Handreiking: AVG en digitaal onderwijs in Coronatijden

Inhoudsopgave

1. Inleiding – omschrijving doel Handreiking

Deze Handreiking is opgesteld door het IBP-team van Kennisnet/saMBO-ICT. Het doel is om mbo-scholen te adviseren hoe om te gaan met de AVG en digitaal onderwijs gedurende de Coronacrisis. Dit document kan door het IBP-team worden gebruikt voor handreikingen, nieuwberichten, FAQ's etc.

De Handreiking kent de volgende opbouw. Er worden allereerst algemene handvatten gegeven zodat een onderwijsinstelling zelf kan nagaan of de voorgenomen vorm van digitaal onderwijs in overeenstemming is met de AVG.
Daarna worden twee vormen van digitaal onderwijs, namelijk digitaal lesgegeven en digitaal toetsen verder onder de loep genomen. Het hoofdstuk over digitaal lesgeven is vormgegeven aan de hand van praktische vragen uit het veld. Daarbij wordt onderscheid gemaakt tussen de positie van docenten en de positie van studenten. Bij digitaal toetsen is gekozen voor een beschrijving van de verschillende vormen van digitaal toetsen en examineren.
De Handreiking wordt afgesloten met praktische tips voor onderwijsinstellingen en docenten.

De Handreiking is specifiek geschreven met het oog op de huidige Coronacrisis en is dus met name bedoeld voor het schooljaar 2020-2021. Dit is een bijzondere en uitzonderlijke situatie, die in bepaalde gevallen een grotere inbreuk op de privacy rechtvaardigt dan in normale omstandigheden het geval zou zijn. De kaders die in dit stuk geboden worden kunnen dus niet zonder meer worden doorgezet naar de tijden na Corona.

2. Algemene handvatten: AVG en digitaal onderwijs

Bij digitale onderwijsactiviteiten (zoals lessen via een online meeting of digitale toetsen) worden altijd persoonsgegevens van studenten en docenten verwerkt. Dit betekent dat de AVG van toepassing is. In de AVG is bepaald dat persoonsgegevens moeten worden verwerkt op een wijze die rechtmatig, behoorlijk en transparant is. Hieronder vind je algemene handvatten die je kunnen helpen om te bepalen of een onderwijsactiviteit in overeenstemming is met de AVG. Overleg zo nodig met de IBP-functionaris of FG van de onderwijsinstelling.

I. Uiteraard wordt eerst het **doel** van de onderwijsactiviteit vastgesteld. Wat moet er bereikt worden met de onderwijsactiviteit? Daarbij wordt ook onderzocht **welke persoonsgegevens** nodig zijn om dit doel te bereiken (bijvoorbeeld: docent of student wel of niet in beeld, wel of geen opname van de activiteit, deel je resultaten van studenten met de hele groep of alleen met de student persoonlijk etc.). Bij de bepaling hiervan is de hoofdregel van de AVG dat je nooit meer persoonsgegevens gebruikt en deelt dan nodig om het doel te bereiken.

II. Dan wordt de **vorm** van de digitale onderwijsactiviteit bepaald en de applicatie/tooling die je daarbij nodig hebt. Zo kan je bijvoorbeeld bij het overdragen van kennis ervoor kiezen om alleen een powerpoint presentatie te laten zien met de stem van de docent die de presentatie geeft. Is er sprake van een interactieve les, waarbij inbrengen en samenwerking van studenten noodzakelijk is dan kan het nodig zijn dat de hele groep in beeld gebracht worden. En wil je achteraf een les, een praktijkvoorbeeld of een activiteit bespreken dan is het opnemen daarvan noodzakelijk. Ook als het gaat om toetsen en examineren zijn er verschillende mogelijkheden. Die worden hieronder besproken in hoofdstuk 4.
Grondregel is hierbij ook weer dat je de keuze voor de vorm moet kunnen onderbouwen. Als je dezelfde onderwijskundige doelstellingen kunt bereiken met een vorm die minder impact heeft op de privacy van de student en docent, dan moet je daarvoor kiezen.

Een veel gestelde vraag over online onderwijs:
Welke applicatie of tooling kan ik veilig gebruiken voor mijn online onderwijs?
Gebruik in eerste instantie applicaties die de schoolorganisatie ter beschikking stelt en ondersteunt. Vermijd zoveel mogelijk het gebruik van gratis online tools. Mocht dat toch

noodzakelijk zijn maak dan gebruik van de appchecker om te bekijken of dat veilig kan. De appchecker vind je op https://www.kennisnet.nl/diensten/kennisnet-appchecker/

III. Vervolgens ga je na welke **wettelijke grondslag** van toepassing is op de digitale onderwijsactiviteit. Als er geen wettelijke grondslag is, dan verbiedt de AVG namelijk het verwerken van persoonsgegevens.

