Privacy van leerlingen in het digitale onderwijs

Digitale leermiddelen en ondersteunende digitale systemen zijn niet meer weg te denken uit het hedendaags onderwijs. De omgang met privacygevoelige leerlinggegevens en correcte naleving van de Wet bescherming persoonsgegevens (Wbp) bleven daarbij lange tijd onderbelicht. Een onderzoek van het College Bescherming Persoonsgegevens en daarop volgende kamervragen aan staatssecretaris Dekker brachten hierin verandering en leidden in april 2015 tot het "Convenant Digitale Onderwijsmiddelen en Privacy".

Mw.mr. I.A. Hoen* en mr. B.A.J. van Lammeren*

Om met convenant en bewerkersovereenkomst uit de voeten te kunnen is basiskennis van de Wbp noodzakelijk. In deze bijdrage zullen de auteurs aan de hand van de Wbp het convenant bespreken en waarschuwen zij voor onduidelijke en algemeen geformuleerde bepalingen in het convenant die scholen gemakkelijk op het verkeerde been kunnen zetten.[1]

1. Waarom een convenant Digitale Onderwijsmiddelen?

Bij gebruik van digitale leermiddelen is sprake van geautomatiseerde verwerking van persoonsgegevens. Het gaat daarbij doorgaans om grote aantallen persoonsgegevens die worden verwerkt.[2] Op deze verwerkingen zijn de regels uit de Wbp van toepassing. De Autoriteit persoonsgegevens (hierna: de 'AP')[3] heeft daarbij vastgesteld dat het bij verwerking van persoonsgegevens in het kader van vastlegging van leergedrag kan gaan om zeer gedetailleerde gegevens over de individuele onderwijsvorderingen van een leerling, waaraan allerhande conclusies kunnen worden verbonden die mogelijk gevolgen hebben voor het latere maatschappelijke leven van de leerlingen.[4] Verwerkingen met betrekking tot leergedrag zijn dan ook – net als gegevens met betrekking tot de gezondheid van de leerling – bijzonder gevoelige persoonsgegevens hetgeen nadere eisen met zich brengt ten aanzien van de verwerking daarvan.

Een onderzoek van het voormalige College Bescherming Persoongsgevens in 2013[5] legde op pijnlijke wijze bloot dat op de meeste scholen kennis en kunde ontbreekt om passende waarborgen te treffen voor een correcte naleving van de privacyregelgeving. Uit het onderzoek bleek dat het voor veel scholen onduidelijk is wat de leverancier van de digitale diensten nu wel of niet met de gegevens van de leerlingen kan, mag en doet. Scholen zijn in veel gevallen ook onvoldoende op de hoogte van de ((softwarematige) mogelijkheden van de) techniek achter de digitale middelen. Ook weten zij niet wat die digitale leermiddelen (kunnen) registreren bij het gebruik daarvan. Door deze achterstand in kennis kunnen scholen de (ouders van de) leerlingen niet volledig informeren over wat er met de persoonsgegevens van de leerlingen gebeurt.

Het betreffende onderzoek dat was gericht op softwareontwikkelaar Snappet die de haar ter beschikking gestelde leerlinggegevens bleek te gebruiken voor doeleinden waarvoor deze gegevens niet waren verstrekt en waarvoor evenmin toestemming was gegeven, en leidde tot grote publieke belangstelling voor de wijze waarop scholen omgingen met vertrouwelijke leerlinggegevens. Het onderzoek leidde tot kamervragen waarna staatssecretaris Dekker de Tweede Kamer toezegde de naleving van de privacywetgeving in het onderwijs te verbeteren.[6] De staatssecretaris hield woord en deelde in zijn brief d.d. 3 juli 2015 de Tweede Kamer mee dat de betrokkenen bij het zogenaamde 'Doorbraakproject'[7] waren gekomen tot het convenant 'Digitale onderwijsmiddelen en Privacy-leermiddelen en toetsen' (hierna: het 'convenant') en tevens een model 'bewerkersovereenkomst' hadden gesloten.[8] Het convenant en de bewerkersovereenkomst zouden volgens de staatsecretaris de scholen maximaal ontzorgen bij het aangaan van contracten met leveranciers[9] en bij het gebruik van digitale leermiddelen.

Studie van dit convenant en de bewerkersovereenkomst leert dat het convenant en de modelbewerkersovereenkomst zich toespitsen op de relatie tussen school en aanbieder. Daarmee zijn voor de school echter nog zeker niet alle verplichtingen afgedekt aan welke zij moet voldoen op basis van de Wbp. Nogal wat (kern)verplichtingen van de school blijven onderbelicht. Handvatten op welke wijze scholen invulling moeten geven aan deze (kern)verplichtingen ontbreken eveneens.

* Mw.mr. I.A. Hoen en mr. B.A.J. van Lammeren zijn advocaat bij Wille Donker Advocaten te Alphen aan den Rijn

De volgende (voor het onderwijs nieuwe) uitgangspunten in het convenant vragen om een uitgebreidere en duidelijkere toelichting dan het convenant biedt.

1.1 Regievoering door de scholen (artikel 3 lid 1 en 2 van het convenant)

Een school neemt nu nog vaak een (standaard)leermiddel af als het past in haar leersysteem zonder acht te slaan op de (andere) mogelijkheden die het leermiddel biedt, dan wel de doelen waarvoor de persoonsgegevens van de leerlingen (kunnen) worden verwerkt door de leverancier, welke gegevens worden verwerkt, aan wie deze worden verstrekt en hoelang deze gegevens worden bewaard. Onder het convenant wordt hierin verandering gebracht. De vaststelling van de doelen en middelen voor de verwerking van de persoonsgegevens is nu uitdrukkelijk bij de scholen neergelegd. Deze verandering betekent een wijziging in de juridische verhouding tussen de scholen en hun leveranciers. Dit blijkt onvoldoende bij een oppervlakkige lezing van het convenant.

