AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens

Trends, risico's en aanbevelingen over de bescherming van persoonsgegevens bij digitalisering in het onderwijs

Bijdrage ten behoeve van het commissiedebat Digitalisering in het onderwijs, 11 november 2021

Vaste Kamercommissie Onderwijs, Cultuur en Wetenschap

November 2021

AUTORITEIT
PERSOONSGEGEVENS

Bijdrage ten behoeve van het commissiedebat Digitalisering in het onderwijs

De minister voor Basis- en Voortgezet Onderwijs en Media schrijft in zijn brief van 24 september 2021 aan de Kamer dat de randvoorwaarden voor privacy en informatiebeveiliging op orde dienen te zijn om de kansen van de voortschrijdende digitalisering van het onderwijs te kunnen benutten.[1]

Als onafhankelijk toezichthouder heeft de Autoriteit Persoonsgegevens (AP) de trends en risico's over de bescherming van persoonsgegevens in het onderwijs in kaart gebracht. Daarbij heeft de AP **zes aanbevelingen** gedaan, die verderop in dit document nader zijn toegelicht.

In gesprekken met de PO- en VO-raad, MBO Raad, Vereniging Hogescholen en de VSNU in 2021 heeft de onderwijssector aangegeven de trends, ontwikkelingen en aanbevelingen te herkennen. De onderwijssector is reeds aan de slag met de aanbevelingen van de AP, maar stelt ook dat om voldoende opvolging te kunnen geven aan een deel van de aan de sector gerichte aanbevelingen, **een faciliterende rol vanuit de overheid noodzakelijk is.** Op verzoek van de gesprekpartners in de onderwijssector brengt de AP haar bevindingen en aanbevelingen daarom in dit paper onder de aandacht van de Kamercommissie.

De AP heeft de minister voor Basis- en Voorgezet Onderwijs en Media en de minister van Onderwijs, Cultuur en Wetenschap bij brief van 31 mei 2021[2] reeds met klem geadviseerd om als stelselverantwoordelijke een pakket aan maatregelen te nemen. Door middel van deze maatregelen moet worden bewerkstelligd dat onderwijsinstellingen ook in de praktijk kunnen zorgdragen voor veilig onderwijs, omdat niet iedere onderwijsinstelling over voldoende kennis en middelen beschikt om de privacyrisico's van de inzet van digitale middelen in het onderwijs te mitigeren.

De AP is van mening dat de brief[1] van de minister nog onvoldoende duidelijk maakt op welke wijze er concreet invulling zal worden gegeven aan deze stelselverantwoordelijkheid. In het verlengde daarvan maakt de AP zich zorgen over de vraag of onderwijsinstellingen in staat zijn om opvolging te kunnen geven aan de aanbevelingen van de AP. Zolang niet voldoende duidelijk is welke partij de regie dient te pakken bij welke vraagstukken loopt de sector een groot risico dat het recht op bescherming van persoonsgegevens van leerlingen in het geding komt.

De AP verzoekt de Kamercommissie dan ook:

- Om kennis te nemen van de aanbevelingen van de AP.
- De ministers op te roepen om voor onderwijsinstellingen inzichtelijk te maken welke verantwoordelijkheden zij individueel dienen in te vullen, waar in gezamenlijkheid zal worden opgetreden en waar de overheid een faciliterende en aanjagende rol oppakt.
- De ministers op te roepen om concreet invulling te geven aan de aanvullende coördinerende en ondersteunende maatregelen die vanuit de overheid nodig zijn om de bescherming van persoonsgegevens van leerlingen en studenten in het digitaliserende onderwijs te borgen.

Hieronder licht de AP de trends, risico's en aanbevelingen voor de onderwijssector toe. Deze zijn gebaseerd op gesprekken van de AP met functionarissen gegevensbescherming, koepelorganisaties en kennis van onze inspecteurs.

