DePrivacyGuru

Online onderwijs

Hoe regel je het veilig en zorg je er voor aan de AVG te voldoen?

Mr. Nico J. Mookhoek CIPP/E

Inhoudsopgave

Door de corona crisis zijn veel onderwijsinstellingen overgestapt naar online onderwijs.

Tijdens de lock down betekende dat razendsnel overstappen naar allerlei nieuwe toepassingen om het onderwijs zo goed en zo kwaad mogelijk doorgang te laten vinden

Na de lock down gingen de lagere en middelbare scholen weer open en gingen deze weer terug naar fysiek onderwijs. Veel HBO en Universitaire opleidingen bleven het onderwijs geheel of deels online verzorgen.

Door de snelheid waarmee over geschakeld moest worden naar online, bleven de privacyaspecten wel eens onderbelicht. Nu het onderwijs voorlopig online gegeven zal worden en een terugkeer naar online onderwijs voor de lagere en middelbare school ook niet uitgesloten kan worden, is het goed om ook aandacht te besteden aan de privacyaspecten. De privacy waakhond, de Autoriteit Persoonsgegevens kwam begin oktober met een reeks aanbevelingen.

In deze white paper behandelen we deze op een praktische manier en vullen we ze aan met onze eigen ervaringen.

In een apart paragraafje staan we stil bij proctoring, het online surveilleren tijdens tentamens

De 5 aanbevelingen van de AP in de praktijk

AUTORITEIT
PERSOONSGEGEVENS

De eerste 2 stappen zijn vrij voor de hand liggend en wijken niet veel af van de stappen die de school heeft genomen voor de andere verwerkingen van persoonsgegevens.

1. **Bepaal het doel waarvoor de online toepassing wordt ingezet**.

In de praktijk zal het doel niet anders zijn dan het doel waarvoor de school ook andere persoonsgegevens vastlegt. Dat doel zal zijn het verzorgen van goed onderwijs. Of meer precies omschreven: het geven van onderwijs in een periode waarin fysiek onderwijs niet mogelijk of toegestaan is.

2. **Bepaal grondslag voor de verwerking**.

De grondslag zal mijns inziens geen andere zijn dan de grondslag waarop de onderwijsinstelling ook andere persoonsgegevens verwerkt: het algemeen belang van goed onderwijs.

De 3e stap zal voor de meeste verwerkingen van persoonsgegevens binnen de onderwijsinstelling niet nodig zijn, maar wordt door de AP expliciet aangeraden voor onlineonderwijs.

3. Maak een Data Protection Impact Asessment (DPIA)

Een DPIA is een instrument om zicht te krijgen op de risico's van bepaalde verwerking van persoonsgegevens en de maatregelen die de organisatie gaat treffen om deze risico's af te dekken.

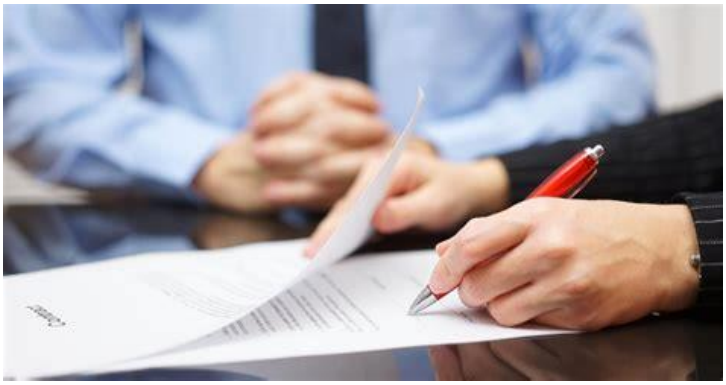
De AVG geeft vrij open normen wanneer een DPIA uitgevoerd dient te worden. De Autoriteit Persoonsgegevens heeft dit nader invulling gegeven door een lijst te publiceren waarvoor de AP een DPIA noodzakelijk acht. Voor online lessen raadt de AP dus ook een DPIA aan.

Er is geen vaste vorm voor een DPIA, je mag dus zelf kiezen hoe je deze doet. De AVG geeft aan dat een DPIA in elk geval moet voldoen aan:

- Een systematische beschrijving van de beoogde gegevensverwerkingen en de doeleinden hiervan.
- Een beoordeling van de noodzaak en de proportionaliteit van de verwerkingen. Dat houdt in: is het verwerken van persoonsgegevens op deze manier noodzakelijk om uw doel te bereiken? En is de inbreuk op de privacy van de betrokkenen (de mensen van wie je gegevens verwerkt) niet onevenredig in verhouding tot dit doel?
- Een beoordeling van de privacy risico's voor de betrokkenen.
- De beoogde maatregelen om
    - de risico's aan te pakken (zoals waarborgen en veiligheidsmaatregelen) en
    - aan te tonen dat je aan de AVG voldoet

Op basis van deze criteria hebben we een format ontwikkeld voor een DPIA, je kunt dat op onze site vinden.

