3. **'*Realiseren - Samen vooruit*':** richt zich op grotere onderwerpen, die elke organisatie vanuit de AVG geregeld moet hebben. Dit zijn onderwerpen die we samen op kunnen pakken, zoals het aanstellen van een Functionaris voor gegevensbescherming, de DPIA, het voldoen aan de documentatieplicht en daarmee het ontwikkelen van een dataregister, het omgaan met (D)DoS en het continue verbeteren.

Aan de hand van deze planning kun je aantonen dat alle elementen de aandacht hebben en dat je stapsgewijs IBP op orde gaat krijgen. Het laat zien dat eraan gewerkt wordt om (aantoonbaar) te voldoen aan de AVG.

a. Aan de slag

Toelichting

In de eerste module van Realiseren richten we ons als eerste op wat je al geregeld had moeten hebben sinds het invoeren van de Wet bescherming persoonsgegevens in 2001. Het gaat om onderwerpen, die *gisteren* al klaar hadden moeten zijn; maar ook om onderwerpen, waarvoor we binnen de muren van de school, achter de voordeur, afspraken moeten maken.

Aan bod komen onder andere:

- Procedure melden **beveiligingsincidenten** / meldplicht **datalekken**
- **Rechten van betrokkenen** vastleggen
- **Privacyreglement** voor leerlingen en medewerkers
- **Afspraken met leveranciers** maken over het gebruik van leerlinggegevens en het afsluiten van **verwerkersovereenkomsten**
- Het **gebruik** van **beeldmateriaal**

In deze aanpak is al rekening gehouden met de invoering van de Europese Algemene verordening gegevensbescherming (25 mei 2018). Verder wordt uitgegaan van de meest recente tekst van de Wet bescherming persoonsgegevens. Hierdoor voldoet deze aanpak IBP zowel aan de huidige als toekomstige privacywetgeving!

Ok, aan de slag!

Procedure melden beveiligingsincidenten

Op 1 januari 2016 is de meldplicht datalekken ingegaan. Deze meldplicht houdt in dat alle organisaties (dus ook onderwijsorganisaties) een datalek moeten melden bij de Autoriteit Persoonsgegevens. In een aantal gevallen moet het datalek ook gemeld worden bij de betrokkenen (de personen van wie de persoonsgegevens zijn gelekt).

Verschil datalek en beveiligingsincident

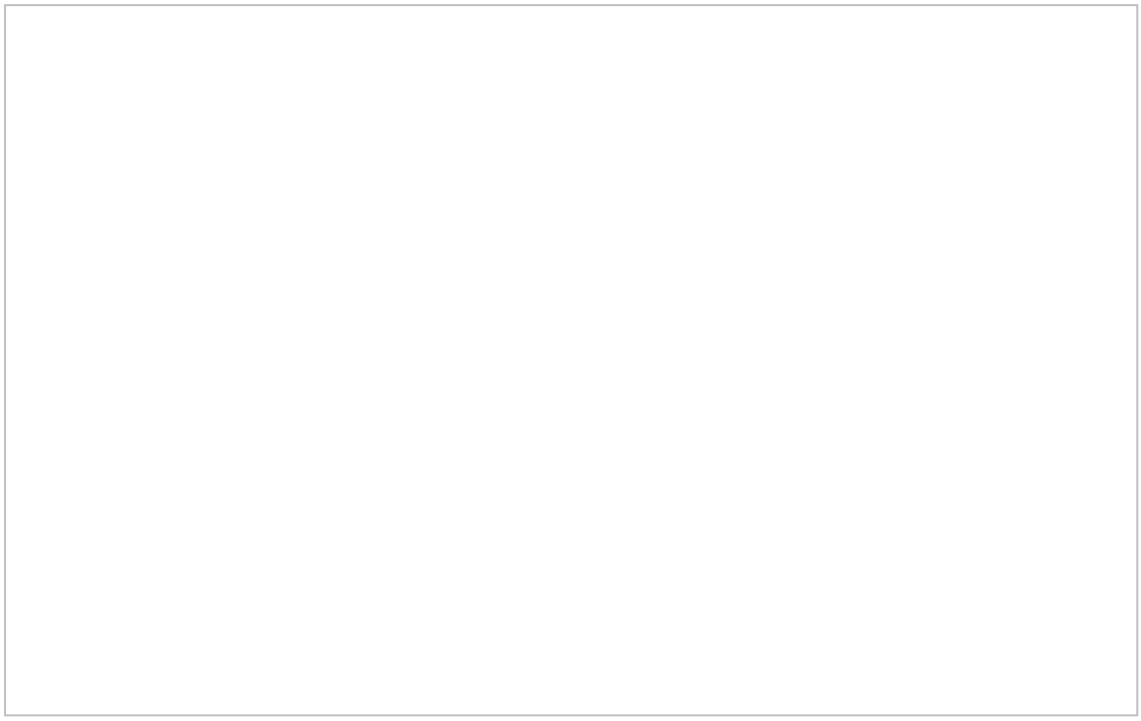
- Een **beveiligingsincident** is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatieverwerkende systemen in gevaar is of kan komen.
- Een **datalek** is een beveiligingsincident, waarbij persoonsgegevens verloren raken of onrechtmatig worden verwerkt (opgeslagen, aangepast, verzonden, enz.).

Alle datalekken zijn dus beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken!

LET OP: Zorg ervoor dat alle medewerkers weten wat een beveiligingsincident of een datalek is, en waar ze een beveiligingsincident moeten melden. Medewerkers moeten weten dat zij niet alleen het verlies van een usb-stick, een gestolen laptop et cetera met daarop persoonsgegevens van leerlingen en/of medewerkers moeten melden, maar ook melding moeten doen van die verstuurde e-mail naar de verkeerde geadresseerde.

Wel of niet melden

Het is belangrijk dat je weet wanneer je een gebeurtenis moet melden bij de Autoriteit Persoonsgegevens (AP) en eventueel ook aan de betrokkene. De AP heeft een richtsnoer meldplicht datalekken gepubliceerd, waarin het onderstaande schema staat. Dit schema helpt om de juiste afwegingen te maken en is **hier** te downloaden om in het procotol op te nemen.



Ook op de **website van Kennisnet** kun je verdere informatie vinden over hoe te handelen bij een datalek.

Protocol en incidentenregistratie

Naast de meldplicht is er ook de verplichting om alle **beveiligingsincidenten registreren.** Dat geldt óók voor alle incidenten die niet gemeld hoeven te worden. De Autoriteit Persoonsgegevens kan altijd om inzage hiervan vragen.

Om alles rondom het melden van datalekken en het registreren goed te regelen is het belangrijk om een protocol beveiligingsincidenten en datalekken op te stellen. Een voorbeeld staat onderaan deze pagina. Dit template kun je aanpassen aan de situatie op jouw school. Zorg er wel voor dat de onderstaande punten in het protocol worden meegenomen.

- Zorg dat het voor iedereen duidelijk is dat een incident gemeld moet worden. Stel bijvoorbeeld het e-mailadres van de manager-IBP / security-officer / informatiemanager beschikbaar.
- Een technisch onderzoek kan zowel intern als extern belegd zijn. Dit laatste zal het geval zijn als een school het IT-beheer heeft uitbesteed. Benoem dit in het protocol.
- De manier van communiceren met betrokkenen en eventueel met de pers: Leg dit vast in het protocol.
- Het omgaan met signalen van buitenaf over een mogelijk datalek.
- Onder welke omstandigheden je gebruik wilt/moet maken van externe deskundigen.
- Registreer en archiveer alle incidenten. Als je niet de beschikking hebt over een passend registratiesysteem (zoals b.v. *Topdesk*), dan kun je gebruik maken van het document onder

aan deze pagina om incidenten te registreren.

- Maak het melden van een incident door de ontdekker makkelijk door een standaard meldingsformulier te maken. Het onderstaande document ‘Incidentenregistratie’ bevat een tabblad '*Meldingsformulier ontdekker*'. Hierin staan de basisgegevens waarmee een dergelijk formulier gemaakt kan worden.

Protocol beveiligingsincidenten en datalekken
kn.nu/ww.412a68b (docx, maken.wikiwijs.nl)

incidentenregistratie
kn.nu/ww.2ba3959 (xlsx, maken.wikiwijs.nl)

Rechten van betrokkenen

Door de Algemene verordening gegevensbescherming (AVG) krijgen betrokkenen (degenen van wie persoonsgegevens worden verwerkt) meer mogelijkheden om voor zichzelf op te komen als het gaat om de verwerking van hun gegevens. Onder de AVG zijn de rechten van betrokkenen verder uitgebreid.

Rechten

Als het gaat om de rechten van betrokkenen is transparantie een belangrijke voorwaarde. Leerlingen en ouders moeten actief betrokken worden en er moet ze verteld worden wat hun rechten zijn. De organisatie moet betrokkenen de gelegenheid geven hun rechten eenvoudig en met redelijke tussenpozen uit te kunnen oefenen. Zorg ervoor dat zowel leerlingen als ouders en ook medewerkers goed geïnformeerd zijn over hun rechten en de procedure om van hun rechten gebruik te kunnen maken.

Maar welke rechten hebben leerlingen en/of hun ouders (als de leerlingen jonger zijn dan 16 jaar) en medewerkers eigenlijk? In het document 'transparantie en rechten betrokkenen' wordt dit verder uitgewerkt.

Transparantie en rechten betrokkenen
kn.nu/ww.0e7eba0 (pdf, maken.wikiwijs.nl)

Procedure

Informeer ouders en leerlingen op het moment dat zij – voor het eerst – persoonsgegevens actief en bewust gaan delen met de school over hun rechten. Vertel en leg uit welke gegevens er worden vastgelegd of doorgegeven aan een andere instantie en waarom. Zorg ervoor dat betrokkenen weten hoe zij van hun rechten gebruik kunnen maken. Leg in een

procedure vast hoe betrokkenen hun rechten kunnen uitoefenen. Neem rechten van betrokkenen op in het leerlingstatuut en/of in het privacyreglement. Zet ook op de website en eventueel in de schoolgids meer achtergrondinformatie over privacy en de rechten van betrokkenen.

In onderstaand document zijn de afspraken en procedures rondom de rechten van betrokkenen op een rij gezet.

Procesbeschrijving rechten betrokkenen
kn.nu/ww.563c16d (pdf, maken.wikiwijs.nl)

Privacyreglement

Iedere school verwerkt persoonsgegevens van personeel en leerlingen. In het privacyreglement leg je vast voor welke doelen je persoonsgegevens registreert. Het gaat hierbij niet alleen om gewone persoonsgegevens zoals naam, geboortedatum en overige contactgegevens, maar soms ook om bijzondere persoonsgegevens met betrekking tot bijvoorbeeld gezondheid, afkomst en godsdienst.

In het privacyreglement zijn in ieder geval alle onderdelen en processtappen beschreven die je in het vorige onderdeel hebt geregeld. Het bevoegd gezag is verantwoordelijk voor de bescherming van de privacy van leerlingen en medewerkers en stelt dan ook het privacyreglement vast. Het privacyreglement is daarmee voor alle scholen die onder hetzelfde gezag vallen van toepassing.