Voor een goed begrip van de essentie van het convenant is een nadere beschouwing van de Wbp van belang en de verschillende rollen die in de Wbp worden onderscheiden.

– *Hoofd- en bijrollen in de Wbp*

Allereerst is van belang de hoofdrolspelers in de Wbp goed voor ogen te hebben. Dat zijn er feitelijk twee: de betrokkene en de verantwoordelijke. De betrokkene is de natuurlijke persoon wiens persoonsgegevens worden verwerkt. In dit geval is dat de leerling. De verantwoordelijke is de natuurlijke persoon, rechtspersoon, het bestuursorgaan of ieder ander die het doel van en de middelen voor verwerking van de persoonsgegevens vaststelt. Oftewel, degene die uiteindelijk bepaalt of er gegevens worden verwerkt en zo ja, welke verwerking, van welke persoonsgegevens en voor welk doel en die beslist op welke wijze de gegevensverwerking zal plaatsvinden. Het convenant benoemt de onderwijsinstelling als 'verantwoordelijke'.

Een bijrol is er voor de bewerker. De bewerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt zonder aan diens rechtstreekse gezag te zijn onderworpen. De bewerker verwerkt de persoonsgegevens dan ook niet ten eigen behoeve maar slechts op de wijze zoals de verantwoordelijke hem voorschrijft.[10]

– *School als verantwoordelijke?*

Als aanbieder van het onderwijs is het – zeker vanuit het oogpunt van de (ouders van de) leerlingen) een logische en vanzelfsprekende keuze dat in het convenant de scholen als verantwoordelijke worden aangemerkt. Op basis van de feitelijke omstandigheden in combinatie met de privacywetgeving is dat minder vanzelfsprekend. De verantwoordelijke dient op basis van de Wbp namelijk het doel en de middelen van de verwerking van de persoonsgegevens vast te stellen. Nuancering is dat het moet gaan om de aspecten die van wezenlijk belang zijn.[11] Meestal stelt de school – zoals hiervoor reeds aangestipt - de punten die van wezenlijk belang zijn niet zelf vast. Scholen weten vaak wel dat door leveranciers persoonsgegevens van de leerlingen zullen worden verwerkt, maar door het ontbreken van kennis en informatie over welke persoonsgegevens er worden verwerkt en voor welke doeleinden, is de school niet in staat feitelijk zeggenschap uit te oefenen over welke persoonsgegevens worden verwerkt en voor welke doeleinden. In de meeste gevallen zal de aanbieder van de digitale leermiddelen het doel en middelen van de verwerking van de persoonsgegevens van de leerlingen vaststellen. Als gevolg dient op basis van de Wbp de aanbieder als verantwoordelijke te worden aangemerkt. Op deze aanbieder rusten in de praktijk dan ook de verplichtingen zoals die jegens de betrokkene (leerling) op basis van de Wbp in acht moeten worden genomen (en niet op de school).

Allereerst is van belang de hoofdrolspelers in de Wbp goed voor ogen te hebben. Dat zijn er feitelijk twee: de betrokkene en de verantwoordelijke. De betrokkene is de natuurlijke persoon wiens persoonsgegevens worden verwerkt. In dit geval is dat de leerling. De verantwoordelijke is de natuurlijke persoon, rechtspersoon, het bestuursorgaan of ieder ander die het doel van en de middelen voor verwerking van de persoonsgegevens vaststelt. Het convenant benoemt de onderwijsinstelling als 'verantwoordelijke'.

Het convenant probeert dit te doorbreken door het vaststellen van het doel van, en de middelen voor, de werking van de persoonsgegevens van de leerlingen tot de verantwoordelijkheid van de scholen te maken. De formele taakverdeling zoals tussen partijen overeengekomen in het convenant is echter niet beslissend[12], beslissend is de feitelijke situatie. De school wordt uitsluitend als verantwoordelijke aangemerkt wanneer de school in staat is feitelijke zeggenschap uit te oefenen over de aard van de gegevensverwerking en kan bepalen welke persoonsgegevens voor welke doeleinden worden verwerkt. Als hier in de praktijk geen invulling aan wordt gegeven is de school geen verantwoordelijke, de afspraken in het convenant ten spijt.

De aanbieder zal de school in staat moeten stellen haar rol als verantwoordelijke te vervullen. Dat is de reden dat in artikel 3 lid 2 van het convenant is bepaald dat de aanbieder voorafgaand aan de aanvang van de dienstverlening de school dient te informeren met betrekking tot de verwerking van de persoonsgegevens en de keuzes die de school daarbij heeft. Het is vervolgens aan de school om aan te geven met welke verwerking van persoonsgegevens en daarbij behorende diensten zij in het kader van het gebruik van de digitale leermiddelen akkoord gaat. Als dat het geval is verwordt de aanbieder tot bewerker; hij voert de verwerkingen uit overeenkomstig de doelen en middelen zoals die door de school zijn vastgesteld. De initiatiefnemers van het convenant hebben gekozen om de verantwoordelijkheid aan de school toe te wijzen op basis van een beoordeling van de feitelijke omstandigheden met betrekking tot de contractuele verhoudingen tussen de school en de aanbieder van de digitale leermiddelen. Daarmee wordt beoogd de contractuele verhoudingen tussen partijen zodanig om te buigen dat niet de aanbieder van de digitale leermiddelen maar de school als verantwoordelijke wordt aangemerkt. Naast de feitelijke vaststelling zijn er een tweetal andere categorieën op basis waarvan kan worden vastgesteld dat een instantie als verantwoordelijke voor de verwerking moet worden aangemerkt.[13] Deze twee categorieën zijn in het convenant buiten beschouwing gelaten door de initiatiefnemers.

De keuze die thans is gemaakt om op basis van de feitelijke omstandigheden de verantwoordelijkheid bij de school neer te leggen (in

plaats van bij de aanbieders) is naar de mening van auteurs om twee redenen voor discussie vatbaar.

