AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Aan de leden van de Eerste Kamercommissie
voor Digitalisering

Datum
20 februari 2024

Ons kenmerk
2024-12-AWO-HDO

Contactpersoon
Huib van Doorn

Onderwerp
Aanbieding Sectorbeeld Onderwijs

Geachte leden van de vaste commissie,

Als bijlage bij deze brief deel ik graag met u het Sectorbeeld Onderwijs van de Autoriteit Persoonsgegevens (AP) over de periode 2021-2023. In het sectorbeeld staat de AP stil bij de belangrijkste trends en ontwikkelingen op het gebied van privacy in de onderwijssector. De bescherming van persoonsgegevens in deze sector is essentieel, want we vertrouwen grote hoeveelheden soms (zeer) gevoelige persoonsgegevens aan onderwijsinstellingen toe: van medewerkers, ouders, en natuurlijk leerlingen en studenten. Kinderen hebben door hun kwetsbare positie bovendien extra bescherming nodig om zich in een vrije en veilige onderwijsomgeving te kunnen ontwikkelen.

Uit het Sectorbeeld Onderwijs volgt dat er door de onderwijssector goede stappen worden gezet om naleving van privacywetgeving in de sector te verbeteren. Toch ziet de AP dat er door de toegenomen inzet van digitale methoden, waaronder systemen met algoritmes & artificiële intelligentie (AI), mogelijkheden zijn voor verbetering. Daarom staat de AP in het sectorbeeld stil bij de maatregelen die onderwijsinstellingen nu al nemen, maar ook bij wat nodig is om de basis op orde te krijgen.

Daarnaast zouden wij u gezien de raakvlakken tussen het werk van de AP en uw commissie graag willen uitnodigen voor een kennismakingsgesprek of een werkbezoek aan de AP. Wij horen graag of u hiervoor openstaat.

Hoogachtend,
Autoriteit Persoonsgegevens,

Aleid Wolfsen
voorzitter

AUTORITEIT
PERSOONSGEGEVENS

Sectorbeeld Onderwijs

Uit dit sectorbeeld komt naar voren dat maatschappelijke uitdagingen ook privacyuitdagingen geven voor de onderwijssector, dat algoritmes & artificiële intelligentie (AI) nu vragen om nader beleid en een gesprek over de wenselijkheid ervan, dat er weinig grip is op software binnen onderwijsinstellingen en dat er nog veel onduidelijkheid is over het gebruik van persoonsgegevens voor wetenschappelijk onderzoek. Positief is dat de sector zich de afgelopen jaren sterk heeft ingezet om de privacycompliance te verhogen met zelfregulering en dat er steeds meer samenwerking is. Over het algemeen is de onderwijssector dan ook van goede wil om te voldoen aan de privacywetgeving. Dat neemt echter niet weg dat er nog steeds verbeteringen nodig zijn om de basis op orde te krijgen.

Vooraf

Onderwijsinstellingen moeten zorgvuldig omgaan met de aan hun zorg toevertrouwde persoonsgegevens van medewerkers, leerlingen/studenten en ouders. Kinderen hebben door hun kwetsbare positie bovendien extra bescherming nodig, zodat zij zich in een vrije en veilige (onderwijs)omgeving kunnen ontwikkelen. Dit maakt de bescherming van persoonsgegevens in de onderwijssector essentieel.

Over dit sectorbeeld

Met dit sectorbeeld analyseert de Autoriteit Persoonsgegevens (AP) de belangrijkste trends en ontwikkelingen op privacygebied in de sector Onderwijs. We kijken in dit verband met name naar de mate waarin het onderwijs voldoet aan de privacywet, de Algemene verordening gegevensbescherming (AVG) en de (mogelijke) consequenties daarvan voor betrokkenen: de kinderen, jongeren en volwassenen van wie onderwijsinstellingen persoonsgegevens verwerken.

Het sectorbeeld gaat over de periode 2021-2022, en deels over ontwikkelingen van begin 2023. De bevindingen zijn gebaseerd op informatie uit (thema)onderzoeken, AP-adviezen, ontvangen klachten, signalen, tips, vragen en op gesprekken in het toezichtsveld van de AP. Om dit beeld te verrijken hebben ook belanghebbenden, zoals sectororganisaties, het ministerie van Onderwijs, Cultuur en Wetenschap (OCW), functionarissen gegevensbescherming (FG's) en andere toezichthouders, gereflecteerd op de privacyuitdagingen die zij zien binnen de onderwijssector. Sommige informatie komt uit externe bronnen. Met dit sectorbeeld wil de AP waarnemingen, aandachtspunten en aanbevelingen delen en de inzet van de AP in de onderwijssector schetsen.

Dit sectorbeeld gaat over het bekostigde primair onderwijs, voortgezet onderwijs, (voortgezet) speciaal onderwijs, middelbaar beroepsonderwijs en hoger onderwijs. De instellingen in deze subsectoren verschillen niet alleen qua omvang, capaciteit en beschikbare middelen, maar ook qua type leerlingen/studenten. Hoewel we in dit sectorbeeld spreken van 'de' sector onderwijs, is de diversiteit binnen het onderwijsstelsel en tussen de subsectoren groot. Er bestaan dan ook geen algemene oplossingen voor de gehele onderwijssector.

