Aandachtspunten AVG en het Privacyconvenant voor leveranciers in de onderwijsketen

Een nieuwe Europese wet

In Nederland is de bescherming van persoonsgegevens momenteel geregeld in de Wet bescherming persoonsgegevens (Wbp). Op 25 mei 2018 zal deze wet vervangen worden door een Europese wet die rechtstreeks van toepassing is in alle landen van de Europese Unie: de Algemene Verordening Gegevensbescherming (AVG).

In de basis verschilt de Wbp uit 2001 niet zoveel van de AVG. De AVG geeft personen wiens gegevens worden verwerkt meer rechten om hierop invloed uit te oefenen. Daarnaast legt de AVG meer nadruk op de eigen verantwoordelijkheid van organisaties om de wet na te leven, om transparant te zijn over de omgang met persoonsgegevens én om te kunnen aantonen dat zij zich aan de wet houden.

Het Privacyconvenant

Ook leveranciers van digitale leermiddelen moeten informatiebeveiliging en privacy (IBP) goed regelen. Dat is een belangrijke randvoorwaarde voor het gebruik van ICT in het onderwijs. In 2015 hebben alle partijen in de onderwijsketen daarom een convenant gesloten over hoe zij omgaan met IBP en wat hun rolverdeling is bij de verwerking van leerlinggegevens, het Privacyconvenant (lees hier meer). Het Convenant helpt scholen en leveranciers bij het nakomen van hun verplichtingen, evenals de bijbehorende bijlagen: de Bewerkersovereenkomst, de Privacybijsluiter en de Beveiligingsbijlage. In 2016 is versie 2.0 van het Convenant in werking getreden.

In de loop van het eerste kwartaal van 2018 zal er een nieuwe versie van het Convenant bekend worden gemaakt, versie 3.0. Deze versie zal rekening houden met de nieuwe eisen vanuit de AVG en met de nieuwe AVG terminologie. Zo heet een “verantwoordelijke” vanaf mei 2018 een “verwerkingsverantwoordelijke” en een “bewerker” een “verwerker”.

Rolverdeling tussen scholen en leveranciers

Het Convenant is erop gebaseerd dat schoolbesturen optreden als de “verwerkingsverantwoordelijke” en leveranciers als “verwerkers”. Dat is een belangrijk onderscheid. De verwerkingsverantwoordelijke is de partij die het doel en de middelen bepaalt van de gegevensverwerking. De verwerker voert de gegevensverwerking slechts uit in opdracht en op instructie van de verwerkingsverantwoordelijke. De verwerker mag gegevens uitsluitend verwerken voor doeleinden die door de verwerkingsverantwoordelijke zijn vastgesteld, niet voor eigen doeleinden.

De AVG is nog strenger ten aanzien van de eigen verantwoordelijkheid van de verwerker. Die kan zich onder de AVG niet meer verschuilen achter de verwerkingsverantwoordelijke. Regelt de verwerker zijn zaken niet goed, dan kan hij aansprakelijk zijn op dezelfde wijze als de verwerkingsverantwoordelijke.

In deze aandachtspunten wordt een volledig overzicht gegeven van de verplichtingen waaraan leveranciers moeten voldoen. Het betreft echter verplichtingen die continu de aandacht blijven vragen. Ook na het aflopen van deze checklist zal permanent moeten worden gemonitord in hoeverre er nog aan wordt voldaan.

Met de blik op mei 2018 worden in deze Aandachtspunten reeds de nieuwe AVG- en Convenant 3.0-begrippen gebruikt. Dat zijn dus net andere begrippen dan momenteel worden gebruikt in de Wbp en het Convenant 2.0. Deze Aandachtspunten bevatten echter nog hyperlinks naar alle 2.0-documenten, maar ook – vooruitlopend op mei 2018 – al naar enkele 3.0-documenten (waar dat het geval is, wordt dat vermeld). Zodra het Convenant 3.0 bekend is gemaakt, zullen alle hyperlinks worden bijgewerkt.