Allereerst is de beoordeling of een school als verantwoordelijke kan worden aangemerkt sterk casuïstisch. Zo veronderstelt het vereiste om doel en middelen vast te stellen een bepaalde keuzevrijheid bij de school. Ook in de toelichting bij het convenant is door de initiatiefnemers gesteld dat indien een school een afweging en keuze met betrekking tot het doel en de middelen van de verwerking niet voldoende kan maken, de kans bestaat dat niet de school maar de aanbieder als verantwoordelijke moet worden aangemerkt. Er moet kennelijk dus ook iets te kiezen zijn.[14] Maar wat als die keuze er niet is omdat het aangeboden digitale leermiddel geen opties biedt? Stel: er is door gebruik van een digitaal leermiddel simpelweg sprake van verwerking van bepaalde persoonsgegevens voor een aantal doelen en daar kan niets aan gekozen of gewijzigd worden. Indien een school dat digitale leermiddel vervolgens inkoopt, is er dan sprake van vaststelling van doel en middelen door de school? De praktijk zal dat moeten uitwijzen. De auteurs betwijfelen of in dat geval de school wel als verantwoordelijke kan worden aangemerkt. De school weet in een dergelijke situatie welke verwerkingen plaatsvinden maar van vaststellen is geen sprake. Er is in dit verband ook denkbaar dat wordt geoordeeld dat als gevolg van een te beperkte informatieverstrekking en daarmee een te beperkt inzicht in de aard van de gegevensverwerking en daarmee dus onvoldoende feitelijke zeggenschap, de school en aanbieder gezamenlijk als verantwoordelijke voor de verwerking moeten worden aangemerkt.

De beoordeling of een school als verantwoordelijke kan worden aangemerkt is sterk casuïstisch. Zo veronderstelt het vereiste om doel en middelen vast te stellen een bepaalde keuzevrijheid bij de school. Er moet kennelijk dus ook iets te kiezen zijn. Maar wat als die keuze er niet is omdat het aangeboden digitale leermiddel geen opties biedt?

Een tweede aspect is - waar het convenant niet over rept, althans wat in het concept onderbelicht blijft – dat, naast het doel, ook de middelen voor de verwerking door de school moeten worden vastgesteld. Bij het vaststellen van de middelen gaat het naast de technische en organisatorische wijze (o.a. welke hardware en software?) waarop persoonsgegevens worden verwerkt ook over het "hoe" van de verwerking, waartoe onder andere de vragen behoren als "welke gegevens moeten worden verwerkt?", "welke derden moeten toegang tot de gegevens hebben?", "wanneer moeten gegevens gewist worden?", enz. Bij de beoordeling of een partij verantwoordelijke is voor de vaststelling van de middelen dient gekeken te worden naar de wezenlijke aspecten van de middelen. Het betreft de keuzes te maken over het "hoe" van de verwerking. Aangenomen wordt dat de technische en organisatorische middelen door de bewerker kunnen worden vastgesteld zonder dat dat consequenties heeft voor de vraag wie verantwoordelijke is. In die gevallen – waarin de doelen goed zijn omschreven, maar weinig of geen aanwijzingen worden gegeven over technische en organisatorische middelen – moeten de gestelde doelen redelijkerwijs met de middelen kunnen worden bereikt en behoort de verantwoordelijke volledig op de hoogte te zijn gebracht van de gebruikte middelen.[15] [16] Uit het convenant is niet op te maken dat aan een dergelijke informatieplicht wat betreft de technische en organisatorische middelen moet worden voldaan door de aanbieder. De informatieplicht zoals verwoord ziet op de informatie te verstrekken aan de school om voldoende tot afweging en keuze van gegevensverwerking te komen en niet om de (vastliggende) keuzes die de aanbieder heeft gemaakt ten aanzien van de technische en organisatorische middelen volledig aan de school te communiceren. Het convenant schiet hier in de ogen van auteurs tekort.

Vorenstaande onduidelijkheid - en daarmee onzekerheid voor scholen (en aanbieders) - zou in een klap weggenomen kunnen worden indien bij wet zou worden vastgesteld dat de school verantwoordelijke is voor verwerkingen van persoonsgegevens van leerlingen met gebruikmaking van digitale leermiddelen. De specifieke feiten en omstandigheden doen dan niet meer ter zake. Op de school zou in zoverre dan een risicoaansprakelijkheid komen te rusten waarbij het aan de school is om te zorgen dat zij dat risico – door afspraken met de aanbieders – zoveel mogelijk onder controle houdt.

1.2 Naleving verplichtingen Wbp (artikel 3 lid 3)

Over artikel 3 lid 3 in het convenant zou eenvoudig kunnen worden heengelezen. Het bevat indirect echter een belangrijke vingerwijzing dat het convenant een beperkt bereik heeft. Het artikel benadrukt het belang dat partijen op de hoogte zijn van de verplichtingen op grond van de Wbp en die ook naleven. Er is dus ook nadrukkelijk nog een eigen verplichting van scholen en aanbieders om afwegingen te maken en dienovereenkomstig te handelen. Enkel met toepassing van het convenant (en de daarbij behorende bewerkersovereenkomst) zijn partijen er inderdaad niet. Het convenant voorziet alleen in een regeling met betrekking tot artikel 14 Wbp; de relatie tussen bewerker en de verantwoordelijke.