In dit sectorbeeld gaat de AP eerst in op een aantal van de belangrijkste privacyuitdagingen in de onderwijssector. Vervolgens schetst de AP een aantal belangrijke ontwikkelingen van de afgelopen twee jaar die impact hebben (gehad) op de mate van AVG-compliance in de sector. In het derde hoofdstuk geeft de AP op basis van gesprekken met het onderwijsveld weer hoe de onderwijssector tegen de eigen mate van AVG-compliance aankijkt. In hoofdstuk 4 volgt de visie van de AP op de sector. In hoofdstuk 5 staat wat de AP de afgelopen twee jaar heeft gedaan in de onderwijssector en wat de AP nog gaat doen. Dit sectorbeeld sluit af met de verantwoording.

1. Trends in het onderwijsveld

De onderwijssector staat voor een groot aantal uitdagingen bij de bescherming van persoonsgegevens. Een aantal van de belangrijkste uitdagingen voor de hele onderwijssector schetst de AP in dit sectorbeeld. We noemen deze uitdagingen 'trends', omdat het uitdagingen zijn die al langere tijd spelen in de sector en die complexe (privacy)vraagstukken met zich meebrengen. Met name door de versnelde digitalisering sinds de coronapandemie hebben hybride werken en online onderwijs een vlucht genomen en is het belang van privacy alleen maar toegenomen.

Volledige zekerheid over wat 'het juiste' is, is bij deze trends niet vooraf te geven, ook niet door de AP. Daarom is het van belang dat onderwijsinstellingen afwegingen maken en vastleggen over de kansen en de risico's voor betrokkenen bij deze vraagstukken en daarin zo nodig ook de FG's betrekken. De sector kan ook *guidance* ontwikkelen of sectorbrede afspraken maken die raken aan deze trends. De AP staat ervoor open om hierbij – waar mogelijk –mee te denken.

Maatschappelijke uitdagingen dringen sterk door in het onderwijs

Onderwijsinstellingen vervullen een belangrijke maatschappelijke taak en staan middenin de samenleving. Onderwijs gaat immers niet alleen over het overbrengen van kennis; onderwijsinstellingen krijgen ook te maken met maatschappelijke kwesties. Bij steeds meer kwesties wordt verwacht dat zij daarop acteren. Voorbeelden daarvan zijn het psychisch welzijn van leerlingen en studenten, veiligheid, armoede, kansen(on)gelijkheid, polarisatie en het terugdringen van verzuim.

Ondanks deze verwachtingen en de vaak goedbedoelde intenties, is de vraag of er een AVG-grondslag is voor onderwijsinstellingen als zij persoonsgegevens (verder) verwerken voor bovengenoemde doeleinden, omdat de taak van onderwijsinstellingen op deze punten vaak (nog) niet duidelijk is omschreven in de wet. Zeker wanneer het gaat over zeer gevoelige persoonsgegevens, die onderwijsinstellingen soms registreren en delen met (publieke) organisaties. De AP ziet dat onderwijsinstellingen niet altijd goed analyseren of dit soort gegevensverwerkingen mogen en zo ja, onder welke voorwaarden. Daarnaast is het de rol van de wetgever om zo nodig voor nieuwe wetgeving te zorgen.

Grote kansen én risico's bij algoritmes & AI in het onderwijs

Door de opkomst van adaptieve leermiddelen en *learning analytics* hebben onderwijsinstellingen steeds meer gegevens tot hun beschikking over het gedrag en de ontwikkeling van leerlingen en studenten. Deze gegevens kunnen waardevolle inzichten en mogelijkheden bieden om meer gedifferentieerd onderwijs aan te bieden dat rekening houdt met de behoeften van individuele leerlingen en studenten. Daarnaast komt er steeds meer aanbod op de markt om geautomatiseerd toetsen te ontwikkelen en om leerlingen en studenten te beoordelen op basis van algoritmes en kunstmatige intelligentie (AI).[1] Ook kunnen

onderwijsinstellingen algoritmes inzetten voor het selecteren van studenten voor opleidingen of worden er algoritmes ontwikkeld en ingezet voor onderzoeksdoeleinden. Bovendien heeft ook het gebruik van generatieve AI door zowel leerlingen/studenten als onderwijspersoneel een grote impact op het onderwijs.[2]

Er zijn risico's bij het gebruik van dit soort gegevens en diensten die de ontwikkeling van leerlingen en studenten kunnen schaden. Denk aan verkeerde interpretatie van data, vooringenomenheid (bias) of het verlies van controle over persoonsgegevens.[3] Soms is de werking van deze systemen niet transparant, mede door de complexiteit van nieuwe vormen van AI. Ook ethische vraagstukken, zoals de autonomie van docenten, leraren, leerlingen en studenten, diversiteit en kansengelijkheid vragen hierbij de aandacht. Het is van belang om deze risico's waar geschikt ook te bespreken met leerlingen en studenten.