Via onderstaande stappen stel je het privacyreglement voor jouw school op.

Stap 1. Ken de wetgeving

Voor je met het privacyreglement aan de gang gaat is het goed om te weten wat er in de wet staat. Lees **dit artikel** op de website van Kennisnet om helemaal up-to-date te zijn, of kijk nog eens op de **betreffende pagina** in deze training.

Stap 2. Stel een privacyreglement op

Kennisnet helpt scholen om hun privacyreglement op te stellen door een voorbeeld-reglement ter beschikking te stellen. Deze kun je downloaden en voor je eigen school aanpassen.

Voorbeeld privacyreglement (conform AVG)
kn.nu/ww.a06669c (docx, maken.wikiwijs.nl)

Voorbeeld privacyreglement (conform WBP)
kn.nu/ww.f0d72ca (docx, maken.wikiwijs.nl)

***Let op**: het privacyreglement gaat over de rechten en plichten van betrokkenen. Dat betekent dat de (G)MR het reglement moet goedkeuren.*

Stap 3. Communiceer over privacy

Richting vaste medewerkers worden de afspraken rondom de bescherming van persoonsgegevens vaak als onderdeel van de arbeidsovereenkomst vastgelegd. Voor minder vaste medewerkers, stagiaires en ingehuurd personeel worden deze afspraken vaak niet opgenomen in de contracten. In dat geval kun je gebruik maken van een geheimhoudingsverklaring.

Geheimhoudingsovereenkomst onderwijs
kn.nu/ww.259d16c (docx, maken.wikiwijs.nl)

Een school heeft een informatieplicht en moet uitleggen hoe de school met de gegevens van leerlingen omgaat. Ouders hebben daarover recht op volledige transparantie van de school. Via onderstaande knop kun je praktische voorbeeldteksten downloaden die scholen kunnen gebruiken om ouders te informeren over privacy op school. Bijvoorbeeld door ze op te nemen in de schoolgids of op de website.

Voorbeeldteksten transparantie over privacy
kn.nu/ww.f04ddca (docx, maken.wikiwijs.nl)

In de module '**Communiceren**' vind je meer informatie over zowel de interne als externe communicatie rondom IBP.

Wachtwoordbeleid

Veel applicaties die in het po en vo gebruikt worden zijn online. Leerlingen moeten allemaal inloggen met een gebruikersnaam en een wachtwoord. Hoe ga je daar als school nu mee om en hoe hou je dat praktisch uitvoerbaar?

Hoe moet het niet?

Kies als school niet voor één simpel wachtwoord voor elke leerling om veel 'gedoe' te voorkomen.

De zorg zit niet zozeer in het feit dat leerlingen onderling bij elkaar kunnen kijken, maar meer in de onveiligheid en risico's naar buiten toe. Uit de programma's kunnen veel gegevens afgeleid worden, totaalscores, gesprekken via de chat enz.

Als het gaat om digitale vaardigheden en IBP, dan spreekt het vanzelf dat je leerlingen zo vroeg mogelijk leert om zorgvuldig om te gaan met hun persoonsgegevens en dus ook met hun

wachtwoorden. Dit sluit aan bij het mediawijs maken van leerlingen en de ict-*basisvaardigheden*. En dat leer je ze niet door ze allemaal hetzelfde wachtwoord te geven...

Hoe ga je dat nu aanpakken?

De drie basisregels voor wachtwoorden zijn voor iedereen gelijk. Ook jonge kinderen moeten we deze aanleren:

1. **Je wachtwoord mag je nooit delen, dat is iets van jou.**
2. **Je wachtwoord mag niet makkelijk te raden zijn** (Gebruik bijvoorbeeld een **'wachtzin'** `Mijnkatisliefennietgroen!`**)**
3. **Je wachtwoord mag je niet hergebruiken.** Gebruik voor alles een apart wachtwoord.

De *eerste regel* sluit dus uit dat wachtwoorden voor alle kinderen hetzelfde zijn. Een wachtwoord is persoonlijk.

De *tweede regel* heeft te maken met complexiteit. Hier wordt het wat lastiger, want kinderen moeten het wel kunnen onthouden. Mensen mogen je wachtwoord niet kunnen raden, maar ook computers niet.

- Mensen kunnen je wachtwoord makkelijk raden wanneer je iets heel simpels of bekends gebruikt, zoals de naam van je hond.
- Computers kunnen je wachtwoord makkelijk raden wanneer het kort is.

Vroeger werden korte, maar complexe wachtwoorden aanbevolen. Deze zijn voor een mens moeilijk te raden (maar wel te onthouden). Echter de huidige snellere computers kunnen deze wachtwoorden wél snel achterhalen. Een lang wachtwoord of een 'wachtzin' is dan ook beter dan een kort complex wachtwoord.

De *derde regel* zal voor jonge kinderen (po) niet realistisch zijn. In het vo kun je deze regel wel hanteren.

Kijk hier voor de video over **Een goed wachtwoord bedenken is superbelangrijk!**

Voorbeeld

Een pragmatische en effectieve oplossing kan zijn om (jonge) kinderen een zinnetje te laten maken. Ga hiervoor met de leerling als volgt te werk:

1. Maak een goed te onthouden zin, zoals 'Mijn kat is lief en niet groen'

2. Verwerk ook een hoofdletter, cijfer en/of leesteken in het wachtwoord, bijvoorbeeld `Mijnkatisliefennietgroen!`

Responsible disclosure

Voor schoolbesturen speelt ict een steeds grotere rol in de ondersteuning van het onderwijs. Het is hun verantwoordelijkheid te zorgen dat het onderwijs altijd door kan gaan en dat de veiligheid van een informatiesysteem en (software)producten wordt gegarandeerd.

Ondanks alle aandacht voor de beveiliging van systemen kan het voorkomen dat er toch een zwakke plek, een kwetsbaarheid, is. Als iemand een zwakke plek in één van de systemen heeft gevonden hoor je dat als school graag zo snel mogelijk, zodat de juiste maatregelen kunnen worden getroffen.

Ook al worden kwetsbaarheden zonder kwade bedoelingen bij toeval ontdekt, vaak worden ze niet gemeld bij de scholen. Wanneer scholen nadenken over hoe ze omgaan met beveiligingsproblemen en dit duidelijk naar buiten communiceren weten medewerkers en leerlingen beter waar ze aan toe zijn wanneer ze een kwetsbaarheid willen melden. Dit voorkomt onzekerheid en paniek aan beide kanten en beperkt eventuele schade zoveel mogelijk.

Model responsible disclosure leerlingen
kn.nu/ww.903ef42 (docx, maken.wikiwijs.nl)

Model responsible disclosure medewerkers
kn.nu/ww.6a59f11 (docx, maken.wikiwijs.nl)

Het responsibledisclosure-beleid heeft als doel om de drempel tot het melden van deze kwetsbaarheden te verlagen, waardoor het beveiligingsniveau van informatiesystemen en het netwerk verhoogd kan worden en schade voor de schoolbestuurder kan worden beperkt en/of voorkomen. Het responsibledisclosure-beleidis een oplossing om op een maatschappelijk verantwoorde en effectieve manier om te gaan met het melden van ict-kwetsbaarheden. Het geeft de mogelijkheid om af te spreken dat bij eventueel strafrechtelijk handelen van de melder geen aangifte zal worden gedaan of civielrechtelijke stappen zullen worden ondernomen.

Voor zowel de school als voor de melder schept het beleid duidelijkheid in de verantwoordelijkheden die beide partijen hebben. Het aanbieden van een beloning kan leerlingen mogelijk (extra) motiveren om een kwetsbaarheid te melden.

Afspraken met leveranciers: verwerkersovereenkomsten

In het IBP-beleid is al aangegeven dat een school verantwoordelijk is voor de zorgvuldige omgang met de persoonsgegevens van leerlingen. Om dit te kunnen garanderen zijn goede afspraken met aanbieders van digitale leermiddelen van belang.

Let op: In de Aanpak IBP gebruiken we vast de benamingen vanuit de AVG, dus we hebben het over **ver**werkers, **ver**werkersovereenkomsten en **verwerkingsverantwoordelijke**.

Model verwerkersovereenkomst

Dankzij het convenant '**Digitale Onderwijsmiddelen en Privacy 3.0**' is het voor scholen eenvoudiger om afspraken te maken met leveranciers. Belangrijkste punt in het convenant is de rolverdeling: scholen hebben de regie op wat er gebeurt met de persoonsgegevens. Dit mag je niet overlaten aan een leverancier (een verwerker). De school beslist wat de leverancier wél en niet met de gegevens mag doen.

Voor een groot deel is het convenant een vertaling van eisen uit privacywetgeving naar de onderwijspraktijk. Het convenant gaat niet alleen over het gebruik van digitaal leermateriaal, maar ook over school- en leerlingadministratiesystemen zoals ParnasSys, Magister en SOM.

Bijlagen bij het model

Bij het convenant hoort een modelverwerkersovereenkomst waarmee je schoolbestuur (de verwerkingsverantwoordelijke) de juiste afspraken maakt met leveranciers. Er is afgesproken met vertegenwoordigers van de leveranciers, dat de tekst van het model zo belangrijk is, dat het niet de bedoeling is om het model te wijzigen. Als dat echt noodzakelijk is, moet de leverancier dat in een *aparte* bijlage uitleggen.

Bij de modelverwerkersovereenkomst horen 2 bijlagen. In de **privacybijsluiter** wordt uitgelegd wat het product van de leverancier doet, welke gegevens er worden uitgewisseld met de leverancier, wat het doel is van die uitwisseling en of de leverancier andere bedrijven inschakelt (Deze noemen we subbewerkers). De tweede bijlage is de beveiligingsbijlage. Daarin staat bijvoorbeeld wat de afspraken zijn in geval van een beveiligingsincident zoals een datalek.

Via onderstaande knop kun je de modelverwerkersovereenkomst Versie 3.0 downloaden en gebruiken om afspraken met leveranciers vast te leggen.

Verwerkersovereenkomst 3.0

Aandachtspunten gebruik digitale onderwijsmiddelen

De onderstaande checklist gebruik digitale onderwijsmiddelen laat in een aantal stappen zien waar je rekening mee moet houden bij het inzetten van digitaal lesmateriaal en wat je eventueel moet regelen met de leveranciers ervan.

Checklist gebruik digitale onderwijsmiddelen (inclusief een schematische beslisboom)

Als een leverancier het convenant niet heeft ondertekend is het extra belangrijk om de privacy-afspraken goed vast te leggen. De 'checklist afspraken leveranciers' bevat de onderwerpen die de Autoriteit Persoonsgegevens benoemt om in een schriftelijke overeenkomst tussen verwerkingsverantwoordelijke en verwerker vast te leggen.