Persoonsgegevens studenten

Voor het vo vallen de uitvoering van onderwijs, het rapporteren van de vorderingen van leerlingen/studenten, het afnemen van eindexamens en het uitreiken van diploma's onder de wettelijke taak van de school op grond van de Wet op het voortgezet onderwijs (artikelen 2, 23b en 29 WVO).
Dit geldt ook voor de verzuimregistratie in verband met de Leerplichtwet.
In de meeste gevallen is de wettelijke taak van de onderwijsinstelling dan ook de grondslag voor het uitvoeren onderwijs en het verwerken van de persoonsgegevens van leerlingen in het vo. Deze grondslag wordt ook wel de vervulling van een publieke taak genoemd.

Voor het mbo geldt dat in ieder geval tot studiejaar 2022-2023 een onderwijsovereenkomst is afgesloten met de student (art. 8.1.3 Web) en dat de grondslag voor de uitvoering van onderwijs, toetsing en examinering de uitvoering van deze onderwijsovereenkomst is. Daarnaast heeft het mbo ook wettelijke taken, bijvoorbeeld als het gaat om verzuimregistratie in verband met de kwalificatieplicht (art. 4a en 4c Leerplichtwet) en het uitreiken van diploma's. In die gevallen is de grondslag de wettelijke taak.

Persoonsgegevens docenten
Als het gaat om persoonsgegevens van docenten dan is in de meeste gevallen de grondslag de uitvoering van de arbeidsovereenkomst.

IV. **Informeer** de studenten en docenten over de verwerking van de persoonsgegevens. Dit kan bijvoorbeeld in een algemeen privacy statement.
Als er incidenteel persoonsgegevens op een andere wijze dan gebruikelijk worden verwerkt, dan is het goed om die informatie apart te verstrekken voordat wordt overgegaan tot die incidentele verwerking van persoonsgegevens.

V. Check met de IBP-functionaris of de onderwijsactiviteit in deze vorm is vastgelegd in het **dataregister**. De IBP-functionaris zal dit zo nodig aanvullen.

3. Digitaal lesgeven

3.1. Algemeen

Onder digitale of online lessen worden zowel lessen verstaan die voor iedereen digitaal zijn (dus zowel de docent als alle studenten maken gebruik van een eigen device om de les te geven of te volgen) als lessen die worden gestreamd. In dat geval is bijvoorbeeld de docent met de helft van de klas op school en volgen de andere studenten de les thuis of in een ander lokaal via een device. Over digitaal lesgeven worden veel vragen gesteld. Hieronder vind je de meest gestelde vragen.

Mag een docent online lessen opnemen?
Je mag online lessen opnemen als je vooraf hebt bepaald voor welk onderwijsdoel je de opname nodig hebt. Als er studenten in beeld komen heb je wel hun toestemming nodig. Hoe formeel je die toestemming wilt regelen is afhankelijk de manier waarop de opgenomen activiteit vervolgens wordt gebruikt. Als het alleen gaat om het eenmalig kunnen terugkijken door afwezige studenten volstaat de

mondelinge mededeling bij de start van de opname. Studenten die bezwaar hebben om in beeld te komen kunnen dan hun webcam uitzetten tijdens de les.
Wil je de opname structureel gaan aanbieden in de ELO? Dan moet je je afvragen of je wel van toestemming van studenten afhankelijk wilt zijn (toestemming kan immers altijd worden ingetrokken en dan is de opname niet meer bruikbaar). Hou daarom bij voorkeur de studenten buiten beeld en verwerk vragen en reacties anoniem (lees ze voor vanuit de chat).
Voor de docent geldt dat deze de mogelijkheid moet hebben om de video-opname aan te passen (bijvoorbeeld de bloopers eruit knippen) voordat de opname beschikbaar wordt gesteld.

Bij het streamen van een les is het belangrijk dat de studenten die in het lokaal aanwezig zijn niet in beeld komen. Het opnemen van hun stem is toegestaan. Als dit nodig is voor de bescherming van de privacy van een student of de docent kan een gedeelte van de opname na afloop van de les uit de opname worden geknipt.

Aandachtspunten:
1. Vertel vooraf aan de studenten dat de les wordt opgenomen, en voor welk doel.
2. Vertel wie toegang heeft tot de opname (wie gaat de video terugkijken?).
3. Zorg dat de video op een veilige plek wordt opgeslagen, gebruik daarvoor de digitale omgeving van de onderwijsinstelling. Maak géén gebruik van een usb-stick en zorg dat het niet op een privé-computer of telefoon wordt opgeslagen.
4. Deel de video niet publiek (bijvoorbeeld via een publieke link/YouTube etc.).
5. Bewaar de beelden niet langer dan nodig is.
6. Zorg dat er geen studenten in beeld komen, omdat hier toestemming van iedere student voor nodig is (zie hierboven). Start de opname dus pas na de aanwezigheidscontrole waarbij namen worden opgenoemd.
7. Leg in de gedragscode of – regels voor studenten vast dat zij de opnames alleen mogen bekijken voor hun schoolwerk, dus niet bewerken/delen via social media etc.