Vanwege de belangrijke maatschappelijk taak, doet de onderwijssector er goed aan om niet te wachten op de AI-verordening maar zich nu al voor te bereiden op aankomende normen bij het onderzoeken, ontwikkelen, implementeren of updaten van systemen of toepassingen. Hierbij hoort ook nadrukkelijk het gesprek over de wenselijkheid van de inzet van algoritmes in het onderwijs. De AP adviseert daarom om beleidsstrategieën en beheersingsprocessen voor algoritmes en AI in te richten binnen onderwijsinstellingen. Ook is het vergroten van AI-kennis onder leerkrachten en docenten een aandachtspunt om te zorgen voor een zorgvuldige inbedding en beheersing van algoritmes in het onderwijs.[4]

Onvoldoende overzicht door schaduw-ICT

Voor veel onderwijsinstellingen is het een uitdaging om overzicht te houden op alle verwerkingen van persoonsgegevens in de organisatie. Door onder andere de autonome positie van docenten om eigen software te gebruiken en de 'wildgroei' in het gebruik van (gratis) apps en software, is het voor onderwijsinstellingen lastig om controle te houden over de gegevensverwerkingen waarvoor zij verantwoordelijk zijn en ontstaat 'schaduw-ICT'.[5]

Hoewel het gebruik van apps en software nuttig kan zijn voor het onderwijs, mag dit niet ten koste gaan van de privacy van leerlingen, studenten en onderwijspersoneel. Persoonsgegevens kunnen immers in verkeerde handen vallen door een datalek of voor eigen doelen van leveranciers worden gebruikt. Onderwijsinstellingen, en met name schoolbesturen, zouden daarom instellingsbreed beleid moeten maken om deze software in beeld te krijgen en zo nodig maatregelen treffen, zodat het gebruik ervan verenigbaar is met de AVG.[6]

Nog veel onduidelijkheid over onderzoeksgegevens

Naast onderwijs speelt ook (wetenschappelijk) onderzoek een grote rol binnen de onderwijssector. Onderzoek is essentieel ter bevordering van de innovatie in de maatschappij en bij (wetenschappelijk) onderzoek kunnen ook persoonsgegevens worden verwerkt. De sector heeft daarbij te maken met een aantal uitdagingen.

Allereerst spelen er zorgen over anonimisering van gegevens. Anonimisering van persoonsgegevens is in de praktijk vaak moeilijk te realiseren, bijvoorbeeld vanwege de onderzoeksopzet. Daarnaast bestaat nog weleens het misverstand dat het hashen of pseudonimiseren van datasets ook een vorm van anonimiseren is. De AP benadrukt dat de AVG weliswaar bepaalt dat bij (wetenschappelijk) onderzoek de gegevens bij voorkeur geanonimiseerd zijn, maar dat dit geen verbod op het gebruik van niet-anonieme gegevens

betekent, mits de noodzaak daarvan kan worden onderbouwd. Ook gelden vanzelfsprekend alle andere vereisten van de AVG.

In de praktijk zijn er ook veel vragen over 'hergebruik' van persoonsgegevens voor (wetenschappelijk) onderzoek. Het gaat om zowel hergebruik van persoonsgegevens die (eerst) voor een ander doel zijn verzameld als hergebruik van persoonsgegevens verzameld voor een bepaald onderzoeksproject voor andere, nieuwe onderzoeksprojecten. Bij dergelijk hergebruik moet een instelling namelijk opnieuw bepalen op basis van welke grondslag uit de AVG dat kan. Ook is er een informatieplicht richting betrokkenen. Gebrek aan kennis, vaardigheden en bruikbare tools op dit vlak leveren vaak veel handelingsonzekerheid bij en tussen betrokken partijen op.

De AP constateert ook andere knelpunten bij samenwerkingen tussen verschillende instellingen op het gebied van onderzoek, zowel op nationaal als op internationaal niveau. Het bepalen van de AVG-rollen (verwerkingsverantwoordelijke, verwerker, gezamenlijke verwerkingsverantwoordelijken) in zulke samenwerkingsverbanden blijkt in de praktijk lastig, ook omdat lidstaten van de EU daar verschillend over denken. Onduidelijkheid over welke AVG-verplichtingen bij welke partij liggen, is te vermijden door hier zo vroeg mogelijk helderheid over te creëren en vast te leggen. Ook moet men, wanneer een van de betrokken partijen (inclusief softwareleveranciers en andere verwerkers) zich buiten de EER bevindt, alert zijn op de vereisten voor doorgifte van persoonsgegevens op grond van de AVG.

Partijen in de sector zijn gebaat bij meer specifieke, concrete handreikingen om met zulke kwesties om te gaan. De AP nodigt onderwijsinstellingen en FG's in de sector uit om met de AP het gesprek aan te gaan en samen te werken aan praktische guidance.

"Van de zandbak tot de collegebank: het onderwijs is de springplank om vorm te geven aan je leven. Te ontdekken wie je bent en je dromen waar te maken. En dat met behoud van de normen en waarden die we belangrijk vinden. Het serieus nemen van de privacy van leerlingen, studenten en onderwijspersoneel is daarbij essentieel, zodat het onderwijs ook daadwerkelijk de plek is waar je je vrij en beschermd kunt ontwikkelen."