Verplichtingen in de AVG	Inhoud	In de praktijk	Wat moet ik doen?
Verwerkingsverantwoordelijke bepaalt doel en middelen en geeft instructies (1 / 28.3.a)	De verwerkingsverantwoordelijke is de partij die doel en middelen van de gegevensverwerking vaststelt. De verwerker mag slechts verwerken ten behoeve van de verwerkingsverantwoordelijke en op basis van schriftelijke instructies van de verwerkingsverantwoordelijke. De verwerker die een dienst aanbiedt dient de verwerkingsverantwoordelijke duidelijk te informeren over de wijze waarop daarmee gegevens worden verwerkt. De verwerkingsverantwoordelijke dient een geïnformeerde beslissing te kunnen nemen over het gebruik van de dienst en zijn rol als verantwoordelijke daadwerkelijk invulling te kunnen geven. De verwerker mag niet voor eigen doeleinden verwerken en mag niet treden buiten de door de verwerkingsverantwoordelijke vastgestelde doeleinden en instructies.	Scholen en leveranciers houden zich aan het Privacyconvenant en de Model Verwerkersovereenkomst. Daarin is limitatief vastgelegd voor welke doeleinden er mag worden verwerkt en worden schriftelijke instructies gegeven, zoals ten aanzien van bewaartermijnen.	Pas het Privacyconvenant toe en stel Privacybijsluiters op voor elk product of elke productgroep. Bied de school keuzemogelijkheden voor zover dat praktisch mogelijk, redelijk en nuttig is. Waarborg binnen de organisatie dat niet wordt getreden buiten de doeleinden zoals vastgelegd in de Verwerkersovereenkomst: - Communiceer duidelijk over de doeleinden en de rolverdeling tussen scholen en leveranciers. - Monitor eigen compliance door periodiek te evalueren of doeleinden worden overschreden (zie ook de registratieplicht).

Verplichtingen in de AVG	Inhoud	In de praktijk	Wat moet ik doen?
De Verwerkersovereenkomst (28.3 / 28.9)	Er dient een verwerkersovereenkomst te worden gesloten tussen verwerker en verwerkingsverantwoordelijke. Dit is primair een verantwoordelijkheid van de verwerkingsverantwoordelijke, maar de verwerker loopt het risico zelf als verwerkingsverantwoordelijke te worden aangemerkt indien hij te weinig doet om de verwerkingsverantwoordelijke te faciliteren. De overeenkomst dient schriftelijk gesloten te worden, waaronder begrepen elektronisch.	Scholen en leveranciers gebruiken de Model Verwerkersovereenkomst bij het Convenant. Meestal wordt uitsluitend gepubliceerd op de website, soms wordt ook (digitaal of per post) toegezonden.	Sluit Model Verwerkersovereenkomsten met scholen. Stel indien mogelijk de Verwerkersovereenkomst ter hand (post, fax, e-mail of web-interface). Bij voorkeur op een wijze die dat aantoonbaar maakt (digitaal). Optimaal is een (fysieke of elektronische) handtekening van het bevoegd gezag.
Inschakelen van subverwerkers (28.2 / 28.4)	De verwerker mag slechts subverwerkers (onderaannemers) inschakelen na voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke. Bij algemene toestemming dient de verwerker de verwerkingsverantwoordelijke steeds in te lichten bij toevoeging of vervanging van subverwerkers. De verwerkingsverantwoordelijke kan daartegen bezwaar maken. Verwerker dient met alle subverwerkers een subverwerkersovereenkomst sluiten.	Er wordt algemene toestemming verleend in de Model Verwerkersovereenkomst, met vermelding van de subverwerkers in de Privacybijsluiter.	Vul (per product/productgroep) de Privacybijsluiter in conform instructies, waaronder bij naam noemen van subverwerkers. Informeer scholen over nieuwe subverwerkers: publiceer en informeer (bijv. per e-mail). *In Verwerkersovereenkomst 3.0 wordt verplichting expliciet opgenomen.* Sluit subverwerkersovereenkomsten af met alle subverwerkers. Gebruik indien mogelijk Model Verwerkersovereenkomst.