Mogen studenten (online) lessen opnemen?
Het opnemen van digitale lessen of andere digitale onderwijsactiviteiten door studenten is niet toegestaan, omdat dat inbreuk maakt op de veilige leeromgeving en privacy van zowel de docent als de andere studenten.

Aandachtspunten:
1. Informeer studenten hierover door middel van een gedragscode en ook aan het begin van de les. Leg uit dat de reguliere school- en gedragsregels van toepassing zijn, ook al is de les digitaal.
2. Richt de digitale omgeving zo in dat alleen de docent een opname kan starten.
3. Het is niet helemaal uit te sluiten dat een student met bijvoorbeeld een mobiele telefoon een opname maakt, net zoals dit ook mogelijk is in een fysieke les. Hiervoor kunnen de reguliere disciplinaire maatregelen worden opgelegd op basis van de huisregels/gedragscode voor studenten.

3.2 Digitaal lesgeven – de persoonsgegevens van de docent

Kan je als docent verplicht worden om de webcam te gebruiken bij het verzorgen van online onderwijs?
Ja, maar het in beeld brengen van de docent moet wel nodig zijn voor het doel dat je wilt bereiken met de les.
De grondslag hiervoor is de overeenkomst die is gesloten tussen de onderwijsinstelling en de docent op grond waarvan de docent de taak heeft om goed onderwijs te verzorgen. Mocht een docent zwaarwegende bezwaren hebben dan is het belangrijk om met de docent in gesprek te gaan en samen naar oplossingen te zoeken. Het argument dat er van alles met de beelden kan gebeuren (als studenten stiekem opnames maken) speelde in de fysieke lessituatie ook al. Hierbij geldt dat de onderwijsinstelling de privacy van de docenten moet beschermen, zoals dat ook het geval is in een normale lessituatie. Dit doet de onderwijsinstelling door te zorgen dat de afspraken over digitaal lesgeven helder zijn gecommuniceerd met studenten en ook worden gehandhaafd. Hoe beter en scherper de afspraken met studenten zijn en kunnen worden afgedwongen, des te minder docenten bezwaar zullen hebben tegen het in beeld komen tijdens digitaal lesgeven.

Aandachtspunten:
1. Het moet voor de docent duidelijk zijn wat het doel van de les is en waarom het nodig is dat de docent in beeld komt.
2. Zorg dat er binnen de instelling duidelijke regels/gedragscodes voor studenten zijn met een verbod op het maken van opnames en (dus ook) het bewerken en plaatsen van materiaal op social media etc. Help docenten door een standaarddocument met een samenvatting van de regels beschikbaar te stellen, die docenten bij de start van de les aan studenten kunnen laten zien.
3. Als docent is het van belang om te zorgen voor privacywaarborgen op de thuiswerkplek:
    - zorg dat je bureau (voor zover in beeld) leeg is;
    - zorg dat je geen documenten hebt openstaan die niet voor de studenten bestemd zijn als je je scherm deelt;
    - zet je eigen achtergrond in de online omgeving uit en zorg voor een rustige andere achtergrond.
4. Onderwijsinstellingen moeten voor duidelijke instructies/handleidingen zorgen, zodat de docent bijvoorbeeld de achtergrond eenvoudig zelf kan aanpassen.

3.3 Digitaal lesgeven – de persoonsgegevens van de leerling/student

Kun je bij online onderwijs je studenten verplichten om hun camera aan te zetten?
Allereerst moet je vaststellen wat het doel van de digitale les is en of het daarvoor nodig is dat de studenten in beeld komen/zijn. Het kan bijvoorbeeld nodig zijn om de student te zien om de aanwezigheid te registreren (zie ook de vraag hieronder). Verder kan het voor het uitvoeren van goed onderwijs belangrijk zijn dat de studenten in beeld zijn, bijvoorbeeld bij een interactieve les, om de ze goed te kunnen begeleiden. Ook als studenten met elkaar moeten samenwerken kan het van belang zijn dat ze elkaar kunnen zien. Het is dus mogelijk om studenten te verplichten om hun camera aan te zetten en de professional (docent) bepaalt of en wanneer dit noodzakelijk is.
De grondslag voor het verzorgen van goed onderwijs is de wettelijke taak (in het vo) en de onderwijsovereenkomst in geval van mbo-scholen.