- Katja Mur, bestuurslid van de AP

2. Ontwikkelingen 2021-2022

De laatste jaren is, mede naar aanleiding van cyberaanvallen bij enkele onderwijsinstellingen, de aandacht voor informatiebeveiliging en privacy in de sector flink toegenomen. De AP heeft in mei 2021 de ministers van OCW geadviseerd een coördinerende rol te nemen in de aanpak van gegevensbescherming binnen het onderwijs en *data protection impact assessments* (DPIA's) uit te (laten) voeren op veelgebruikte digitale middelen in het onderwijs.[7] De ministers van OCW hebben in juli 2022 aangekondigd in te zetten op de verhoging van digitale veiligheid in onderwijs en onderzoek.[8]

Sectorbrede kaders

Voor het funderend onderwijs ontwikkelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad een normenkader voor informatiebeveiliging en privacy.[9] Volgens de minister van OCW moeten in 2027 alle scholen in het funderend onderwijs aan het normenkader voldoen en zal er toezicht en

handhaving plaatsvinden.[10] Daarnaast zijn besturen in het funderend onderwijs per 2024 verplicht om in hun jaarverslag expliciet aandacht te besteden aan informatiebeveiliging en privacy.[11] FG's uit het funderend onderwijs reageren over het algemeen positief op de komst van het normenkader; het biedt houvast voor de gehele sector bij de vraag waar scholen aan moeten voldoen en welke maatregelen ze moeten treffen. Dat is wenselijk omdat het niveau van privacyvolwassenheid nog erg verschilt per onderwijsinstelling.

In SURF-verband wordt het toetsingskader privacy doorontwikkeld; een evaluatiemiddel dat onderwijsinstellingen in het hoger onderwijs en mbo helpt hun volwassenheidsniveau op het gebied van gegevensbescherming te bepalen.[12] Er is geen verplichting om te voldoen aan een bepaald volwassenheidsniveau van het toetsingskader. Wel is bijvoorbeeld het mbo van plan om een ambitieniveau in te stellen, waarbij alle onderwijsinstellingen gemiddeld een bepaald volwassenheidsniveau zouden moeten scoren op basis van het toetsingskader privacy.[13]

Hoewel er positief wordt gesproken over deze normenkaders, worden er wel zorgen geuit over de vraag of met name de kleine onderwijsinstellingen en besturen zonder extra mensen en middelen in staat zijn om te voldoen aan de normenkaders. Zelfs wanneer een instelling is aangesloten bij een samenwerkingsorganisatie als SURF/SIVON of een (IBP-)netwerk, is praktische toepassing van de kennis in de eigen organisatie een grote uitdaging.

Meer samenwerking en gemeenschappelijke diensten

Er vindt steeds meer samenwerking plaats om AVG-compliance gezamenlijk te organiseren. Belangrijk hierin zijn met name de gemeenschappelijke diensten die worden ontwikkeld om de lasten voor (kleine) onderwijsinstellingen te verminderen. Met het programma Digitaal Veilig Onderwijs krijgen scholen in het funderend onderwijs onder andere ondersteuning door het centraal toetsen van verwerkersovereenkomsten, het uitvoeren van DPIA's op veelgebruikte softwareapplicaties en de ontwikkeling van een Computer Emergency Response Team (CERT).[14] De PO-Raad, VO-raad, SIVON en Kennisnet spelen hierin een belangrijke rol, hoewel schoolbesturen eindverantwoordelijk zijn en blijven.

In de mbo-sector is een vergelijkbare aanpak te zien met het programma Cyberveiligheid[15], waarin ook op centraal niveau verwerkersovereenkomsten worden beoordeeld en DPIA's worden uitgevoerd op veelgebruikte applicaties in het mbo. Het programma bevat daarnaast nog vele andere acties om privacycompliance te ondersteunen, zoals het oprichten van een vraagbaak/helpdesk voor privacyvragen en kennisdeling over awareness-activiteiten. De mbo-sector zoekt ook actief de samenwerking met SURF. (Vrijwel) alle mbo-instellingen zijn lid van SURF, zodat zij ook toegang hebben tot SURFcert en SURFsoc.

Ten slotte worden ook in het hoger onderwijs en de mbo-sector meer zaken in samenwerking opgepakt. In SURF-verband voeren de leden samen regelmatig risicoanalyses uit op privacy en security bij leveranciers, onder andere met DPIA's en *data transfer impact assessments* (DTIA's), het beoordelen van certificeringen, checks op datadoorgiftes buiten de EER, en met juridisch en technisch onderzoek. Via SURF maken onderwijsinstellingen afspraken met leveranciers over het mitigeren van privacy- en securityrisico's, onder meer door verwerkersovereenkomsten af te sluiten.

Dit biedt onderwijsinstellingen als verwerkingsverantwoordelijken handvatten om zelf een goede afweging te maken voor een veilig gebruik van applicaties. Daarnaast zet het hoger onderwijs sterk in op de verbetering van informatiebeveiliging binnen de onderwijsinstellingen. Tot slot vindt er ook veel

kennisuitwisseling plaats in andere gremia, zoals binnen het verband van Universiteiten van Nederland en het Platform Integrale Veiligheid Hoger Onderwijs (Platform IV-HO).

De AP vindt deze samenwerkingen goed aansluiten op het AP-advies en een mooie stap voorwaarts om de bescherming van persoonsgegevens binnen de gehele sector te verbeteren. Zo delen onderwijsinstellingen kennis en zijn zij gezamenlijk een stevige gesprekspartner richting leveranciers. De AP vindt het daarom van belang dat onderwijsinstellingen zich aansluiten bij en participeren in de verschillende initiatieven, en voor het funderend onderwijs specifiek dat scholen zijn aangesloten bij SIVON.