Certificeringsschema; een veilige en betrouwbare onderwijsketen

Het is voor onderwijsinstellingen lastig om eenvoudig vast te stellen of een leverancier de juiste beveiligingsmaatregelen heeft genomen. Omgekeerd is het voor leveranciers niet eenvoudig om aan te tonen dat zij tenminste aan de minimale eisen voldoen. Het hanteren van een eenduidige meetlat lost dit probleem op.

Digitale leermiddelen en (administratie)systemen moeten soepel werken en in navolging van de AVG moeten de gegevens, die hierbij verwerkt worden, betrouwbaar en goed beveiligd zijn. Het **certificeringsschema voor informatiebeveiliging** is die meetlat; het is de standaard die hiervoor is ontwikkeld.

Dit certificeringsschema is enerzijds bedoeld voor leveranciers van ict-toepassingen in de onderwijsketen. Zij kunnen op een eenduidige manier aantoonbaar maken dat ze de informatiebeveiliging en privacy van hun diensten en producten op orde hebben.

Anderzijds is het certificeringsschema bedoeld voor onderwijsinstellingen. Bij het specificeren van informatiebeveiligingseisen kun je eenvoudig verwijzen naar het certificeringsschema, in plaats van specifieke eisen te stellen met betrekking tot (veelal technische) maatregelen. Je kan als school met het toetsingskader eenvoudiger (laten) toetsen of de leverancier de informatiebeveiliging op orde heeft. Vraag aan de leverancier of hij zijn dienst heeft beoordeeld met het certificeringsschema en of hij een rapportage kan overleggen. Hoe meer scholen dit vragen van hun leveranciers, hoe meer leveranciers het ook als standaard zullen gaan zien. Op deze manier kunnen we samen de beveiliging in de hele keten naar een hoger niveau brengen. Kijk voor meer informatie over het certificeringsschema bij Edu-K

Gebruik beeldmateriaal leerlingen

Schoolfeestje, gezellig! En nu die filmpjes en foto's gelijk op de website... Nee dus. Foto's en video's van leerlingen zijn persoonsgegevens, daarom gelden er vanuit de privacywetgeving eisen voor het gebruik van beeldmateriaal.

Toestemming vragen

Het gebruiken van beeldmateriaal, het delen van foto's en video's van leerlingen door scholen, vormt zelden een probleem en is meestal goedbedoeld. Toch eist de wetgever dat de school vooraf toestemming vraagt aan ouders voor het gebruik van beeldmateriaal van leerlingen als de leerling jonger is dan 16 jaar. Als de leerling 16 jaar of ouder is moet hij/zij zelf toestemming geven. Zonder die toestemming mag je geen foto's en video's van leerlingen gebruiken.

Bij het vragen van toestemming zijn drie punten van belang:

- De toestemming moet **in vrijheid** gegeven worden; toestemming moet geweigerd kunnen worden zonder dat leerlingen daardoor benadeeld zouden worden.
- De toestemming moet **'ondubbelzinnig'** zijn. Toestemming mag niet verborgen zijn in schoolregels en er mag niet van uitgegaan worden dat ouders toestemming geven als zij niet reageren. Ouders/verzorgers moeten **expliciet** kunnen aangeven waar ze wel of geen toestemming voor verlenen. De school moet de toestemming altijd kunnen aantonen.
- De toestemming moet **specifiek** zijn. Het moet duidelijk zijn waar toestemming voor gegeven wordt en met welk doel. Zorg voor **gelaagde** toestemming: wil je toestemming voor foto's op de website, in de schoolgids, nieuwsbrief of in sociale media? De keuze moet duidelijk aan te geven zijn, bijvoorbeeld door een kruisje in een vakje te zetten bij bepaalde type media (foto's/film) of bij bepaalde uitingen (website, schoolkrant, etc.).

Zorg dat je als school vóóraf de juiste afspraken hebt gemaakt en dat iedereen ook weet wat die afspraken zijn. Lees voor extra informatie ook het artikel Nieuwe beleidsregels voor gebruik beeldmateriaal leerlingen.

Onderstaande voorbeeldbrief kan gebruikt worden om toestemming te regelen.

Toestemmingsformulier gebruik beeldmateriaal
kn.nu/ww.dda4c30 (docx, maken.wikiwijs.nl)

Tip: Foto's veilig delen

Naast toestemming vragen is de school ook verantwoordelijk voor het **veilig delen** van beeldmateriaal. Een openbaar fotoalbum mag niet meer. Plaats daarom foto's op een beveiligde site waarbij ouders moeten inloggen. Hou er wel rekening mee dat ook hier alléén foto's komen van kinderen waarvan de ouders toestemming hebben gegeven om foto's te delen!

Filmen/fotograferen door ouders

Het aantal ouders dat met camera's en smartphones foto's maakt of filmt op school is in de afgelopen jaren flink toegenomen. Ook deze foto's komen al snel op Facebook of YouTube. En wat als een ouder de foto van de beveiligde site kopieert en zelf deelt?

Ook hier geldt dat een school voor álle kinderen een veilige omgeving moet zijn, en niet een plek waar zij (en hun ouders) het risico lopen ongewenst gefotografeerd te worden. Maar het maken van foto's en video's door ouders op school kun je moeilijk verbieden. En als een ouder de foto kopieert en zelf deelt neemt de ouder daar de verantwoordelijkheid voor. De school kan niet verbieden dat ouders die foto's overnemen en verder delen (zelfs niet als dat bijvoorbeeld publiek op Facebook is)... Je kan er wel **afspraken** over maken, want een school is niet zomaar een openbare plaats waar iedereen toegang toe krijgt. Zo kun je het gesprek met ouders aangaan.

De volgende artikelen geven aanvullende informatie. Lees ze goed door, zodat je de do's en don'ts op jouw school met alle betrokkenen kunt delen.

- **Foto's van leerlingen gebruiken? Zo mag het wel!**
- **Mogen leraren en ouders foto's maken van leerlingen?**
- **Leidraad omgaan met online verspreiding ongewenste beelden**

Informatieplicht

Het realiseren van het IBP-beleid zal voor een groot deel uit **informeren** bestaan. De Algemene verordening gegevensbescherming (AVG) legt vanaf 25 mei 2018 een wettelijke verplichting op met betrekking tot informatieverstrekking. Schoolbesturen moeten de betrokkenen nog meer informeren over hoe zij met hun persoonsgegevens omgaan.

Een schoolbestuur moet transparant zijn over de privacyafspraken en -processen, en daar proactief informatie over verstrekken. Dat betekent bijvoorbeeld dat er in de schoolgids of op de website voldoende informatie is te vinden over hoe de school omgaat met persoonsgegevens, welke afspraken er zijn rondom privacy en welke maatregelen er zijn getroffen om de persoonsgegevens te beschermen.

Eigenlijk moet er bij iedere stap die je zet, elk proces dat je inregelt en ieder document dat je vastlegt een lampje gaan branden met de vraag:

Wie moet ik hierover inlichten en op welke manier?

Communiceer!

Het met regelmaat praten over het belang van informatiebeveiliging en privacy helpt om het bewustzijn bij iedereen te vergroten. In het hoofdstuk 'Communiceren' bieden we je tips hoe je met zowel medewerkers, leerlingen als ouders over deze onderwerpen een dialoog kunt starten. Wil je al direct van start, dan kun je via onderstaande links meteen het gewenste onderwerp opzoeken:

Dialoog met medewerkers

Dialoog met leerlingen

Dialoog met ouders

b. Goed op weg

Toelichting

Dat gaat lekker! In de vorige module heb je gerealiseerd wat je *gisteren* al geregeld moest hebben binnen de deuren van de eigen organisatie. In deze module kijken we naar de onderwerpen die naar voren komen als de voordeur opengaat, als we gebruik gaan maken van sociale media of gegevens moeten uitwisselen.

In deze module gaan we aan de slag met:

- **Afspraken over sociale media**
- **Gedragscode internetgebruik en meer;** gedragscode verantwoord gebruik bedrijfsmiddelen
- **Uitwisselen van gegevens**
- **Toegang tot gegevens**

Deze onderwerpen kun je in iedere gewenste volgorde oppakken. Misschien heb je bepaalde zaken al prima op orde; zelfs dan raden we je aan om toch even het betreffende onderwerp door te lezen, wellicht dat je nog verbeterpunten tegenkomt.

Zet ook deze activiteiten op de jaarkalender, zodat je het niet vergeet. Als er gevraagd wordt hoe het er voor staat, dan kan je laten zien wanneer je het opgepakt wordt .

Succes!

Afspraken over sociale media

Deel je artikelen met collega's via Twitter? Heeft jouw school een Facebook-pagina? Posten jullie video's van musicals op YouTube? Heb je al een Snapchat-account? En hoe up-to-date is je LinkedIn-profiel?... Vrijwel iedereen gebruikt tegenwoordig wel een of meerdere 'social media'. Media waarop wij als gebruikers *zelf* berichten kunnen zetten, in tekst, video, audio of afbeeldingen. Vaak erg handig en leuk, maar uiteraard ook met de nodige risico's.

Iedere school heeft wel positieve en negatieve verhalen te vertellen over het gebruik van sociale media door leerlingen (en medewerkers!). Om de online veiligheid van iedereen op school te verbeteren stellen scholen protocollen op, organiseren ze informatieavonden of sluiten ze bepaalde diensten af.

Met een protocol voor gebruik van sociale media (en internet) kun je als school afspraken maken over het gebruik hiervan, zodat voor iedereen duidelijk is wat de regels zijn. Je kunt er voor kiezen om voor leerlingen andere afspraken te maken dan voor medewerkers. Een belangrijk punt hierbij is om te bepalen of medewerkers, die namens of voor de school communiceren, hun eigen socialemedia-accounts mogen gebruiken.

Er is geen wettelijke verplichting om zo'n reglement of protocol te maken, maar het helpt wel om bewust om te gaan met sociale media binnen je school en draagt bij aan een sociaal veilig klimaat. Let er wel op dat een protocol of reglement weer de instemming vereist van de (G)MR. Kennisnet helpt je op weg met een **modelreglement**:

De volgende documenten kunnen helpen bij het maken van afspraken over sociale media bij jou op school.

Modelreglement sociale media voor leerlingen
kn.nu/ww.fff5bf8 (docx, maken.wikiwijs.nl)

Modelreglement sociale media voor medewerkers
kn.nu/ww.ef63f00 (pdf, maken.wikiwijs.nl)

Kijk bij **dialoog met leerlingen** voor mediawijsheid bij jongeren.

LET OP: De AVG stelt nieuwe eisen aan het gebruik van digitale diensten onder de 16 jaar. Wil je als school dat leerlingen *tijdens de les sociale media* gebruiken? Houd er dan rekening mee dat leerlingen jonger dan 16 jaar hiervoor de uitdrukkelijke toestemming moeten krijgen van hun ouders/verzorgers.

- Een bedrijf als Facebook, of een aanbieder van een app, moet straks op zijn beurt (kunnen) controleren of de wettelijk vertegenwoordiger die toestemming echt heeft gegeven. De school moet dit kunnen aantonen. Deze regel kan gevolgen hebben voor de snelheid waarmee je als school gebruik kan maken van digitale diensten tijdens de lessen.

