

CONVENANT DIGITALE ONDERWIJS- MIDDELEN EN PRIVACY

Digitalisering is in het onderwijs niet meer weg te denken. Door de juiste inzet van digitale leermiddelen, passend bij de schoolvisie op leren, kunnen veel wensen van docenten, ouders en leerlingen worden ingevuld. Zo is gepersonaliseerd leren eenvoudiger realiseerbaar en is het mogelijk lesmateriaal leerlinggericht te optimaliseren. Keerzijde is dat de inzet van digitale leermiddelen het online gebruik van leerlinggegevens noodzakelijk maakt, evenals transport en opslag hiervan. Persoonsgegevens van een kwetsbare groep minderjarigen. Hoe kan in deze situatie op de juiste wijze invulling worden gegeven aan de privacybescherming van de leerlingen? Op deze vraag vindt u het antwoord in deze factsheet.



Privacy leerling als uitgangspunt

In een schoolomgeving worden allerlei persoonsgegevens verwerkt: gegevens van personeel en van leerlingen. Daarbij gaat het ook om gevoelige informatie als niveaus, toetsresultaten en gezondheidsinformatie van de leerlingen. Kinderen hebben recht op hun privacy en de vertrouwelijke behandeling van hun persoonlijke gegevens. Vanuit de Algemene Verordening Gegevensbescherming (AVG) zijn scholen primair verantwoordelijk voor de invulling van deze rechten.

Gelukkig staat u als school hierin niet alleen, uw leveranciers en dienstverleners hebben ook belang bij een kwalitatief goede invulling van privacybescherming binnen hun product- en dienstenaanbod. Een aantal marktpartijen (waaronder Heutink ICT, Reinders en Heutink) heeft daarom met de PO-en de VO-raad, als vertegenwoordiger van de scholen, een convenant gesloten. Dit convenant draagt de naam 'Convenant Digitale Onderwijsmiddelen en Privacy'.

Het convenant en bijbehorende verwerkersovereenkomst

Als u gebruikmaakt van digitale leermiddelen en toetsen, worden gegevens van leerlingen tussen de school en de leveranciers van deze onderwijsmiddelen uitgewisseld. Duidelijke afspraken met de leveranciers zijn dan ook essentieel. Het convenant vertaalt de AVG naar de onderwijspraktijk. Het bevat afspraken over hoe wordt omgegaan met persoonsgegevens bij het gebruik van

digitale leermiddelen en toetsen. Zo weten scholen en aanbieders wat ze over en weer van elkaar mogen verwachten, zijn de afspraken werkbaar in de praktijk en heeft iedereen dezelfde gemeenschappelijke uitleg bij deze afspraken.

De PO-Raad heeft het convenant daarna verwerkt tot een modelverwerkersovereenkomst. U moet vervolgens wel zelf deze overeenkomst, die wettelijk verplicht is, sluiten met de leverancier. Vergeet daarbij niet de privacybijsluiter in te laten vullen door de leverancier, waarin onder meer beschreven wordt welke typen persoonsgegevens de leverancier verwerkt.

Welke maatregelen zijn nodig?

Als verantwoordelijke zult u vanuit de AVG een aantal maatregelen moeten nemen om leerlinggegevens afdoende te beschermen. Primair gaat het daarbij om volgende maatregelen:

Wijs een eindverantwoordelijke aan voor alle werkzaamheden rondom privacy.

Er volgen een aantal maatregelen waarvoor het handig is een verantwoordelijke aan te wijzen binnen uw organisatie (privacyfunctionaris). Dit is niet per se de Functionaris Gegevensbescherming, de wettelijke functie die u ook zult moeten invullen voor uw organisatie.

Inventariseer welke gegevens binnen uw school van leerlingen worden vastgelegd, op welke plek en met welke reden.

Bespreek deze vastlegging met de directie, met docenten, de IT-verantwoordelijke en ander niet-onderwijzend personeel. Stel duidelijke regels vast voor de verwerking van privacygevoelige gegevens en benoem benodigde maatregelen. Ga als privacyverantwoordelijke binnen de school met de ondernemingsraad en medezeggenschapsraad om tafel en informeer hen over hoe met de gegevens van leerlingen en docenten wordt omgegaan. Privacy en informatiebeveiliging zijn vervolgens ook van belang voor docenten, niet-onderwijzend personeel en de ouders van leerlingen. Deze informatie zult u ook moeten delen via schoolgids en/of website.

Stel vast welke maatregelen reeds getroffen zijn om bedoelde gegevens te beveiligen tegen onrechtmatig gebruik.

Bij onrechtmatig gebruik gaat het om elk gebruik dat niet in overeenstemming is met de vastgelegde reden van het vastleggen van de betreffende leerlinggegevens. Ongetwijfeld zijn al veel maatregelen getroffen. Die brengt u in kaart.



Kijk kritisch naar de leverancierscontracten.

Dit is een belangrijke beveiligingsmaatregel. Enerzijds wilt u vaststellen dat u de juiste afspraken over beveiliging en verantwoordelijkheidsverdeling heeft gemaakt, anderzijds heeft u ook overzicht nodig ten aanzien van de lopende contracten en contactpersonen daarbij. Het is dus verstandig om uw contracten voor digitale onderwijsmiddelen onder te brengen bij één partij. Daardoor voorkomt u een complexe administratie aan uw kant.

Zorg ervoor dat u een stevige gesprekspartner bent. Als sprake is van medeondertekenaars van het convenant dan weet u dat u goed zit. Wel is het van belang dat u kritisch nagaat of de in de verwerkersovereenkomst opgenomen informatie voor u toereikend is (de verwerkersovereenkomst is voor wat betreft de inhoud van de privacybijsluiter leverancier specifiek).

Beoordeel of de getroffen beveiligingsmaatregelen toereikend zijn.

De in kaart gebrachte beveiligingsmaatregelen toetst u vervolgens met hetgeen u aan maatregelen nodig acht gezien de aard en omvang van de vastgelegde gegevens. Als uitkomst van deze toets zult u mogelijk vaststellen dat verdere beveiligingsmaatregelen getroffen moeten worden.

Heutink ICT kan u hierbij helpen

Als u verdere informatie ten aanzien van bescherming van persoonsgegevens en het Convenant digitale onderwijsmiddelen en privacy wenst zijn wij u graag van dienst. Belt of mailt u ons gerust.