Afhankelijkheid van (grote) leveranciers

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

Toch is er volgens de sector de laatste jaren (langzaam) een beweging te zien om AVG-randvoorwaarden en eisen te stellen richting grote leveranciers, door toegenomen samenwerking bij de aanbesteding/inkoop en het stellen van gezamenlijke eisen aan leveranciers. Door ondersteuning, regie en coördinatie richting leveranciers te beleggen bij een samenwerkingsorganisatie (SURF, SIVON), zoals hierboven geschetst, kan de gehele sector hiervan profiteren. Medewerking van leveranciers bij bijvoorbeeld het uitvoeren van een DPIA is, volgens de sector, echter niet vanzelfsprekend. Sommige leveranciers zien de DPIA als een bedreiging en niet als een kans om de bescherming van persoonsgegevens te verbeteren en eventuele risico's te beperken.

FG's geven aan dat de rol van leveranciers eveneens belangrijk is voor onderwijsinstellingen bij het naleven van de hierboven genoemde normenkaders. Indien een softwareapplicatie bijvoorbeeld onvoldoende functionaliteiten biedt voor logging of verwijdering van persoonsgegevens, kan de onderwijsinstelling niet voldoen aan het normenkader. Onderwijsinstellingen moeten dit soort functionaliteiten daarom meenemen bij de aanbesteding/inkoop van deze diensten en hierover afspraken maken met de leverancier.

3. Hoe ziet de sector zichzelf?

Over het algemeen is de onderwijssector van goede wil om te voldoen aan de AVG. Beperkingen in tijd, geld en capaciteit vormen echter een uitdaging. Bij enkele onderwijsinstellingen ontbreekt een intrinsieke overtuiging dat aandacht voor privacy een randvoorwaarde is voor goed en veilig onderwijs. Uit de gesprekken met de sector blijkt er een verband te zijn tussen de grootte van een onderwijsinstelling en de naleving van de AVG; hoe groter de instelling, hoe volwassener over het algemeen de privacycompliance is.[16] Dit neemt niet weg dat veel instellingen nog stappen te maken hebben, zeker de kleinere.

Met de input van (sector)organisaties en FG's in het onderwijs heeft de AP in dit sectorbeeld op basis van een aantal thema's onderzocht hoe de organisaties zelf naar hun compliance kijken:

Leiderschap en toezicht

- Privacy en security zijn terugkerende thema's op de agenda van de sectorraden in het onderwijs. De sectorraden brengen dit onderwerp op verschillende manieren onder de aandacht van onderwijsbesturen.
- De kennis en het bewustzijn van en de betrokkenheid bij het thema gegevensbescherming zijn in de directielagen van veel onderwijsinstellingen verbeterd. Bij grotere onderwijsinstellingen zijn de lagere managementlagen echter nog niet altijd voldoende betrokken.
- FG's geven aan dat niet altijd duidelijk is bij wie in de organisatie de verantwoordelijkheden liggen voor gegevensbescherming.
- De positie en professionaliteit van de FG zijn de afgelopen jaren verbeterd. Waar de FG voorheen (ook) uitvoerende taken had, komt de FG nu over het algemeen meer terecht in een toezichthoudende rol. Toch zijn er nog steeds onderwijsinstellingen waarin dit nog geen staande praktijk is.
- De formatieruimte en het kennisniveau van *privacy officers* en eerste- en tweedelijnsmedewerkers is wisselend. Veel FG's zien hier grote verbetermogelijkheden in, zowel qua formatie als deskundigheid.

Risicobeoordelingen

- Hoewel de kwaliteit van DPIA's varieert in het onderwijs, voert de sector bij steeds meer leveranciers gezamenlijke/centrale DPIA's uit. Deze helpen onderwijsinstellingen om zelf de juiste afwegingen te maken en de DPIA uit te werken voor hun organisatie. Deze samenwerking komt de kwaliteit van de DPIA's in alle subsectoren ten goede.
- Voor veel onderwijsinstellingen is het een uitdaging om overzicht te houden op alle verwerkingen van persoonsgegevens. Door de autonome positie van docenten, de 'wildgroei' aan software en de soms grote hoeveelheid onderzoeken en samenwerkingen met andere organisaties, is het voor onderwijsinstellingen lastig om controle te houden over de gegevensverwerkingen waarvoor zij verantwoordelijk zijn, laat staan daar een (goede) DPIA op uit te voeren.

