www.pwc.nl

Ministerie van Onderwijs, Cultuur en Wetenschap

Nulmeting Privacy & Beveiliging Primair en Voortgezet Onderwijs

7 april 2014

2014-0420a/ADB/ek/jv/ae/ms

Status
Deze rapportage heeft de status definitief.

pwc

Ministerie van Onderwijs, Cultuur en Wetenschap
T.a.v. de heer P. Kantebeen
Directie Kennis – Cluster Strategisch Informatiebeleid
Postbus 16375
2500 BJ DEN HAAG

Geachte heer Kantebeen,

Graag presenteren wij u onze definitieve rapportage over de nulmeting op informatiebeveiliging en privacy. Doel van onze inzet was het uitvoeren van een nulmeting die een globaal beeld geeft van de huidige situatie ten aanzien van de bescherming van persoonsgegevens bij DUO en in het veld (primair en voortgezet onderwijs).

Wij hebben de nulmeting uitgevoerd en deze rapportage opgesteld in overeenstemming met onze offerte met kenmerk 2013-1418/ADB/ek/ms van 22 oktober 2013.

Deze rapportage is bestemd voor het Ministerie van OCW. De rapportage is opgesteld ten behoeve van intern gebruik binnen de eigen organisatie van het Ministerie, de koepelorganisaties PO-raad en VO-raad, Kennisnet en de geïnterviewde instellingen. Op de bevindingen in dit rapport mag door derde partijen niet worden gesteund. Bijgevolg accepteren wij geen aansprakelijkheid jegens derde partijen.

Indien u nog vragen heeft, neemt u dan gerust contact op.

Hoogachtend,

PricewaterhouseCoopers Advisory N.V.

w.g.

Adri de Bruijn RE RA
Partner Technology
088 – 792 6587

Inhoudsopgave

Managementsamenvatting (1/5)

Achtergrond en aanleiding
Door de komst van nieuwe communicatietechnologieën heeft de mens de mogelijkheden om steeds meer digitaal te kunnen werken. Ook het onderwijs gaat in deze ontwikkelingen mee: digitale leermiddelen, 'cloud', 'social media' en 'software as a service' zijn toepassingen die ook in het onderwijs steeds meer worden gebruikt. Het Ministerie van Onderwijs, Cultuur en Wetenschap wil, mede naar aanleiding van deze ontwikkelingen, een globaal beeld krijgen van hoe de huidige situatie van informatiebeveiliging van privacygevoelige gegevens is bij DUO en in het veld. Dit onderzoek draagt daaraan bij.

Doelstelling en reikwijdte
De doelstelling van het onderliggende onderzoek is om een nulmeting uit te voeren op het gebruik en de beveiliging van privacygevoelige gegevens binnen de sectoren primair onderwijs en voortgezet onderwijs. Dit onderzoek heeft als doel te komen tot een globaal beeld van:

- Het gebruik (welke gegevens worden verzameld en gebruikt door een onderwijsinstelling, wat is de grondslag en aan welke andere partijen worden deze gegevens verstrekt (bewerkers en ketenpartners)).
- De beveiliging van de gegevens door verantwoordelijken en bewerkers (waar zijn verantwoordelijkheden voor het nemen van maatregelen belegd, welke maatregelen zijn getroffen en welke restrisico's zijn te onderscheiden).

Dit onderzoek is uitgevoerd voor een drietal ketens, te weten:

Aanmelden en inschrijven: (uitgebreid met "genieten onderwijs" en "overdracht vervolg keten"): delen van informatie tussen instellingen onderling en DUO.

Social Media en tooling: het delen van informatie tussen leerling, docent en clouddienstaanbieders door middel van de ad-hoc inzet van digitale middelen zoals social media, learning analytics of digitaal leermateriaal.

Digitale leermiddelen: het delen van (examen) resultaten met behulp van digitale middelen en de verwerking daarvan door uitgevers, softwareleveranciers, distributeurs, administratie, scholen en leerlingen.

Aanpak
Ons onderzoek heeft een inventariserend karakter en beperkt zich tot de getroffen maatregelen gerelateerd aan de uitwisseling van gegevens binnen de keten. Wij hebben geen inhoudelijke beoordeling van de kwaliteit van de getroffen maatregelen bij de instellingen of andere ketenpartners uitgevoerd.

Het onderliggende onderzoek is gebaseerd op een deelwaarneming van zeer beperkte omvang bij een viertal onderwijsinstellingen die actief zijn binnen het primair en voortgezet (speciaal) onderwijs. De waarnemingen gelden daarom voor deze instellingen, en geven hoogstens een indicatie van de stand van zaken voor de sectoren als geheel.

Leeswijzer
Deze rapportage begint met een managementsamenvatting (p. 4), gevolgd door een beschrijving van de doelstellingen, reikwijdte en objecten van onderzoek (p. 9). De hoofdbevindingen, conclusies en aanbevelingen zijn elk beschreven voor het aanmeld- en inschrijfproces (p. 12), digitale leermiddelen (p. 24) en social media (p. 31). Hierop volgt een overzicht van de inherente risico's (p. 33) en een totaaloverzicht van aanbevelingen voor elke partij (p. 35). De bijlagen bevatten inventarisaties van het gebruik van gegevens (p. 37) en waarnemingen per instelling (p. 43). Tot slot het referentiekader voor maatregelen (p. 54).

Managementsamenvatting (2/5)

Kernboodschap

De essentie van onze management samenvatting kan als volgt worden samengevat:

- De scholen in het onderzoek passen de Wet Bescherming Persoonsgegevens toe op basis van “gezond verstand”. Dit omvat in de eerste plaats de aard en hoeveelheid gegevens die worden vastgelegd. De *precieze* eisen die de Wet Bescherming Persoonsgegevens stelt t.a.v. de verwerking zijn bij geen van de door ons geïnterviewde instellingen bekend. We hebben enkele malen kunnen waarnemen dat deze scholen gegevens vastleggen die niet strikt noodzakelijk zijn en mogelijk zelfs strijdig met de Wbp zijn, overigens met de beste bedoelingen voor het welzijn van de leerling.
- De scholen in het onderzoek passen ook beveiligingsmaatregelen toe binnen hun invloedssfeer op basis van “gezond verstand”. Deze maatregelen worden getroffen op basis van ervaring en incidenten. Het is onduidelijk in hoeverre de leveranciers (bijvoorbeeld de ICT-leveranciers die de infrastructuur beheren) voldoende maatregelen hebben getroffen, en of deze effectief functioneren. De scholen in het onderzoek hebben hier beperkt inzicht in en de leveranciers verantwoorden zich niet proactief.
- De markt voor Leerlingvolgsystemen en Digitale Leermiddelen is in handen van een klein aantal leveranciers. De scholen hebben niet voldoende gewicht om tegenwicht aan leveranciers te bieden en eisen te stellen t.a.v. privacy en beveiliging. Zij accepteren de door de leveranciers gestelde voorwaarden.
- De leveranciers van Leerlingvolgsystemen en Digitale Leermiddelen verwerken gegevens over bijvoorbeeld leerlingen en docenten. Het is onduidelijk hoe deze gegevens gebruikt worden, met welke partijen deze gegevens worden gedeeld en hoe deze gegevens adequaat worden beschermd. De beschikbare documentatie zoals privacy statements laten hiertoe ruimte. Er kan worden gesteld dat er een commercieel belang is om breder gebruik te maken van data.

De risico’s die uit deze bevindingen voortvloeien moeten ook worden beschouwd in het licht van de volgende ontwikkelingen. Deze ontwikkelingen zullen naar onze verwachting de risico’s voor de toekomst vergroten:

- Het gebruik van ICT-middelen door onderwijsinstellingen zal in de toekomst toenemen, en daarmee ook de data die verzameld (kunnen) worden over betrokkenen (leerlingen, docenten en ouders). De scholen moeten met het oog op toekomstige ontwikkelingen (bijvoorbeeld Passend Onderwijs) meer en meer gevoelige gegevens vastleggen.
- De technische mogelijkheden om grote hoeveelheden data te combineren en te analyseren, en hieruit zinvolle informatie over individuele personen te destilleren nemen toe. De gesprekken geven aan dat deze ontwikkeling bij scholen en bij de overheid nog in de kinderschoenen staat, het gebruik door leveranciers is niet bekend. Het is onze verwachting dat deze ontwikkeling zich zeker en in snel tempo zal doorzetten, zowel bij onderwijsinstellingen als bij leveranciers.

Het is gezien deze bevindingen en ontwikkelingen van belang dat er in deze fase geacteerd wordt, op een wijze die effectief is voor de sectoren primair en voortgezet onderwijs. Het belang wordt door de onderzochte instellingen erkend. Het ontbreekt bij hen aan tijd en capaciteit om zich in de materie te verdiepen en additionele capaciteiten zoals regievoering op leveranciers in te richten. Wij zien hier een rol voor koepelorganisaties en belangenorganisaties zoals Kennisnet om een voortrekkersrol in te nemen. Daarnaast is het van belang om de sector PO en VO bewust te maken van privacy en beveiliging, en hen de praktische handreikingen te geven om hun rol als Verantwoordelijke zoals die is omschreven in de Wbp te kunnen nemen. Daarnaast zijn er activiteiten (zoals toezicht op leveranciers) die het best sectorbreed kunnen worden aangepakt.

Wij gaan in het resterende deel van de managementsamenvatting dieper op onze bevindingen en aanbevelingen in. Deze rapportage is gebaseerd op een deelwaarneming bij een beperkt aantal instellingen. Wij adviseren om vast te stellen of de sfeerschildering, en de bevindingen en aanbevelingen in deze rapportage breed door de ketenpartijen herkend en gedragen worden, en om in overleg met de ketenpartijen de passende vervolgacties te initiëren.

Managementsamenvatting (3/5)

Digitalisering en innovatie leidt in toenemende mate tot vraagstukken op het gebied van privacy en verantwoordelijkheid
De onderwijsinstellingen in het onderzoek leggen in het kader van Aanmelden en inschrijven verschillende gegevens vast, waarmee een (zeer) gedetailleerd beeld wordt vastgelegd van de sociale, emotionele en cognitieve vaardigheden van leerlingen en hun ontwikkeling daarin en de sociale context van de leerlingen. Het is voor niet al deze gegevens altijd duidelijk wat de noodzaak of toegevoegde waarde is van de vastlegging, bijvoorbeeld de geloofsovertuiging van de leerlingen.

De gegevens die in het kader van speciaal onderwijs en onderwijs in een gesloten instelling worden vastgelegd voegen een extra klasse toe aan privacygevoeligheid. Deze gegevens betreffen veelal medische gegevens en details over een eventueel strafblad van de leerling.

De reguliere gegevens voor bekostiging worden gestructureerd verzameld door de instelling op basis van aanmeldformulieren, de medische gegevens en strafbladgegevens variëren in informatiewaarde, waarbij afgevraagd mag worden of niet te veel gegevens worden aangeleverd en vastgelegd. De uitwisseling van gegevens vindt in gevarieerde vorm plaats, van fysieke dossiers tot digitale dossiers per e-mail. De gegevens worden in verschillende vormen verstrekt aan legitieme externe partijen voor legitieme doeleinden.

DUO is één van deze partijen. DUO geeft aan dat uitsluitend gegevens verzameld worden waar een wettelijke grondslag voor is. De verstrekkingen die aan derde partijen worden gedaan zijn in wetgeving met name benoemd. DUO geeft aan dat er in het veld in toenemende mate behoefte is aan data die in bulk beschikbaar wordt gesteld. Deze verzoeken komen nu vooral vanuit de koepelorganisaties zoals de PO-Raad en de VO-raad. DUO bekijkt per verzoek of deze verstrekkingen gedaan mogen worden. Dergelijk gebruik van grote datasets is op dit moment nog beperkt en “staat nog in de kinderschoenen”. De huidige verstrekkingen zijn beperkt tot enkele informatieproducten die door het Ministerie van OCW worden opgevraagd / gemaakt voor de evaluatie en bepaling van beleid. DUO verwacht overigens wel dat het gebruik van gegevens (o.m. in het kader van ‘learning analytics’) binnen onderwijsinstellingen maar wellicht ook op basis van gegevens van DUO de komende jaren een flinke sprong zal gaan maken. Dit zal naar verwachting in toenemende mate tot vraagstukken voor het borgen van privacy leiden.

Social Media worden gebruikt naar het inzicht van de individuele docent, maar dit gebruik is thans nog beperkt. Enkele van de door ons geïnterviewde scholen hebben informeel afspraken gemaakt over het gebruik, maar laten veel ook over aan het inzicht van de medewerker.

Een veelvoorkomend incident bij de geïnterviewde scholen rondom leerlingen betreft **digitaal pesten**. Dit vindt soms binnen, maar vaak buiten de schoolomgeving plaats. In het laatste geval echter ook soms in het ‘gezichtsbereik’ van de betrokken docenten. Het vraagstuk is in hoeverre scholen mogen, moeten en kunnen ingrijpen. Binnen de schoolomgeving mogen leerlingen tijdens de les mobiele telefoons niet gebruiken en moeten deze aan het begin van de les inleveren. De geïnterviewde instellingen geven aan nu niet te controleren op het gebruik door leerlingen en niet in te grijpen op digitaal pesten, omdat men dit niet als hun verantwoordelijkheid beschouwt en er geen middelen beschikbaar zijn om dit effectief aan te pakken.

Digitale leermiddelen worden door de scholen in het onderzoek breed ingezet om de vaardigheden en kennis van leerlingen te oefenen en te toetsen. De applicaties bouwen een historie op van de leerontwikkeling van de leerling. De leveranciers van digitale leermiddelen hebben enige informatie over privacy en beveiliging op hun website staan (zie onze bevindingen), maar dit zijn voor de onderwijsinstellingen geen criteria voor de selectie van een leverancier.

Managementsamenvatting (4/5)

Wij benoemen in het vervolg van deze management samenvatting onze bevindingen en aanbevelingen.

De betrokkenheid van de scholen bij het welzijn van de leerling is hoog

De medewerkers op verschillende niveaus binnen de onderzochte instellingen handelen vanuit het welzijn en belang van de individuele leerling, en proberen binnen de beperkingen van tijd en geld de maximale zorg en aandacht te leveren. Dit komt zonder uitzondering tot uitdrukking in de gesprekken en workshops die we gevoerd hebben. Dit komt ook tot uitdrukking in de behandeling van gegevens van de leerling. Enerzijds worden veel gegevens vastgelegd vanuit de beleving dat hoe meer men van een leerling weet en tussen leerkrachten kan overdragen, des te beter een leerling begeleid kan worden. Tegelijkertijd is er het besef dat de gegevens van de leerling voldoende beveiligd moeten zijn.

