PO VO BVE

Door **Chris Zintel, secretaris Edu-K**

Algemene Verordening Gegevensbescherming

Maak goede afspraken met je leveranciers

"Wat weet een uitgever eigenlijk allemaal over mijn dochter? "Wat mag een distributeur doen met de gegevens van onze leerlingen?" "Zijn we als school klaar voor de Algemene Verordening Gegevensbescherming ?" "En met welke partijen moet ik eigenlijk allemaal afspraken maken over die leerlinggegevens?"

Als het goed is heeft een schooldirecteur of onderwijsbestuurder de afgelopen tijd minimaal een van deze vragen gehad of gesteld. Per 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Een van de zaken die ieder schoolbestuur daarvoor moet regelen, is het maken goede afspraken met alle leveranciers van digitale leermiddelen, (administratie)software en andere digitale diensten. Maar draai het eens om: je moet als school niet alleen goed omgaan met de privacy van de leerling, je wil dit toch ook? Zoals je als consument op internet wilt weten dat er goed met jouw gegevens wordt omgegaan door bijvoorbeeld Facebook, zo wil je dat toch ook voor je leerlingen? Sectorraden en brancheorganisaties van leveranciers werken samen aan veilig en betrouwbaar gebruik van digitale middelen in het onderwijs.

Chris Zintel is als secretaris Edu-K werkzaam bij Kennisnet.

Afspraken over privacy en beveiliging geregeld in Edu-K

Op scholen wordt steeds meer gebruik gemaakt van digitale producten: denk aan leermiddelen die adaptief zijn en zich aanpassen aan het niveau van de leerling, denk aan overzichtelijke dashboards waar je allerlei informatie over leerlingen kunt zien, makkelijke administratiesystemen die al het contact met DUO regelen en ouderportalen waarmee leraren ouders op de hoogte houden van de vorderingen van hun zoon of dochter. Wat al deze systemen gemeen hebben, is dat er veel informatie over leerlingen de school 'uit' gaat. Deze systemen draaien namelijk op een server buiten de school.

Wettelijk gezien is het schoolbestuur verantwoordelijk voor wat er met persoonsgegevens van leerlingen gebeurt: met wie worden ze gedeeld? Welke gegevens worden gedeeld? Wat mag (of moet) een leverancier met deze gegevens doen? En hoe weet je of de gegevens goed zijn beveiligd? Om scholen te ondersteunen

met het goed regelen van privacy en beveiliging hebben de sectorraden (PO-Raad, VO-raad en MBO Raad) en de brancheorganisaties van uitgeverijen, distributeurs en softwareleveranciers (respectievelijk GEU, KBb-e en VDOD) met elkaar gezorgd voor goede afspraken die door iedere school en leverancier te gebruiken zijn. Dit gebeurt in het publiek-private platform Edu-K (zie kader).

Ik vind het goed omgaan met leerlinggegevens een belangrijke verantwoordelijkheid van elk schoolbestuur." vertelt Gerard Oud, lid van het college van bestuur van het Clusius College in Noord-Holland. "Dat vind ik niet alleen omdat de wet ons hiertoe verplicht, maar ook omdat ik dit goed aan onze leerlingen en ouders wil kunnen uitleggen. Wij sluiten met al onze leveranciers verwerkersovereenkomsten af volgens het convenantsmodel. Als een leverancier hier niet aan mee wil werken of zich hier niet aan houdt, kunnen wij besluiten om die producten niet meer te gebruiken. Dit is al eens gebeurd."

Leerlinggegevens goed beschermd door privacyconvenant

De afspraken voor goede omgang met leerlinggegevens zijn vastgelegd in het Convenant Digitale Onderwijsmiddelen en Privacy (het privacyconvenant). Eenduidigheid is zowel voor een schoolbestuur als voor een leverancier handig. Inmiddels hebben rond de 300 leveranciers zich aangesloten bij het convenant en daarmee geven ze aan deze afspraken toe te passen. Het privacyconvenant kent vier belangrijke pijlers: de model verwerkersovereenkomst, de privacybijsluiter, de beveiligingsbijlage en het ECK iD.