Beleid en procedures

- Vrijwel alle onderwijsinstellingen hebben op papier regels en beleid opgesteld waarin de AVG-principes zijn vertaald. Sectorraden en organisaties als SURF, Kennisnet en SIVON 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 met (werk)instructies voor personeel en procedures/maatregelen, is een volgende stap die veel onderwijsinstellingen nog moeten zetten.
- Risicomanagement wordt zelden cyclisch georganiseerd, waardoor bijvoorbeeld het toepassen van *privacy by design* reactief plaatsvindt.[17] Bij de aanbesteding/inkoop wordt gegevensbescherming meer meegenomen, onder andere door de toegenomen samenwerking.
- Onderwijsinstellingen in het mbo en hoger onderwijs werken steeds meer vanuit een digitaliseringsstrategie of zien het belang daarvan in. Gegevensbescherming en informatiebeveiliging worden daarmee steeds nadrukkelijker verbonden met publieke waarden.[18]

Transparantie

- De meeste onderwijsinstellingen hebben een algemene privacyverklaring en een privacyreglement opgesteld en beschikbaar gesteld aan betrokkenen. Deze bevatten alleen niet altijd alle verwerkingen van de onderwijsinstelling.
- 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. Vanuit onder andere studenten is de wens om meer inzicht te krijgen in wie er toegang heeft tot hun gegevens, en hier invloed op te kunnen uitoefenen.
- Het contact tussen de FG en de AP verdient verbetering. Zo weten nog niet alle FG's wat ze kunnen verwachten van de AP of laat een reactie van de AP soms langere tijd op zich wachten.[19]

Training en bewustzijn

- Over het algemeen is er vooruitgang in kennis van en bewustwording over gegevensbescherming. Eerdere beveiligingsincidenten in het onderwijs hebben bijgedragen aan deze bewustwording.
- Awareness onder bestuur, onderwijspersoneel en studenten wordt nog steeds gezien als verbeterpunt en vraagt blijvende aandacht.[20]
- Een aantal FG's is van mening dat scholing en training aan onderwijspersoneel een dwingender karakter zouden moeten krijgen binnen de organisatie, omdat de deelname daaraan te beperkt is.

Zelfmonitoring en controles

- Op subsectorniveau zijn enkele zelfevaluaties ontwikkeld of nog in ontwikkeling.[21] Binnen verschillende netwerken delen en bespreken instellingen de evaluaties 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 om aan de slag te gaan met resultaten en verbeterpunten van de evaluatie. Een goede privacygovernance in de organisatie is daarom essentieel. Kleinere onderwijsinstellingen hebben soms problemen met opvolging van de aanbevelingen uit de audits wegens gebrek aan capaciteit en middelen.
- FG's brengen periodiek rapportages uit.

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.
- De sector is van mening dat instellingen AVG-verzoeken adequaat en tijdig oppakken.
- Het melden van datalekken blijft een aandachtspunt. Er zijn nog veel medewerkers die datalekken niet herkennen. Er zijn zelfs onderwijsinstellingen die nog nooit een datalek hebben gemeld aan de AP.

"Binnen de onderwijssector heerst er een non-competitieve instelling, wat zorgt voor veel openheid naar elkaar op dit onderwerp."

- Een FG in het onderwijs

4. Wat ziet de AP binnen de sector?

Op basis van het zelfbeeld van de sector trekt de AP de conclusie dat bij veel onderwijsinstellingen de 'basis AVG-compliance' de goede kant opgaat, maar ook nog verbetering nodig heeft. Dit kwam ook al naar voren uit het beeld dat de AP in 2021 publiceerde. [22] De aanbeveling van de AP aan de sector om de basis op orde te brengen, blijft daarom onverminderd staan.

Een praktische uitwerking hiervan ziet de AP bijvoorbeeld bij datalekken. Het aantal datalekmeldingen uit het onderwijs aan de AP in het onderwijs was in 2022 ongeveer 3% van het totaal, oftewel ruim 700 meldingen. Afgezet tegen de meer dan 7000 onderwijsinstellingen en de ruim 4 miljoenen betrokkenen (onderwijsdeelnemers en onderwijspersoneel) vindt de AP dit een laag getal.[23] Zeker omdat de sector relatief veel (gevoelige) persoonsgegevens verwerkt, ook van kwetsbare groepen. [24] De AP onderstreept daarom, net als de sector, het belang van awareness en van het opstellen van beleid voor 'de werkvloer', zodat mensen datalekken goed herkennen en waar nodig melden aan de AP.

Daarnaast is de AP van mening dat de sector nog een slag kan maken op het gebied van dataminimalisatie en oude systemen. Door meldingen van cyberaanvallen zien we dat veel persoonsgegevens onnodig op straat belanden, omdat instellingen deze principes onvoldoende toepassen. Deze gegevens en/of systemen waar de gegevens in stonden, hadden geen functie meer. De onderwijsinstellingen hadden deze al eerder moeten verwijderen.

Zoals in hoofdstuk 2 staat, ziet de AP wel een positieve ontwikkeling bij de aanbeveling van de AP uit 2021 om meer samenwerking te zoeken, onder andere richting grote leveranciers. Ook vindt de AP de ontwikkeling van gezamenlijke normenkaders, gekoppeld aan toezicht/handhaving, een goede stap om onderwijsinstellingen aan te sporen hun privacycompliance op orde te krijgen.

Tot slot merkt de AP op dat het onderwijs bij uitstek de plek is om de volgende generaties kennis bij te brengen over het veilig leren omgaan met digitale technologie. De AP roept de sector daarom op om ook aandacht te vragen voor dit thema in het onderwijs en de privacyuitdagingen van digitale technologie onder de aandacht te brengen.

5. Toezicht van de AP op de sector

Wat heeft de AP gedaan binnen de sector?