De instellingen in het onderzoek zijn niet precies bekend met alle relevante wettelijke kaders voor het gebruik van gegevens of de gevolgen van de toepassing van deze wettelijke kaders voor de te nemen maatregelen

De workshops geven aan dat de medewerkers niet bekend zijn met (wettelijke) kaders voor het verzamelen, bewerken, bewaren en vernietigen van gegevens en archiefstukken specifiek voor gegevens die in het primair onderwijs en voortgezet onderwijs worden verzameld. Het bestaan van de Wbp is bekend bij de medewerkers, maar niet welke rol zij precies hebben in de context van de Wbp (verantwoordelijke of (sub)bewerker) of wat dit in de dagelijkse praktijk precies betekent voor de te nemen maatregelen. De instellingen in het onderzoek vullen gebruik van gegevens en beveiliging vooral praktisch in, waarbij men zelf een afweging maakt bezien vanuit de wettelijke verplichtingen die men beter kent en vanuit het belang van de leerling.

De onderwijsinstellingen in dit onderzoek leggen in de praktijk mogelijk te veel gegevens vast. Voorbeelden zijn in ieder geval de structurele vastlegging van geloofsovertuiging in het leerlingvolgsysteem, kopieën van identiteitsbewijzen van de leerling, pasfoto's van leerlingen en de BSN-nummers van de ouders. Sommige gegevens mogen uitsluitend na expliciete toestemming vastgelegd worden, maar het vragen van expliciete stemming wordt niet gedaan in de aanmeldformulieren die ouders in moeten vullen. Andere gegevens (bijvoorbeeld kopieën van identiteitsbewijzen) mogen in het geheel niet vastgelegd worden.

De instellingen kunnen conform de Wbp als "verantwoordelijke" voor de verwerking van persoonsgegevens van leerlingen worden benoemd. De instellingen maken zonder uitzondering gebruik van de dienstverlening van externe ICT-leveranciers. Het initiatief voor het nemen van maatregelen lijkt vanuit de instellingen te liggen bij de leverancier. Deze instellingen hebben inzicht in de genomen maatregelen voor zover deze zichtbaar zijn voor hen (het verplicht inloggen met gebruikersnaam en wachtwoord, schoning van gegevens). De instellingen in het onderzoek erkenden in de meeste gevallen dat er geen precies inzicht bestaat in de genomen maatregelen, omdat dit geen structureel onderwerp van discussie is in de relatie tussen instelling en leverancier, en de externe leveranciers zich niet proactief verantwoorden over de kwaliteit van de genomen maatregelen.

Wij adviseren in overleg met overheid, instellingen en andere belangenorganisaties een plan op te stellen voor het bevorderen van 'awareness' van het onderwerp informatiebeveiliging en privacy binnen de sector. Wij adviseren de ketenpartijen om naar elkaar duidelijk te maken waar je binnen de keten verantwoordelijk voor bent (bijvoorbeeld verantwoordelijke of bewerker in de zin van de Wbp) en wat dit betekent voor taken, verantwoordelijkheden en bevoegdheden voor ketenactiviteiten. Maak duidelijk welke risico's jij als ketenpartij ziet en neem (in samenspraak en samenhang met de ketenpartijen) effectieve maatregelen.

Wij adviseren tevens handreikingen op te stellen voor de praktische implementatie van de Wbp door PO en VO: welke gegevens mogen wel en niet opgeslagen worden, hoe lang mogen en moeten deze gegevens bewaard worden, en wat zijn best practices voor het praktisch nemen van maatregelen door de instelling. Wij adviseren tevens bij nieuwe wet- en regelgeving zoals Passend Onderwijs aandacht te besteden aan de implicaties op het gebied van privacy (Privacy Impact Assessment), zoals de vast te leggen gegevens en de benodigde maatregelen bij de instellingen. Wij adviseren tot slot het gebruik van sectorbrede standaarden waarin dataminimalisatie al is toegepast te bevorderen.

Managementsamenvatting (5/5)

De afhankelijkheid van leveranciers is groot, en er is twijfel of de leveranciers op een verantwoorde wijze omgaan met leerlinggegevens

De onderwijsinstellingen in het onderzoek hebben in alle gevallen een leerlingvolgsysteem en maken in meer of mindere mate gebruik van digitale leermiddelen. Deze systemen worden vaak als een cloudoplossing door externe partijen gehost. De leveranciers van de digitale leermiddelen hebben de beschikking over de gegevens die over het leerlingen worden verzameld.

De markt in Nederland kent slechts enkele aanbieders van leerlingvolgsstemen, ICT leveranciers voor het onderwijs en aanbieders van digitale leermiddelen. Hierdoor hebben scholen geen sterke onderhandelingspositie ten opzichte van de leveranciers, en kunnen niet veel eisen. De instellingen zijn zelf meestal klein van omvang. De instellingen erkenden in de meeste gevallen dat er geen precies inzicht bestaat in de genomen maatregelen door de leverancier.

Wij hebben als deelwaarneming de privacy statements van enkele van deze dienstverleners kritisch bekeken. Deze privacy statements laten de indruk achter dat niet beseft wordt hoe de Wbp toegepast dient te worden, en welke gevolgen de wet heeft voor de te nemen maatregelen. Voorbeelden zijn:

- Er worden gegevens vastgelegd van verschillende betrokkenen, in deze context de leerkrachten, beheerders van schoolapplicaties en leerlingen. De leverancier vraagt, en de school geeft namens alle betrokkenen toestemming voor de verwerking van persoonsgegevens door de leverancier. Deze constructie is volgens de Wbp echter niet mogelijk, omdat de individuele betrokkenen toestemming moeten geven.
- Eén online portalleverancier van digitale leermiddelen betreft een stichting die toegang geeft tot de applicaties van de aangesloten uitgeverijen en andere leveranciers. De melding bij het College Bescherming Persoonsgegevens meldt dat de gegevens door de portalleverancier worden geleverd aan de uitgeverijen, waarbij documentatie tevens vermeldt dat nieuwe partijen nog kunnen aansluiten. Het is onduidelijk welke gegevens verzameld en verstrekt worden, door wie en voor welke doeleinden.
- De doelstelling van de zojuistgenoemde stichting is het verschaffen van online toegang tot leermiddelen (authenticeren van gebruikers). De gegevens die hiertoe worden vastgelegd (geslacht, geboortedata) van docenten, leerlingen en ICT-coördinatoren lijken uitgebreider dan voor deze doelstelling nodig is.

Wij adviseren de onderwijsinstellingen om de leveranciers te laten onderbouwen op welke wijze hun systemen en/of dienstverlening voldoen aan die eisen de vanuit de Wbp worden gesteld. Laat de leveranciers zich periodiek verantwoorden over de maatregelen die zij hebben getroffen om de adequate beveiliging van de gegevens te waarborgen. De meest praktische aanpak (om te voorkomen dat elke onderwijsinstelling z'n eigen onderzoek doet) is om de vraagstelling en beoordeling voor één leverancier over alle sectoren heen door één organisatie te laten coördineren. Neem privacy en beveiliging als onderwerp op in de leidraad Programma van Eisen voor de selectie van leveranciers.

De instellingen ervaren geen ondersteuning door externe organisaties op het gebied informatiebeveiliging en privacy

De in het onderzoek betrokken instellingen geven aan dat zij niet proactief handreikingen krijgen van koepel- of belangenorganisaties. De behoefte hiertoe is wel aanwezig, met name waar het de praktische invulling van wet- en regelgeving betreft. Er zijn echter handreikingen voor verschillende onderwerpen beschikbaar. Er is blijkbaar een leemte tussen wat aan documentatie beschikbaar is en wat de onderwijsinstellingen percipiëren dat beschikbaar is.

Wij adviseren tevens handreikingen op te stellen voor de praktische implementatie van de Wbp door PO en VO (zie eerder in deze management samenvatting). Creëer een cultuur van leren en verbeteren in de keten. Ruim een belangrijke plaats in voor transparantie in de eigen maatregelen, knelpunten en vraagstukken. Faciliteer deze cultuur door een platform te creëren waar onderwijsinstellingen in het PO en VO hun privacy- en beveiligingsvraagstukken kunnen voorleggen aan collega-instellingen en ketenpartijen, en waar zij best practices op het gebied van informatiebeveiliging kunnen delen.

Doelstelling, reikwijdte en objecten van onderzoek

Achtergrond, aanleiding en doelstelling

Achtergrond en aanleiding

Door de komst van nieuwe communicatietechnologieën hebben wij de mogelijkheden om steeds meer digitaal te kunnen werken. Ook het onderwijs gaat in deze ontwikkelingen mee: digitale leermiddelen, 'cloud', 'social media' en 'software as a service' zijn toepassingen die ook in het onderwijs steeds meer worden gebruikt. Het Ministerie van Onderwijs, Cultuur en Wetenschap wil, mede naar aanleiding van deze ontwikkelingen, een globaal beeld krijgen van hoe de huidige situatie van informatiebeveiliging van privacygevoelige gegevens is bij DUO en in het veld. Dit onderzoek draagt daaraan bij.

Doelstelling

De doelstelling van deze opdracht is als volgt gedefinieerd:

> Komen tot een globaal beeld van hoe informatiebeveiliging en het gebruik van persoonsgegevens is geregeld binnen de verschillende geselecteerde ketens. En welke risico's zijn er?

Om deze doelstelling te realiseren is een viertal onderzoeksgebieden met vragen gedefinieerd die betrekking hebben op de informatie-uitwisseling binnen het onderwijs:

1. Uitwisseling gegevens. Welke persoonsgegevens worden uitgewisseld, op welk niveau (individueel, geaggregeerd, proces), tussen welke partijen, met welk doel, wat doet deze partij met de gegevens?
2. Verantwoordelijkheid. Wat is er geregeld, welke kaders zijn er? Bij wie is de verantwoordelijkheid voor informatiebeveiliging en privacybescherming belegd (per ketenpartner)?
3. Technisch. Welke passende technische (en organisatorische) maatregelen zijn genomen?
4. Risico's. Is een risicoanalyse uitgevoerd waarmee de gevoeligheid van de gegevens is bepaald, welke maatregelen zijn getroffen om de risico's te beperken, zowel binnen de onderwijsinstelling als bij de leverancier of dienstverlener?

Objecten van onderzoek en aanpak

Objecten van onderzoek

Het onderzoek richt zich op de volgende ketens:

- **Digitale leermiddelen**: Het delen van (examen) resultaten met behulp van digitale middelen en de verwerking daarvan door uitgevers, softwareleveranciers, distributeurs, administratie, scholen en leerlingen.
- **Werken in de cloud**: Tooling en sociale media: het delen van informatie tussen leerling, docent en clouddienstaanbieders door middel van de ad-hoc inzet van digitale middelen zoals social media, learning analytics of digitaal leermateriaal.
- **Aanmelden en inschrijven:** Het delen van informatie tussen instellingen onderling en DUO.

Aanpak

Ons onderzoek heeft een inventariserend karakter gehad en beperkt zich tot de getroffen maatregelen gerelateerd aan de uitwisseling van gegevens binnen de keten. Hierbij hebben wij primair naar de instellingen en DUO gekeken. De wijze waarop andere ketenpartners invulling geven aan verantwoordelijkheden hebben wij enkel op basis van openbare bronnen voor slechts enkele van deze ketenpartners (uitgeverijen, leveranciers van digitale leermiddelen) onderzocht. Ook hebben wij geen inhoudelijke beoordeling van de kwaliteit van de getroffen technische maatregelen bij de instellingen of andere ketenpartners uitgevoerd.

De voor dit onderzoek benodigde gegevens zijn verkregen door het houden van workshops met medewerkers van vier verschillende onderwijsinstellingen, het DUO en het raadplegen van (publiek beschikbare) documentatie. Enkelen van deze instellingen verzorgden speciaal basisonderwijs en/of speciaal voortgezet onderwijs, terwijl één instelling tevens onderwijs geeft in een gesloten instelling. Waar in deze tekst wordt gesproken over “de instellingen”, is bedoeld de instellingen betrokken bij de workshops.

Gedurende deze workshops is informatie ingewonnen over het gebruik van gegevens voor de eerdergenoemde ketens, en zijn de toegepaste maatregelen op hoofdlijnen geïnventariseerd. Wij hebben daarnaast enkele documenten beoordeeld. Wij hebben geen onderzoek verricht naar het bestaan of de werking van de maatregelen.

Voor het inventariseren van de getroffen maatregelen hanteren wij als handvat de onderwerpen uit het SURF toetsingskader voor het meten van volwassenheid van informatiebeveiliging aangevuld met de privacyonderwerpen uit het Privacy audit raamwerk van het College bescherming persoonsgegevens.

Wij hebben ons onderzoek naar de leveranciers van de scholen beperkt tot een globale inventarisatie van de publiek beschikbare informatie zoals op de website. Wij hebben geen gesprekken gevoerd of anderszins contact met deze leveranciers gehad.

Hoofdbevindingen, conclusies en aanbevelingen

Aanmelden en inschrijven

Grote betrokkenheid bij welzijn leerlingen …

De betrokkenheid van de scholen bij het welzijn van de leerling is hoog

De medewerkers op verschillende niveaus binnen de instellingen handelen vanuit het welzijn en belang van de individuele leerling, en proberen binnen de beperkingen van tijd en geld de maximale zorg en aandacht te leveren. Dit komt zonder uitzondering tot uitdrukking in de gesprekken en workshops die wij gevoerd hebben.

Dit komt ook tot uitdrukking in de behandeling van gegevens van de leerling. Enerzijds worden veel gegevens vastgelegd vanuit de beleving dat hoe meer men van een leerling weet en tussen leerkrachten kan overdragen, des te beter een leerling begeleid kan worden. Dit zijn vrijwel altijd alleen gegevens die relevant kunnen zijn voor de begeleiding van een leerling.

Tegelijkertijd is er het besef dat de gegevens van de leerling voldoende beveiligd moeten zijn, en dat zorgvuldig omgegaan moet worden met toegang en verstrekking. Dit wordt ook toegepast in de dagelijkse praktijk, waarbij maatregelen vooral op basis van “gezond verstand” worden toegepast.

De deelnemers aan onze workshops realiseren zich dat verbetering altijd mogelijk is, en er is bereidheid om verbeteracties op te pakken op het moment dat wij in de workshops suggesties doen ter verbetering. De workshops zelf hebben ook toegevoegde waarde gehad door bewustwording te creëren dat informatiebeveiliging een belangrijk onderwerp is. Tijdens de workshops werden al situaties benoemd waarin men zich bewust was geworden dat aanpassing nodig was. Er werd tijdens de workshops ook aangegeven dat men deze punten zou gaan oppakken.