Het is van belang om vooraf een goede afweging te maken over de inzet van sociale media in de lessen. Bedenk ook wat je doet als ouders géén toestemming geven. (Je wilt leerlingen niet uitsluiten van bepaalde lessen). Leg uit en leg vast wat de overweging is om sociale media in te zetten tijdens de les als digitaal lesmateriaal.

Meer informatie over sociale media vind je hier. Gebruik deze informatie om voor jouw school een duidelijk beleid rondom dit type media te formuleren.

Gedragscode gebruik bedrijfsmiddelen waaronder ict en internet

Wettelijk gezien heb je als werkgever het recht om regels te stellen aan hoe iemand zijn werk moet doen, zolang maar duidelijk is welke regels je stelt en die regels binnen het redelijke blijven.

Zo is het verplicht om werknemers enige vrijheid te geven bij het privégebruik van internet en e-mail, maar mogen er wel regels gesteld worden over hoe dat privégebruik dan wordt uitgevoerd (“Niet storend voor de dagelijkse werkzaamheden” is de standaardzin.) Ook mag je een internetfilter instellen en niet-werkgerelateerde sites blokkeren. De regels moeten ook rekening houden met privacy, het bedrijfsbelang en ze moeten tegelijk algemeen genoeg zijn om alle situaties te dekken.

Scholen moeten niet alleen de AVG naleven, zij moeten ook kunnen aantonen dat zij deze naleven. De AVG vraagt daarmee een uitbreiden van de afspraken rondom ict, internet en e-mail gebruik omwille van het bedrijfsbelang.

Aanvullende regels over het veilig omgaan met persoonsgegevens, het melden van beveiligingsincidenten en datalekken, regels rondom aanschaf digitaal lesmateriaal en informatiesystemen (denk aan de verwerkersovereenkomsten en mogelijke DPIA) en het gebruik van eigen devices worden noodzakelijk. Het gaat steeds meer over het verantwoord gebruik van bedrijfsmiddelen, waarvan het gebruik van ict, internet en e-mail een onderdeel is.

Een gedragscode voor verantwoord gebruik van bedrijfsmiddelen (ook wel acceptable use policy genoemd) geeft aan wat het opgestelde IBP-beleid voor medewerkers in de praktijk betekent. Het legt vast wat er van de medewerkers verwacht wordt met betrekking tot het gebruik van de ter beschikking gestelde bedrijfsmiddelen en de inzet van eigen devices voor schoolwerkzaamheden. De gedragscode beschrijft ook de regels voor de controle op de naleving ervan.

Onderstaande handreiking geeft de school de mogelijkheid om een gedragscode 'op maat' te maken.

Handreiking verantwoord gebruik van bedrijfsmiddelen voor medewerkers
kn.nu/ww.d393b65 (docx, maken.wikiwijs.nl)

Let op: een gedragscode vereist de instemming van de (G)MR omdat het te maken heeft met de privacy van leerlingen en/of medewerkers.

Uitwisselen van gegevens

Passend onderwijs

Als leerlingen extra zorg of begeleiding nodig hebben, legt een school extra persoonsgegevens over de leerling vast, bijvoorbeeld over gezondheid of gedrag. Deze informatie ziet de wet als **bijzondere persoonsgegevens**. Een school moet extra zorgvuldig omgaan met deze gegevens.

Aparte afspraken

Op het moment dat de school gegevens wil uitwisselen met een andere organisatie, bijvoorbeeld een

onderwijskundige, pedagoog of psycholoog, dan moet je daar **aparte afspraken** over maken. Deze afspraken leg je vast in een verwerkersovereenkomst waarin vertrouwelijkheid van de gegevens centraal staat. Let er ook op dat je bij het inschakelen van een externe deskundige zoals een psycholoog ook de **toestemming** nodig hebt van de wettelijk verzorgers (ouders).

Soms lukt het niet om de juiste begeleiding op de school zelf te regelen. Dan schakel je het **samenwerkingsverband passend onderwijs** (afgekort: swv) in, bijvoorbeeld voor een toelaatbaarheidsverklaring passend onderwijs.

Samenwerkingsverband passend onderwijs (Swv)

Het swv is een **zelfstandige organisatie**. De wet beschrijft dat het swv een zelfstandige wettelijke taak heeft. In privacytermen is het swv een 'verwerkingsverantwoordelijke', en dus zelf verantwoordelijk voor de gegevens van leerlingen. Zodra de school leerlinggegevens aanlevert aan het swv, is het swv verantwoordelijk voor de privacybescherming. Het swv is dus géén verwerker voor de school. Een schoolbestuur sluit dus géén verwerkersovereenkomst af met het swv. De wet regelt dat de school gegevens mag uitwisselen met het swv. De **vijf vuistregels** blijven uiteraard wél van toepassing.

Meer informatie over passend onderwijs is **hier** te vinden, of via de site van het steunpunt passend onderwijs van de VO-raad.

Jeugdhulpverlening

Het kan voorkomen dat een leerling extra ondersteuning nodig heeft, dat er thuis problemen zijn of dat een leerling met politie en justitie in aanraking is gekomen. In al deze gevallen wissel je gevoelige gegevens uit over leerlingen. Omdat de school gegevens uitwisselt met andere organisaties, moet duidelijk zijn hoe iedereen omgaat met de privacy van de leerlingen.

Basiszorg

De basiszorg voor jeugd en gezin is meestal per gemeente geregeld. Om gegevens met deze organisaties uit te kunnen wisselen is het belangrijk om afspraken te maken in een **convenant** ('privacyconvenant sociale wijkteams'), en om in een **privacyreglement** te beschrijven wat ieders rechten en plichten zijn. Zie voor meer informatie het Convenant en privacy samenwerking jeugdhulpverleners.

Externe partners

Het Nederlands Jeugdinstituut heeft een handreiking gemaakt voor scholen die samenwerken met externe partners. Deze handreiking geeft informatie en praktische tips over hoe je om moet gaan met privacy en wat wel en niet mag binnen de kaders van de wet. Lees meer in de Handreiking samenwerking externe partners

Gezondheidsprojecten

Scholen krijgen regelmatig de vraag om mee te werken aan onderzoeken over de gezondheid van leerlingen. Wat er wel en niet mag bij deze gezondheidsprojecten lees je in Gegevensuitwisseling bij gezondheidsonderzoeken

Uitwisseling leerlingdossiers en OKR

Om leerlingen zo goed mogelijk te begeleiden en het beste onderwijs te geven verzamelen scholen veel gegevens. Als een leerling overstapt naar een andere school, is het verplicht om informatie te delen met de nieuwe school. Met welke privacyaspecten moet de school dan rekening houden?

Primair onderwijs

Om ervoor te zorgen dat leerlingen in het basisonderwijs op hun nieuwe school de juiste ondersteuning en begeleiding krijgen, is in de 'Wet primair onderwijs' geregeld dat de basisschool de nieuwe school voorziet van een onderwijskundig rapport (**okr**). Bij de overstap naar de middelbare school noemt men dit ook wel het **overstapdossier**. Na overleg met het onderwijzend personeel stelt de directie dit rapport op. Het rapport moet een goede, doorlopende leerlijn voor elke leerling garanderen.

Voor de uitwisseling van het okr tussen de basisschool en de nieuwe school (po of vo), is geen toestemming van de ouders nodig. Ouders kunnen dan ook geen bezwaar maken tegen de uitwisseling van die informatie: de school moet de informatie hoe dan ook uitwisselen. Wel hebben ouders het recht op inzage van het overstapdossier vóórdat dit wordt uitgewisseld. Inzage heeft geen aanpassing van het rapport tot gevolg. Bezwaren en opmerkingen van de ouders worden apart vastgelegd en toegevoegd aan het dossier. De school moet de mogelijkheid tot inzage van ouders schriftelijk vastleggen in het leerlingdossier. Hiermee maakt de school het controleerbaar dat de informatieplicht is nageleefd. Deze informatieplicht ligt immers wettelijk vast.

Voortgezet onderwijs

Ook de 'Wet voortgezet onderwijs' kent een overstapdossier. Het gaat daarbij om het contact met een andere school of instelling voor ander onderwijs, ten behoeve van de in- en uitschrijving van de leerling. Onder dit contact vallen alle uitwisselingen van leergegevens en de direct met het leren samenhangende begeleidingsgegevens.

Het uitgangspunt van het okr is dat de scholen alleen gegevens overdragen die zij relevant vinden voor de nieuwe school.

De oude school mag dus niet het gehele leerlingdossier ongezien doorsturen, maar alleen die gegevens die nodig zijn om de leerling op de nieuwe school goed te begeleiden en te laten leren.

Overstapservice Onderwijs (OSO)

Uitgebreide informatie over de Overstapservice Onderwijs (OSO) en hoe privacy geregeld is vind je bij Overstapservice Onderwijs

Leerplicht en verzuim

Nederland is verdeeld in 39 Regionale Meld- en Coördinatiepunten (RMC) voor voortijdig schoolverlaters (vsv'ers). Elke RMC-regio heeft een contactgemeente die de melding en registratie van voortijdig schoolverlaters coördineert en zorg draagt voor mogelijkheden van doorverwijzing en herplaatsing in het onderwijs.

Wat mag een leerplicht-/RMC-ambtenaar nu eigenlijk opvragen?

Belangrijk uitgangspunt bij het delen van informatie is:

- Wat regelt de wet (grondslag)
- Dataminimalisatie.

1. Leerplichtambtenaren hebben vanuit de Leerplichtwet een wettelijk recht op informatie, waarbij het vooral gaat om verzuiminformatie.
2. Een leerplichtambtenaar heeft alleen recht op die informatie die hij/zij strikt noodzakelijk nodig heeft voor de uitoefening van het werk. Een leerplichtambtenaar hoeft niet te zien dat een voorbeeldige leerling één uur mist…

Een leerplicht-/RMC-ambtenaar mag geen andere persoonsgegevens verwerken dan:

1. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens van de leerplichtige;
2. een administratienummer dat geen andere informatie bevat dan bedoeld onder a;
3. nationaliteit en geboorteplaats;
4. gegevens als bedoeld onder 1, van de ouders, voogden of verzorgers van de leerplichtige;
5. gegevens met betrekking tot de inschrijving of afschrijving van de leerplichtige;
6. gegevens ten aanzien van het schoolverloop, het schoolverzuim en van het beroep op een vrijstelling van de leerplicht;
7. andere dan de onder 1 tot en met 6 bedoelde gegevens waarvan de verwerking is vereist of noodzakelijk is met het oog op de toepassing van de Leerplichtwet 1969 of een andere wet.

Andere informatie delen mag niet. Een account in een leerlingvolgsysteem (Magister, Parnasys , SOMtoday, enz) mag dan ook niet! (Daar mag een ambtenaar van gemeente of RMC zelfs niet eens om vragen!)

Wie mogen gegevens inzien?