Verplichtingen in de AVG	Inhoud	In de praktijk	Wat moet ik doen?
Personeel en onderaannemers (28.3.b / 29 / 32.4)	Personeel en onderaannemers met verwerking belast of met toegang tot persoonsgegevens: - Moeten door de verwerker worden verplicht tot vertrouwelijkheid. - Mogen slechts verwerken in opdracht van de verwerkingsverantwoordelijke.		Controleer arbeidsovereenkomsten en overeenkomsten met opdrachtnemers. Vul eventueel aan met: - Specifieke geheimhoudingsplichten voor persoonsgegevens, bijvoorbeeld door een afzonderlijke geheimhoudingsverklaring. - Verplichting zich te houden aan de opdracht van de verwerkingsverantwoordelijke. Neem bijvoorbeeld een verwijzing naar het Privacyconvenant op.
(Bijstand verlenen bij) Beveiliging van gegevens (28.3.c / 32)	De verwerker moet zelf passende technische en organisatorische beveiligingsmaatregelen nemen, o.a.: - Garanderen vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van systemen. - Vermogen om na incident beschikbaarheid van en toegang tot persoonsgegevens te herstellen. - Procedure voor testen, beoordelen en evalueren van doeltreffendheid van beveiliging. De verwerker moet bijstand verlenen aan de verwerkingsverantwoordelijke bij het uitvoeren van diens beveiligingsplicht.	Het ECKiD wordt stapsgewijs geïmplementeerd. Gebruik van het ECKiD is een belangrijk onderdeel van pseudonimisering en daarmee een belangrijke beveiligingsmaatregel. Door Edustandaard is een Certificeringsschema opgesteld. Dat voorziet in een baseline van maatregelen om ICT systemen en persoonsgegevens passend te beveiligen. Zowel ECKiD als Certificeringsschema worden naar verwachting meegenomen in het Privacyconvenant 3.0.	Gebruik het Certificeringsschema en pas ECKiD toe. Houd rekening met de benodigde capaciteitsinzet om deze te implementeren. Let op: het Certificeringsschema legt de minimale sectorale technische beveiligingsstandaard neer. Beveiliging blijft een eigen verantwoordelijkheid. Er dient continu te worden afgewogen of zwaardere beveiligingsmaatregelen noodzakelijk zijn. Zorg ervoor dat aan de school te allen tijde inzichtelijk kan worden gemaakt hoe beveiliging is geregeld: - Verwijs naar het Certificeringsschema of toegepaste ISO normen.