Tegelijkertijd is er bij betrokkenen het besef dat er beperkingen gelden in termen van tijd, geld en kennis, en dat het ambitieniveau voor het onderwerp informatiebeveiliging waarschijnlijk beperkt zal blijven tot toepassing van praktische maatregelen binnen de eigen omgeving. Daar komt nog bij dat de aandacht zich het komende jaar vooral richt op de implementatie van nieuwe grote ontwikkelingen zoals passend onderwijs.

… leidt tot de vastlegging van een gedetailleerd beeld met gegevens over leerlingen

Onderwijsinstellingen leggen een gedetailleerd beeld van leerlingen en hun omgeving vast

Gedurende de schoolloopbaan wordt een gedetailleerd beeld van de sociale, emotionele en cognitieve vaardigheden van leerlingen en hun ontwikkelingen daarin opgebouwd. Ook de bredere sociale context van de leerlingen wordt in beeld gebracht, bijvoorbeeld door gegevens vast te leggen van familieleden zoals hun opleiding, culturele achtergrond, geloofsovertuiging, beroep en financiële verantwoordelijkheid.

Hoe groter de behoefte aan passend onderwijs en goede begeleiding hoe meer gegevens worden vastgelegd. De geloofsovertuiging wordt in de dagelijkse praktijk niet of nauwelijks gebruikt. De docenten weten uit de omgang met kinderen en ouders of, en zo ja welke, geloofsovertuiging van toepassing is.

Dataminimalisatie (het opslaan van zo min mogelijk gegevens om het gestelde doel te bereiken) wordt niet bewust toegepast.

De meeste van deze gegevens worden bij aanmelding vastgelegd op een gestandaardiseerd aanmeldformulier van de school, waarbij beide ouders moeten tekenen voor de betrouwbaarheid. De gegevens worden vastgelegd in een leerlingvolgsysteem dat gedurende de schoolloopbaan van de leerlingen wordt aangevuld, met als doel passend onderwijs en goede begeleiding.

De onderwijsinstellingen hebben in alle gevallen een leerlingvolgsysteem en maken in meer of mindere mate gebruik van digitale leermiddelen. Deze systemen worden vaak als een cloudoplossing door externe partijen gehost. De leveranciers hebben daarnaast de beschikking over de gegevens die over de leerlingen worden verzameld.

Veel partijen betrokken (1/2)

Gegevens worden gedeeld met een groot aantal partijen

De gegevens die gedurende de schoolloopbaan worden verzameld en verwerkt worden op verschillende momenten gedeeld met een groot aantal partijen. In sommige gevallen zijn deze direct betrokken bij het geven van onderwijs of de goede begeleiding van de leerling, in andere gevallen staan deze op meer afstand (Overheidsinstanties en Uitgeverijen) of hebben zij een ondersteunende taak (ICT-dienstverleners). Ook deze partijen geven gegevens door aan hen gelieerde partijen.

De onderwijsinstelling is in veruit de meeste gevallen verantwoordelijk (of in belangrijke mate uitvoerend en daarmee bepalend) voor de kwaliteit van de invoer van gegevens. Dit is van toepassing bijvoorbeeld voor de invoer van het leerlingvolgsysteem en bij het aanmaken van accounts bij leveranciers voor digitale leermiddelen als clouddiensten.

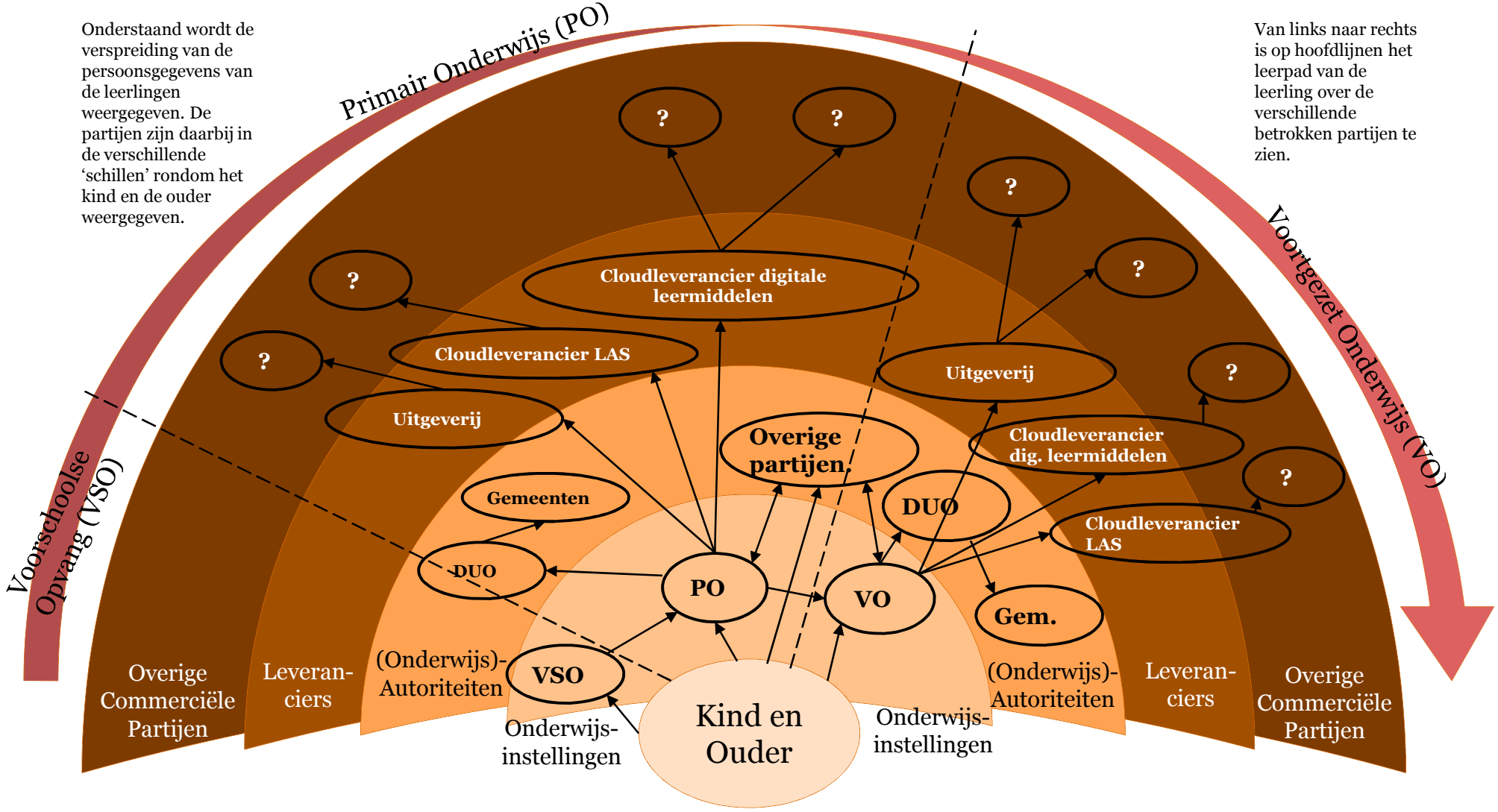
De aard en inhoud van de gegevensuitwisseling tussen de onderwijsinstelling met een derde partij varieert per type partij. Voor de uitwisseling tussen de onderwijsinstelling en DUO is de gegevensuitwisseling bijvoorbeeld in hoge mate gestandaardiseerd en wordt de informatie digitaal uitgewisseld. De wijze waarop deze gegevensuitwisseling plaats dient te vinden (XML-berichten) wordt voorgeschreven door DUO. De onderwijsinstelling meldt daarnaast afwezigheid van leerlingen via het Verzuimloket van DUO. DUO geeft aan dat de onderwijsinstelling verantwoordelijk is en blijft voor de gegevensuitwisseling.

De voorschriften van DUO omvatten tevens beveiligingsmaatregelen (geënt op Wbp risicoklasse 2) zoals een SSL-verbinding tussen DUO en het leerlingvolgsysteem van de onderwijsinstelling. DUO faciliteert dit door bijvoorbeeld de benodigde middelen voor de gegevensuitwisseling (zoals de certificaten) beschikbaar te stellen.

Veel partijen betrokken (2/2)

Onderstaand wordt de verspreiding van de persoonsgegevens van de leerlingen weergegeven. De partijen zijn daarbij in de verschillende 'schillen' rondom het kind en de ouder weergegeven.

Van links naar rechts is op hoofdlijnen het leerpad van de leerling over de verschillende betrokken partijen te zien.



Wettelijke kaders niet precies bekend bij instellingen (1/2)

De instellingen zijn niet precies bekend met alle relevante wettelijke kaders

De workshops geven aan dat de medewerkers niet bekend zijn met (wettelijke) kaders voor het verzamelen, bewerken, bewaren en vernietigen van gegevens en archiefstukken specifiek voor gegevens die in het primair onderwijs en voortgezet onderwijs worden verzameld. Het bestaan van de Wbp is bekend bij de medewerkers, maar niet welke rol in de context van de Wbp (verantwoordelijke of (sub)bewerker) zij precies hebben (verantwoordelijke of (sub)bewerker) en wat dit precies betekent voor de te nemen maatregelen. De instellingen vullen gebruik en beveiliging vooral praktisch in, waarbij men zelf een afweging maakt bezien vanuit de wettelijke verplichtingen die men beter kent en het belang van de leerling. Dit stelt de onderwijsinstellingen soms voor dilemma's. Enkele voorbeelden:

- Het PO kent de wettelijke verplichting tot "warme overdracht" van PO naar VO. Het kan voorkomen dat de ouder aan de PO-instelling geen toestemming geeft om een fysiek of digitaal dossier over te dragen naar de VO-instelling. De invulling van deze wettelijke verplichting en de wens om (in het belang van de leerling) een betere begeleiding op de VO-instelling mogelijk te maken, krijgt invulling door telefonisch informatie te delen naar de VO-instellingen.
  De interpretatie van de wet door de instellingen is overigens niet geheel juist. De wet benoemt dat een volledig dossier altijd overgedragen kan worden, ook al geven de ouders geen toestemming. De ouders moeten geïnformeerd worden, mogen het dossier aanvullen, maar kunnen een overdracht niet blokkeren.
- Een ander voorbeeld betreft de gegevens die men vanuit andere organisaties ontvangt, vooral waar het speciaal basis onderwijs, speciaal voortgezet onderwijs en onderwijs in de gesloten jeugdinrichtingen betreft. Dit betreft vaak dossiers van andere instanties, zoals delict gegevens, een rapport Ondertoezichtsstelling of DSM-gegevens (classificatie van stoornis) met onderliggende rapporten. Deze rapportages zijn niet in alle gevallen strikt noodzakelijk om goed onderwijs te geven, maar worden bewaard "voor het geval dat". Deze gegevens worden in het dossier opgenomen en blijven daar bewaard.
- Een voorbeeld betreft het wettelijke recht op inzage van de ouder. Dossiervorming betreft meestal het leerlingvolgsysteem, waarin bijvoorbeeld waarnemingen van docenten worden vastgelegd. Dit kunnen zeer voorlopige waarnemingen zijn. De ouders hebben recht op inzage in het dossier van de leerling, maar er is niet gedefinieerd wat de ouders precies mogen inzien en wat niet. Dit leidt soms tot reacties wanneer inzage wordt gegeven in voorlopige waarnemingen.

De onderwijsinstellingen leggen in de praktijk mogelijk te veel gegevens vast. Voorbeelden zijn in ieder geval de structurele vastlegging van geloofsovertuiging in het leerlingvolgsysteem, kopieën van identiteitsbewijzen van de leerling, pasfoto's van leerlingen en de BSN-nummers van de ouders.

Risico

Het risico is aanwezig dat instellingen te veel gegevens bewaren of overdragen naar ander partijen, met als mogelijk gevolg dat onbevoegden kennis kunnen nemen van gevoelige persoonsgegevens. De onderwijsinstelling voldoet niet aan de eisen die in de Wbp gesteld worden (non-compliance). Dit kan onder meer stigmatisering, aantasting eigenwaarde of ongelijke behandeling voor de leerling tot gevolg hebben.

Wettelijke kaders niet precies bekend bij instellingen (2/2)

Aanbeveling

- Stel in overleg met overheid, instellingen en andere belangenorganisaties een plan op voor het bevorderen van ‘awareness’ van het onderwerp informatiebeveiliging en privacy binnen de sector.
- Maak duidelijk naar je ketenpartners waar je binnen de keten verantwoordelijk voor bent (bijvoorbeeld verantwoordelijke of bewerker in de zin van de Wbp) en wat dit betekent voor taken, verantwoordelijkheden en bevoegdheden voor ketenactiviteiten. Maak duidelijk welke risico’s jij als ketenpartij ziet en neem (in samenspraak en samenhang met de ketenpartijen) effectieve maatregelen.
- Stel handreikingen op voor de praktische implementatie van de Wbp door PO en VO, zoals:
  - handreikingen die inzicht geven welke gegevens wel en niet opgeslagen mogen worden en wat de bewaartermijnen zijn.
  - best practices voor het praktisch nemen van maatregelen door de instelling.
- Bevorder het gebruik van sectorbrede standaarden, waarin dataminimalisatie is toegepast.
- Besteed bij nieuwe wet- en regelgeving zoals Passend Onderwijs aandacht aan de implicaties op het gebied van privacy (Privacy Impact Assessment), zoals de vast te leggen gegevens en de benodigde maatregelen bij de instellingen.

Verantwoordelijkheid voor maatregelen niet bekend

De instellingen zijn niet precies bekend met wat de toepassing van de wettelijke kaders in de praktijk betekent voor het nemen van maatregelen

De instellingen maken zonder uitzondering gebruik van de dienstverlening van externe ICT-leveranciers. Voorbeelden van de diensten die externe leveranciers leveren:

- de hosting en het technisch (applicatie)beheer van de ICT-omgeving (kantoorautomatisering, fileservers, technisch applicatiebeheer);
- de hosting van leerlingvolgsystemen (als cloudoplossing);
- de hosting van digitale leermiddelen (als cloudoplossing).

De instellingen zijn verantwoordelijke conform de Wbp, en daarmee verantwoordelijk om naar de bewerkers (waaronder ICT leveranciers) aan te geven welke eisen en maatregelen door de bewerker gerealiseerd moeten worden. De workshops geven echter aan dat het onderwerp slechts bij uitzondering ter sprake komt in de relatie tussen de instelling en leverancier. Het onderwerp wordt een enkele keer besproken, bijvoorbeeld bij de Europese Aanbesteding voor de selectie van een ICT-leverancier.