Wie mogen eigenlijk de gegevens op school inzien? De vuistregel dataminimalisatie zegt het volgende:

- **Je gebuikt niet meer persoonsgegevens dan strikt noodzakelijk.**
- **Je zorgt ervoor dat niet meer mensen toegang hebben tot die persoonsgegevens dan nodig is.**

Een conciërge zal niet altijd hoeven te weten welke leerlingen extra begeleiding nodig hebben, en de cijfers van wiskunde zijn niet altijd relevant voor een aardrijkskundedocent.

Dat betekent dat vastgelegd moet worden met wie persoonsgegevens uitgewisseld en intern gedeeld worden, wie toegang heeft tot bepaalde persoonsgegevens in de verschillende informatiesystemen.

Zodat het inzichtelijk is wie, of welke rol, geautoriseerd is om bepaalde verwerkingen van (persoons)gegevens te doen. De (informatie)systemen die de school gebruikt, moeten zijn ingericht op basis van deze rolverdeling.

Het is van belang om (informatie)systemen zo in te richten, dat alleen die medewerkers geautoriseerd zijn om bepaalde persoonsgegevens te verwerken, die dat voor hun werkzaamheden nodig hebben.

Maar informatie over autorisatie is terug te vinden in de dataregisters. Hierin kan aangegeven worden welke rollen toegang hebben tot welke persoonsgegevens in bepaalde informatiesystemen en in specifieke interne documenten.

c. Samen vooruit

Toelichting

De basis is nu op orde. We zijn aan de slag gegaan met IBP, we zijn goed op weg. Maar IBP is nooit af. We zullen regelmatig moeten evalueren en continu moeten verbeteren. We moeten nu groeien; groeien in uitvoering van het beleid, maar ook groeien in het verder vereenvoudigen en waar nodig aanscherpen van de processen rondom IBP.

Kennisnet biedt je daar graag ondersteuning bij. We willen je vragen het IBP-beleid regelmatig intern te evalueren en eventuele aanvullende vragen aan ons voor te leggen. Op die manier kunnen we deze online Aanpak IBP steeds aanvullen met relevante onderwerpen, die mogelijk ook op andere scholen spelen. Op die manier komen we samen vooruit.

Daarnaast zullen in deze module de grotere onderwerpen, die we samen op kunnen pakken, worden uitgewerkt, zoals de gegevensbeschermingseffectbeoordeling, de verantwoordingsplicht, DDoS en meer.

Heb je nu al onderwerpen die je graag in deze Aanpak IBP terug zou zien, neem dan contact op met de IBP-helpdesk

via ibp@kennisnet.nl of 0800-3212233.

Evalueren en verbeteren

Om te kunnen groeien moet je continu kunnen verbeteren. Maar hoe pak je dat aan? Hoe weet je *wat* je moet verbeteren? Aanpassingen en verbeteringen komen onder andere naar voren bij het evalueren van IBP en de controle ervan. Maar ook kunnen ontwikkelingen zoals nieuwe processen of nieuwe systemen vragen om aanpassingen.

Continu verbeteren kun je organiseren op basis van Plan Do Check Act, ofwel de **PDCA-cyclus**.

Dit proces omvat vier stappen:

Stap 1. Plan

in deze stap formuleer je beleid ten aanzien van informatiebeveiliging en privacy. Je analyseert de bestaande situatie en brengt de kwaliteit van bestaande beveiligingsmaatregelen in beeld. Je kijkt welke bedreigingen onacceptabele risico's voor de organisatie vormen en wat het gewenste niveau van informatiebeveiliging is. Ook beschrijf je hoe de organisatie dit beleid ten uitvoer brengt.

Stap 2. Do

Tijd en middelen zijn beperkt, daarom maak je in deze stap een planning en een selectie van beveiligingsmaatregelen die het gewenste beveiligingsniveau dichterbij brengen. Ook voer je de maatregelen daadwerkelijk uit in de organisatie, applicaties en/of infrastructuur.

Stap 3. Check

Je beoordeelt alle activiteiten van het IBP-proces van de controle op naleving van het beleid, controle van de (voortgang van) de implementatie tot onafhankelijke controle.

Stap 4. Act

Daar waar nodig pas je bijvoorbeeld documenten, processen of maatregelen aan en kan bijsturing plaatsvinden van de planning of het beleid.

Ons advies is om deze cyclus **jaarlijks** terug te laten komen. Vanuit dit evaluatieproces kun je gewenste activiteiten in de kalender opnemen.

Functionaris voor gegevensbescherming (FG)

Onder de AVG zijn onderwijsinstellingen, op grond van artikel 37-39, verplicht vanaf 25 mei 2018 een Functionaris voor gevensverwerking (FG) aan te stellen. Dit is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG.

Wat is een FG?

Een Functionaris voor gegevensverwerking (FG) is een interne toezichthouder op de verwerking van persoonsgegevens binnen een onderwijsinstelling. Deze functionaris heeft geen formele sanctiebevoegdheden, maar wel controlebevoegdheden. Hij adviseert het schoolbestuur (bevoegd gezag) over privacy en houdt toezicht daarop, handelt vragen en klachten over privacy af, ontwikkelt (interne) regelingen rondom privacy en geeft advies over technologie en beveiliging (privacy by design). De FG moet voldoende kennis hebben van de organisatie en van privacywetgeving, betrouwbaar zijn en moet in onafhankelijkheid zijn werkzaamheden kunnen verrichten. De FG heeft dezelfde ontslagbescherming als leden van de (G)MR.

De verplichting om en FG aan te wijzen is één van de zaken die een schoolbestuur moet regelen vanaf 25 mei 2018. Niet alle schoolbesturen zullen dan al een FG hebben aangewezen, bijvoorbeeld omdat er nog afspraken moeten worden gemaakt met de schoolbesturen waarmee samen een FG wordt geregeld of omdat het schoolbestuur eerst de basis onder informatiebeveiliging en privacy wil hebben gelegd. Het advies is dat het schoolbestuur documenteert waarom er (nog) geen FG is aangewezen, en wat de planning is om dat wel te gaan doen. Het is verdedigbaar dat een schoolbestuur eerst andere verplichtingen uit de AVG op orde wil hebben gebracht voordat een FG daarop intern toezicht gaat houden.

Wat moet je doen?

In onderstaande 'Handreiking FG voor po/vo' wordt uitgelegd op welke grond een schoolbestuur een FG moet aanwijzen, hoe je die aanwijzing regelt, wat diens taken en bevoegdheden zijn en wat de functie-eisen zijn. Daarnaast worden een aantal praktijkvoorbeelden gegeven over hoe een FG geregeld kan worden.

Handreiking FG voor po/vo
kn.nu/ww.9a8f0d8 (pdf, maken.wikiwijs.nl)

Gegevensbeschermingseffectbeoordeling (PIA)

D e **Gegevensbeschermingseffectbeoordeling.** De AVG gebruikt hiervoor de termen ‘data protection impact assessment (DPIA) of Privacy Impact Assessment (PIA). Ook scholen zijn straks verplicht in bepaalde gevallen een “gegevensbeschermingseffectbeoordeling” te doen. Wanneer geldt die plicht? En hoe kun je dat als school oppakken.

In voorbereiding; verwacht half mei 2018. (*De vermelde datum is een indicatie, als daar wijzigingen in komen worden die hier ook weergegeven)*

Verantwoordings- en informatieplicht

Met ingang van 25 mei 2018 vervalt niet alleen de Wet bescherming persoonsgegevens, maar ook het Vrijstellingsbesluit. Hierin stond welke persoonsgegevens een onderwijsinstelling mocht verwerken zonder dat te melden bij de Autoriteit Persoonsgegevens. Onder de AVG komt hiervoor de documentatieplicht of beter gezegd de verantwoordingsplicht in de plaats.

Verantwoordingsplicht

De nieuwe regels dwingen onderwijsinstellingen om goed na te denken over hoe persoonsgegevens worden verwerkt en beschermt. De verantwoordingsplicht houdt in dat je moet kunnen aantonen dat alle verwerkingen aan de regels van de AVG voldoen. Dat je de juiste organisatorische en technische maatregelen hiervoor hebt genomen.

Denk hierbij aan de volgende punten:

- Zorg er als onderwijsinstelling voor dat alles wat je doet in het kader van IBP, wordt vastgelegd.
- Zorg er bijvoorbeeld voor dat het IBP-beleid op papier staat en dat het duidelijk is dat je medewerkers heb verteld wat de AVG is en welke gevolgen dat voor hun werkzaamheden heeft.
- Zorg ervoor dat gegevens van de risicoanalyse bewaard blijven op een centrale plek.
- Als voor de verwerking toestemming is vereist, bijvoorbeeld voor het gebruik van beeldmateriaal, zorg er dan voor dat die verkregen toestemming ook aangetoond kan worden.

Daarnaast moet elke **verwerkingsverantwoordelijke en verwerker** (schoolbestuur en leverancier van digitaal lesmateriaal) een register van de verwerkingsactiviteiten bijhouden. Dit is een overzicht van alle verwerkingen van persoonsgegevens die zij uitvoeren. Dit kunnen verwerkingen zijn die een wettelijke grondslag hebben, maar ook verwerkingen waarvoor toestemming gegeven is door de betrokkene of op basis van een overeenkomst.

Als verwerkingsverantwoordelijke (lees schoolbestuur) moet je een dergelijk overzicht kunnen tonen aan de Autoriteit Persoonsgegevens als deze daar om vraagt. Artikel 30 van de AVG stelt eisen aan het register van verwerkingsactiviteiten.

Dit specifieke onderdeel van de verantwoordingsplicht wordt onder het kopje dataregister verder uitgewerkt.

Informatieplicht

Naast een verantwoordingsplicht heeft elke school ook en een informatieplicht. Dat betekent dat je verplicht bent om nieuwe en bestaande leerlingen en ouders van leerlingen, maar ook medewerkers duidelijk te informeren over wat de school met hun persoonsgegevens doet. In de AVG staat dat de informatie over verwerkingen in principe schriftelijk gegeven moet worden. De beste manier om er zeker van te zijn dat de informatie voor de meeste mensen

goed vindbaar is, is het publiceren van een online **privacyverklaring**. Daarnaast mag je altijd andere middelen inzetten.

De AVG stelt een aantal specifieke eisen waar een privacyverklaring aan moet voldoen. Deze eisen gaan over de inhoud, de toegankelijkheid en de duidelijkheid van de informatie.

Tip: om de informatie in een (online) privacyverklaring zo toegankelijk mogelijk te maken, kan de verklaring in meerdere lagen opgesteld worden. Bijvoorbeeld:

- In de eerste laag geef je de contactgegevens aan en welke gegevensverwerkingen de meeste impact hebben op de betrokkenen en hoe de school daarmee omgaat.
- In de tweede laag van de privacyverklaring kan dan meer in detail aangeven worden welke persoonsgegevens er voor welk doel verwerkt worden en hoe betrokkenen hun rechten kunnen uitoefenen.