[1] Kamerstuk 31293, nr. 593
[2] Bijlage van Kamerstuk 32034, nr. 40

Inleiding

Onze samenleving digitaliseert en het onderwijs kan daarin niet achterblijven. Technologie en digitalisering bieden veel kansen in deze sector, maar brengen ook risico's met zich mee. Zo creëren onderwijsinstellingen steeds meer datastromen met (gevoelige) informatie over leerlingen en studenten. Onderwijsinstellingen vervullen een maatschappelijke taak en hebben een zorgplicht voor de kwaliteit van het onderwijs. Dit vraagt dat scholen zorgvuldig omgaan met de persoonsgegevens van leerlingen, studenten en ouders die aan hun zorg zijn toevertrouwd. De kwetsbare positie van kinderen vereist bovendien dat zij extra beschermd worden, zodat zij zich in een vrije en veilige (school)omgeving kunnen ontwikkelen. Dit maakt de bescherming van persoonsgegevens in de onderwijssector essentieel.

Dit paper gaat over het primair onderwijs, voortgezet onderwijs, speciaal (voortgezet) onderwijs, (middelbaar) beroepsonderwijs en het hoger onderwijs. De instellingen in deze subsectoren verschillen niet alleen qua omvang, capaciteit en beschikbare middelen, maar ook qua type leerlingen/studenten. Hoewel de AP spreekt van dé sector onderwijs, is het dus van belang te benoemen dat de diversiteit binnen de sector en tussen de subsectoren groot is.

Trends en risico's in de sector

1. **Monitoring van leerlingen en studenten**

Onderwijsinstellingen hebben steeds meer gegevens tot hun beschikking door de inzet van nieuwe toepassingen als adaptieve leermiddelen en *learning analytics*. Deze gegevens bevatten veel informatie over het gedrag en de ontwikkeling van leerlingen en studenten. Hieraan zijn risico's gekoppeld die de ontwikkeling van kinderen en jongeren kunnen schaden. Zoals verkeerde interpretatie of misbruik van deze gegevens. Recente grote datalekken in het onderwijs tonen aan dat de beveiliging van de gegevens van leerlingen en studenten extra aandacht verdient, omdat voorkomen moet worden dat (gevoelige) gegevens op straat komen te liggen. De AP ontvangt regelmatig klachten over de inzet van nieuwe digitale toepassingen waarbij niet duidelijk is wat er precies met persoonsgegevens van leerlingen of studenten gebeurt.

2. **Afhankelijkheid van grote leveranciers**

Veel essentiële zaken in het gedigitaliseerde onderwijs, zoals leerlingvolgsystemen en digitale leermiddelen, worden geleverd door grote (internationale) leveranciers. Door hun dominante positie kunnen die een zekere macht uitoefenen op de markt. Deze macht van grote leveranciers, hun gebrek aan transparantie en het gebrek aan kennis bij vooral de kleine onderwijsinstellingen maken het lastig om de juiste waarborgen voor gegevensbescherming te bepalen en indien nodig af te dwingen bij de leverancier.

3. **Meer uitwisseling van gegevens in samenwerkingsverbanden**

Onderwijsinstellingen verstrekken steeds vaker gegevens van leerlingen of studenten aan samenwerkingsverbanden en data- en informatieknooppunten waarbij verschillende (publieke) partijen zijn aangesloten. Het is hierbij van belang dat het voor leerlingen/ouders en studenten inzichtelijk blijft aan wie persoonsgegevens worden verstrekt, dat er niet meer gegevens worden verstrekt dan noodzakelijk en dat het belang van kinderen/jongeren altijd voorop staat.

Aanbevelingen van de AP aan de sector

1. Breng de basis op orde

- **Verhoog kennis en bewustzijn in alle lagen van het onderwijs**

Het verbeteren van de digitale geletterdheid van leerlingen, studenten en docenten zorgt ervoor dat zij beter in staat zijn om zelf privacyrisico's te beoordelen bij het gebruik van een nieuw softwareprogramma of een nieuwe app. Door de kennis en het bewustzijn onder het onderwijspersoneel in alle lagen binnen de onderwijsinstelling te vergroten, verbetert de sector de doorstroom van op bestuursniveau vastgesteld beleid naar andere lagen van de organisatie om zorgvuldig met persoonsgegevens om te gaan.