Weliswaar worden in het convenant ook zaken geregeld met betrekking tot andere verplichtingen uit de Wbp[17] maar deze zaken hebben uitsluitend betrekking op de verwerkingen die de aanbieder van de digitale leermiddelen doet ten behoeve van de school.[18] Het convenant (noch de modelbewerkersovereenkomst) regelen hoe de school heeft te handelen met betrekking tot de persoonsgegevens die zij zelf verwerkt als gevolg van het gebruik van de digitale leermiddelen. Ook de school zelf zal met betrekking tot deze gegevens in haar eigen systemen moeten zorgdragen voor onder andere de vertrouwelijkheid, bewaartermijnen, beveiliging, informatieplicht (opgenomen in artikel 7 van het convenant) en de waarborging van de (privacy)rechten van de leerling. Daarnaast zal de school - als verantwoordelijke - een juiste invulling moeten geven aan de (kern) verplichtingen zoals opgenomen in artikel 6 Wbp (behoorlijke en zorgvuldige verwerking van persoonsgegevens), artikel 7 Wbp (de doeleinden voor verwerking), artikel 8 (de grondslagen voor verwerking) en artikel 9 (verenigbaar gebruik gegevens. Het enkel hanteren van het convenant zorgt dan ook zeker niet voor een garantie dat persoonsgegevens rechtmatig worden verwerkt.

1.3 Doeleinden voor verwerking (artikel 5)

Verwerking van persoonsgegevens van een betrokkene door een verantwoordelijke kan slechts rechtmatig zijn als daarvoor *'welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden'* voor aanwezig zijn (artikel 7 Wbp).[19]

Het convenant geeft in artikel 5 lid 1 een opsomming van doeleinden voor verwerking. Aangenomen wordt dat de bedoeling is een 'bevoegdheid' toe te kennen en dat scholen vrij zijn een keuze uit de genoemde doeleinden te maken. Het convenant is hier echter niet duidelijk. Ook niet duidelijk is of de opsomming van doeleinden limitatief is. Gezien het doel en strekking van het convenant lijkt dit wel aannemelijk. Het convenant verdient op dit punt meer helderheid.[20] Het verdient dan ook aanbeveling om in het kader van de 'ontzorging' van de scholen artikel 5 van het convenant duidelijker te formuleren en aan te geven waar de grenzen liggen.

Behalve een doel voor gegevensverwerking dient de verantwoordelijke ook altijd te beschikken over een wettelijke grondslag om de persoonsgegevens te verwerken. Dit vloeit voort uit artikel 8 van de Wbp. Bij afwezigheid van één van beide is de verwerking van persoonsgegevens in strijd met de Wbp en dus verboden.

Iedere verantwoordelijke zal in staat zijn aan de wettelijke voorwaarde van het vaststellen van doeleinden te kunnen voldoen: het is een kwestie van het formuleren van een (gerechtvaardigd) doel. Dit ligt anders voor het vereiste van een wettelijke grondslag (rechtvaardigingsgrond) om de persoonsgegevens te kunnen verwerken. De Wbp kent namelijk slechts zes rechtvaardigingsgronden op basis waarvan persoonsgegevens mogen worden verwerkt.[21] In het kader van de verhouding tussen de school en de po- en voleerling zouden in de praktijk een viertal grondslagen in aanmerking kunnen komen:

a. de betrokkene heeft voor de verwerking zijn ondubbelzinnige toestemming verleend;
b. de verwerking is noodzakelijk om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
c. de verwerking is noodzakelijk voor de goede vervulling van een publiekrechtelijke taak door het betreffende bestuursorgaan;
d. de verwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

Het convenant geeft aan dat er verschillende grondslagen zijn maar werkt dit niet uit. Het convenant geeft als voorbeeld van een grondslag genoemd onder b)[22] de in de WEC neergelegde verplichting voor het voortgezet speciaal onderwijs een leerlingvolgsysteem te hebben. Bij de meeste verwerkingen door middel van digitale leermiddelen zal een wettelijke verplichting echter niet aan de orde zijn. In deze gevallen zal de school een andere grondslag moeten hebben voor de verwerking. De toelichting op het convenant suggereert dat grondslag d)[23] in sommige gevallen uitkomst kan bieden. Deze suggestie gaat eraan voorbij dat deze grondslag in wezen een soort restbepaling is zonder sluitende begrenzing. Bovendien worden hoge eisen gesteld aan dit gerechtvaardigd belang. De verwerking is uitsluitend toelaatbaar indien zij noodzakelijk is met het oog op belang van de verantwoordelijke of een derde én het belang van de betrokkene niet prevaleert. Artikel 8 sub f Wbp impliceert een motiveringsplicht voor de verantwoordelijke. Deze dient voor zichzelf verschillende vragen te beantwoorden, zoals:

- Is er werkelijk een belang dat verwerking van persoonsgegevens rechtvaardigt?
- Wordt met de verwerking een inbreuk gemaakt op belangen of fundamentele rechten van degene wiens gegevens worden verwerkt en zo ja, dient dan - afhankelijk van de ernst van de inbreuk - gegevensverwerking niet achterwege te blijven?
- Kan het doel dat met de verwerking wordt nagestreefd ook langs andere weg zonder verwerking - worden bereikt?
- Is de verwerking in de mate die is beoogd evenredig aan het nagestreefde doel?

Kunnen de belangen van betrokkene anderszins of met minder ingrijpende middelen worden gediend, dan is de voorgenomen gegevensverwerking niet toegestaan. De noodzakelijkheidseis die in artikel 8 van de Wbp besloten ligt, veronderstelt dat de verantwoordelijke een bevredigende afweging maakt in dit kader. Desgevraagd dient deze afweging ook zichtbaar te worden gemaakt, zodat zij door de rechter kan worden getoetst.

Veel digitale leermiddelen zullen deze strenge toets van het noodzakelijkheidsvereiste niet kunnen doorstaan.[24] Immers, ook zonder de betreffende digitale leermiddelen kan nog steeds onderwijs en begeleiding worden gegeven. In dat geval rest voor de school voor de verwerking van leerlinggegevens feitelijk nog maar één grondslag, te weten de uitdrukkelijke toestemming van de (ouders van de) leerling. De toelichting bij het convenant noemt deze grondslag niet.[25]

– *Informatieplicht (artikel 7 lid 1)*

In het convenant is de (algemene) verplichting opgenomen om (ouders van) leerlingen te informeren (artikel 7 lid 1). De bepaling bepaalt echter niet waarover scholen hen precies dienen te informeren. Op grond van artikel 33 en 34 Wbp dient een school ten eerste aan de (ouders van de) leerlingen i) haar identiteit kenbaar te maken en ii) de doeleinden van de verwerking. Dit zal door de opstellers van het convenant zijn beoogd bij de formulering van de plicht om te informeren. Het verdient aanbeveling dat het convenant op dit punt wordt verduidelijkt zodat hier voor scholen geen onduidelijkheid kan ontstaan. Zeker niet nu - waarover hieronder meer – als gevolg van de wijziging van de Wbp per 1 januari 2016 tevens op overtreding van de informatieplicht een (substantiële) bestuurlijke boete kan worden gesteld door het CBP.