Het initiatief voor het nemen van maatregelen wordt door de instellingen in de praktijk aan de leverancier overgelaten. De instellingen hebben alleen inzicht in de genomen maatregelen voor zover deze zichtbaar zijn voor hen (het verplicht inloggen met gebruikersnaam en wachtwoord, schoning van gegevens).

> “Ik ga er vanuit dat zij dat goed regelen. Zij hebben daar kennis van”

De instellingen nemen zelf praktische, concrete maatregelen, zoals het afsluiten van ruimtes met dossierkasten en het beperken van toegang tot gegevens binnen het leerlingvolgsysteem op basis van autorisatierollen. Er liggen hier geen ‘best practices’ zoals ISO 27002 aan ten grondslag, deze maatregelen worden getroffen op basis van “gezond verstand”, incidenten die zich hebben voorgedaan en de adviezen van externe leveranciers en de accountant.

Risico

Het risico is aanwezig dat er onvoldoende maatregelen zijn genomen om de integriteit, exclusiviteit en continuïteit van privacygevoelige gegevens en de verwerking/informatievoorziening daarvan te waarborgen. Dit heeft tot gevolg dat de onderwijsinstelling niet aan de Wbp voldoet (vanuit het oogpunt van de rol van verantwoordelijke).

Aanbeveling

- Laat de leveranciers onderbouwen op welke wijze hun systemen en/of hun dienstverlening voldoen aan de eisen die vanuit de Wbp worden gesteld.
- Neem privacy en beveiliging als onderwerp op in de leidraad Programma van Eisen voor de selectie van leveranciers.
- Laat de leveranciers zich periodiek verantwoorden over de maatregelen die zij (op basis van het Programma van Eisen) hebben getroffen om de adequate beveiliging van de gegevens te waarborgen. De meest praktische aanpak (om te voorkomen dat elke onderwijsinstelling z’n eigen onderzoek doet) is om de vraagstelling en beoordeling voor één leverancier over alle sectoren heen door één organisatie te laten coördineren.

Afhankelijkheid van leveranciers is groot

De instellingen zijn sterk afhankelijk van de leveranciers van digitale leermiddelen en de ICT leveranciers

De markt in Nederland kent slechts enkele aanbieders van leerlingvolgsystemen, ICT-leveranciers voor het onderwijs en aanbieders van digitale leermiddelen. De grotere aanbieders van digitale leermiddelen (Uitgeverijen) hebben zich *bijvoorbeeld* vrijwel allemaal verenigd in een stichting die een deel van de infrastructuur aanbiedt voor het beschikbaar maken van digitale leermiddelen. Dit is Stichting Basispoort.

Hierdoor hebben de onderwijsinstellingen geen sterke onderhandelingspositie ten opzichte van de leveranciers, en kunnen niet veel eisen. De instellingen zijn zelf meestal klein van omvang.

De instellingen erkenden in de meeste gevallen dat er geen precies inzicht bestaat in de genomen maatregelen of verantwoording daar over, omdat dit geen structureel onderwerp van discussie is in de voortdurende relatie tussen instelling en leverancier, en de externe leveranciers zich niet proactief verantwoorden over de kwaliteit van de genomen maatregelen.

"Ik neem toch aan dat zo'n grote partij dat goed heeft geregeld"

Risico

Het risico is aanwezig dat er bij de verschillende betrokken partijen onvoldoende maatregelen zijn genomen om de integriteit, exclusiviteit en continuïteit van privacygevoelige gegevens en de verwerking/informatievoorziening daarvan te waarborgen, omdat er geen druk bij de leveranciers aanwezig is om een minimaal niveau van beveiliging te realiseren.

Aanbeveling

- Laat de leveranciers onderbouwen op welke wijze hun systemen en/of hun dienstverlening voldoen aan de eisen die vanuit de Wbp worden gesteld.
- Neem privacy en beveiliging als onderwerp op in de leidraad Programma van Eisen voor de selectie van leveranciers.
- Laat de leveranciers zich periodiek verantwoorden over de maatregelen die zij (op basis van het Programma van Eisen) hebben getroffen om de adequate beveiliging van de gegevens te waarborgen. De meest praktische aanpak (om te voorkomen dat elke onderwijsinstelling z'n eigen onderzoek doet) is om de vraagstelling en beoordeling voor één leverancier over alle sectoren heen door één organisatie te laten coördineren.
- Werk met andere onderwijsinstellingen samen op het gebied van inkoop, zodat er ruimte ontstaat om de vraagkant naar onderwijs ICT te professionaliseren en zodat er een betere onderhandelingspositie ontstaat.

Instellingen ervaren geen ondersteuning

De instellingen ervaren geen ondersteuning door externe organisaties op het gebied informatiebeveiliging en privacy

De instellingen geven aan dat zij niet proactief handreikingen krijgen van koepel- of belangenorganisaties. De behoefte hiertoe is wel aanwezig, met name waar het de praktische invulling van wet- en regelgeving betreft.

Dit wordt met name aangegeven waar het de toepassing van Passend Onderwijs betreft. Het besef is aanwezig dat dit bekent dat men in een aantal gevallen nieuwe gegevens over een leerling zal gaan vastleggen (bijvoorbeeld indicatie of medische gegevens), maar het is niet precies bekend welke eisen die aanvullend aan de verwerking stelt of de maatregelen die genomen moeten worden.

Een kort onderzoek leert dat er handreikingen openbaar beschikbaar gesteld worden voor deze onderwerpen. Voorbeelden hiervan zijn:

- Pingen, whappen, tweeten, taggen en liken… social media en schoolveiligheid (politie, geen datum/versienummer);
- Hoe? Zo! ICT en Recht (SaMBO-ICT en Kennisnet, september 2013);
- Cloud Computing en Privacy: De Wet Bescherming Persoonsgegevens (Stichting SURF, geen datum/versienummer).

Er is blijkbaar een leemte tussen wat aan documentatie beschikbaar is en wat door de onderwijsinstellingen percipiëren dat beschikbaar is.

Risico

Het risico is aanwezig dat er onvoldoende maatregelen zijn genomen om de integriteit, exclusiviteit en continuïteit van privacygevoelige gegevens en de verwerking/informatievoorziening daarvan te waarborgen. Dit heeft enerzijds tot gevolg dat de onderwijsinstelling niet aan de Wbp voldoet (vanuit het oogpunt van de rol van verantwoordelijke). Dit kan onder meer stigmatisering, aantasting eigenwaarde of ongelijke behandeling voor de leerling tot gevolg hebben.

Aanbeveling

- Stel handreikingen op voor de praktische implementatie van de Wbp door PO en VO, zoals:
  - handreikingen die inzicht geven welke gegevens wel en niet opgeslagen mogen worden en wat de bewaartermijnen zijn.
  - best practices voor het praktisch nemen van maatregelen door de instelling.
- Creëer een cultuur van leren en verbeteren in de keten. Ruim een belangrijke plaats in voor transparantie in de eigen maatregelen, knelpunten en vraagstukken.
- Creëer een loket waar onderwijsinstellingen in het PO en VO met hun privacy- en beveiligingsvraagstukken terecht kunnen.
- Creëer een platform waar onderwijsinstellingen best practices op het gebied van informatiebeveiliging kunnen delen.

Er is twijfel of door aanbieders van leerlingvolgsystemen op de juiste wijze invulling geven wordt aan bescherming van persoonsgegevens (1/2)

Er is twijfel of de leveranciers op een verantwoorde wijze omgaan met leerlinggegevens ....

De systemen die worden gebruikt binnen de instellingen voor het geven van onderwijs en het registreren van leerlinggegevens worden vaak als een cloudoplossing door externe partijen gehost. De leveranciers hebben de beschikking over de gegevens die over de leerlingen worden verzameld. Het aantal aanbieders is gering.

Alle instellingen geven aan geen inzicht in de bescherming van persoonsgegevens bij hun aanbieders te hebben. Ook stellen zij geen eisen aan de aanbieders. Zij gaan er vanuit dat de aanbieders bescherming van persoonsgegevens goed hebben georganiseerd. Wij hebben als deelwaarneming de websites van 2 van deze aanbieders onderzocht op uitlatingen op het terrein van privacy of bescherming van persoonsgegevens.

Voorbeeld 1: Leerlingvolgsysteem van Magister: onduidelijk of invulling gegeven wordt aan de bescherming van persoonsgegevens

De website geeft aan dat de privacy gewaarborgd is omdat het e-mailadres van de gebruikers niet wordt doorgegeven. Dit statement is ogenschijnlijk bedoeld om een lezer gerust te stellen dat aan de Wbp voldaan wordt. Onduidelijk is wie precies met “de gebruiker” bedoeld wordt , wat er met de andere persoonsgegevens van de gebruikers gebeurt, of die worden doorgegeven en waarvoor ze worden gebruikt. Verdere privacy statements zijn niet te vinden op de website. Het lijkt er op dat ‘privacy’ in de statement niet de lading van bescherming van persoonsgegevens dekt.

Er kan geconcludeerd worden dat deze maatregel door de leverancier op zichzelf volstrekt onvoldoende is om te voldoen aan de eisen die vanuit de Wet bescherming persoonsgegevens gesteld worden. Het is onduidelijk welke maatregelen de leverancier aanvullend heeft genomen.

Er is twijfel of door aanbieders van leerlingvolgsystemen op de juiste wijze invulling geven wordt aan bescherming van persoonsgegevens (2/2)

…. Maar er is ook een geruststellender voorbeeld

De website van ParnasSys bevat geen privacystatement. Wel zijn diverse delen op de site gewijd aan privacy zoals bijvoorbeeld de overwegingen om wel of niet aan basispoort deel te nemen. Ook is een beschrijving van de maatregelen die door de leverancier zijn genomen te vinden:

Voorbeeld 2: ParnasSys (3)

Beveiliging van de verbinding
Voor het verbinding maken maken wij gebruik van een beveiligde verbinding middels een SSL-certificaat. Dit is dezelfde beveiliging die banken toepassen bij telebankieren. Door middel van dit certificaat kan de gebruiker zien dat hij daadwerkelijk met de server van ParnasSys communiceert.

Versleutelde gegevensstroom
Tevens worden de gegevens van dit certificaat gebruikt om de gegevensstroom tussen de browser van de gebruiker en de ParnasSys-applicatie te versleutelen. ParnasSys gebruikt hiervoor een certificaat met een lange sleutel (256 bit), waardoor browsers aangeven dat er een sterke encryptie gebruikt wordt.

Beveiligde locatie
De ParnasSys-applicatie wordt gehost op een server bij een professionele hostingpartij. Deze hostingpartij heeft diverse maatregelen en barrières ingeregeld om te voorkomen dat onbevoegden (fysieke) toegang hebben tot de server van ParnasSys.
Enkele van deze maatregelen zijn:

- Bezoekers moeten zich vooraf melden en moeten zich legitimeren voordat ze het pand kunnen betreden.
- De ParnasSys-servers bevinden zich in een extra beveiligde zone in het datacentrum.
- Toegang tot de individuele server is ook niet mogelijk zonder de juiste sleutel.
- Er zijn diverse controle en alarmsystemen aanwezig om dit in de gaten te houden.

ISO/IEC 270001 certificering
Onze hostingpartner beschikt over een ISO/IEC 270001 certificering.

Scheiding applicatie en database
Onder andere voor de veiligheid is de applicatie gescheiden van de database. De database draait op een aparte server. De databaseserver is vervolgens niet bereikbaar via het internet. Ook de applicatieserver is grotendeels afgeschermd van het internet middels een firewall.

De sectoren staan mogelijk aan de vooravond van grootschalig gebruik van gegevens

Verwerken van gegevens (BRON)

DUO geeft aan dat uitsluitend gegevens verwerkt worden die nodig zijn om de Basisregister Onderwijs (BRON) te kunnen vullen. De onderwijssectoren PO en VO zijn beide onderdeel van het BRON. De wettelijke grondslag voor de vastlegging in BRON betreft de verschillende wetten die op de verschillende sectoren van toepassing zijn. De Minister is in de Wet op het Onderwijstoezicht (artikel 24b lid 3) benoemd als Verantwoordelijke conform de Wbp.

Deze gegevens worden verzameld met onder meer als grondslag het berekenen van de bekostiging van de onderwijsinstelling. Dataminimalisatie wordt al in het ontwerp van de gegevensuitwisseling (i.c. de XML-berichten) meegenomen. Dit is voor de toekomst geborgd doordat dataminimalisatie wordt meegenomen in de verschillende referentie-architecturen voor de gegevensuitwisseling in het onderwijs. Zulke standaarden worden voor het onderwijs beheerd bij EduStandaard nadat zij in gezamenlijk overleg met betrokkenen zijn vastgesteld in de Standaardisatieraad.

Verwerken van gegevens (Verzuimloket)

DUO verzamelt via een apart kanaal verzuimgegevens van leerlingen in het Verzuimloket. Het Verzuimloket is een portaal waar onderwijsinstellingen online of via hun leerlingvolgsysteem de afwezigheid van leerlingen kunnen melden. DUO geeft de verzuimgegevens door aan de gemeenten, die via hun leerplichtambtenaar hier actie op dienen te ondernemen. De onderwijsinstelling heeft de plicht dit te melden en DUO verzamelt deze gegevens conform de Leerplichtwet. De Minister is in de Wet op het Onderwijstoezicht (artikel 24h lid 2) benoemd als Verantwoordelijke conform de Wbp.

Verstrekking van gegevens

DUO levert de gegevens uit het BRON door aan overheidspartijen die hier volgens verschillende wetgevingen gebruik van mogen maken. Dit zijn bijvoorbeeld het Ministerie van OCW, het Inspectie van het Onderwijs, het Centraal Bureau voor de Statistiek (CBS), de Sociale Verzekeringsbank (SVB) en gemeenten. DUO gebruikt deze gegevens zelf om de hoogte van de bekostiging voor de onderwijsinstellingen te bepalen.

DUO geeft aan dat er in het veld in toenemende mate behoefte is aan data die in bulk beschikbaar wordt. Deze verzoeken komen nu vooral vanuit de koepelorganisaties zoals de PO-Raad en de VO-raad. DUO bekijkt per verzoek of deze verstrekkingen gedaan mogen worden. Hier is een afdeling toe ingericht. DUO houdt daarnaast toezicht op de interne verwerking van gegevens en heeft daarvoor een Functionaris voor de Gegevensbescherming aangesteld.