De AP heeft diverse toezichtsinterventies ondernomen in de onderwijssector. De belangrijkste hiervan zijn:

- De AP heeft in 2021 advies uitgebracht over de inzet van Google Workspace en de ministers van OCW opgeroepen een pakket aan maatregelen te treffen, zodat onderwijsinstellingen veilig gebruik kunnen maken van digitale onderwijsmiddelen. Voor het Commissiedebat over digitalisering in het onderwijs heeft de AP deze oproep eind 2021 herhaald met een set aanbevelingen.[25] Begin 2023 heeft de AP de ministers gevraagd duidelijkheid te scheppen over de veiligheid van Googleproducten in het onderwijs.[26]

- In 2021 heeft de AP kritisch geadviseerd over de wijziging van de Wet register onderwijsdeelnemers.[27] Naar aanleiding hiervan zijn de subsidiariteit en proportionaliteit van de gegevensverstrekkingen uit het register onderwijsdeelnemers onderbouwd. Ook is verduidelijkt dat alleen gepseudonimiseerde gegevens zullen worden verstrekt. Daarnaast is in het Besluit register onderwijsdeelnemers door opmerkingen van de AP afgezien van een aantal gegevensverwerkingen.
- In 2021 heeft de AP op diverse aspecten guidance uitgebracht over onderwijs tijdens corona, zoals het vragen van toestemming voor de verwerking van coronabesmettingen in het onderwijs.
- De Inspectie van het Onderwijs heeft in oktober en november 2022 rondetafelgesprekken georganiseerd over cyberveiligheid in het onderwijs, waarbij de AP twee workshops heeft geleid.[28]
- De AP heeft in 2023 guidance uitgebracht over onder andere het uitwisselen van persoonsgegevens tussen scholen en gemeenten binnen het sociaal domein, omdat het onderliggende convenant onvoldoende duidelijk was over de beoogde doeleinden, de verwerkingsverantwoordelijken en de grondslagen van de verwerkingen.
- De AP voert periodieke overleggen met sectororganisaties en FG's in het onderwijsveld en blijft dit doen.
- Er wordt in EDPB-verband gewerkt aan guidelines voor de verwerking van persoonsgegevens voor medisch en wetenschappelijk onderzoek.

Wat wil de AP nu doen binnen de sector?

De AP zal op verschillende manieren aandacht besteden aan de onderwijssector:

- De AP gaat aandacht besteden aan de inzet van algoritmes en AI in het onderwijs.
- Er is behoefte aan ontwikkeling van nadere guidance over de verwerking van persoonsgegevens voor onderzoek. De AP nodigt de sector uit om daarover in gesprek te gaan met de AP.
- De AP draagt binnen de EPDB bij aan het opstellen van guidelines voor de verwerking van persoonsgegevens van kinderen.
- De AP blijft de ontwikkelingen volgen bij cross-sectorale gegevensdeling, onder andere bij de Wet aanpak meervoudige problematiek sociaal domein.
- Aangezien er binnen het onderwijs veel gebruikt wordt gemaakt van online diensten van grote techbedrijven, zowel tijdens de les als daarbuiten, is de AP van plan om meer guidance op dit gebied te geven.
- De AP ziet grote uitdagingen bij de bescherming van kinderen (online). Het ontbreekt de AP echter aan middelen en capaciteit om hier goed toezicht op te houden.[29]

6. Verantwoording

Voor het schrijven van dit sectorbeeld heeft de AP de volgende organisaties en personen bevraagd:

- Inspectie van het Onderwijs;
- Interstedelijk Studenten Overleg;
- Kennisnet;
- Landelijke Studentenvakbond;

- MBO Raad en MBO Digitaal;
- Ministerie van OCW;
- Ouders & Onderwijs;
- PO-Raad;
- SIVON;
- SURF;
- Universiteiten van Nederland;
- Vereniging Hogescholen;
- VO-raad;
- Verschillende FG's vanuit alle subsectoren.

De AP dankt iedereen hartelijk voor het beantwoorden van de vragen van de AP en de bijdrage aan dit sectorbeeld.

---

[1] Deze systemen en toepassingen van algoritmes en AI kunnen zowel simpele toepassingen als complexe modellen zijn. Omdat het in dit sectorbeeld gaat over de verwerking van persoonsgegevens waarbij algoritmes en AI een rol kunnen spelen en de mogelijke risico's en effecten daarvan, kunnen de termen 'algoritmes' en 'AI' door elkaar gebruikt worden.

[2] In de Rapportage AI- & Algoritmerisico's Nederland najaar 2023 gaat de AP gaat hier nader op in.

[3] Zie: https://www.onderwijsraad.nl/binaries/onderwijsraad/documenten/adviezen/2022/09/28/inzet-van-intelligente-technologie/OWR_technologie-opmaak-WEB.pdf

[4] Zie: Rapportage AI- & Algoritmerisico's Nederland najaar 2023, p. 30 e.v.

[5] Schaduw-ICT omvat hardware, software of diensten die voor werkzaamheden worden ingeregeld, ingevoerd en/of gebruikt zonder uitdrukkelijke goedkeuring of medeweten van de organisatie. Zie: https://communities.surf.nl/cybersecurity/artikel/schaduw-ict-in-onderwijs-en-onderzoek-wat-moet-je-er-als-instelling-mee.