Verplichtingen in de AVG	Inhoud	In de praktijk	Wat moet ik doen?
			- Biedt SLA's aan (in verschillende gradaties). - Maak beveiligingsafspraken met subverwerkers inzichtelijk.
Privacy by Design en Privacy by Default (25)	De verwerkingsverantwoordelijke moet privacy-verhogende maatregelen nemen in het ontwerp van systemen en uitgaan van standaardinstellingen waarbij (indien er een keuze kan worden gemaakt) zo min mogelijk gegevens worden verwerkt.	In het Privacyconvenant 3.0 wordt het gebruik van het ECKiD en het Attributenbeleid naar verwachting opgenomen. In het Attributenbeleid is vastgelegd welke gegevens leveranciers mogen verwerken naast het ECKiD.	Maak gebruik van het ECKiD en werk zoveel mogelijk conform het Attributenbeleid. Het verwerken van meer attributen is uitsluitend mogelijk indien de school kan motiveren waarom dat noodzakelijk is. *Vanuit de GEU worden eventuele nadere sectorafspraken gecommuniceerd.*
Transparantie en rechten van betrokkenen (28.3.e / 12 – 22)	Verwerker moet bijstand verlenen aan de verwerkingsverantwoordelijke voor voldoen aan informatieverplichtingen en verzoeken van betrokkenen. Transparantie, voorafgaand en op verzoek o.a.: - Informatie over ontvangers van persoonsgegevens. - Bewaartermijnen. - Bestaan van geautomatiseerde besluitvorming, o.a. profilering. - Verwerking voor andere doeleinden dan waarvoor de persoonsgegevens zijn verzameld. Verzoeken van betrokkene: - Inzage, o.a.: kopie van de gegevens. - Rectificatie van onjuiste of onvolledige gegevens. - Wissen van gegevens.	Dit is een verplichting van de school. De school dient verzoeken van leerlingen/ouders te beoordelen en eventueel informatie uit te vragen bij de leverancier. - Informatie is opgenomen in Model Verwerkersovereenkomst. - Idem. - Idem. - Niet toegestaan. Doeleinden limitatief opgenomen in Model Verwerkersovereenkomst.	Waarborg dat kan worden voldaan aan verzoeken van de school: bouw opties in systemen in en houdt informatie beschikbaar. Alle communicatie in begrijpelijke taal gericht op het niveau van de betrokkene. Sluit Model Verwerkersovereenkomsten en vul de Privacybijsluiter in. Publiceer op de website. Pas de Privacybijsluiter aan indien omstandigheden wijzigen. Waarborg: - Dat verzoeken van ouders/leerlingen worden doorgestuurd aan de school. - Dat procedures zijn ingericht op verstrekken van informatie t.a.v. specifieke betrokkenen.

Verplichtingen in de AVG	Inhoud	In de praktijk	Wat moet ik doen?
	- Beperking van verwerking (bevriezing), waaronder tegengaan van wissen. - Verplicht ontvangers te informeren over rectificatie, wissen of beperking. - Recht van verzet. Dataportabiliteit: verwerkingsverantwoordelijke dient mogelijkheid te bieden tot overdragen van gegevens aan andere verwerkingsverantwoordelijke in gestructureerde, gangbare en machineleesbare vorm.	In PO en VO is deze plicht niet van toepassing op scholen. Wel hebben zij een verplichting gegevens over te dragen vanuit onderwijsrecht (zoals onderwijskundig rapport). Die ziet niet op gegevens in leermiddelen van uitgeverijen.	- Beschikbaarheid van kopieën van gegevens. - Mogelijkheid tot rectificatie. - Mogelijkheid tot wissen. - Mogelijkheid tot bevriezen. - Mogelijkheid verwerking te staken.
Wissen of overdragen van gegevens (28.3.g)	Verplichting om, naar keuze van de verwerkingsverantwoordelijke, gegevens na einde verwerking te wissen of aan verwerkingsverantwoordelijke terug te bezorgen, met verwijdering van alle kopieën.	Model Verwerkersovereenkomst bepaalt na einde overeenkomst gegevens te vernietigen en de school daarover te informeren.	Indien niet anders overeengekomen, verwijder na einde overeenkomst de gegevens en informeer de school daarover (bij voorkeur een concrete bevestiging van verwijdering (zoals per e-mail), anders op voorhand in de Privacybijsluiter).
Aantonen van compliance, meewerken aan audits en register (28.3.h / 30.2 / 30.3 / 30.4 / 30.5)	Verwerker dient aan de verwerkingsverantwoordelijke te kunnen aantonen dat aan alle verplichtingen is voldaan en dient mee te werken aan audits. Verwerker dient een schriftelijk (waaronder elektronisch) register van alle verwerkingscategorieën bij te houden en beschikbaar te houden, o.a.: - Naam en contactgegevens van subverwerkers. - Categorieën verwerkingen voor iedere verwerkingsverantwoordelijke.	Deze informatie wordt opgenomen in de Privacybijsluiters.	Vul Privacybijsluiters in en houd up-to-date. Werk mee aan audits voor zover noodzakelijk en proportioneel. Kosten voor audits die een controle van de bijgehouden registratie overschrijden dienen in overleg te worden gedragen.