- **Houd documentatie up-to-date en voldoe aan de verantwoordingsplicht**

Veel onderwijsinstellingen denken de AVG-documentatie (zoals verwerkingsregister, verwerkersovereenkomsten, privacybeleid etc.) op orde te hebben. Uit gesprekken met de sector blijkt echter dat veel van deze documentatie toe is aan een evaluatie of update. Als een onderwijsinstelling intern niet kan verantwoorden welke persoonsgegevens worden verwerkt, dan zal de onderwijsinstelling dat ook niet kunnen aan leerlingen, ouders, onderwijspersoneel en toezichthouders wanneer zij vragen hebben over bepaalde gegevensverwerkingen. Koepel- en/of samenwerkingsorganisaties in het onderwijs kunnen hieraan bijdragen door de modellen en templates die zij aanbieden regelmatig te controleren en actualiseren.

- **Richt governance in en versterk de rol van de FG**

Om de vertaling van beleid en procedures van papier naar de praktijk te verbeteren, moeten onderwijsinstellingen taken, verantwoordelijkheden en bevoegdheden rondom gegevensbescherming helder beleggen en daar de benodigde capaciteit aan verbinden. Daarbij moeten zij in het bijzonder aandacht hebben voor de rol van de functionaris gegevensbescherming (FG). In veel gevallen krijgt de FG nog weinig de kans om zijn toezichtsrol adequaat in te vullen.

2. Versterk samen de positie van de onderwijssector in de digitale maatschappij

- **Breng proactief risico's van grote digitaliseringsthema's in kaart**

De AP raadt de sector aan om samen met sectorraden, koepel- en samenwerkingsorganisaties risico's in kaart te (blijven) brengen en te vertalen naar concrete handvatten en leidraden voor onderwijsinstellingen. Daarbij is naast aandacht voor de beveiliging van gegevens ook aandacht nodig voor maatschappelijke en ethische waarden, zoals autonomie, gelijkheid en betrokkenheid van studenten/leerlingen en docenten.

- **Verbeter de positie van de sector tegenover grote leveranciers**

De sector kan gezamenlijke eisen stellen en de onderhandelingspositie verbeteren door gezamenlijke risicoanalyses uit te voeren. Goede afspraken maken met leveranciers is een essentiële voorwaarde om de juiste waarborgen te treffen tegen privacyrisico's, vooral met leveranciers buiten de EER.

- **Zoek (verdere) samenwerking in de sector op**

Uit de gesprekken met de sector is gebleken dat er diverse netwerken ontstaan om kennis uit te wisselen over gegevensbescherming (en informatiebeveiliging), waaronder bij digitale toepassingen. De AP ziet dit als een positieve ontwikkeling, die kan helpen om de uitdagingen in de sector op te pakken.

Zelfreflectie vanuit de sector

Accountability, 'zelf verantwoordelijkheid nemen', is een groot thema in de AVG. Het betekent dat de wet voorschrijft dat organisaties moeten kunnen aantonen dat ze compliant zijn. Hiervoor is het nodig goed zicht te hebben op de eigen organisatie en waar de mogelijke risico's zich bevinden. Daarom is deze paragraaf gewijd aan hoe de organisaties zelf naar hun compliance kijken. Onderstaande is door de AP opgesteld op basis van de punten die zijn aangedragen tijdens de zelfbeeldgesprekken met (koepel)organisaties aan de hand van een enquêteformulier over accountability.[3] De punten zijn van toepassing op het hele onderwijsveld.