In het geval van online lessen raadt de AP aan om bij de DPIA ook de betrokkenen, dat zijn dus de studenten en de docenten, te betrekken. Daarnaast merkt de AP op dat je ook rekening moet houden met andere privacy risico's dan die van de persoonsgegevens alleen. Denk daarbij aan het recht op privacy van je privé leefomgeving. Meer daarover kun je te weten komen in de eerste module van onze onlinetraining "Efficiënt werken met de AVG".



4. **Sluit een verwerkersovereenkomst af met de leverancier van de online toepassing**

Om online onderwijs te geven zul je gebruikmaken van een standaard online toepassing. Dergelijke platforms zijn bijvoorbeeld Blackboard Collaborate, de Virtual classroom van Bongo, Webex van Cisco, Microsoft Teams of Zoom. Die laatste raden we vanwege privacy risico's overigens af te gebruiken.

Omdat de online toepassing persoonsgegevens van jouw organisatie verwerkt (in casu beelden van docenten en studenten) zijn zij verwerker van die gegevens. Dat betekent dat jij als verwerkingsverantwoordelijke de plicht hebt om met hen een verwerkersovereenkomst af te sluiten.

In de praktijk zullen deze verwerkers je hoogstwaarschijnlijk al kort na de introductie van de AVG in mei 2018 een verwerkersovereenkomst toegestuurd hebben. Het is goed om dit even te checken en ook te kijken of deze getekend en geretourneerd is.

5. **Betrek de FG bij de inzet van onlineonderwijs**

Een goede FG denkt vanuit zijn discipline proactief mee over de inzet van onlineonderwijs. Daarmee heeft de FG mijns inziens een faciliterende (hoe maken we dit mogelijk met inachtneming van bescherming van de persoonsgegevens) en een toezichthoudende rol (een vertegenwoordiging namens de AP).

6. **Zorg voor beleid en richtlijnen voor online lessen**

Bij een beleid denken mensen vaak meteen aan dikke pakken papier die door niemand gelezen worden. Daarom raden we eerder aan om een aantal richtlijnen op papier vast te leggen. Daarbij is ook de cultuur en omvang van het opleidingsinstituut bepalend. Een grote hbo-instelling of universiteit zal eerder een uitgebreid beleid hebben; bij een middelbare school zal een aantal richtlijnen kunnen volstaan.

In het beleid of de richtlijnen leg je een aantal wezenlijke en praktisch zaken over de online lessen vast.

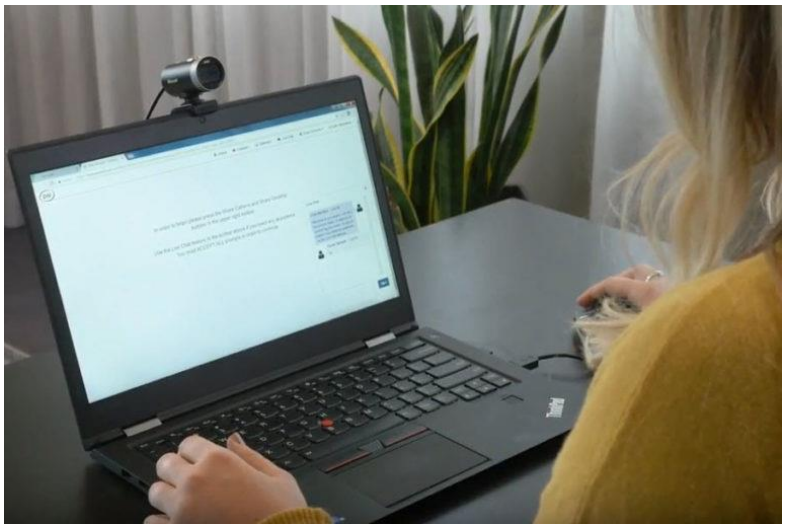
Allereerst de afspraken over het in beeld brengen van studenten/leerlingen en docenten en het maken van opnames. Hierin wijs je de studenten/leerlingen en docenten er onder andere op om te zorgen voor een neutrale omgeving zonder persoonlijke voorwerpen als ze in beeld gebracht worden, om de microfoon en camera uit te schakelen als die niet meer functioneel zijn etc.

Wat betreft het opnemen van de lessen, daarover blijkt in de praktijk veel reuring te bestaan. Sommige scholen nemen de lessen op met het argument dat studenten/ leerlingen die de lessen niet kunnen volgen die later terug kunnen kijken, andere scholen hebben het beleid om geen opnamen te maken van de lessen. Van docenten krijg ik ook nogal eens vragen hierover omdat ze zich hier niet prettig bij voelen. Ik zie geen reden om de lessen op te nemen, immers in de fysieke lessen gebeurt dit ook niet. Nu de lessen online worden gegeven en het platform deze mogelijkheid biedt, zou de onderwijsinstelling opeens wel een belang hebben om dit te doen?
De Autoriteit Persoonsgegevens adviseert onderwijsinstelling bij de opnamen geen studenten/ leerlingen in beeld te brengen als dit niet noodzakelijk is om het doel te realiseren.