Vraagstukken

DUO geeft aan dat men tegen het vraagstuk aanloopt in hoeverre het wenselijk is dat gegevens aan partijen in het onderwijs in bulk worden geleverd. Het vraagstuk dat specifiek speelt is of data die geanonimiseerd worden aangeleverd, anoniem kunnen blijven wetende dat de ontvangende partij de dataset met andere bronnen kan combineren.

Het gebruik van grote datasets is op dit moment nog beperkt en "staat nog in de kinderschoenen". De huidige verstrekkingen zijn beperkt tot enkele informatieproducten die door het Ministerie van OCW worden opgevraagd / gemaakt voor de evaluatie en bepaling van beleid. DUO verwacht overigens wel dat het gebruik van gegevens (o.m. in het kader van 'learning analytics' binnen onderwijsinstellingen maar wellicht ook op basis van gegevens van DUO, de komende jaren een flinke sprong zal gaan maken). Dit zal naar verwachting in toenemende mate tot vraagstukken voor het borgen van privacy leiden.

Hoofdbevindingen, conclusies en aanbevelingen

Digitale leermiddelen

Inventarisatie van gebruik van gegevens
Proces Digitale Leermiddelen

Gebruik
De instellingen maken breed gebruik van verschillende soorten leermiddelen. Dit betreffen veelal applicaties die via het internet benaderbaar zijn, en gebruikt worden voor:

- Het beschikbaar stellen van onderwijsmateriaal en oefenstof voor leerlingen op het gebied van hoofdrekenen, spelling en begrijpend lezen.
- Het afnemen van oefentoetsen.
- Het afnemen van Cito-toetsen (door Cito).

Het gebruik van deze applicaties vereist in alle gevallen dat er een account aangemaakt wordt, waarbij persoonlijke gegevens ingevuld worden. Dit account kan op naam van de docent of van de leerling worden aangemaakt. De vastgelegde gegevens zijn meestal als volgt:

- Een identificerend kenmerk (gebruikersnaam, NAW of leerlingnummer), soms aangevuld met enige NAW-gegevens.
- Geboortedatum (met als doel een normniveau voor ervaring te bepalen op basis van de leeftijd en jaargang, waar de daadwerkelijke prestaties tegen worden afgezet).
- BRIN-nummer van de onderwijsinstelling.

Deze applicaties houden de historie van de oefenvragen en oefentoetsen vast. De applicaties bevatten daarmee een historie van de leerontwikkeling van een populatie van leerlingen, gekoppeld aan een onderwijsinstelling.

Maatregelen
De onderwijsinstellingen hebben geen specifieke maatregelen getroffen voor het gebruik van digitale leermiddelen. De leveranciers van digitale leermiddelen hebben enige informatie over privacy en beveiliging op hun website staan (zie onze bevindingen), maar dit zijn voor de onderwijsinstellingen geen criteria voor de selectie van een leverancier.

Er is twijfel of in de keten van digitale leermiddelen goed invulling wordt gegeven aan de bescherming van persoonsgegevens (1/4)

De leveranciers vragen en de instellingen geven goedkeuring voor het gebruik van gegevens waar dit wettelijk niet kan

De instellingen geven aan dat bij het gebruik van de online dienstverleners, zoals een leerlingvolgsysteem of een aanbieder van digitale leermiddelen, zij degene zijn die toestemming geven voor het gebruik van de gegevens van docenten en leerlingen. Dit is de gangbare werkwijze van leveranciers. De digitale leermiddelen die op de onderzochte scholen worden gebruikt worden over het algemeen aangeboden door de grotere Nederlandse uitgeverijen. Deze hebben zich verenigd in Stichting basispoort. Basispoort haalt uit de database van een leerlingvolgsysteem de identiteitsgebonden gegevens van alle medewerkers en leerlingen. Deze worden dus opnieuw opgeslagen in een aparte database. Deze worden gebruikt voor het verlenen van toegang tot de digitale leermiddelen.

Deze waarneming komt bijvoorbeeld expliciet tot uitdrukking in het privacy statement van Basispoort, waarin is geformuleerd:

> *Van Basispoort kan gebruikgemaakt worden, na uitdrukkelijke toestemming van de onderwijsinstelling voor het mogen gebruiken van genoemde gegevens. Bij het inrichten van het Basispoort account door de school, dient de ICT-coördinator de gebruikersovereenkomst namens de school te accepteren. Middels het aanklikken van een vinkje in een van de eerste schermen in het beheermenu van Basispoort. Daarbij wordt er van uitgegaan dat hij/zij daartoe is gemandateerd door het schoolbestuur.*
>
> *Van Basispoort kan gebruikgemaakt worden, na uitdrukkelijke toestemming van de onderwijsinstelling voor het mogen gebruiken van genoemde gegevens. Scholen hebben een eigen verantwoordelijkheid om aan ouders van leerlingen te melden welke persoonsgegevens zij verwerken in systemen die het onderwijsproces ondersteunen.*

De gebruikersovereenkomst vermeldt:

> *De persoonsgegevens van leerkrachten, beheerders van schoolapplicaties en databases en van leerlingen en hun groepsprofielen ontvangt Basispoort van de onderwijsinstelling, na uitdrukkelijke toestemming van die onderwijsinstelling door acceptatie van deze Gebruikersovereenkomst.*
>
> Basispoort verwerkt slechts persoonsgegevens indien aan een van onderstaande voorwaarden is voldaan:
> - Als betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend.

De betrokkenen zijn in deze context echter de leerkrachten, beheerders van schoolapplicaties en leerlingen. Er is in dit opzicht geen sprake van toestemming van alle betrokkenen, maar slechts door één entiteit namens alle betrokkenen. Deze constructie is volgens de Wbp echter niet mogelijk. Een oplossing waarin de Wbp voorziet is dat de scholen als verwerker de verantwoording dragen, en de andere entiteiten als bewerker uitsluitend onder de verantwoording van scholen met gegevens omgaan.

Er is twijfel of in de keten van digitale leermiddelen goed invulling wordt gegeven aan de bescherming van persoonsgegevens (2/4)

Voorbeeld 2: Basispoort (2a): Het is onduidelijk aan welke partijen welke gegevens worden verstrekt en waarom

In de gebruikersovereenkomst** is opgenomen dat “De gegevens die worden opgeslagen in Basispoort mogen en zullen enkel en alleen gebruikt worden voor het regelen van de toegang tot de educatieve applicaties en nooit aan derden”.

In de melding ***bij het CBP (1538319) is echter opgenomen dat ontvangers van de gegevens zijn:

- Aan de bij de stichting Basispoort aangesloten uitgeverijen, waarbij geldt dat de scholen klant zijn bij, c.q. over licenties beschikken voor het gebruik van (educatieve) applicaties.
- Aan de bij de stichting Basispoort aangesloten netwerkbeheerders van scholen, waarbij geldt dat de scholen klant zijn bij, c.q. over licenties beschikken voor het gebruik van deze applicatie(s).

Uit de gebruikersovereenkomst blijkt dat Basispoort samenwerkt met uitgeverijen, distributeurs en netwerkaanbieders die samen het grootste deel dekken van de leermiddelenvoorziening en -gebruik in het primair onderwijs. De volgende partijen worden genoemd:

Uitgeverijen:	**Distributeurs:**	**Netwerkaanbieders:**
Uitgeverij Malmberg	Heutink Primair Onderwijs	Heutink ICT
Uitgeverij Zwijssen	KG & Rolf	QL-ICT
ThiemeMeulenhoff	Reinders Oisterwijk	Reinders ICT
Noordhoff Uitgevers	Alberts Onderwijs	Skool

Eveneens wordt aangegeven dat: ‘Lopende deze overeenkomst het mogelijk is dat andere dan genoemde partijen tot de samenwerking toetreden”.

* http://info.basispoort.nl/Privacy.aspx
** http://info.basispoort.nl/Portals/76/docs/gebruikersovereenkomst.pdf
*** Wbp-Meldingenregister Cbp: http://www.cbpweb.nl/Pages/ind_reg_meldreg.aspx

Er is twijfel of in de keten van digitale leermiddelen goed invulling wordt gegeven aan de bescherming van persoonsgegevens (3/4)

Voorbeeld 2: Basispoort (2b): Het is onduidelijk aan welke partijen welke gegevens worden verstrekt

Uit de gebruikersovereenkomst van Basispoort blijkt eveneens dat op sites van de partners van Basispoort niet is terug te vinden op welke wijze haar partners omgaan met persoonsgegevens.

Als voorbeeld hebben wij de site van Zwijssen bekeken.

De website van Uitgeverij Zwijssen geeft aan:

"....Uw gegevens zijn niet alleen toegankelijk voor de bij ASSU aangesloten uitgeverijen maar ook voor toekomstige deelnemende educatieve uitgeverijen en andere bij het onderwijs betrokken zorgvuldig geselecteerde partijen. De educatieve uitgeverijen en de andere genoemde partijen gebruiken deze gegevens om u te kunnen voorzien van presentexemplaren van nieuwe schoolboeken en leermiddelen, om u gerichte (vak)informatie te verstrekken, u te informeren over onderwijsvernieuwing, algemene onderwijskundige zaken, anderszins voor het onderwijs relevante zaken of voor het verrichten van marktonderzoek..."

Het Privacy en cookie statement van Uitgeverij Zwijssen geeft aan:

"... Uitgeverij Zwijssen BV is onderdeel van WPG Uitgevers B.V. Dit privacy statement is van toepassing op alle producten, diensten en activiteiten van WPG Uitgevers B.V. en haar dochterondernemingen. WPG Uitgevers legt in het kader van haar dienstverlening gegevens vast. Dit is bijvoorbeeld het geval wanneer u zich abonneert op een uitgave of nieuwsbrief, een training volgt, een publicatie bestelt, uw interesse kenbaar maakt, gebruik maakt van onze (online) diensten of anderszins contact heeft met WPG Uitgevers. Uw persoonsgegevens worden gebruikt voor de uitvoering van met ons gesloten overeenkomsten, verbetering van de dienstverlening van WPG Uitgevers, ten behoeve van de financiële administratie en de uitvoering van accountantscontroles, om de website van WPG Uitgevers te beveiligen en webstatistieken op te stellen. Ook kunnen de gegevens worden gebruikt om u, met uw toestemming, op de hoogte te houden van interessante informatie en aanbiedingen van producten en diensten van WPG Uitgevers, waaronder ook (elk van) haar dochterondernemingen wordt verstaan, eventueel ook na beëindiging van uw abonnement. Om deze informatie en aanbiedingen zoveel mogelijk af te stemmen op uw interesses, is het mogelijk dat wij deze gegevens (laten) combineren met de bij de onderlinge ondernemingen van WPG Uitgevers bekende (persoons)gegevens...".

Er is twijfel of in de keten van digitale leermiddelen goed invulling wordt gegeven aan de bescherming van persoonsgegevens (4/4)

Voorbeeld 2: Basispoort (2b) vervolg:

Dit voorbeeld van Basispoort geeft aan dat er achter deze online dienst een stelsel van organisaties aanwezig is die in meer of mindere mate toegang kunnen hebben tot de gegevens die er mogelijk over leerlingen worden verzameld.

Het is onduidelijk welke gegevens precies verzameld worden, door wie en voor welke doeleinden. Dit kan variëren van beperkt NAW van leerlingen, tot of zij al dan niet gebruikmaken van de online diensten en tot gegevens betreffende hun cognitieve vaardigheden en de ontwikkeling daarin op het gebied van bijvoorbeeld taal en rekenen.

Voorbeeld 2: Basispoort (3): Het is onduidelijk waar de verwerkte gegevens voor noodzakelijk zijn

De gebruikersovereenkomst en de melding bij het CBP geven onder andere aan dat de volgende gegevens worden verwerkt door Basispoort.

> Geslacht en geboortedatum van leerlingen, leerkrachten en netwerkbeheerders in het kader van single sign on authenticatie en identificatie.

De combinatie van de gegevens en de doelen is niet voor de hand liggen. Mogelijk is dit bedoeld voor het kunnen resetten van wachtwoorden (controlevragen), maar daar kunnen ook andere gegevens voor gebruikt worden.

Risico

Het risico is aanwezig dat niet aan de eisen vanuit de Wbp wordt voldaan omdat betrokkenen onvoldoende regie kunnen voeren over het gebruik en de actualiteit van hun persoonsgegevens. Er wordt hiermee feitelijk niet aan de eisen van de Wbp voldaan.

Aanbeveling

Laat de leveranciers onderbouwen op welke wijze hun systemen en/of hun dienstverlening voldoen aan de eisen die vanuit de Wbp worden gesteld. Neem privacy en beveiliging als onderwerp op in de leidraad Programma van Eisen voor de selectie van leveranciers. Laat de leveranciers zich periodiek verantwoorden over de maatregelen die zij (op basis van het Programma van Eisen) hebben getroffen om de adequate beveiliging van de gegevens te waarborgen. De meest praktische aanpak (om te voorkomen dat elke onderwijsinstelling z'n eigen onderzoek doet) is om de vraagstelling en beoordeling voor één leverancier over alle sectoren heen door één organisatie te laten coördineren.

Hoofdbevindingen, conclusies en aanbevelingen

Werken in de cloud: Social Media en tooling

Inventarisatie van gebruik van gegevens
Proces Social Media en Tooling

Beleid
De geïnterviewde instellingen hebben (met één uitzondering) geen formeel beleid voor het gebruik van social media. De instellingen kennen geen structurele toepassing van social media voor pedagogische/didactische doeleinden. Er zijn in de meeste gevallen impliciete afspraken over de “do’s” en “don’ts” van het gebruik van social media, dat in door één van de instellingen ook daadwerkelijk op schrift is gesteld.

De instelling die dit op schrift heeft gesteld legt in het beleidsdocument in de eerste plaats vast dat het de verantwoordelijkheid is van de medewerker om social media naar eigen inzicht te gebruiken, en geeft daarnaast richtlijnen en tips/trucs voor het gebruik, die moeten voorkomen dat zowel de medewerker als de instelling geen schade ondervinden. De richtlijnen geven onder meer aan dat de medewerker niet wordt geacht vertrouwelijke gegevens van leerlingen, leveranciers en de school bekend te maken.

De andere scholen hebben informeel afspraken gemaakt over het gebruik, maar laten veel ook over aan het inzicht van de medewerker. Er zijn tussen de scholen een aantal gedeelde uitgangspunten te onderkennen, zoals:

- Medewerkers worden niet geacht “friends” te worden met leerlingen op Facebook.
- Medewerkers worden niet geacht om foto’s of ander materiaal op hun Facebook-pagina te plaatsen die aanstootgevend kunnen zijn of schadelijk voor het gezag van de leraar in de klas.