Duidelijker is het tweede deel van de bepaling: ook geïnformeerd dient te worden over de maatregelen die zijn getroffen om de privacy van de leerlingen te waarborgen. Dat handelt dus over welke persoonsgegevens worden verwerkt, bewaartermijnen die worden gehanteerd en de technische en organisatorische beveiligingsmaatregelen die zijn genomen.

Duidelijker is het tweede deel van de bepaling: ook geïnformeerd dient te worden over de maatregelen die zijn getroffen om de privacy van de leerlingen te waarborgen. Dat handelt dus over welke persoonsgegevens worden verwerkt, bewaartermijnen die worden gehanteerd en de technische en organisatorische beveiligingsmaatregelen die zijn genomen. Ook dient de school de leerlingen nadere informatie te verstrekken voor zover dat - gelet op de aard van de persoonsgegevens, de omstandigheden waaronder zij worden

verkregen of het gebruik dat ervan gemaakt wordt -, nodig is om tegenover de leerling een behoorlijke en zorgvuldige verwerking te waarborgen. Gezien de gevoeligheid van de persoonsgegevens die worden verwerkt van de leerlingen en de wijze waarop zij worden verkregen, namelijk door middel van het gebruik van digitale leermiddelen en vervolgens de analyse daarvan, lijkt specifieke informatieverstrekking aan de leerlingen noodzakelijk. Artikel 7 lid 1 van het convenant bepaalt terecht dat ouders geïnformeerd moeten worden over de maatregelen die zijn getroffen om de privacy van de leerlingen te waarborgen.

1.4 Meldingsplicht (artikel 7 lid 3)

Een belangrijke administratieve verplichting van een verantwoordelijke is melding van de verwerking(en) bij de AP.[26] Daar waar voorafgaand aan de verwerking gemeld had moeten worden maar niet (tijdig) is gemeld, is sprake van overtreding van deze verplichting, welke overtreding kan leiden tot het opleggen door de AP van een bestuurlijke boete (artikel 66 Wbp). Artikel 7 lid 3 van het convenant voorziet in een verwijzing naar die wettelijke verplichting .

"De Onderwijsinstelling onderzoekt of de Verwerking van Persoonsgegevens in de zin van het Convenant valt onder een wettelijke meldingsplicht, en draagt zorg voor een eventuele melding."

Onderbelicht in deze bepaling is dat melding hoofdregel is en dat van melding alleen is vrijgesteld een aantal in de dagelijkse praktijk veel voorkomende en gebruikelijke verwerkingen. Deze vrijgestelde verwerkingen zijn limitatief opgenomen in het Vrijstellingsbesluit Wbp.[27] Vrijgesteld van melding zijn op basis van artikel 19 Vrijstellingsbesluit – voor zover in dit kader relevant - verwerkingen die slechts plaatsvinden (zakelijk weergegeven) voor:

a. de organisatie of het geven van het onderwijs;
b. de begeleiding van leerlingen, deelnemers of studenten of het geven van studieadviezen;
c. het verstrekken of ter beschikking stellen van leermiddelen;
d. het bekend maken van informatie over de hierboven genoemde organisatie en leermiddelen, alsmede informatie over de leerlingen, deelnemers of studenten op de eigen website;
e. het bekendmaken van de activiteiten van de instelling of het instituut op de eigen website.

De vraag is nu of de verwerkingen die de school laat uitvoeren op basis van het gebruik van de digitale leermiddelen vallen onder *'het geven van het onderwijs', 'begeleiding van leerlingen, deelnemers of studenten' en/of 'het geven van studieadviezen'*. Dat zal feitelijk van geval tot geval moeten worden beoordeeld op basis van de specifieke verwerkingen die plaatsvinden. Zonder meer kan worden gesteld dat toegestane doeleinden zeer ruim zijn geformuleerd. Dat houdt dan niet direct in dat daarmee de bepalingen zeer breed toepasbaar zijn als gevolg van de huidige technologische ontwikkelingen.[28]

Indien de persoonsgegevens van de leerlingen voor alle doeleinden genoemd in artikel 5 lid 1 van het convenant worden toegepast dan is zonder meer duidelijk dat de school een melding zal moeten doen bij de AP ten aanzien van enkele van de verwerkingen. Onderzoek en analyse van persoonsgegevens van de leerlingen ten behoeve van (het optimaliseren van) het leerproces of het beleid van de school, lijken te ver verwijderd van de beoogde verwerking als genoemd in artikel 19 van het Vrijstellingsbesluit. Hetzelfde geldt naar de mening van auteurs in ieder geval voor de beoordeling van de leer- en toetsresultaten van één leerling ten opzichte van een normgroep, om inzicht te krijgen hoe een leerling presteert ten opzichte van deze groep. Melding van de verwerking voor deze doeleinden zou om die reden moeten plaatsvinden door een school.[29]

Een belangrijke administratieve verplichting van een verantwoordelijke is melding van de verwerking(en) bij de AP. Daar waar voorafgaand aan de verwerking gemeld had moeten worden maar niet (tijdig) is gemeld, is sprake van overtreding van deze verplichting, welke overtreding kan leiden tot het opleggen door de AP van een bestuurlijke boete.