In het beleid regel je ook je ook hoe je betrokkenen informeert. Hiervoor gelden dezelfde eisen als voor de andere verwerkingen van persoonsgegevens: deel het doel mee, de bewaartermijnen, de verantwoordelijke etc.
Om dit te regelen raad ik je aan om te starten met het toevoegen van de verwerking "online lessen" aan het Register Gegevensverwerking. Daarmee heb je meteen de punten waarover je de betrokkenen dient te informeren, en je houdt je Register up-to-date.

Vergeet niet dat uiteindelijk de docent "in de klas" er mee uit de voeten moet kunnen. Die heeft behoeft aan duidelijke en eenvoudige instructies waar hij mee aan de slag kunnen. Vertaal daarom het beleid en de richtlijnen daarom altijd naar heldere instructies.

Proctoring



Over proctoring, het online surveilleren met software tijdens tentamens is veel te doen geweest.
Jongerenorganisaties liepen hiertegen te hoop met privacy-bezwaren en 2 Hogescholen, Avans Hogeschool en de Hogeschool van Leiden hebben gezegd deze methode niet toe te zullen passen. Zij vertrouwen erop dat de studenten tijdens het tentamen niet zullen frauderen.

Uiteindelijk heeft de centrale studentenraad van de Universiteit van Amsterdam (UvA) een kort geding aangespannen tegen het gebruik van de software.
De Rechtbank van Amsterdam stelde de UvA in het gelijk: het is haar toegestaan om online surveillance software te gebruiken.
De UVA, zo oordeelt de voorzieningenrechter, heeft ook voldaan aan alle regels en beginselen van de AVG.
De grondslag voor de gegevensverweking ligt in artikel 6 lid 1 sub e AVG. De UvA heeft een in de wet geregelde publieke taak en in verband met Covid-19 is er een noodzaak om online proctoring in te zetten bij het afnemen van tentamens die vanuit huis worden gemaakt. Van een onrechtmatige inbreuk op de privacy is dan ook geen sprake.
De overwegingen geven een goed beeld van de voorwaarden waaraan voldaan moet worden bij het gebruik van online surveillance software.

Allereerst merkt de rechter op dat de UvA op de surveillance software, in dit geval van het bedrijf Proctorio een DPIA heeft gedaan om de risico's van de verwerking in kaart te brengen. Bij die DPIA zijn onder andere de Security Officer, de Informationmanager, de Privacy Officer, de FG en de Chief Information Security Officer (CISO) betrokken.
Uit de DPIA blijkt dat blijkt dat de gegevensbeschermingsfunctionarissen (de FG en de CISO) hun goedkeuring hebben gegeven aan de inzet van de software.

Voorafgaand aan het besluit om de surveillance software in te zetten heeft de UvA een pilot gehouden. Daarbij is de FG om advies gevraagd en deze heeft positief geadviseerd.

Met de verwerker, Proctorio, is een verwerkersovereenkomst afgesloten. Daarin onderwerpt deze zich aan de Europese privacywetgeving. De gegevens worden opgeslagen op een server in München (Duitsland) en er zullen dus geen gegevens buiten de Europese Unie worden verwerkt of opgeslagen. Bij gebruik van de helpdesk (die in Servië is gevestigd) worden geen gegevens gedeeld, tenzij de student daar toestemming voor geeft

Kortom met de nodige waarborgen is het toegestaan om online surveillance software in te zetten.

Zoek draagvlak

Bij alle technische aspecten zou je het haast over het hoofd zien maar een belangrijk uitgangspunt is ook de "softe" kant: zorg voor draagvlak. Ook voor het privacy beleid voor online lessen en proctoring geldt: zoek draagvlak binnen de organisatie voor het beleid en de richtlijnen. Probeer studentenraad, medezeggenschapsraad, ouder- en leerlingenraad hierbij te betrekken. Dat scheelt achteraf een hoop onnodig gedoe en creëert draagvlak voor de instructies.

DePrivacyGuru

Wij helpen je graag met al je vragen over online toepassingen in het onderwijs. Of het nu gaat om een second opinion over een toepassing, een uitgewerkt advies in een bepaalde situatie, tips om beleid te vertalen in instructies of het maken van een DPIA: wij staan voor je klaar.

Ruime ervaring in het onderwijs

Wij hebben ruime ervaring in het onderwijs, zowel in adviserende rollen als in uitvoerende rol als Functionaris Gegevensbescherming.
Wij snappen dus de cultuur en kennen het klappen van de "onderwijszweep".

Maak meteen een afspraak voor een online consult op de website

info@deprivacyguru.nl

085-2223232

DePrivacyGuru: "Privacy zonder gedoe"