Het onderstaande format voor een privacyverklaring met betrekking tot leerlinggegevens staat eveneens in het dataregister voor leerlingen po/vo. Pas dit format aan zodat het bij de school past.

Privacyverklaring gebruik leerlinggegevens
kn.nu/ww.fa45b11 (docx, maken.wikiwijs.nl)

Dataregister

Het bijhouden van een **register van de verwerkingsactiviteiten** is een onderdeel van de verantwoordingsplicht. Dit register bevat informatie over de persoonsgegevens die binnen of ten behoeve van de onderwijsinstelling worden verwerkt. Artikel 30 van de AVG geeft aan wat het register van de verwerkingsactiviteiten minimaal moet bevatten.

Er is voor gekozen om naast de wettelijk verplichte informatie over de verwerkingsactiviteiten nog een aantal extra onderwerpen toe te voegen om er voor het onderwijs een bruikbaar totaaloverzicht van te maken.

Dit totaaloverzicht noemen we het **DATAREGISTER**.

Het dataregister bevat als extra een BIV-classificatie op het niveau van de gebruikte persoonsgegevens, een overzicht van de brondocumenten en de mogelijkheid om aan te geven tot welke persoonsgegevens interne gebruikers toegang hebben (Autosisatie). Verder een overzicht van persoonsgegevens die worden opgeslagen in interne applicaties en specifieke documenten.

De dataregisters zijn gebaseerd op de categorie van betrokkenen, uiteindelijk zullen de volgende dataregisters, elk voorzien van een eigen handleiding, beschikbaar zijn voor po/vo:

- dataregister voor leerlingen po/vo

- dataregister voor medewerkers in loondienst po/vo
- dataregister voor medewerkers niet in loondienst po/vo
- dataregister voor relaties po/vo

Dataregister leerlingen po/vo
kn.nu/ww.a178013 (xlsx, maken.wikiwijs.nl)

Handleiding dataregister leerlingen po/vo
kn.nu/ww.ee8d723 (pdf, maken.wikiwijs.nl)

Dataregister medewerkers in loondienst po/vo
kn.nu/ww.a3fac5f (xlsx, maken.wikiwijs.nl)

Handleiding dataregister medewerkers in loondienst po/vo
kn.nu/ww.b5626f3 (pdf, maken.wikiwijs.nl)

Dataregister relaties po/vo
kn.nu/ww.be220d0 (xlsx, maken.wikiwijs.nl)

Handleiding dataregister relaties po/vo
kn.nu/ww.bdc81ee (pdf, maken.wikiwijs.nl)

(D)DoS, wat moet ik weten...

Een (D)Dos-aanval op school: dit kan iedereen overkomen. Je systemen liggen plat, je netwerk is traag en iedereen belt je met vragen. En jij vraagt je af: Wat moet ik doen?

Wat is een DDoS-aanval?

Een (distributed) denial-of service of (D)DoS-aanval is één van de bedreigingen, die de continuïteit van het onderwijs steeds vaker in gevaar brengen. De aanval heeft als doel om de beschikbaarheid van een systeem te onderbreken. Het zorgt er bijvoorbeeld voor dat de website of de geplande digitale toets niet bereikbaar is. Dit gebeurt meestal door het versturen van meer verzoeken dan het systeem

kan afhandelen. Wanneer een aanval vanaf meerdere computers (soms wel duizenden tegelijk) wordt uitgevoerd, dan is er sprake van een DDoS-aanval. Vaak wordt gebruik gemaakt van een zogenaamd botnet, een verzameling van computers die onder de controle van de aanvaller(s) zijn gekomen. Het is dan ook belangrijk om maatregelen tegen deze bedreiging te nemen, zodat het onderwijs door kan gaan.

DDoS-aanval op school: wat nu?

Het is niet eens de vraag of je als school te maken krijgt met een DDoS-aanval, maar meer wanneer. Wees er op voorbereid. Kennisnet heeft, in samenwerking met politie, scholen en leveranciers, een handig informatiedossier opgesteld over DDoS-aanvallen op school. In dit dossier vind je meer informatie over dit onderwerp.

Behalve informatie over DDoS-aanvallen, behandelt het dossier ook de maatregelen die bestuurders, ict-coördinatoren en technisch medewerkers moeten nemen vooraf en tijdens een aanval. Zij zijn tenslotte samen verantwoordelijk voor de continuïteit van goed werkende en veilige ict-toepassingen op school. In de drie stappen herkennen, aanpak en preventie, wordt per takenpakket uitgelegd hoe jij jouw school zo goed mogelijk kan beschermen tegen DDoS-aanvallen en/of de gevolgen daarvan.

Bekijk het dossier DDoS-aanval op school

Cameratoezicht

Cameratoezicht wordt vaak ingezet om veiligheid te waarborgen, maar hoe zit het met de privacy?Het inzetten van cameratoezicht past in een groter pakket aan fysieke maatregelen dat wordt toegepast om de veiligheid van medewerkers, leerlingen en bezoekers binnen en in de directe omgeving van locaties van po- en vo-instellingen te waarborgen.

Op po- en vo-instellingen hangen steeds vaker camera's. Om bijvoorbeeld vernielingen of diefstal tegen te gaan. Maar hiermee is de inbreuk op de privacy van leerlingen, medewerkers en bezoekers groot. Daarom mogen po- en vo-instellingen alleen camera's ophangen als zij aan een aantal voorwaarden voldoen. Ook moeten zij ervoor zorgen dat de inbreuk op de privacy zo klein mogelijk is. Een camera in bijvoorbeeld een toilet gaat te ver, omdat mensen dan ontkleed in beeld kunnen komen.

De handreiking cameratoezicht helpt po- en vo-instellingen om het gebruik van camera's goed te regelen, en daarbij de privacy van leerlingen, medewerkers en bezoekers te waarborgen. Het bijgesloten modelreglement cameratoezicht heeft betrekking op die locaties van een po- en vo-instelling, waar toezicht door middel van camerasystemen wordt ingezet. De handreiking geeft een beschrijving van taken, verantwoordelijkheden en procedures over het cameratoezicht, met het oog op integer gebruik van het camerasysteem en de bescherming van privacy van leerlingen, medewerkers en bezoekers.

Handreiking cameratoezicht

Handreiking cameratoezicht in het PO- en VO-instellingen
kn.nu/ww.08e4f20 (pdf, maken.wikiwijs.nl)

3. Communiceren

Waarom communiceren?

Mooi! Je ben bij de derde stap aangekomen. Nu moet je ervoor zorgen dat IBP geen papieren tijger blijft, maar echt in de school gaat leven. Dat doe je door erover te **communiceren**.

Medewerkers

Vertel je medewerkers wat informatiebeveiliging voor hen betekent en hoe ze verstandig omgaan met persoonsgegevens. Er zijn verschillende manieren voor om dit te bereiken. Het organiseren van een 'security awareness training' is een veelgebruikte methode om alle medewerkers te trainen in IBP.

Leerlingen

Aan je leerlingen leg je uit hoe je met hun gegevens omgaat en hoe zij zélf verstandig omgaan met bijvoorbeeld hun schoolaccounts en wachtwoorden.

Ouders

En vergeet de ouders niet: zij beslissen over de privacy van hun kinderen (die jonger zijn dan 16 jaar). Ouders willen weten hoe IBP op jouw school geregeld is, zodat ze het vertrouwen krijgen dat de gegevens van hun kinderen bij jou veilig zijn.

Dialoog met medewerkers

Beleid en maatregelen zijn niet voldoende om risico's op het gebied van informatiebeveiliging en privacy uit te sluiten. Meestal speelt de mens een belangrijke rol als er beveiligingsincidenten of datalekken zijn ontstaan. Daarom is het erg belangrijk om het bewustzijn bij de medewerkers te vergroten en aan te scherpen.

Bewustwording

Onderdeel van het IBP-beleid is dat je regelmatig terugkerende bewustwordingscampagnes voor medewerkers organiseert. Je kunt daarbij algemene scholing geven aan alle medewerkers, of specifieke trainingen organiseren voor groepen medewerkers die vaker met informatiebeveiliging en privacy te maken hebben. Denk bijvoorbeeld aan een bijeenkomst voor medewerkers van de administratie, of zorgcoördinatoren.

Elke medewerker en leerling moet ervan uit kunnen dat er altijd zorgvuldig met zijn of haar persoonsgegevens wordt omgegaan. Naleving van de wetgeving is wel de verantwoordelijkheid van de bestuurder, maar naleving en borging hiervan kunnen alleen bereikt worden wanneer iedereen binnen de schoolorganisatie zorgvuldig en verantwoord met persoonsgegevens weet om te gaan.

Om dit te faciliteren zijn er twee mogelijkheden:

1. De eerste is een model-PowerPointpresentatie. Een medewerker, die belast is met IBP,

kan deze presentatie binnen zijn organisatie aan de medewerkers geven. Hij wordt hierbij ondersteund door een inhoudelijke toelichting die in de notities van de slides is verwerkt.

2. Een tweede optie is dat medewerkers op eigen gelegenheid de online workshop "training bewustwording IBP voor medewerkers" in Wikiwijs doorlopen.

Klik voor de online workshop: "training bewustwording IBP voor medewerkers" of ga naar onderstaande presentatie "IBP voor medewerkers".

Presentatie - IBP voor medewerkers
kn.nu/ww.a988463 (pptx, maken.wikiwijs.nl)

Inhoudelijk komen de beide mogelijkheden overeen en wordt er ingegaan op hoe we met persoonsgegevens moeten omgegaan. Maar wat zijn nu precies persoonsgegevens? En wat betekent de wetgeving in de praktijk voor mij als medewerker in het primair of het voortgezet onderwijs?

Onderstaande workshop geeft de mogelijkheid om kort en krachtig aan medewerkers op een deels interactieve manier het belang van IBP te laten zien en aan te geven wat er gedaan kan en moet worden om de privacy van leerlingen en collega's te beschermen.

Aan het einde van de workshop kan iedere medewerker de onderstaande vragen beantwoorden:

- **Waarom** is IBP belangrijk?
- **Wat** zijn persoonsgegevens?
- **Waar** kan verantwoord met persoonsgegevens worden gewerkt?
- **Wanneer** mogen persoonsgegevens worden uitgewisseld?
- **Wie** is binnen de organisatie verantwoordelijk voor IBP?

Zie voor aanvullende informatie over informatiebeveiliging en privacy ook:

- de publicatie **ict-bekwaamheid van de leraar**
- de **do's en dont's van privacy**.

Dialoog met leerlingen

Ook leerlingen maken steeds meer gebruik van digitale middelen om te leren en te communiceren. Als je bedenkt dat 95% van de leerlingen in groep 8 een smartphone heeft en een groot deel actief is op sociale media, is het helemaal niet gek om in de klas het gesprek aan te gaan over hoe zij hun privacy kunnen bewaken en hoe zij met de privacy van mede-leerlingen omgaan. Want mag je je wachtwoord met iemand delen? Maar ook: He gaan we met elkaar om op sociale media?