Wordt door de school gekozen om niet te melden, is het aan te bevelen om de onderbouwing om niet te melden duidelijk vast te leggen en te documenteren zodat in een mogelijke toekomstige discussie met de AP inzage kan worden gegeven in de overwegingen die aan het besluit om niet te melden ten grondslag hebben gelegen.[30]

2. Wet uitbreiding bestuurlijke boetebevoegdheid

Gelijktijdig met de Wet Meldplicht Datalekken[31] is op 1 januari 2016 de Wet uitbreiding bestuurlijke boetebevoegdheid CBP ingevoerd. De wetgever heeft de AP in geval van overtreding van de Wbp in veel meer gevallen de mogelijkheid gegeven (hogere) boetes op te kunnen op te leggen. Onder het oude regime was de AP in drie gevallen - die alle betrekking hebben op de meldplicht bij de AP - gerechtigd een bestuurlijke boete op te leggen.[32] De boete werd dus feitelijk verschuldigd indien niet is voldaan aan de administratieve verplichting tijdig en correct te melden. De AP kon maximaal een boete opleggen van € 4.500,00. Als gevolg van de wetswijziging verandert dit rigoureus: bij overtreding van een groot deel van de bepalingen uit het Wbp kan het AP voortaan een bestuurlijke boete opleggen. Dit ziet dus op de bepalingen die in dit artikel de revue zijn gepasseerd en waar de school als verantwoordelijke aan dient te voldoen. Daarbij komt dat de hoogte van de boetes in sommige gevallen kunnen oplopen tot € 810.000,00 (of, als dat bedrag hoger is, 10% van de jaaromzet van de verantwoordelijke).[33] Deze wetswijziging vergroot derhalve alleen maar het belang van een correcte en volledig convenant en bijbehorende bewerkersovereenkomst omdat overtreding van het Wbp in meer gevallen en tot hogere boetes kan leiden.[34] Zeker nu de praktijk heeft uitgewezen dat de AP met de Snappet-zaak heeft laten zien de rechtmatige verwerking van persoonsgegevens van leerlingen met gebruik van digitale leermiddelen in het oog te houden.

3. Doorgifte persoonsgegevens buiten EER

In dit verband verdient ook aandacht een recente uitspraak van het Europese Hof van Justitie (EHJ). In deze uitspraak heeft het Europese Hof bepaald dat met onmiddellijke ingang de doorgifte van persoonsgegevens naar partijen in de Verenigde Staten (VS) per direct niet langer is toegestaan. Door de Europese Commissie was al eerder bepaald dat doorgifte van persoonsgegevens naar par-

tijen in de VS uitsluitend mogelijk is indien deze de 'Safe Harbor principes' hebben aanvaard. Deze garanderen dat er een passend beschermingsniveau voor die gegevens is.[35] Het EHJ heeft echter met haar uitspraak de 'Safe Harbor beschikking' van de EU Commissie ongeldig verklaard, tenzij op een andere manier de bescherming van privacy voldoende is gewaarborgd.[36]

Deze uitspraak heeft verstrekkende gevolgen, ook voor scholen en uitgevers. Zij mogen persoonsgegevens van de leerlingen dus niet (langer) zomaar doorgeven naar de VS. Die doorgifte is ook aan de orde als de uitgever de persoonsgegevens via Gmail, Hotmail, Messenger, Dropbox, Whatsapp en/of WeTransfer zou verzenden aan de school (en omgekeerd natuurlijk). De servers van deze diensten staan namelijk in de VS.[37] Dit geldt overigens ook als de school zelf deze diensten intern zou gebruiken voor het verzenden van persoonsgegevens van leerlingen (bijvoorbeeld van docent naar docent).

Is verzending naar een server in de VS niet langer mogelijk? Dat niet. Er kan gebruik gemaakt worden van door de Europese Commissie opgestelde modelovereenkomsten. Deze overeenkomst zal dan met de Amerikaanse partij (eigenaar van de servers) gesloten moeten worden. De vraag is echter of zo een partij bereid is een overeenkomst met de inhoud van die van de modelovereenkomst af te sluiten.[38] Ondertussen is het wachten welke oplossing er vanuit de EU en de VS gevonden wordt om dit manco op te lossen. Waakzaamheid op dit punt is voor de school in de tussentijd het devies.

4. Conclusies en aanbevelingen

Voor zover scholen zich nog onvoldoende bewust waren van hun rol als hoeder van de privacy van hun leerlingen en dan met name met betrekking tot de verwerkingen die plaatsvinden bij het gebruik van digitale leermiddelen, zorgt het convenant wel voor het bewustzijn dat leerlinggegevens gevoelige materie zijn, en ook tussen de schoolmuren adequate bescherming behoeven. Met die bewustwording komt mogelijk bij de school ook een gevoel van zorg om de hoek kijken. Bewustwording impliceert namelijk nog niet dat door de school de privacywetgeving correct kan worden uitgevoerd en toegepast. Het convenant zal niet steeds als 'ontzorgend' worden ervaren. Ten onrechte kan bij scholen de indruk ontstaan dat zij door het convenant te volgen en de bewerkersovereenkomst te gebruiken voldoen aan alle verplichtingen op grond van de Wbp. Dit is nadrukkelijk niet het geval. Een enkele ondertekening van de bewerkersovereenkomst (inclusief ingevulde bijlagen) volstaat in ieder geval niet. De feitelijke situatie dient aan te sluiten bij de veronderstelde uitgangspunten in het convenant. Dat is zoals in het artikel is uiteengezet niet altijd even gemakkelijk. Een school dient als verantwoordelijke daarnaast op vele andere vlakken te schakelen en afwegingen te maken op het gebied van de waarborging van de privacy van de leerlingen. Het convenant beoogt enkel in de verhouding met de aanbieder van de digitale leermiddelen een standaard te bieden en kent daarom een beperkte reikwijdte als het gaat om gegevensbescherming van leerlingen. Het convenant is daarin naar de mening van de auteurs niet voldoende toereikend. Onbewuste overtredingen van de Wbp ligt daardoor op de loer met het risico op een boete van het CBP.
In de huidige vorm voldoet het convenant niet volledig aan de eisen van de Wbp en lopen de gebruikers daarvan risico's. Aanbevolen wordt aan de opstellers het convenant (en de bewerkersovereenkomst) in overeenstemming te brengen met de Wbp en het convenant te voorzien van een uitgebreidere toelichting. Concrete handvatten voor de wijze waarop invulling kan worden gegeven aan de overige verplichtingen van de Wbp is in dit verband geen overbodige luxe. Gepleit wordt ten slotte voor een aanvulling in de 'bijsluiter' bij de bewerkersovereenkomst, waarin wordt gewaarschuwd voor het feit dat bij de toepassing van de Wbp de feitelijke situatie leidend is en niet de contractuele werkelijkheid. Indien voornoemde verbeteringen plaatsvinden zullen het convenant en de bewerkersovereenkomst de scholen daadwerkelijk kunnen gaan ontzorgen. Maar ook na deze verbeteringen zal de bewerkersovereenkomst steeds op de specifieke situatie moeten worden aangepast en nageleefd. Geadviseerd wordt dit te doen in samenspraak met een Wbp kundig specialist.