Verplichtingen in de AVG	Inhoud	In de praktijk	Wat moet ik doen?
	- Doorgiften aan derde landen en documenten inzake passende waarborgen. - Beschrijving technische en organisatorische beveiligingsmaatregelen.		
(Bijstand verlenen bij) Melding van inbreuk (Datalekken) (28.3.f / 33 / 34)	Verwerker moet verwerkingsverantwoordelijke zonder onredelijke vertraging informeren over datalek: elke inbreuk op beveiliging die leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of toegang tot persoonsgegevens. Verwerker moet bijstand verlenen aan de verwerkingsverantwoordelijke voor meldingsplicht aan AP en betrokkene. - Melding aan AP binnen 72 uur. - O.a.: aantal betrokkenen, mogelijke gevolgen, maatregelen ter beperking van verder nadeel. - Documentatieplicht.	In de Model Verwerkersovereenkomst 3.0 wordt opgenomen dat bij een groot datalek dat meerdere scholen betreft, de leverancier melding mag doen namens de scholen. Modelverwerkersovereenkomst verplicht tot het hanteren van een passend datalekkenprotocol.	Stel een datalekkenprotocol en meldingenregister op. Voor scholen bestaan standaarddocumenten van Kennisnet (Aanpak IBP). Houd rekening met piek in capaciteitsinzet bij grote datalekken.
Bijstand verlenen bij uitvoeren PIA (28.3.f / 35 / 36)	Bij verwerkingen met hoog risico dient verwerkingsverantwoordelijke een privacy impact assessment uit te voeren (*gegevensbeschermingseffectbeoordeling*). Verwerker moet bijstand verlenen aan de verwerkingsverantwoordelijke.		Werk mee aan het opstellen van PIA's voor zover noodzakelijk en proportioneel. Kosten dienen in overleg te worden gedragen.
Functionaris Gegevensbescherming (37 / 38 / 39)	Er dient een FG aangesteld te worden indien sprake is van verwerkingen die gelet op aard, omvang en/of doeleinden regelmatige en stelselmatige observatie van betrokkenen op grote schaal vereisen, of	Het bijhouden van de leerprestaties van leerlingen wordt aangemerkt als regelmatige en stelselmatige observatie van gedrag en er kan vanuit worden gegaan	Stel een FG aan en laat de FG een cursus volgen indien nodig. Waarborg de onafhankelijke positie van de FG binnen de organisatie.

Verplichtingen in de AVG	Inhoud	In de praktijk	Wat moet ik doen?
	indien bijzondere gegevens worden verwerkt. - Geen instructies met betrekking tot uitvoering van FG taken. - Geen belangenconflict. - Rechtstreeks verslag hoogste leidinggevende. - Professionele kwaliteiten en deskundigheid op het gebied van gegevensbescherming.	dat sprake is van grootschaligheid. Leveranciers die dit doen, moeten een FG aanstellen. Hetzelfde geldt voor leveranciers die gezondheidsgegevens verwerken, zoals over dyslexie.	
Doorgifte derde landen (44 - 50)	Doorgifte aan landen buiten de EER slechts toegestaan indien voor dat land een regeling geldt: - Adequaatheidsbesluit (EU-VS: Privacyshield). - Standard Contractual Clauses (SCC's). - Bindende bedrijfsvoorschriften.	Veel subverwerkers die worden ingeschakeld van buiten de EER hebben eigen regelingen. Bij grote subverwerkers bestaat ook geen ruimte iets anders overeen te komen (Microsoft, Amazon, etc.). In andere gevallen zijn de SCC's het meest praktisch.	Indien subverwerkers zelf geen regeling aanbieden, bij voorkeur werken met Standard Contractual Clauses. Pas hiervoor de SCC aan die is gepubliceerd voor de overdracht verwerkingsverantwoordelijke -> verwerker.