Naast slachtoffer op internet kunnen jongeren ook dader zijn door bijvoorbeeld de schoolwebsite te hacken of het systeem plat te leggen met een DDos-aanval. Wanneer er anti-pestregels zijn, een anti-pestcontract of een gedragscode ict- en internetgebruik, wordt dit meestal klassikaal besproken. Maar

hoe praat je nu eigenlijk in de klas over informatiebeveiliging en privacy?

Hoe ga je het gesprek aan met leerlingen over IBP?

We hebben 25 hulpvragen opgenomen om met leerlingen van 10 tot 18 jaar het gesprek aan te gaan over deze twee moeilijke onderwerpen.

25 hulpvragen informatiebeveiliging
kn.nu/ww.4a1150f (pdf, maken.wikiwijs.nl)

25 hulpvragen privacy
kn.nu/ww.649c455 (pdf, maken.wikiwijs.nl)

Digitale geletterdheid

21e-eeuwse vaardigheden worden gezien als competenties die leerlingen nodig hebben in een snel veranderende maatschappij waarin technologie een belangrijke rol speelt. Onderdeel van die vaardigheden is het onderwerp digitale geletterdheid dat bestaat uit de vier vaardigheden computational thinking, mediawijsheid, informatievaardigheid en ict-basisvaardigheid. Deze laatste vaardigheid gaat over het kennen van basisbegrippen en functies van computers en netwerken en het kunnen aansluiten en bedienen van hardware. Daarnaast gaat het over het kunnen omgaan met kantoortoepassingen, presentatiesoftware en het kunnen werken met internet, met mobiele apparaten en op de hoogte zijn van **beveiligings- en privacyaspecten.**

Meer informatie over digitale geletterdheid vind je hier: https://www.kennisnet.nl/publicaties/werken-aan-digitale-geletterdheid-van-visie-naar-praktijk/

Sociale media; maak iedereen mediawijs

We hebben gezien dat digitale geletterdheid ook inspeelt op beveiligings- en privacy aspecten. Mediawijsheid omvat hier de kennis, vaardigheden en mentaliteit die nodig zijn om bewust, kritisch en actief om te gaan met media. Deze zijn onderverdeeld in:

- **Begrip**: inzicht hebben in de medialisering van de samenleving, begrijpen hoe media gemaakt worden, zien hoe media de werkelijkheid kleuren
- **Gebruik**: apparaten, software en toepassingen gebruiken, je kunnen oriënteren binnen mediaomgevingen

- **Communicatie**: informatie vinden en verwerken, content creëren, participeren in sociale netwerken
- **Strategie**: reflecteren op het eigen mediagebruik, doelen realiseren met media.

Via onderstaande knoppen kun je nog meer informatie vinden over specifieke deelgebieden.

- **Mediawijsheid op de basisschool**
- **Sociale media in het speciaal onderwijs**
- **Onderzoek mediagebruik onder jongeren**
- **Workshop mediawijsheid**

Veilig online

Gebruik deze **filmpjes** van Alert Online om leerlingen te laten zien wat ze moeten doen om veilig online te zijn.

Ook de Autoriteit Persoonsgegevens heeft een aantal lessen gemaakt over privacy om in de klas te gebruiken, deze zijn beschikbaar via de volgende link: Lessenserie Autoriteit Persoonsgegevens

(D)Dos; Van kattenkwaad tot strafblad

Naast slachtoffer op internet kunnen jongeren ook dader zijn. Een (D)Dos-aanval op school, dat kan iedereen overkomen… Maar in de praktijk blijken de 'daders' vaak leerlingen te zijn, waarbij het uitvoeren van de (D)Dos-aanval als een grapje of middel om die digitale toets uit te stellen begint.

Het uitvoeren van een (D)Dos-aanval is strafbaar volgens de wet, met een maximale celstraf van zes jaar. Bewustwording van de gevolgen van het uitvoeren van een (D)Dos-aanval en het hebben van een strafblad is belangrijk voor leerlingen. Je krijgt bijvoorbeeld geen baan bij de politie als je een strafblad hebt en ook is een baan als ethisch hacker niet waarschijnlijk. Praat hierover met de leerlingen en maak ze bewust van de gevolgen die dit soort grapjes kunnen hebben. Zie voor meer informatie over (D)DoS de rubriek (D)DoS, wat moet ik weten.

Leerlingenraad

Voor een middelbare school zal een leerlingenraad een uitstekende gesprekspartner zijn om eens samen stil te staan bij privacy op school. Ga constructief het overleg in: leerlingen moeten ook leren dat hun gegevens het beschermen waard zijn. Als je als school het goede voorbeeld geeft, doet dat voorbeeld misschien wel goed volgen!

Dialoog met ouders

Scholen verzamelen en gebruiken steeds meer persoonsgegevens van en over leerlingen. Je bent wettelijk verplicht om te verantwoorden wat je met die gegevens doet. Ouders, en leerlingen (als zij 16 jaar en ouder zijn), hebben het recht om (ongevraagd) in begrijpelijke taal, uitgelegd te krijgen hoe privacy op jouw school is geregeld.

Zorg dat je als school vragen over privacy kan beantwoorden en hen uit kan leggen wat de school doet met de gegevens van hun kinderen. We beschrijven hier een aantal onderwerpen waar ouders regelmatig vragen over hebben.

Privacybijsluiter

Om uit te leggen welke afspraken je hebt gemaakt met uitgevers, distributeurs of leveranciers van software, kun je verwijzen naar de privacybijsluiter die bij de bewerkersovereenkomsten zit (we hebben dit behandeld in het hoofdstuk '**Realiseren - verwerkersovereenkomsten**'). In de privacybijsluiter vertelt de leverancier wat het product doet, welke gegevens hij gebruikt en wat het doel van dat gebruik is.

Wees transparant over privacy

Als ouders het vertrouwen hebben dat je IBP goed hebt geregeld, dan zullen ze veel sneller bereid zijn om gegevens te delen. Om je te helpen, zijn een aantal voorbeeldteksten gemaakt die je kunt gebruiken in je schoolgids of voor op je website:

Voorbeeldteksten communicatie privacy
kn.nu/ww.9ea4187 (docx, maken.wikiwijs.nl)

Filmen en fotograferen door ouders

De school maakt afspraken over het gebruik van foto's van leerlingen voor de website, schoolgids enz. Ouders moeten hiervoor specifiek toestemming geven en bezwaar kunnen maken als zij niet willen dat een foto van hun kind hiervoor gebruikt wordt. Zie voor meer informatie **'afspraken over foto's en video's'**

Maar wat doe je met ouders die op school foto's maken? Hoe ga je om als ouders foto's van de beveiligde site kopiëren en vervolgens delen? Het is aan de school hoe zij hiermee omgaan. Verbieden is lastig, maar afspraken maken kan een oplossing zijn. Lees onderstaand document om enkele voorbeeldafspraken te zien:

Afspraken gebruik beeldmateriaal door ouders
kn.nu/ww.9465ce3 (pdf, maken.wikiwijs.nl)

Wat is de rol van de (G)MR rondom privacy?

Het is verstandig om ook jaarlijks met de (G)MR te praten over hoe jouw school omgaat met leerlinggegevens. Openheid en transparantie over het gebruik van leerlinggegevens is het uitgangspunt in alle communicatie met ouders! De MR heeft ook instemmingsrecht als het gaat over onderwerpen waarbij privacy van leerlingen en medewerkers een rol speelt. Zo moet het privacyreglement worden

goedgekeurd door de (P)MR.

Mogen grootouders en pleegouders ook vragen om inzage?

Bij leerlingen onder de 16 jaar heeft de wettelijk vertegenwoordiger het gezag over het kind en beslist deze namens het kind over de privacy. Dat zullen in de meeste gevallen één of beide ouders zijn. Maar ook pleegouders, die officieel het gezag over het kind hebben, hebben recht op inzage van het dossier. Grootouders mogen het dossier van hun kleinkind niet inzien, dat ligt anders, zij zullen niet snel de wettelijk vertegenwoordiger zijn.

Maar... hoe ver ben ik nu?

Heb je alle stappen uitgevoerd? Prima, je bent goed bezig om informatiebeveiliging en privacy te regelen!

Door bewust en zorgvuldig om te gaan met leerlinggegevens is jouw school er klaar voor om deze gegevens nóg beter en efficiënter in te zetten. Informatiebeveiliging of privacy zijn geen bedreiging meer. Gepersonaliseerd leren met ict? Kom maar op!

Maar... Hoe ver ben jij eigenlijk?

Hoe ver ben je nu met jouw school? Ben je net aan de slag gegaan, al goed op weg of werk je aan 'samen vooruit'? En ben je nu klaar?

Informatiebeveiliging en privacy kun je niet in één keer regelen het is een *proces*. Het belangrijkste is dat je *begint* om IBP te regelen, zodat ook jouw school straks gereed is voor de AVG in mei 2018. Met deze Aanpak IBP heb je de belangrijkste risico's en maatregelen in beeld. Als je alle maatregelen uit de aanpak hebt ingevoerd ben je aardig 'in control'. Maar IBP is een *proces*, het is nooit 'af'. Door vooruit te kijken kun je rekening houden met risico's die er nu nog niet zijn, maar wel gaan komen. Daarmee ben je klaar voor de toekomst en kun je vol vertrouwen gebruik maken van (nieuwe) ict-toepassingen zonder bang te zijn voor datalekken of misbruik van persoonsgegevens.

Met onderstaande checklist kun je controleren hoe ver je daadwerkelijk bent met het regelen van IBP. Het geeft een snel overzicht van wat er gereed is en wat je op de planning hebt staan.

Checklist Aanpak IBP _docx
kn.nu/ww.eb90c9e (docx, maken.wikiwijs.nl)

Checklist Aanpak IBP _pdf
kn.nu/ww.2d331ae (pdf, maken.wikiwijs.nl)

IBP is nooit af...

Heb je alle stappen doorlopen en denk je dat je klaar bent? Mooi! Maar eigenlijk ben je niet klaar. Bij Kennisnet zeggen we wel eens dat het échte werk pas begint als je de Aanpak IBP doorlopen hebt! Alle genomen maatregelen en afspraken worden nu in de praktijk gebracht. Er kan gekeken worden hoe het in de dagelijkse praktijk gaat werken. En volgend jaar komt de risicoanalyse weer terug met misschien wel nieuwe risico's en uitdagingen die opgelost moeten worden. De PDCA-cyclus gaat zijn werk dus doen!

Het regelen van IBP is iets dat elke organisatie in Europa moet doen. Ervoor zorgen dat je **'aantoonbaar compliant'** bent met wet- en regelgeving doe je voor jezelf! Elke organisatie heeft zo haar eigen risico's in beeld en weet wat haar te doen staat om IBP goed te regelen. Je bent dus niet de enige school, ook scholen in Duitsland, Polen, Spanje, Portugal, enzovoorts moeten IBP regelen.