Noten

1. Hoewel ook over het model bewerkersovereenkomst veel valt te zeggen beperken de auteurs zich in dit artikel tot bespreking van het convenant.
2. Via de software van Snappet werden bijvoorbeeld in 2014 dagelijks al 1,5 miljoen opgaven gemaakt door leerlingen, welke resultaten daarvan worden verwerkt.
3. De Autoriteit Persoonsgegevens is per 1 januari 2016 de nieuwe naam van het College bescherming persoonsgegevens (CBP).
4. Onderzoek CBP naar de verwerking van persoonsgegevens door Snappet, Rapport definitieve bevindingen d.d. 19 september 2014 College bescherming persoonsgegevens www.cpbweb.nl, blz. 52.
5. Onderzoek CBP naar de verwerking van persoonsgegevens door Snappet,Rapport definitieve bevindingen d.d. 19 september 2014 College bescherming persoonsgegevens www.cpbweb.nl.
6. Kamerbrief Onderwijs persoonlijker maken met moderne leermiddelen, 28 mei 2014, *Kamerstuk* 32 034, nr. 3.
7. Doorbraakproject' is een gezamenlijk initiatief van de PO-Raad, VO-raad en de ministeries van Onderwijs, Cultuur en Wetenschap en Economische Zaken met de aanbieders van digitale systemen (de vereniging Groep Educatieve Uitgeverijen, de Vereniging Digitale Onderwijs Dienstverleners en vereniging Koninklijke Boekverkopersbond).
8. http://www.rijksoverheid.nl/ministeries/ocw/documenten-en-publicaties/kamerstukken/2015/07/03/kamerbrief-over-privacy-en-informatiebeveiliging-in-het-primair-en-voortgezet-onderwijs.html.
9. Zie noot 8.
10. Zodra de bewerker dat wel zou gaan doen dan wordt hij zelf ook verantwoordelijke jegens de betrokkene voor die specifieke verwerking.
11. In de opinie van de Artikel 29-werkgroep, het onafhankelijke advies- en overlegorgaan van Europese privacytoezichthouders, wordt over de begrippen 'verantwoordelijke' en 'bewerker', toegelicht dat punten van wezenlijk belang door de verantwoordelijke dienen te worden vastgesteld. Het doel waarvoor gegevens worden verwerkt, de gegevens die moeten worden verwerkt, de duur van de opslag van de gegevens en de toegang tot de gegevens zijn punten van wezenlijk belang.
12. Zie Artikel 29-werkgroep WP 169, Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", 16 februari 2010, blz. 11.
13. Zie Artikel 29-werkgroep WP 169, Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", 16 februari 2010, blz. 12 en 13. Allereerst is dat de categorie waarbij de verantwoordelijkheid op basis van de wet aan een instantie wordt toebedeeld. Daarnaast is er de categorie waarbij de verantwoordelijk op basis van een impliciete bevoegdheid aan een instantie toekomt. Er is dan geen sprake van een toewijzing op basis van de wet of rechtstreeks voortvloeiend uit expliciete wettelijke bepalingen, maar wel op basis van juridische praktijken en traditionele rollen. Er is kennelijk door het Doorbraakproject nadrukkelijk niet voor gekozen om een school op grond van haar (juridische) positie ten opzichte van de leerlingen als

verantwoordelijke voor de verwerking van de gegevens van de leerlingen op basis van het gebruik van de digitale leermiddelen aan te merken. Naar de mening van de auteurs zou er wel basis aanwezig kunnen zijn om op basis van de traditionele verhouding tussen school en leerling, de school verantwoordelijk te achten.