De instellingen leggen geen regels op aan leerlingen voor het gebruik van social media.

Gebruik
Social media worden gebruikt naar het inzicht van de individuele docent, maar dit is in de meeste gevallen zeer beperkt. Het gebruik door de docent betreft in de meeste gevallen Facebook of Twitter. Naast het privégebruik door een docent worden sociaal media uitsluitend gebruikt door docenten om lesuitval door te geven of leerlingen er aan te herinneren om een werkstuk in te leveren.

Controle
De onderwijsinstellingen voeren controles uit op de toepassing van social media. Dit geldt zowel voor het gebruik door docenten als het gebruik door leerlingen. Incidenten met docenten komen vrijwel niet voor.

Een veelvoorkomend vraagstuk bij de scholen betreft digitaal pesten. De instellingen geven aan dat het beleid is om niet in te grijpen op digitaal pesten, ook omdat dit veelal plaatsvindt buiten de schoolomgeving. De instellingen verwijzen ouders nu door naar de politie. De maatregel die de scholen treffen is dat leerlingen mobiele telefoons vaak aan het begin van de les moeten inleveren. Deze maatregel is in de eerste plaats ingevoerd zodat de leerlingen tijdens de les niet afgeleid raken.

Totaaloverzicht risico's voor de instelling en de leerling

Totaaloverzicht risico's voor de instelling en de leerling

Wij hebben een korte inventarisatie uitgevoerd van de risico's die van toepassing kunnen zijn op betrokkenen en stakeholders. Dit overzicht bevat *inherente risico's,* dit wil zeggen de risico's die van toepassing zijn indien geen enkele maatregel is genomen. Deze risico's zijn ook naar voren gekomen in de workshops.

Dit overzicht beperkt zich daarom niet tot de risico's ten gevolge van de bevindingen die in deze rapportage zijn benoemd, maar de risico's die per bevinding zijn benoemd zijn wel uit het overzicht afgeleid.

Risico's voor de leerling

- Verlies aan zelfstandigheid (bijvoorbeeld door beperking van de mogelijkheid om handelingen niet meer uit te voeren: onder toezicht, ouderlijke inmenging, uit huis plaatsing).
- Stigmatisering (bijvoorbeeld de wijze waarop betrokkene behandeld wordt op basis van bepaalde kenmerken: dommerik, hulpbehoevend, beperkt, kampbewoner).
- Ongelijkheid (bijvoorbeeld het op verschillende wijze benaderen van betrokkenen in verband met achtergrond of land van herkomst).
- Beperking van bewegingsvrijheid (beperken van de toegang tot bepaalde gebieden, etablissementen of ruimtes op basis van gedragingen).
- Aantasting eigenwaarde (bijvoorbeeld door afbreuk aan persoonlijkheid).
- Personen (bijvoorbeeld uit de ouderlijke macht gezette ouders) kunnen leerlingen vinden.

Risico's voor de docent

- Aantasting van het gezag in de klas.
- Onprettige leef- en werksfeer.
- Vermenging van zakelijk leven met privéleven (integriteit).

Risico's voor de instelling

- Non-compliance met wet- en regelgeving (boetes).
- Imagoschade met als gevolg dalende leerlingaantallen en gederfde inkomsten.
- Verstoorde onderwijs(logistieke) processen door niet-integere gegevens of discontinuïteit van processen.
- Gederfde inkomsten door bekostiging door onjuiste gegevens.
- Extra administratieve lasten door verscherpt toezicht.
- Extra administratieve lasten en/of boetes als gevolg van juridische geschillen.

Totaaloverzicht aanbevelingen

Totaaloverzicht Aanbevelingen

Wij hebben bij elke bevinding de risico's en aanbevelingen benoemd. Wij hebben in dit hoofdstuk de aanbevelingen gegroepeerd per doelgroep.

Allen	• Maak duidelijk naar je ketenpartners waar je binnen de keten verantwoordelijk voor bent (bijvoorbeeld verantwoordelijke of bewerker in de zin van de Wbp) en wat dit betekent voor taken, verantwoordelijkheden en bevoegdheden voor ketenactiviteiten. Maak duidelijk welke risico's jij als ketenpartij ziet en neem (in samenspraak en samenhang met de ketenpartijen) effectieve maatregelen. • Creëer een cultuur van leren en verbeteren in de keten. Ruim een belangrijke plaats in voor transparantie in de eigen maatregelen, knelpunten en vraagstukken.
Ministerie	• Stel vast of de sfeerschildering en de bevindingen in deze rapportage breed door de ketenpartijen herkend en gedragen wordt. Initieer in overleg met de ketenpartijen de passende vervolgacties met als doel informatiebeveiliging naar een hoger volwassenheidsniveau te brengen. • Besteed bij nieuwe wet- en regelgeving zoals Passend Onderwijs aandacht aan de implicaties op het gebied van privacy (Privacy Impact Assessment), zoals de vast te leggen gegevens en de benodigde maatregelen bij de instellingen.
Koepelorganisaties en andere belangenorganisaties	• Stel in overleg met overheid, instellingen en andere belangenorganisaties een plan op voor het bevorderen van bewustzijn over het onderwerp informatiebeveiliging en privacy binnen de sector. • Stel handreikingen op voor de praktische implementatie van de Wbp door PO en VO, zoals: 1. Handreikingen die inzicht geven welke gegevens wel en niet opgeslagen mogen worden, en wat de bewaartermijnen zijn. 2. Best practices voor het praktisch nemen van maatregelen door de onderwijsinstelling. • Neem privacy en beveiliging als onderwerp op in de leidraad Programma van Eisen voor de selectie van leveranciers. • Creëer een platform waar onderwijsinstellingen in het PO en VO met hun privacy- en beveiligingsvraagstukken terecht kunnen. • Creëer een platform waar onderwijsinstellingen best practices op het gebied van informatiebeveiliging kunnen delen. • Bevorder het gebruik van sectorbrede standaarden, waarin dataminimalisatie is toegepast.
Instelling	• Laat de leveranciers onderbouwen op welke wijze hun systemen/dienstverlening voldoen aan de eisen de vanuit de Wbp worden gesteld. • Laat de leveranciers zich periodiek verantwoorden over de maatregelen die zij (op basis van het Programma van Eisen) hebben getroffen om de adequate beveiliging van de gegevens te waarborgen. De meest praktische aanpak (om te voorkomen dat elke onderwijsinstelling z'n eigen onderzoek doet) is om de vraagstelling en beoordeling voor één leverancier over alle sectoren heen door één organisatie te laten coördineren. • Werk met andere onderwijsinstellingen samen op het gebied van inkoop, zodat er ruimte ontstaat om de vraagkant naar onderwijs ICT te professionaliseren en zodat er een betere onderhandelingspositie ontstaat
Leveranciers	• Maak inzichtelijk op welke wijze de systemen en/of dienstverlening voldoen aan de eisen die vanuit de Wbp worden gesteld. • Leg verantwoording af over de maatregelen die (op basis van het Programma van Eisen) zijn getroffen om de adequate beveiliging van de gegevens te waarborgen.

Bijlage 1: Inventarisatie van gebruik van gegevens

Inventarisatie van gebruik van gegevens
Proces aanmelden en inschrijven (1/5)

Wij hebben in de hierop volgende pagina's de betrokkenen en het gebruik van gegevens over de betrokkenen door de instellingen geïnventariseerd, waarbij de nadruk ligt op een volledig beeld. Dit impliceert niet dat *alle* instellingen in ons onderzoek deze gegevens vastleggen, maar minimaal één of meerdere.

Betrokkenen

Het aanmeld- en inschrijfproces is in de context van deze opdracht breed geïnterpreteerd, en omvat in deze interpretatie ook de processen "genieten onderwijs" en "overdracht keten" (naar een volgende onderwijsinstelling in de keten, bijvoorbeeld de "warme overdracht" van PO naar VO).

Het aanmeld- en inschrijfproces verschilt afhankelijk van het soort onderwijs. Het initiatief tot inschrijven ligt bij "regulier" PO en VO bij de ouders, terwijl in het geval van "speciaal onderwijs" of "onderwijs in een gesloten instelling" hier vrijwel altijd een derde partij bij is betrokken. Wij hebben daarom voor de volledigheid het gebruik van gegevens voor elk van deze onderwijssoorten apart benoemd.

De betrokkenen zijn in alle vormen van onderwijs hetzelfde:

	Regulier	Speciaal onderwijs	Onderwijs in gesloten instelling
Betrokkenen	• Leerling; • Broers en zussen van de leerling; • Ouders/verzorgers.	• Leerling; • Broers en zussen van de leerling; • Ouders/verzorgers.	• Leerling; • Broers en zussen van de leerling; • Ouders/verzorgers.

Inventarisatie van gebruik van gegevens
Proces aanmelden en inschrijven (2/5)

Regulier onderwijs

De onderwijsinstellingen die regulier basis- of voortgezet onderwijs bieden, leggen normaliter de in onderstaande tabel opgenomen gegevens vast (indien van toepassing), en verstrekken deze aan de in de eerste kolom opgenomen partijen. In de tweede en derde kolom zijn de door de instelling aangegeven doelen en grondslagen opgenomen.

Partij	Doel	Door instelling aangegeven grondslag	Onderwijsinstelling verzamelde en opgeslagen gegevens
Onderwijsin-stelling	• Bekostiging van de instelling. • Begeleiding van de leerling.	• Wettelijke verplichting in het kader van bekostiging. • Wettelijke verplichting in het kader van het geven van onderwijs. • Toestemming van de ouders.	• **Personalia van de leerling:** volledige naam, geboortedatum, BSN-nummer, onderwijsnummer, nationaliteit, adres- en contactgegevens (mobiel/vast telefoonnummer, e-mailadres en postadres), polisnummer verzekering. Kopie identiteitsbewijs/paspoort van leerling en ouders. • **Medicijngebruik en huisarts.** • **Geloofsovertuiging.** • **Foto's van de leerling:** opname in leerlingvolgsysteem, schoolgids, website, inclusief toestemming ouders voor gebruik. • **Personalia van beide ouders:** volledige naam, geboortedatum, BSN-nummer, contactgegevens (mobiel/vast telefoonnummer, e-mailadres en postadres) en overige gegevens zoals hoogst genoten opleiding, culturele achtergrond, financiële verantwoordelijkheid, beroep en werkgever. • **Vooropleiding:** verslagen van peuterspeelzaal, informatieblad van ouders over ontwikkelingsniveau (indicatief voor IQ). • **Inschrijfgegevens:** schoolgegevens (BRIN-nummer, naam en adres van de school), een datum van inschrijving en (eventueel) een datum van uitschrijving; historische inschrijfgegevens (vorige school). • **Resultaatgegevens:** Resultaten van toetsingen, het schoolloopbaanadvies en het resultaat van een mogelijk afgelegde eindtoets. • **Waarnemingen docent en begeleiders**: incidenten, thuissituatie en andere aandachtspunten. • **Waarnemingen schoolarts.**

Inventarisatie van gebruik van gegevens
Proces aanmelden en inschrijven (3/5)

Regulier onderwijs (vervolg)

Partij	Doel	Door instelling aangegeven grondslag	Onderwijsinstelling ingevoerde of verstrekte gegevens
Dienst Uitvoering Onderwijs	• Bekostiging van de onderwijsinstelling. • Handhaving leerplichtwet (VO).	Wettelijke verplichting.	• Persoonsgegevens van de leerling (zie verder onderwijsinstelling). • Gegevens van de ouders (zie verder onderwijsinstelling). • Inschrijfgegevens (zie verder onderwijsinstelling). • Melding verzuim leerling bij Verzuimloket.
Leverancier leerlingvolgsysteem	Ondersteuning van onderwijsinstelling t.b.v. bekostiging en begeleiding van de leerling.	Contractuele verplichting met onderwijsinstelling (bewerker namens de instelling).	• Persoonsgegevens van de leerling (zie verder onderwijsinstelling). • Gegevens van de ouders (zie verder onderwijsinstelling). • Inschrijfgegevens (zie verder onderwijsinstelling). • Resultaatgegevens (zie verder onderwijsinstelling). • Begeleiding- en zorggegevens (zie verder onderwijsinstelling).
Gemeente (leerplichtambtenaar)	Handhaving van leerplichtwet voor Primair en Speciaal Onderwijs.	Wettelijke verplichting. Toestemming ouders niet nodig, krijgen wel melding.	• Verzuimmelding (verzuimmelding voor PO en SO vindt plaats door school aan gemeente). • Mondeling afstemming naar behoefte op initiatief leerplichtambtenaar (verzuimmelding vindt plaats bij DUO voor VO en wordt verder gemeld aan leerplichtambtenaar).
Centrum voor Jeugd en Gezin	Adviseren van ouders over opvoeding kind.	Melding naar de ouders.	• Mondelinge afstemming naar behoefte.
Zorg Advies Team (politie, GGD, begeleiders “Op de Rails” en “Rebound”, leerplichtambtenaar gemeente, zorgcoördinator school, medewerker Bureau Jeugdzorg)	Begeleiding van leerlingen die dreigen uit te vallen.	Toestemming ouders.	• Dossier met informatie naar behoefte.
Samenwerkingsverband (Permanente Commissie Leerlingenzorg, PLC)	Plaatsing van leerlingen die extra zorg en aandacht nodig hebben.	Wettelijke verplichting. Toestemming ouders niet nodig, krijgen wel melding.	• Dossier met informatie naar behoefte (in elk geval onderwijskundig rapport).

Inventarisatie van gebruik van gegevens
Proces aanmelden en inschrijven (4/5)

Regulier onderwijs (vervolg)

Partij	Doel	Door instelling aangegeven grondslag	Gegevens
Meldcode Huiselijk geweld en Kindermishandeling		Melding naar de ouders.	Melding dat er sprake is van een vermoeden tot fysiek of psychisch geweld.
Onderwijsinstelling in de keten (PO naar VO)	Begeleiding van de leerling.	Wettelijke verplichting. Toestemming ouders.	Volledig dossier (inclusief onderwijskundig rapport).

De verstrekking van deze gegevens vindt in velerlei vormen plaats: mondeling, fysiek dossier, e-mail en interface (vanuit het Leerlingvolgsysteem), afhankelijk van de situatie en de ontvangende partij.