De Aanpak IBP is gebaseerd op de wetteksten van AVG en Wbp, daarnaast bevat het een groot aantal onderdelen vanuit de informatiebeveiliging, dus vanuit de ISO27001/2-normen. Verder zijn de maatregelen gebaseerd op het framework IBP voor het mbo, dat weer is gebaseerd op het normenkader informatiebeveiliging zoals dat in het hoger onderwijs wordt toegepast.

En nee, na het doorlopen van de Aanpak IBP is er geen certificaat om aan de muur te hangen. Wel heb je een overzicht voor jezelf, je bestuurder en de toezichthouders van wat er allemaal geregeld is, wat er nog op de planning staat en dat je jaarlijks evalueert en werkt aan bewustwording bij medewerkers, leerlingen en ouders.

En het is ook niet niks wat je gedaan hebt ... Onderwijs met inzet van ict kan op jouw school altijd doorgaan en je hebt de privacy van leerlingen, hun ouders en medewerkers geregeld!

Veelgestelde vragen

De 10 veelgestelde vragen over iBP in het po/vo', die door scholen worden gesteld aan de helpdesk IBP bij Kennisnet zijn:

1. Wanneer moet IBP bij mij geregeld zijn?
2. Kunnen jullie ons bestuur begeleiden om IBP in te zetten op onze scholen?
3. Moet ik met alle leveranciers een bewerkersovereenkomst afsluiten? En hoe zit het met netwerkbeheerder?
4. In welke gevallen mag je als school communiceren met bijzondere persoonsgegevens, zoals het BSN van leerlingen?
5. Wat is de wettelijke bewaartermijn voor leerlinggegevens?

6. Foto’s van leerlingen, waar moet ik rekening mee houden? En mag ik ouders verbieden foto’s te maken in de school?
7. Mogen we camera's ophangen op school om pesten te voorkomen?
8. Mogen er via de e-mail persoonlijke bestanden met privacygevoelige gegevens worden verstuurd?
9. Ik denk dat er bij mijn school sprake is van een datalek; wat moet ik doen?
10. Is het verplicht voor het primair onderwijs (bestuur met meer dan 250 werknemers) een functionaris voor gegevensbescherming (FG) aan te stellen?

Voor andere vragen neem contact op met de IBP-helpdesk via ibp@kennisnet.nl of 0800-3212233

De antwoorden op deze vragen zijn te lezen in het volgende document. Via een rechtermuisklik op het document kun je het als geheel opslaan.

Tien veelgestelde vragen
kn.nu/ww.fce52b8 (pdf, maken.wikiwijs.nl)

Maand van de IBP (oktober)

Presentaties Werkconferentie IBP po/vo 2017

Op woensdag 11 oktober 2017 organiseerde Kennisnet, samen met de PO-Raad en de VO-raad, weer een werkconferentie informatiebeveiliging & privacy voor het primair en voortgezet onderwijs.

Deze bijeenkomst was voor bestuurders, schoolleiders, ict-coördinatoren en iedereen die met IBP bezig is in het primair en voortgezet onderwijs. We kunnen terugkijken op een geslaagde dag met diverse sprekers en workshops.

De presentaties van deze dag zijn hieronder terug te vinden.

Ontbijtsessie voor dummies

Ochtendpresentaties

AVG, wat verandert er?

Van DDoS-aanval naar hackende leerling

Risico's en AVG

Verslag congres

Over het congres is een artikel gepubliceerd (https://www.kennisnet.nl/artikel/verslag-ibp-congres-2017/). Het verslag is hier te downloaden:

Verslag IBP congres po-vo 11 oktober 2017 te Soesterberg
kn.nu/ww.279163f (pdf, maken.wikiwijs.nl)

Maand van de IBP 2017

In oktober 2017 organiseerden de PO-Raad, VO-raad en Kennisnet weer een Maand van de IBP. Het doel was de onderwijssector van alle kanten te laten weten dat er actie nodig is om IBP voor elkaar te krijgen. In die maand stondt bewustwording centraal:

- Wees je ervan bewust dat je IBP op school moet regelen
- Weet dat 25 mei 2018 de nieuwe AVG ingaat die strenger omgaat met privacy, en wat dit voor jou betekent
- Gebruik de maand om IBP op jouw school onder de aandacht te brengen bij collega's én leerlingen!

Naast de landelijke werkconferentie organiseerden we twee masterclasses, een webinar en een bijeenkomst voor leveranciers over IBP in het po en vo.

Kijk hier voor meer informatie: https://www.kennisnet.nl/bijeenkomsten/

Verder lanceerden we eind september 2017 een toolkit met hulpmiddelen waarmee je zelf op je eigen school aan de slag kunt gaan met bewustwording.

Het hele jaar door staan er acties gepland en worden er nieuwe hulpmiddelen gelanceerd om scholen te helpen IBP te regelen.

Presentaties bijeenkomsten en webinar

Tijdens de Maand van de IBP zijn er ook masterclasses po/vo georganiseerd, en een bijeenkomst voor leveranciers. De presentaties daarvan zijn hier te vinden:

Presentatie IBP voor leveranciers van 9 oktober 2017 te Zoetermeer
kn.nu/ww.19fdd74 (pptx, maken.wikiwijs.nl)

Presentatie masterclass IBP po-vo 19 oktober 2017 in Zoetermeer
kn.nu/ww.2b4886f (pptx, maken.wikiwijs.nl)

Presentatie masterclass IBP po-vo 26 oktober 2017 in Utrecht
kn.nu/ww.cc28036 (pptx, maken.wikiwijs.nl)

De webinar IBP van 27 oktober

Werkconferentie IBP po/vo 2016

Schoolbesturen zijn verantwoordelijk voor het regelen van goede informatiebeveiliging en voor het waarborgen van de privacy van leerlingen. Door de digitalisering van het onderwijs kan dat een lastige opgave zijn. De werkconferentie helpt po- en vo-schoolbesturen bij het nemen van deze verantwoordelijkheden. De bijeenkomst was bedoeld voor bestuurders, ict-coördinatoren en beslissers in het onderwijs.

Na deze dag weet je wat informatiebeveiliging en privacy inhouden, waar en hoe de regie gevoerd moet worden door de school, waar je verantwoordelijk voor bent, hoe je afspraken kunt maken met leveranciers, en hoe je ouders en leerlingen informeert over privacy-afspraken. Met deze kennis kun je direct aan de slag om privacy en informatiebeveiliging op je school te verbeteren, zodat je school voldoet aan de eisen van de AVG op 25 mei 2018.

Wil je het verslag van de werkconferentie IBP po/vo van 2016 nalezen, klik dan hieronder

Verslag van de werkconferentie IBP 7 oktober 2016
kn.nu/ww.8efb9f4 (pdf, maken.wikiwijs.nl)

NIEUW in de Aanpak IBP

Voor gebruikers en bezoekers die de Aanpak IBP vaker bezoeken, wordt op deze pagina bijgehouden wat de meest recente grote wijzigingen en nieuwe documenten en handleidingen zijn. Vanaf september 2017 wordt de **Aanpak IBP deels herschreven**. Dit wordt gedaan, om meer actuele informatie aan scholen te kunnen geven rondom IBP en vooral de nadruk te gaan leggen op de praktische invulling hiervan vanuit de eisen van de AVG.

De volgende onderwerpen staan nog op de planning om op te nemen in de Aanpak IBP:

- De **Gegevensbeschermingseffectbeoordeling** (engelse afkorting DPIA) Ook scholen zijn straks verplicht in bepaalde gevallen een gegevensbeschermingseffectbeoordeling te doen. Wanneer geldt die plicht? En hoe kun je dat als school regelen? (verwacht: begin mei 2018).
- Overzicht **bewaartermijnen** (verwacht: eind april 2018, afhankelijk van afstemming met OCW).

De vermelde datum is een indicatie, als daar wijzigingen in komen worden die hier ook weergegeven.

- 20 april een overzicht documenten uit de Aanpak is toegevoegd.
- 20 april Lessenserie AP toegevoegd bij communiceren leerlingen
- 7 april in de handleiding dataregisters is de inleiding aangepast en de opmerking over 250 medewerkers verwijderd zie uitleg Autoriteit Persoonsgegevens.
- 2 april privacyverklaring is toegevoegd bij informatieplicht rondom het verwerken van persoonsgegevens van leerlingen.
- 2 april kopje verantwoordingsplicht is gewijzigd in verantwoordings- en informatieplicht in verband met toevoegen van het format voor een privacyverklaring.
- 30 maart Checklist Aanpak IBP is bijgewerkt.
- 30 maart gedragscode verantwoord gebruik bedrijfsmiddelen is toegevoegd en heeft de plaats ingenomen van gedragscode ict en internetgebruik.

- 19 maart de Dataregisters voor leerlingen, medewerkers in loondienst en relaties zijn gepubliceerd.
- 12 maart uitleg Documentatieplicht toegevoegd.
- 6 maart voorbeeld privacyreglement (conform AVG) toegevoegd.
- 11 februari aangepaste versie IBP beleid is als versie 2.0 geplaatst samen met een apart document met toelichting.

Posters en presentaties

IPON 2018
kn.nu/ww.564b7a9 (pdf, maken.wikiwijs.nl)

Posters voor bewustzijn
kn.nu/ww.bfcfbb7 (kennisnet.nl)

Over dit lesmateriaal

Colofon

De productie van deze Aanpak IBP is een samenwerking tussen Kennisnet (opdrachtgever) en Flooow (e-learning productie). Auteurs Aanpak IBP: Leo Bakker, Erik van den Berg, IJsbrand Buys Ballot, Kiki de Bondt, Ludo Cuijpers, Elly Dingemanse, Axel Eissens, Peter van Essen, Dirk Linden, Bastiaan Vader, Job Vos Met dank aan: Anne Goris (VO-raad), Maurits Huigsloot (PO-Raad)   <u>Contactgegevens:</u> Kennisnet Elly Dingemanse <u>ibp@kennisnet.nl</u>   Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteurs, PO-Raad, VO-raad en Kennisnet geen aansprakelijkheid voor eventuele fouten, onvolkomenheden of schade als gevolg van het gebruik van deze Aanpak IBP. Raadpleeg bij twijfel of geschillen een deskundige zoals een it-consultant, ict-adviseur, jurist of advocaat.

Auteur	Aanpak IBP
Laatst gewijzigd	23 april 2018 om 13:50
Licentie	Dit lesmateriaal is gepubliceerd onder de Creative Commons Naamsvermelding 3.0 Nederlands licentie. Dit houdt in dat je onder de voorwaarde van naamsvermelding 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 3.0 Nederland licentie

Aanvullende informatie over dit lesmateriaal

Van dit lesmateriaal is de volgende aanvullende informatie beschikbaar:

Eindgebruiker	leraar
Moeilijkheidsgraad	gemiddeld
Trefwoorden	avg, ibp, informatiebeveiliging, informatiebeveiliging en privacy, iso 27001, iso 27002, privacy, security, wbp

Bronnen

Bron	Type
Posters voor bewustzijn https://www.kennisnet.nl/artikel/leer-bewuster-omgaan-met-privacy-in-de-maand-van-de-ibp/	Link