14. Ook het CBP oordeelde in de 'Snappet'-zaak dat de school onvoldoende feitelijke zeggenschap had en daarom de aanbieder van de digitale leermiddelen als verantwoordelijke moest worden aangemerkt Zie 'Onderzoek CBP naar de verwerking van persoonsgegevens door Snappet', rapport definitieve bevindingen van 14 juli 2014 met corrigendum van 27 augustus 2014, juli 2014, blz. 43.
15. Zie Artikel 29-werkgroep WP 169, Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", 16 februari 2010, blz. 11.
16. De vraag is of in de praktijk de school volledig op de hoogte is van de technische en organisatorische middelen waarvan de aanbieder van de digitale leermiddelen gebruik maakt bij het verlenen van de diensten aan de school. Als dat niet het geval is, zou dat volgens de beredenering van de Artikel 29-werkgroep kennelijk moeten leiden dat de school niet als verantwoordelijke wat betreft de vaststelling van de middelen kan worden aangemerkt. Verder zal de school in ieder geval ook het "hoe" van de gegevensverwerking moeten vaststellen. Ligt dat echter (gedeeltelijk of op onderdelen) in handen bij de aanbieder van de digitale leermiddelen dan is de aanbieder voor dat deel van de verwerking dan (mede)verantwoordelijke.
17. Onder andere verplichtingen ten aanzien van doeleinden voor het gebruik van de persoonsgegevens (artikel 8 Wbp), bewaartermijnen (artikel 10 Wbp), kwaliteit van gegevens (artikel 11 Wbp), vertrouwelijkheid (artikel 12 Wbp), beveiliging (artikel 13 Wbp), informatieplicht (artikel 33 Wbp) en de rechten van de leerlingen (artikel 35 e.v. Wbp)
18. Het is de wettelijke plicht voor de verantwoordelijke om dat te regelen (artikel 15 Wbp).
19. De doelen waarvoor een verantwoordelijke de persoonsgegevens verwerkt kunnen feitelijk eindeloos zijn. Begrenzing vindt slechts plaats doordat de doeleinden gerechtvaardigd moeten zijn. De doeleinden dienen voorts duidelijk te zijn, noch te vaag of te ruim geformuleerd.
20. Zeker omdat het artikel niet bepaalt dat de verwerking van de gegevens 'uitsluitend' plaatsvindt voor de genoemde doeleinden en anderzijds artikel 5 lid 2 van het convenant bepaalt dat de persoonsgegevens nooit mogen worden verwerkt voor reclamedoeleinden en het doen van aanbiedingen door de aanbieders. Beide bepalingen tezamen lijken dan ook ruimte te bieden voor de uitleg dat toepassing voor andere doeleinden dan genoemd in artikel 5 lid 1 van het convenant mogelijk zou moeten zijn (als het maar niet voor reclamedoeleinden en het doen van aanbiedingen is).
21. Artikel 8 Wbp
22. Artikel 8 sub c Wbp
23. Artikel 8 sub f Wbp
24. Zeker nu met deze verwerking bijzondere persoonsgegevens worden verwerkt wat het belang van een leerling op respectering van zijn privacy alleen maar groter maakt.
25. In de Snappet-kwestie werd door het CBP geoordeeld dat er voor Snappet maar twee grondslagen zouden kunnen dienen als rechtvaardiging voor de verwerkingen van Snappet (als verantwoordelijke). Het betrof de grondslagen genoemd onder a) en d). Aan de voorwaarden van beide grondslagen kon niet worden voldaan zodat de verwerking van de persoonsgegevens door Snappet onrechtmatig was.
26. Het formulier om de verwerking te melden is te vinden op www.cbpweb.nl/nl/melden/meldingsprogramma.
27. Een belangrijke beperking van het Vrijstellingsbesluit is dat het alleen van toepassing is op verwerkingen waarbij slechts één verantwoordelijke is betrokken (artikel 2 Vrijstellingsbesluit). Voor zover de aanbieder van de digitale leermiddelen ten aanzien van een aantal verwerkingen, dan wel de vaststelling van de middelen, zou moeten worden aangemerkt als medeverantwoordelijke, vindt het Vrijstellingsbesluit geen toepassing. De school moet in dat geval altijd de verwerking melden bij de AP.
28. Ter illustratie geldt hiertoe dat in 2012 op onderdelen het Vrijstellingsbesluit is herzien door de wetgever. De verwerkingen genoemd onder artikel 19 d) en e) – derhalve verwerkingen met betrekking tot de organisatie van het onderwijs en verstrekken van leermiddelen (als bedoeld onder a) en b)) op de eigen website van de school - zijn toen toegevoegd aan de verwerkingen die van melding zijn vrijgesteld. Anders beredeneerd: de ruime normen als geformuleerd onder a) en b) werden door de wetgever destijds niet toereikend geacht om tevens te kunnen dienen in het geval die gegevens (digitaal) op de website van de school zouden worden geplaatst.
29. Ook in de toelichting bij artikel 7 lid 3 van het convenant is door de opstellers zelf al opgemerkt dat voorheen de verwerkingen binnen de onderwijsinstellingen in de regel onder de vrijstellingen vielen, maar dat door het gebruik van digitale onderwijsmiddelen dit anders kan zijn.
30. Een andere optie is om de verwerking bij twijfel vrijwillig te melden bij de AP. Die mogelijkheid bestaat en voorkomt het risico op schending van artikel 27 Wbp en daarmee de dreiging van een bestuurlijke boete.
31. Als sprake is van een ernstig datalek, is de school sinds 1 januari 2016 verplicht dit binnen 72 uur te melden bij de AP. Indien daarnaast het datalek "*waarschijnlijk ongunstige gevolgen*" zal hebben voor de persoonlijke levenssfeer van de leerlingen, moet dit bovendien aan de (ouders van de) leerlingen zelf worden gemeld. Het moet dan gaan om schade aan de persoonlijke levenssfeer (artikel 34a Wbp).
32. Dit is bij overtreding van artikel 27, 28 en 79 lid 1 Wbp.
33. Artikel 66 lid 1 en 2 Wbp (nieuw) jo. artikel 23 Wetboek van Strafrecht.
34. Belangrijke nuancering is wel dat de AP een dergelijke boete enkel kan opleggen nadat zij eerst een bindende aanwijzing heeft gegeven aan de verantwoordelijke, tenzij de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid. Er zal dus aan de verantwoordelijke eerst een spreekwoordelijke 'corrigerende tik' moeten worden gegeven alvorens tot het opleggen van boetes kan worden overgegaan.
35. Beschikking van de Commissie van 26 juli 2000 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende Vaak gestelde vragen, die door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd, 2000/520/EG.
36. EHvJ 6 oktober 2015, zaaknr. C-362/14 (Schrems / Safe Harbor).
37. Ten aanzien van WeTransfer geldt dat zij aangeven dat de servers binnen en buiten Europa staan en dat het mogelijk is dat de bestanden in de VS op een server worden opgeslagen.
38. De partijen achter de diensten als in dit artikel genoemd zullen waarschijnlijk op individueel niveau niet bereid zijn dergelijke overeenkomsten aan te gaan.