Speciaal onderwijs

De onderwijsinstellingen die speciaal basis- of voortgezet onderwijs bieden, leggen de volgende aanvullende gegevens vast:

Partij	Doel	Door instelling aangegeven grondslag	Gegevens
Onderwijsinstelling	Bekostiging en begeleiding van de leerling.	• Wettelijke verplichting in het kader van bekostiging. • Wettelijke verplichting in het kader van het geven van onderwijs. • Toestemming van de ouders.	• Diagnostische gegevens van de leerling (beschikking indicatie CvI met rapport, beschikking en inschrijfgegevens Bureau Jeugdzorg). • Geconstateerde leer-/opvoedproblemen. • Behandelplannen en medische gegevens (zoals aandoeningen voor zover voor de school relevant. • Naam van de huisarts. • Medische voorgeschiedenis.

Deze gegevens worden in de meeste gevallen in dossiervorm door een externe instantie (bijvoorbeeld een zorginstelling of samenwerkingsverband) aangeleverd, waarbij er geen sprake is van een gestandaardiseerd format of inhoud. De vorm van aanlevering kan verschillen: fysiek dossier of digitaal dossier (per e-mail). Dit is tevens van toepassing voor de informatiewaarde (veel of weinig). Deze gegevens worden niet overgedragen naar de volgende onderwijsinstelling in de keten.

Inventarisatie van gebruik van gegevens
Proces aanmelden en inschrijven (5/5)

Onderwijs in een gesloten instelling.

De instellingen die onderwijs in een gesloten instelling aanbieden, leggen normaliter de volgende aanvullende gegevens vast:

Partij	Doel	Door instelling aangegeven grondslag	Gegevens
Onderwijsinstelling	Begeleiding van de leerling.	Begeleiding leerling.	• Delictgegevens. • Rapport ondertoezichtstelling. • Psychiatrisch rapport. • Informatie over de achtergrond over de leerling.

Deze gegevens worden in de meeste gevallen in dossiervorm door een externe instantie (bijvoorbeeld Justitie) aangeleverd, waarbij er geen sprake is van een gestandaardiseerd format of inhoud. De vorm van aanlevering kan verschillen: fysiek dossier of digitaal dossier (per e-mail). Dit is tevens van toepassing voor de informatiewaarde (veel of weinig).

Deze gegevens worden niet overgedragen naar de volgende onderwijsinstelling in de keten.

Bijlage 2: Waarnemingen per instelling

Instelling A

Aanmeld- en inschrijfproces

Verzamelde gegevens aanmelding

Bij de aanmelding worden verzameld en geregistreerd in het leerlingvolgysteem:

- Personalia van de leerling, inclusief BSN/Onderwijsnummer.
- Medicijngebruik en overige relevante zorggegevens van de leerling.
- Personalia, opleidingsgegevens en financiële verantwoordelijkheid van de (wettelijke) ouders.
- Geloofsovertuiging van het gezin.
- Informatieblad van de ouders (optioneel) over ontwikkelingsniveau.
- Toestemming van de ouders om foto's op te nemen in de schoolgids en schoolwebsite.

Deze gegevens zijn vaak gebaseerd op vooraf vastgestelde formulieren van de school zoals een aanmeldformulier en een ouderverklaring. Soms komen ook dossiers mee vanuit andere organisaties, zoals:

- Onderzoeksverslagen t.a.v. medische achtergrond (IQ, medisch).
- Verslag van de peuterspeelzaal over ontwikkeling (met toestemming ouders).

Verzamelde gegevens levensloop

- Gegevens over de ontwikkeling van de leerling (cijfers, toetsresultaten et cetera).
- Waarnemingen van de docent.
- Waarnemingen van de schoolarts.

Delen van informatie

De persoonsgegevens van de leerlingen komen in het leerlingvolgsysteem (ParnasSys) terecht.

Op dit moment is ParnasSys enkel nog gekoppeld met de applicatie BRON van DUO en met Basispoort ten behoeve van authenticatie bij het gebruik van de digitale leermiddelen.

Incidenteel zouden dossiers van leerlingen gedeeld kunnen worden met onderstaande partijen, dit gaat altijd via de Interne Begeleider (IB-er):

Meldcode Kindermishandeling en huiselijk geweld; Leerplichtambtenaar (melding naar de ouders); Centrum Jeugd en Gezin (melding naar ouders); Schoolarts (na toestemming ouders); Onderzoeken door externe partijen (bijvoorbeeld student die onderzoek doet naar bepaald aspect. Deze neemt gegevens waar onder begeleiding).

Overdracht naar voortgezet onderwijs

Het dossier wordt opgesteld volgens een centraal model kindenlereninkaart.nl, waarop het dossier (onderwijskundig rapport, maar geen aantekeningen van docenten) naar de VO-school wordt verzonden.

Zodra het kind bij de VO school staat ingeschreven wordt het bij de PO-school uitgeschreven.

Vastlegging en bewaartermijnen:

- Leerlingvolgsysteem ParnasSys. De gegevens worden waarschijnlijk na 5 jaar automatisch geschoond.
- Fysieke dossiers. Deze worden nog 5 jaar bewaard.
- Fysieke dossiers bij samenwerkings-verband (het is betrokkenen niet precies bekend of en waar dossiervorming plaatsvindt).

Instelling A

Social media en digitale leermiddelen

Digitale leermiddelen

Er wordt gebruikgemaakt van een aantal verschillende digitale leermiddelen:

- Nieuwsbegrip;
- Gynzy;
- Ambrasoft;
- Basispoort;
- Cito toetsomgeving. Hierin worden leerlingnummer, BRIN en wachtwoord voor leerlingen in groep 6 tot en met 8 vastgelegd.

Deze digitale leermiddelen zijn vaak webbased en worden gehost “in de cloud” door de aanbieders, veelal uitgevers van lesmethoden.

Over het algemeen worden persoonsgegevens en leerprestaties vastgelegd in de bovenstaande systemen.

Beveiligingsmaatregelen

- Formele beleidsstukken voor informatiebeveiliging zijn niet aanwezig, ICT-beleid is in ontwikkeling. De scholen van de stichting hebben zelf beleidsvrijheid om keuzes t.a.v. maatregelen te nemen. Impliciet worden tussen medewerkers afspraken gemaakt op basis van “gezond verstand” van de betrokken medewerkers.
- Contracten met leveranciers zijn aanwezig, betrokkenen zijn echter niet op de hoogte in hoeverre hier expliciet beveiligingsmaatregelen zijn opgenomen. De leveranciers verantwoorden zich niet expliciet over de genomen maatregelen, in algemene zin heeft men vertrouwen dat de leveranciers verantwoord omgaan met gevoelige gegevens.
- De systemen (zoals het leerlingvolgsysteem) zijn ingericht op basis van rollen en autorisaties. De rollen worden door de scholen van de stichting naar eigen inzicht toegewezen.
- Fysieke toegangsbeveiliging is ingericht (ruimtes en dossierkasten met fysieke dossiers gaan op slot).

Social media

De instelling maakt geen gebruik van social media, de docenten passen dit individueel naar eigen inzicht toe.

Deze toepassing is overigens beperkt. Docenten hebben soms een pagina op bijvoorbeeld Facebook, maar aangeraden wordt om geen leerlingen toe te voegen.

Overige gegevensverzamelingen

- Personeels- en salarisadministratie bij een extern Administratie Kantoor.
- Mobiele telefoons: deze worden door de leerlingen bij de leerkracht ingeleverd en aan het einde van de schooltijd weer opgehaald. Soms worden foto’s of filmpjes, gemaakt door leerkrachten of leerlingen, die door de leerkracht online worden gezet.

Instelling B

Aanmeld- en inschrijfproces

Verzamelde gegevensaanmelding

Bij de aanmelding worden verzameld en geregistreerd in het leerlingvolgsysteem:

- Personalia van de leerling, inclusief BSN/Onderwijsnummer.
- Medicijngebruik van de leerling.
- Personalia, opleidingsgegevens en financiële verantwoordelijkheid van de (wettelijke) ouders.
- Personalia van broertjes en zusjes.
- Geloofsovertuiging.
- Informatieblad van de ouders (optioneel) over ontwikkelingsniveau.
- Toestemming van de ouders om foto's op te nemen in de schoolgids en leerlingvolgsysteem.

Deze gegevens zijn vaak gebaseerd op vooraf vastgestelde formulieren van de school zoals een aanmeldformulier en een ouderverklaring. Soms komen ook dossiers mee vanuit andere organisaties, zoals:

- Onderzoeksverslagen t.a.v. medische achtergrond (IQ, medisch).
- Verslag van de peuterspeelzaal over ontwikkeling (met toestemming ouders).

Verzamelde gegevens levensloop

- Gegevens over de ontwikkeling van de leerling (cijfers, toetsresultaten et cetera).
- Thuissituatie van de leerling.
- Incidenten (bijvoorbeeld ruzies).
- Waarnemingen van de docent.
- Waarnemingen van de schoolarts.

Delen van informatie

- Meldcode Kindermishandeling en huiselijk geweld regio Den Haag (melding naar de ouders).
- Leerplichtambtenaar (melding naar de ouders).
- Centrum Jeugd en Gezin (mondeling, melding naar ouders).
- Schoolarts (na toestemming ouders).
- Permanente Commissie Leerlingenzorg (directeuren, psychiater, orthopedagoog) van Samenwerkingsverband (ouderverklaring, onderwijskundig rapport, stoornisverklaring, verklaring bemoeienis samenwerkingsverband).
- Onderzoeken door externe partijen (bijvoorbeeld student die onderzoek doet naar bepaald aspect. Deze neemt gegevens waar onder begeleiding).

Overdracht naar voortgezet onderwijs

Het dossier gaat in z'n volledigheid (onderwijskundig rapport, maar ook aantekeningen van docenten) naar de VO-instelling, maar altijd na toestemming ouders.

Belangrijk is om hier te onderkennen dat het wettelijk verplicht is dat overdracht van PO naar VO plaatsvindt. De ouders dienen echter toestemming te geven dat gegevens uit het leerlingvolgsysteem worden overgedragen naar de volgende instelling. Deze toestemming is er niet altijd. De praktijk leert dat in deze gevallen geen dossieroverdracht plaatsvindt, maar wel telefonisch aandachtspunten worden meegegeven.

De instelling maakt geen gebruik van OSO.

Vastlegging en bewaartermijnen:

- Leerlingvolgsysteem ParnasSys. De gegevens worden waarschijnlijk na 5 jaar automatisch geschoond.
- Fysieke dossiers. Deze worden na 5 jaar door de shredder gehaald.
- Fysieke dossiers bij samenwerkings-verband (het is betrokkenen niet precies bekend of en waar dossiervorming plaatsvindt).

Instelling B

Social media en Digitale Leermiddelen

Social Media

De instelling heeft geen formeel beleid voor de toepassing van social media, de docenten passen dit individueel naar eigen inzicht toe.

Deze toepassing is overigens beperkt. Docenten hebben soms een pagina op bijvoorbeeld Facebook, maar aangeraden wordt om geen leerlingen toe te voegen.

Overige gegevensverzamelingen

- Personeels- en salarisadministratie bij het interne bestuursbureau.
- Mobiele telefoons. Leerlingen maken filmpjes en foto's van docenten en deze worden online gezet.

Digitale Leermiddelen

Er wordt gebruikgemaakt van een aantal verschillende digitale leermiddelen:

- Hoofdwerk (hoofdrekenen).
- Leskompas (laten zien van filmpjes over bijvoorbeeld geschiedenis).
- Dr. Digi (digitaal schoolbord, zoals laten zien van filmpjes et cetera).
- Cito toetsomgeving. Hierin worden leerlingnummer, BRIN en wachtwoord voor leerlingen in groep 6 tot en met 8 vastgelegd.
- Sociale Competentie ObservatieLijst (Scol) voor het meten van sociale competentie.
- Veilig Leren Lezen (taal-lesmethode).

Deze digitale leermiddelen zijn vaak webbased en worden gehost "in de cloud" door de aanbieders, veelal uitgevers van lesmethoden.

De vastlegging beperkt zich in de meeste gevallen tot basale vastlegging van gegevens van de leerkracht, niet van de leerling.

Beveiligingsmaatregelen

- Formele beleidsstukken voor informatiebeveiliging zijn niet aanwezig, ICT-beleid is in ontwikkeling. De scholen van de stichting hebben zelf beleidsvrijheid om keuzes t.a.v. maatregelen te nemen. Impliciet worden tussen medewerkers afspraken gemaakt op basis van "gezond verstand" van de betrokken medewerkers.
- Contracten met leveranciers zijn aanwezig, betrokkenen zijn echter niet op de hoogte in hoeverre hier expliciet beveiligingsmaatregelen zijn opgenomen. De leveranciers verantwoorden zich niet expliciet over de genomen maatregelen, in algemene zin heeft men vertrouwen dat de leveranciers verantwoord omgaan met gevoelige gegevens.
- De systemen (zoals het leerlingvolgsysteem) zijn ingericht op basis van rollen en autorisaties. De rollen worden door de scholen van de stichting naar eigen inzicht toegewezen.
- Fysieke toegangsbeveiliging is ingericht (ruimtes en dossierkasten met fysieke dossiers gaan op slot).

Instelling C

Aanmeld- en inschrijfproces

Verzamelde gegevens aanmelding

Bij de aanmelding worden verzameld en geregistreerd in het leerlingvolgsysteem:

- Personalia van de leerling, inclusief BSN/Onderwijsnummer.
- Medicijngebruik van de leerling.
- Personalia, opleidingsgegevens en financiële verantwoordelijkheid van de (wettelijke) ouders.
- Geloofsovertuiging.
- Foto's die gedurende de intakedag worden genomen.

Deze gegevens zijn vaak gebaseerd op vooraf vastgestelde formulieren van de school zoals een aanmeldformulier en een ouderverklaring. Daarnaast worden leerlingen geobserveerd door een orthopedagoog en docenten gedurende een intakedagdeel (voor Passend Onderwijs). Er vindt vastlegging plaats van de waarnemingen, die door de toelatings-commissie worden besproken (orthopedagoog, zorgcoördinator, docenten).

Dossiers worden in het leerlingvolgsysteem en fysiek opgebouwd voor leerlingen die worden toegelaten en worden afgewezen.

Verzamelde gegevens levensloop

- Gegevens over de ontwikkeling van de leerling (cijfers, toetsresultaten et cetera).
- Aan- en afwezigheid.
- Ontwikkelingsplan.
- Thuissituatie van de leerling.
- Incidenten (bijvoorbeeld ruzies).
- Waarnemingen van de docent.