1. **Leiderschap en toezicht**
   - Privacy en security zijn terugkerende thema's op de agenda van de sectorraden in het onderwijs. De sectorraden proberen dit onderwerp op verschillende manieren onder de aandacht van schoolbesturen te brengen.
   - Gegevensbescherming is slechts een van de vele onderwerpen waar het schoolbestuur zich mee bezighoudt. Door beperkt budget en beperkte capaciteit varieert het betrokkenheidsniveau van schoolbesturen sterk tussen verschillende onderwijsinstellingen en subsectoren.
   - De kennis en het bewustzijn van en de betrokkenheid bij het gegevensbeschermingsbeleid in de directie- en managementlagen van veel onderwijsinstellingen is niet op niveau.

2. **Risicobeoordelingen**
   - Omdat de onderwijssector veel dezelfde softwarepakketten gebruikt, voeren onderwijsinstellingen steeds vaker gezamenlijke *data protection impact assessments* (DPIA's) uit. Hoewel de kwaliteit van DPIA's varieert in het onderwijs, komt de samenwerking tussen onderwijsinstellingen de kwaliteit van de DPIA's in alle subsectoren ten goede.
   - Voor met name kleinere onderwijsinstellingen is het systematisch beoordelen en beperken van AVG-risico's een struikelblok. Dat komt onder andere door de vaak beperkte capaciteit en aandacht voor dit thema binnen de organisatie.
   - Voor veel onderwijsinstellingen is het een uitdaging om overzicht te houden op alle verwerkingen van persoonsgegevens. Door de autonome positie van docenten en de 'wildgroei' aan apps en software in het onderwijs is het voor onderwijsinstellingen lastig om controle te houden over de gegevensverwerkingen waarvoor zij verantwoordelijk zijn.

3. **Beleid en procedures**
   - Vrijwel alle onderwijsinstellingen hebben op papier regels en beleid opgesteld waarin de AVG-principes zijn vertaald. Onderwijskoepels, samenwerkingsorganisaties en sectorraden spelen een belangrijke faciliterende rol in het beschikbaar stellen van voorbeelden en handreikingen voor het opstellen van beleid en procedures.
   - Het omzetten van papier naar praktijk, bijvoorbeeld door middel van (werk)instructies voor personeel en controle, is een volgende stap die veel onderwijsinstellingen nog moeten zetten.

[3] De vragenlijst is gebaseerd op het CIPL-wheel on accountability, te vinden op www.informationpolicycentre.com.

4. **Transparantie**
    - De meeste onderwijsinstellingen hebben een algemene privacyverklaring en een privacyreglement opgesteld en beschikbaar gesteld aan betrokkenen (de mensen van wie gegevens worden verwerkt).
    - Onderwijsinstellingen worstelen met de balans tussen de volledigheid van hun privacyverklaring en de leesbaarheid ervan voor hun doelgroep. Dit speelt vooral bij de inzet van (nieuwe) digitale leermiddelen.

5. **Training en bewustzijn**
    - Over het algemeen is er een vooruitgang in kennis en bewustwording te zien rondom gegevensbescherming sinds de komst van de AVG.
    - Awareness wordt nog steeds gezien als verbeterpunt.

6. **Zelfmonitoring en -controles**
    - Op subsectorniveau zijn enkele self-assessments ontwikkeld of nog in ontwikkeling. Hoewel er nog wordt nagedacht over de vertaling van de uitkomsten en hoe deze instrumenten kunnen bijdragen aan de doelstellingen van de sector, zijn dit breed gedragen initiatieven. Binnen verschillende netwerken worden evaluaties met elkaar besproken en gedeeld om te leren van elkaar.
    - De opvolging van (zelf)evaluaties is voor sommige onderwijsinstellingen een punt van aandacht. Op directieniveau voelt men zich niet altijd verantwoordelijk voor het oppakken van de resultaten en verbeterpunten van de evaluatie. Een goede governance is daarom essentieel.

7. **Opvolging en handhaving**
    - Onderwijsinstellingen ontvangen over het algemeen weinig individuele AVG-verzoeken en klachten. Leerlingen en studenten kunnen al veel van hun eigen gegevens inzien via verschillende digitale onderwijsapplicaties. Ook gelden er standaardprocedures voor bijvoorbeeld het inzien van afgelegde toetsen en tentamens.