De model verwerkersovereenkomst

In de model verwerkersovereenkomst staan alle afspraken die ervoor zorgen dat er op een eenduidige en praktische manier uitvoering gegeven wordt aan privacywetgeving. Hierin staat beschreven dat de school bepaalt welke gegevens worden gebruikt en met welk doel, wat leveranciers wel en niet met deze gegevens mogen (het sturen van reclame naar leerlingen is bijvoorbeeld niet toegestaan, evenals als het doorverkopen van persoonsgegevens), en hoe om te gaan met boetes of in het geval van een datalek. Alle afspraken zijn juridisch getoetst, en aanpassingen aan de tekst zijn dus niet nodig. Ze zijn zo opgesteld dat elke partij die digitale leermiddelen, toetsen, of leerling- of schooladministratiesystemen (denk aan LAS, ELO, LVS, ouderportaal) levert, deze afspraken een-op-een toe kan passen. André Poot is voor stichting CVO Alblasserwaard-Vijfheerenlanden verantwoordelijk voor het afsluiten van de juiste overeenkomsten. "Het eerste wat ik doe is een leverancier vertellen dat wij graag willen dat hij zich bij het convenant aansluit. Dat het convenant verplicht tot gebruik van een standaard verwerkersovereenkomst helpt mij enorm. Ik hoef geen diepgaande juridische kennis te hebben, maar kan er toch op vertrouwen dat ik de juiste afspraken maak voor ons bestuur en voor onze leerlingen."

De privacybijsluiter

Bij de verwerkersovereenkomst hoort een privacybijsluiter. Vergelijk het met de bijsluiter bij een medicijn. In de privacybijsluiter staat beschreven welke producten het schoolbestuur gebruikt, welke persoonsgegevens de leverancier gebruikt om zijn diensten te kunnen leveren en voor welke doelen deze gegevens gebruikt mogen worden. Dit is dus het onderdeel van de overeenkomst waar je als schoolbestuur kritisch kijkt naar de doelbinding van de gegevens die je ter beschikking stelt aan een leverancier.

> Wettelijk gezien is het schoolbestuur verantwoordelijk voor wat er met persoonsgegevens van leerlingen gebeurt

De beveiligingsbijlage

Als schoolbestuur ben je er ook verantwoordelijk voor dat jouw leverancier de juiste beveiligingsmaatregelen heeft getroffen. Waar het controleren van de privacybijsluiter nog op basis van ervaring en goede dosis gezond verstand kan, is dit voor allerlei technische en organisatorische beveiligingsmaatregelen een stuk ingewikkelder. Ook daarvoor hebben de sectorraden, Kennisnet en leveranciers afspraken gemaakt: het Certificeringsschema voor informatiebeveiliging en privacy. Kort gezegd: leveranciers classificeren hun product op basis van de persoonsgegevens die ze gebruiken. Dit leidt tot een lijst met minimaal te nemen maatregelen. Als een leverancier gebruik maakt van het Certificeringsschema, dan zal hij in de beveiligingsbijlage aangeven of hij die maatregelen daadwerkelijk heeft genomen. Dit gaat volgens het principe van 'pas toe of leg uit'. Komen de maatregelen

Edu-K

Zowel qua kennis, tijd en geld, is het erg onhandig als iedere school zelf afspraken over privacy en beveiliging gaat opstellen. Ditzelfde geldt ook voor leveranciers: dit is erg inefficiënt waardoor een leverancier meer kosten moet maken. Omdat beide kanten van de markt veilig en betrouwbaar gebruik van digitale leermiddelen en software erg belangrijk vinden, zijn er nu breed gedragen afspraken.
Edu-K is het publiek-private platform voor de educatieve keten. Deelnemers van Edu-K zijn: sectorraden PO-Raad, VO-raad, MBO Raad, de brancheorganisaties GEU, KBb-E, VDOD, en Kennisnet. Door het maken van sectorbrede afspraken werken ze aan een veilige en betrouwbare leermiddelenketen. Niet iedere school of leverancier hoeft zelf het wiel uit te vinden en daarmee kunnen alle partijen hun investeringen gericht inzetten.

Aanpak IBP

Goed IBP-beleid (informatiebeveiliging en privacy) is meer dan goede afspraken maken met leveranciers. Om aan de AVG (algemene verordening gegevensbescherming) te voldoen moet er meer gebeuren in de school. Bijvoorbeeld het hebben van een privacyprotocol, goede afspraken maken met ouders en het aanleggen van een dataregister. Wat te doen en hoe dit in de praktijk te brengen vind je in de Aanpak IBP voor po/vo en voor mbo. Deze aanpak is te vinden op http://http://kn.nu/ibponderwijs (po/vo) http://kn.nu/aanpak-IBP-mbo (mbo).

Meer informatie over het privacyconvenant?
Kijk op www.privacyconvenant.nl

overeen, dan weet het schoolbestuur dat de leverancier de juiste beveiligingsmaatregelen heeft getroffen.

"Natuurlijk waren we altijd al bezig met het goed beveiligen van onze systemen en gegevens." vertelt Ernst-Jan Heuseveldt van ROVICT, de maker van het leerlingadministratiesysteem ESIS. "Gebruik van het Certificeringsschema om onze beveiligingsmaatregelen te beschrijven zorgt ervoor dat we hierover met schoolbesturen in gesprek kunnen: dit zijn de maatregelen die we zouden moeten treffen en op deze manier voldoen we daaraan. Dat is voor het schoolbestuur duidelijk, en voorkomt voor ons dat we met allerlei verschillende beveiligingseisen te maken hebben voor hetzelfde systeem."