Delen van informatie

- Leerplichtambtenaar (in geval van langere afwezigheid van de leerling).
- Permanente Commissie Leerlingenzorg van het Samenwerkingsverband (SVB). Deze krijgt het onderwijskundig rapport. De PCL bestaat uit o.m. zorgcoördinatoren en orthopedagoog van de aangesloten scholen.
- Zorg Advies Team (ZAT) (ter voorkoming van uitval van de leerling). Deze bestaat uit politie, Jeugdzorg, begeleiders van "Op de Rails" en "Rebound", leerplichtambtenaar, zorgcoördinator, GGD, orthopedagoog en jeugdpreventiemedewerker. Bespreking vindt plaats na toestemming ouders.

De ouders krijgen melding dat gegevens aan leerplichtambtenaar en PCL zijn verstrekt, toestemming wordt gevraagd voor ZAT.

Overdracht naar voortgezet onderwijs

Het dossier gaat in z'n volledigheid (onderwijskundig rapport, maar ook aantekeningen van docenten) naar de VO-instelling, maar altijd na toestemming ouders.

Het is wettelijk verplicht dat overdracht van PO naar VO plaatsvindt. De ouders dienen echter toestemming te geven dat gegevens uit het leerlingvolgsysteem worden overgedragen naar de volgende instelling. Deze toestemming is er niet altijd. De praktijk leert dat in deze gevallen geen dossieroverdracht plaatsvindt, maar wel telefonisch aandachtspunten worden meegegeven.

Er vindt in een beperkt aantal gevallen mondeling overdracht plaats, daar waar leerlingen naar het buitenland gemigreerd zijn.

De instelling maakt geen gebruik van OSO.

Vastlegging en bewaartermijnen:

- Leerlingvolgsysteem EduArte. De gegevens worden waarschijnlijk na 5 jaar automatisch geschoond.
- Fysieke dossiers. Deze worden na 5 jaar door een verwerkingsbedrijf afgevoerd.
- Fysieke dossiers van afgewezen leerlingen. Deze worden na 2 jaar geschoond.

Instelling C

Social media en Digitale Leermiddelen

Social Media

De instelling heeft geen formeel beleid voor de toepassing van social media, de docenten passen dit individueel naar eigen inzicht toe.

Er zijn een paar docenten die gebruikmaken van Facebook en Twitter. Hiervan wordt door docenten zeer spaarzaam gebruikgemaakt (hoogstens herinnering om werkstukken in te leveren). Roosterwijzigingen worden door de roosteraar via SMS doorgegeven. Leerlingen wisselen dit verder ook via Twitter uit.

Incidenten op social media worden niet door de school opgepakt, hierbij wordt doorverwezen naar de politie.

Overige gegevensverzamelingen

- Personeels- en salarisadministratie bij een extern Administratie Kantoor.
- Foto's van leerlingen worden opgenomen in informatieboekje van de school, maar pas na toestemming van de ouders.
- Beveiligingscamera's zijn onder meer gericht op de openbare weg als preventie tegen vandalisme (met bordje bij de openbare weg). Opnames worden echter niet gemaakt.

Digitale Leermiddelen

Er wordt gebruikgemaakt van een aantal verschillende digitale leermiddelen:

- IT's learning Pebbles.
- Kurzweil. Dit is een leermiddel bedoeld voor dyslectische leerlingen. Leerlingen hebben eigen aanmeldcode en wachtwoord.
- Digitale Toetsen. Dit zijn vaak toetsen aanvullend op een boek, maar betreffen geen volledig digitale lesmethode.

Deze digitale leermiddelen zijn vaak webbased en worden gehost "in de cloud" door de aanbieders, veelal uitgevers van lesmethoden.

De historie van prestaties van leerlingen wordt veelal bijgehouden.

Externe leveranciers

- Het beheer van werkplekken en servers is ondergebracht bij een centrale dienst van de stichting. Deze centrale dienst maakt voor het beheer en hosting van servers en werkplekken gebruik van verschillende externe ICT-leveranciers.
- Het leerlingvolgsysteem wordt als cloudoplossing gehost door een externe leverancier.

Beveiligingsmaatregelen

- Een formeel beveiligingsbeleid is voor zover bekend niet aanwezig.
- Organisatorisch is de verantwoordelijkheid voor privacy en beveiliging waarschijnlijk bij College van Bestuur belegd.
- Het is niet bekend of beveiligingseisen zijn opgenomen in de contracten of Service Level Agreements met externe leveranciers.
- Arbeidscontracten bevatten mogelijk enige zinsnedes over geheimhouding.
- Fysieke beveiligingsmaatregelen worden op basis van "gezond verstand" genomen (ruimtes en patchkasten zijn of worden afgesloten)

Instelling D

Aanmeld- en inschrijfproces (1/2)

Verzamelde gegevens aanmelding

Een aanmelding komt vaak vanuit de ouders, maar er is vaak een 'derde' partij betrokken. Dat kan zijn: Ministerie van Justitie, gemeente, samenwerkingsverband, zorginstelling. Deze instanties hebben vaak hun eigen dossier over de leerling. De aanmelding wordt gedaan bij het samenwerkingsverband, dat de leerling plaatst bij de onderwijsinstelling.

Bij het aanmelden is er geen standaard pakket van informatie dat wordt aangeleverd door de aanmeldende instantie, en de wijze van aanmelding varieert van een fysiek dossier tot een digitaal dossier per e-mail. Soms wordt er een zeer volledig dossier meegestuurd en soms niets en moet de orthopedagoog zelf achter de informatie gaan. Gegevens die worden aangeleverd variëren maar kunnen betreffen:

- Medische gegevens.
- Delictgegevens (voor onderwijs in een instelling).
- Rapport Ondertoezichtstelling.
- DSM-gegevens (classificatie van stoornis) met onderliggende rapporten.

Daarnaast worden de gegevens vastgelegd die ook in het reguliere basisonderwijs en voortgezet onderwijs zijn te onderkennen.

De gevraagden waren niet bekend met kaders of richtlijnen van de gegevens die ze wel en niet zouden mogen bewaren voor hun doeleinden.

Delen van informatie

Het leerlingvolgsysteem MLS wordt gebruikt voor speciaal voortgezet onderwijs, is webbased en bestaat uit 3 delen:

1. Dossier analyse met kernproblematiek. Toegankelijk alleen voor orthopedagoog en leercoördinator.
2. Cognitieve/didactische doelen.
3. Sociaal-emotionele doelen.

2 en 3 worden steeds besproken en geactualiseerd door de leerkrachten en mentorgroep, deel A krijgt niet iedereen te zien (alleen de orthopedagoog?).

Naast MLS wordt ook het leerlingvolgsysteem ESIS (van ROVICT) gebruikt voor speciaal onderwijs en speciaal basisonderwijs, deze bestaat uit twee delen:

1. ESIS-A omvat alle administratieve taken die voor een school van essentieel belang zijn.
2. ESIS-B is het leerlingzorgsysteem voor registratie van toetsresultaten, dossieropbouw, verslag van oudergesprekken en handelingsplannen. Inclusief het Landelijk Model Onderwijskundig Rapport: alle relevante gegevens uit ESIS worden automatisch hierin ingelezen.

Onderwijsplanner

Tenslotte wordt ook het systeem 'Onderwijsplanner' gebruikt. Dit is een systeem voor het bepalen, volgen en bijstellen van het wettelijk voorgeschreven ontwikkelingsperspectief van leerlingen. Het geeft data die nodig zijn om voor elk kind een passend onderwijsarrangement op te stellen. Dit systeem is gekoppeld aan ESIS-B: PO-planning wordt gebruikt voor het volgen van het ontwikkelpad van leerlingen (ontwikkelperspectief, ontwikkeling).

Delen van informatie

De scholen (in de persoon orthopedagoog) hebben vaak een directe lijn met de inrichting/behandelende artsen/psychiater. Er zijn echter geen richtlijnen over wat wel en wat niet gecommuniceerd mag/moet worden en op welke manier. Integriteit staat wel hoog in het vaandel.

Instelling D

Aanmeld- en inschrijfproces (2/2)

Delen van informatie (vervolg)
Het samenwerkingsverband is vaak betrokken met orthopedagoog, directeuren en secretariële ondersteuning.

Jeugdzorg (hoort bij de gemeente).

Dossiers worden digitaal (via de mail) verstuurd en zowel digitaal als uitgeprint op papier bewaard. In het dossier staat alles wat er bekend is over de leerling (zorggegevens, gegevens over ouders, leergegevens et cetera). In het kader van de 'warme overdracht' worden dossiers soms ook op papier aangeleverd.

Overdracht naar Voortgezet onderwijs
Wanneer een leerling van school gaat dan wordt alleen het Programma van Toetsing en Afsluiting (PTA) meegegeven (dit is 1 en 2) van MLS. Deel 1 wordt alleen op aanvraag verstrekt. Er is voor overdracht toestemming nodig van de ouders per ondertekend formulier.

Er is een protocol beschikbaar voor omgaan met schoolverlaters (deze hebben wij ontvangen).

De instelling gaat gebruikmaken van OSO voor overdracht van studie- en begeleidingsgegevens van PO naar VO.

Vastlegging en bewaartermijnen:
Dossiers worden zowel digitaal (in MLS, ESIS en PO-planner) als op papier in fysieke dossiers bewaard. Termijn: tot 5 jaar nadat leerling van school is, het fysieke dossier gaat daarna door de shredder.

Instelling D

Social media en Digitale Leermiddelen (1/2)

Social Media

Er is net een beleid waarin de do's and don'ts staan over social media (Facebook, Twitter et cetera). De scholen moeten wel zelf een vertaalslag maken van beleid naar eigen instructies en richtlijnen. Het is een positief beleid (dus wel gebruiken maar wees bewust van de risico's).

Overige gegevensverzamelingen

- Personeels- en salarisgegevens door het Administratie Kantoor.
- Verzuimmanager van een externe cloudleverancier.
- Cameratoezicht. Dit is van toepassing op ruimtes in de justitiële inrichting, niet op de andere scholen. Hier wordt slechts spaarzaam en na toestemming van leidinggevende gebruik van gemaakt.

Digitale leermiddelen

De stichting gebruikt een groot aantal verschillende digitale leermiddelen. De scholen van de stichting besluiten zelf welke leermiddelen ze gebruiken.

- **Rekentuin**. Leermiddel om rekenen te oefenen. De vastgelegde gegevens betreffen naam en geboortedatum (om je in een niveaugroep te kunnen plaatsen).
- **Taalzee**. Leermiddel om spelling te oefenen.
- **Huiswerk Online.**
- **Nieuwsbegrip**. Leermiddel om begrijpend lezen te oefenen.
- **Basispoort**. Dit is een portal voor toegang tot online leermiddelen van vrijwel alle grotere uitgeverijen. Dit is nog niet operationeel bij deze stichting, maar de stichting gaat er in de loop van 2014 gebruik van maken.
- **AMN-toetsen.** Dit betreffen niveautoetsen voor taal en rekenen. De leerlingen loggen zelf in.

Deze leermiddelen houden historie van de leerling bij gedurende een langere periode. De medewerkers waren desgevraagd niet op de hoogte van hoe privacystatements et cetera zijn ingericht of welke maatregelen de leveranciers hebben getroffen om de gegevens te beschermen.

Algemeen

- Het beheer van werkplekken en servers is ondergebracht bij een centrale dienst van de stichting. Deze centrale dienst maakt voor het beheer en hosting van servers en werkplekken gebruik van verschillende externe ICT-leveranciers.
- De leerlingvolgsystemen wordt als cloudoplossing gehost door een externe leverancier.

Instelling D

Social media en Digitale Leermiddelen (2/2)

Beveiligingsmaatregelen

- De scholen kunnen in belangrijke mate zelf bepalen welke maatregelen zij op locatie kunnen nemen.
- Hier ligt vaak geen formeel beleid aan ten grondslag, maar keuzes worden op basis van “gezond verstand” en leerervaringen uit incidenten genomen.
- Geheimhoudingsverklaringen en Verklaringen omtrent Gedrag (VOG) worden soms wel, soms niet gevraagd.
- Taken tussen aanmaken, bewerken en archiveren van dossiers zijn gescheiden in taken.
- Voorbeelden van praktische maatregelen zijn fysieke maatregelen zoals dossierkasten en beveiligde ruimtes die op slot worden gedaan. Dit is vooral bedoeld om toegang door leerlingen te voorkomen, niet om toegang door doelgroepen medewerkers te beperken.
- Toegang tot systemen wordt beperkt op basis van autorisaties, die in rollen worden toegekend. Toegang is vaak beperkt tot de leerlingen die docenten in hun jaargang hebben.

ICT-beveiligingsmaatregelen worden vaak door externe leveranciers ingericht.

Bijlage 3: Referentiekader voor informatiebeveiliging

Beveiliging: maatregelen

Beleid en Organisatie

Beleidsdocument voor informatiebeveiliging

Evaluatie en actualisering

Bestuurlijke verankering

Toewijzing en vastlegging van verantwoordelijkheden voor IB

Beleid voor gegevensuitwisseling

Overeenkomsten

Analyse en specificatie van beveiligingseisen

Bescherming van persoonsgegevens

Rapporten beveiligingsincidenten

Verantwoordelijkheden en procedures incidentafhandeling.

Personeel, studenten en gasten

8.1.3 Arbeidscontract/voorwaarden

8.2.2 Bewustwording, opleiding en training voor informatiebeveiliging

8.3.3 Blokkering van toegang

Ruimten en Apparatuur

9.1.2 Fysieke toegangsbeveiliging

9.1.5 Werken in beveiligde ruimten

9.2.4 Onderhoud van apparatuur

11.3.3 Clear desk en clear screen policy

Continuïteit

10.1.2 Beheer van wijzigingen

10.4.1 Maatregelen tegen kwaadaardige programmatuur

10.5.1 Reservekopieën

14.1.1 Het proces van continuïteitsbeheer

14.1.2 Bepaling van de continuïteitsstrategie

14.1.3 Ontw. en impl. continuïteitsvoorzieningen en -plannen

14.1.4 Structuur voor continuïteitsplannen

Toegangsbeveiliging

11.1.1 Toegangsbeleid

10.8.4 Geautomatiseerde gegevensuitwisseling (tussen systemen)

10.9.2 Transacties “on line” (tussen personen en systemen)

11.2.1 Registratie van gebruikers (is incl autorisatie)

11.5.2 Gebruikersidentificatie en authenticatie

11.4.6 Beheersmaatregelen voor netwerkverbindingen

11.4.5 Scheiding van netwerken

11.2.2 Beheer van speciale bevoegdheden

11.5.1 Inlogprocedures

11.3.1 Gebruik van wachtwoorden en authenticatiemiddelen

11.6.1 Beperken van toegang tot informatie

11.6.2 Isoleren gevoelige systemen