[6] Wel zijn er op centraal niveau initiatieven (geweest) om inzichtelijk te maken welke applicaties er (binnen een instelling) beschikbaar zijn, zodat docenten betere afwegingen kunnen maken bij de inzet van digitale tools. Voorbeelden hiervan zijn het Toolwiel en het Platform educatieve applicaties. Voor de duidelijkheid: de AP is hierbij niet betrokken geweest.

[7] Zie: https://autoriteitpersoonsgegevens.nl/uploads/imported/brief_minister_van_onderwijs_cultuur_en_wetenschap.pdf

[8] Zie: https://open.overheid.nl/documenten/ronl-309c973b8f6d9d55f691098640393417oc57e7c5/pdf

[9] Zie: https://aanpakibp.kennisnet.nl/app/uploads/Normenkader-IBP.pdf. Ten tijde van het schrijven van dit sectorbeeld was enkel het normenkader over informatiebeveiliging gepubliceerd, nog niet het normenkader over privacy. Het normenkader is volgens de sector afgeleid van het SURF toetsingskader privacy.

[10] Zie: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2023/07/06/visiebrief-digitalisering-in-het-funderend-onderwijs/visiebrief-digitalisering-in-het-funderend-onderwijs.pdf

[11] Idem.

[12] Zie: https://www.surf.nl/surfaudit-toetsingskader-beoordeel-je-privacybescherming. Dit toetsingskader is gezamenlijk met de PO- en VO-sector ontwikkeld.

[13] Zie: https://mbodigitaal.nl/wp-content/uploads/2023/06/2023-06-14-Convenant-cyberveiligheid-mbo.pdf

[14] Zie: https://www.digitaalveiligonderwijs.nl/

[15] Zie: https://mbodigitaal.nl/programmas/programma-cyberveiligheid-mbo/

[16] Zoals aangegeven in de tekst, trekt de AP deze conclusie vooral op basis van de gesprekken met de sector zelf. De steekproef die is uitgevoerd voor de nulmeting IBP-normenkader voor het funderend onderwijs laat een iets ander beeld zien (hoewel deze steekproef enkel betrekking heeft op het IB-kader): https://www.kennisnet.nl/app/uploads/Nulmeting-Normenkader-IBP-FO.pdf. Nader onderzoek zal nodig zijn om dit vast te kunnen stellen.

[17] Zo onderstreept ook het cyberdreigingsbeeld van SURF: https://www.surf.nl/files/2023-06/cyberdreigingsbeeld-onderwijs-en-onderzoek-2023_0.pdf (p. 8 e.v.).

[18] Mbo-instellingen, hogescholen en universiteiten werken de komende jaren samen aan digitalisering in het onderwijs in het landelijke programma Npuls (gefinancierd met 560 miljoen euro subsidie uit het Nationaal Groeifonds). Daarin werken zij bijvoorbeeld aan een sectorale ICT-infrastructuur die de privacy van lerenden en medewerkers van onderwijsinstellingen beschermt.

[19] Meer informatie over wat de AP wel en niet kan betekenen voor FG's is hier te vinden: https://www.autoriteitpersoonsgegevens.nl/fg-informatie/contactgegevens-ap-voor-fgs.

[20] Zo onderstreept ook het cyberdreigingsbeeld van SURF: https://www.surf.nl/files/2023-06/cyberdreigingsbeeld-onderwijs-en-onderzoek-2023_0.pdf (p. 5, 12, 24).

[21] De AP bedoelt met zelfevaluaties de normenkaders, toetsingskaders en zelfevaluaties.

[22] Zie: https://autoriteitpersoonsgegevens.nl/uploads/imported/paper_autoriteit_persoonsgegevens_digitalisering_in_het_onderwijs_2021.pdf

[23] Data afkomstig van NJI, DUO Open onderwijsdata, Vereniging Hogescholen en Universiteiten van Nederland. Het betreft de cijfers over 2022. Bij de cijfers zijn de historische data waar onderwijsinstellingen over beschikken niet meegenomen.

[24] Zie: https://autoriteitpersoonsgegevens.nl/documenten/jaarrapportage-meldplicht-datalekken-2022

[25] Zie: https://autoriteitpersoonsgegevens.nl/uploads/imported/paper_autoriteit_persoonsgegevens_digitalisering_in_het_onderwijs_2021.pdf

[26] Zie: https://autoriteitpersoonsgegevens.nl/actueel/advies-ap-google-producten-in-het-onderwijs

[27] Zie: https://autoriteitpersoonsgegevens.nl/actueel/ap-adviseert-kritisch-over-wijziging-wet-register-onderwijsdeelnemers

[28] Zie: https://www.onderwijsinspectie.nl/documenten/publicaties/2023/02/03/verslag-rondetafelbijeenkomsten-cyberveiligheid

[29] Op 23 mei 2023 nam de Tweede Kamer de motie van het lid Drost (CU) aan, die het kabinet oproept om naar analogie van de Kinderombudsman bij de AP ook een specifieke kinderautoriteit op te richten die zich bezighoudt met de online gegevensbescherming van kinderen. Zie: https://www.tweedekamer.nl/kamerstukken/detail?id=2023Z08798&did=2023D21118