Het ECK iD

Naast doelbinding is ook dataminimalisatie belangrijk om op een goede en veilige manier om te gaan met de gegevens van leerlingen: verstrek niet meer gegevens over leerlingen aan een leverancier dan noodzakelijk is voor het functioneren van het product en eventuele extra functionaliteiten. Het privacyconvenant schrijft voor dat een unieke identifier (nummer) voor iedere leerling wordt gebruikt om dit mogelijk te maken: het ECK iD. Dit nummer is niet herleidbaar en mag maar door een beperkt aantal partijen gebruikt worden (alleen voor het leveren en gebruik van leermiddelen, en alleen binnen een bepaalde onderwijssector). Dit zorgt ervoor dat er minder persoonsgegevens gedeeld hoeven te worden met distributeurs en uitgevers van digitale leermiddelen. Wanneer een groot aantal partijen dit gebruikt, zullen de toegangsvoorzieningen Basispoort en Entree Federatie steeds minder persoonsgegevens hoeven door te leiden van school naar leveranciers. Zo wordt de privacy van leerlingen nog beter gewaarborgd. Vanaf schooljaar 2018/2019 kunnen alle schoolbesturen in het primair onderwijs beschikken over het ECK iD, vanaf schooljaar 2019/2020 kunnen ook alle scholen in het voortgezet onderwijs en het mbo gebruik maken van het ECK iD.

Albert Jagt van leermiddelendistributeur The Learning Network (VanDijk, Studers) vindt het een goede stap vooruit als zijn organisatie straks gebruik kan maken van een uniek iD: "Als we straks van elke leerling een uniek nummer hebben, kunnen we voor onze dienstverlening af met minder persoonsgegevens. Denk bijvoorbeeld aan de geboortedatum van leerlingen: door alle afspraken hoeven we deze niet meer te ontvangen of door te geven aan uitgevers. En met een uniek iD kunnen we het proces met betrekking tot digitale leermiddelen bovendien verbeteren en meer betrouwbaar maken."

Wat moet ik als schoolbestuur doen?

Publieke en private partijen hebben in Edu-K dus goede afspraken gemaakt over privacy en minimale beveiligingsnormen, en partijen werken aan dataminimalisatie. Wat moet je als schoolbestuur zelf nog doen?

1. Vraag bij elke leverancier van een digitaal product een verwerkersovereenkomst conform het model. Als een leverancier het privacyconvenant heeft ondertekend, kun je deze bij hem opvragen, anders is het slim om jouw leverancier te wijzen op het convenant en te vragen zich hierbij aan te sluiten.
2. Controleer of de leverancier inderdaad geen aanpassingen heeft gedaan aan de basistekst, controleer in de privacybijsluiter de doelbinding van de persoonsgegevens, en controleer de maatregelen in de beveiligingsbijlage. Vraag daarbij aan je leverancier om het Certificeringsschema voor informatiebeveiliging te gebruiken voor het invullen van de beveiligingsbijlage. Dit gaat op basis van 'pas toe of leg uit', dus dan weet je dat jouw leverancier de juiste maatregelen neemt of waarom hij dit niet of anders heeft gedaan. Als een leverancier noodzakelijke of gewenste maatregelen niet heeft genomen, moet het schoolbestuur hierover in gesprek gaan met de leverancier.
3. Onderteken de verwerkersovereenkomst en stuur deze naar je leverancier. Deze stuurt je vervolgens een getekende versie retour.
4. Het ECK iD wordt op korte termijn dé standaard die helpt bij veilig en betrouwbaar gebruik van digitale leermiddelen. Scholen in het primair onderwijs kunnen zich op www.kennisnet.nl aan voor gebruik hiervan. Na het tekenen van de overeenkomst doet je LAS-leverancier de rest. Vo- en mbo-scholen krijgen volgend schooljaar bericht over aanmelding voor de nummervoorziening. Daarnaast is voor mbo-scholen gebruik van de ECK-standaard een voorwaarde, kijk hiervoor op www.edu-k.nl/eckmbo.

"Wij vinden het ontzettend belangrijk om goede afspraken te hebben met schoolbesturen over de omgang met de gegevens van leerlingen en medewerkers." zegt Stephan de Valk van brancheverenigingGEU. De GEU heeft ondertekening van het privacyconvenant verplicht gesteld voor alle aangesloten leveranciers van leermiddelen en toetsen. "De afspraken die nu gemaakt zijn, zorgen voor veilige en betrouwbare omgang met leerlinggegevens, maar maken het tegelijkertijd mogelijk om leermiddelen te maken die scholen ondersteunen bij het leveren van maatwerk voor leerlingen."