Aandachtspunten:
1. Instrueer studenten goed over wat ze zelf kunnen doen om de impact op hun privacy te beperken, bijvoorbeeld door het instellen of vervagen van de achtergrond.
2. Als studenten bezwaren hebben, dan ga je met ze in gesprek en zoek je naar een oplossing.
3. Bedenk dat de camera ook niet de gehele les aan hoeft te staan, maar alleen als de docent dat noodzakelijk vindt en er om vraagt.

Hoe registreert een docent aan- en afwezigheid bij online lessen?
Een school heeft de wettelijk verplichting om aanwezigheid (participatie) bij de les te controleren en te registreren. In de digitale omgeving is hiervoor de keuze gemaakt dit middels een combinatie van beeld en geluid te doen. Omdat die controle met stem alleen onvoldoende zeker kan zijn, kan een onderwijsinstelling besluiten dat de docenten door middel van beeld moeten controleren of de juiste persoon aan de les meedoet. De grondslag hiervoor is dus de wettelijke verplichting van scholen om verzuim te registeren. De docent mag de studenten dus verplichten om – aan het begin van de les – hun camera aan te zetten om hun aanwezigheid te registeren.

Aandachtspunten:
1. Leg studenten uit waarom de camera aan het begin van de les aangezet moet worden (en daarna uitgezet wordt als dat niet langer noodzakelijk is).
2. Zorg dat binnen de onderwijsinstelling iedereen dezelfde regels hanteert zodat er geen discussie ontstaat bij studenten.
3. Maak afspraken over een procedure als de student meldt dat zijn camera defect is of zorg voor een alternatief voor studenten als zij geen laptop/telefoon met camera hebben.

4. Bedenk dat het aanzetten van de camera aan het begin van de les geen garantie is dat de leerling/student de rest van de les aanwezig is en/of participeert in de les.

4. Digitaal toetsen

4.1. Inleiding

Door de Coronacrisis hebben scholen de afgelopen maanden de nodige ervaring opgedaan met toetsen op afstand en het inrichten van een veilige en betrouwbare digitale leeromgeving. Voor het toetsen op afstand bestaan veel verschillende mogelijkheden die ieder hun eigen voor- en nadelen kennen, zowel op didactisch vlak als op technisch gebied. Ook heeft iedere manier om toetsen af te nemen weer een andere impact op de privacy van de student.

Bij een mondelinge 1 op 1 toets met behulp van video-bellen, zonder dat de beelden worden opgeslagen, is de privacy-impact bijvoorbeeld lager dan bij een grootschalig digitaal afgenomen examen waarbij alle beelden worden opgeslagen en achteraf door een examensecretaris worden bekeken en geanalyseerd.
Kies je als docent voor een manier om snel de voorkennis van studenten op te halen, dan is een quiz bijvoorbeeld voldoende. Een dergelijke toets hoef je niet te beveiligen omdat deze niet kwalificerend is. Maak daarbij in principe gebruik van applicaties die jouw school standaard aanbiedt.

Na het vaststellen van het doel en de noodzaak van de afname van de digitale toets of het examen is het belangrijk om na te gaan welke persoonsgegevens noodzakelijk zijn om dat doel te bereiken. De grondslag hiervoor is veelal dezelfde als bij online onderwijs: de wettelijke taak van de vo-school of de onderwijsovereenkomst die de mbo-instelling met de student heeft afgesloten.
Daarna is het zaak om een passende vorm te vinden voor toetsafname en ook hier geldt de basis regel dat daarbij die vorm gekozen wordt die het minste impact heeft op de privacy van de leerling/student.
Check tenslotte bij de IBP-functionaris of de toetsafname in deze vorm is vastgelegd in het dataregister. De IBP-functionaris zal het dataregister zonodig bijwerken.

Hieronder worden de verschillende scenario's waarop toetsen op afstand kunnen worden afgenomen besproken. Daarbij wordt aangegeven wat de aandachtspunten zijn op het gebied van beveiliging en privacyaspecten van de betreffende toetsvorm.

Check vooraf: is toetsen op andere wijze mogelijk?

Voordat je een digitale vorm van toetsafname overweegt moet je voor wat betreft summatieve kennistoetsen onderzoeken of het niveau van de kennis en vaardigheden van de studenten ook op een andere manier kan worden bepaald. In het Servicedocument 4.0 en de Handreiking Verantwoord Diplomabesluit wordt uitgebreid ingegaan op de mogelijkheden.

4.2. Leeswijzer

De vormen van digitale examinering zijn gesorteerd op privacy-impact voor de student (van laag naar hoog) en afgezet tegen het toetsdoel. Bij het zoeken van een geschikte wijze van toetsen in de school of op afstand, is het namelijk van belang om altijd te zoeken naar de vorm van toetsafname die de minste impact heeft op de privacy van de student. Je komt dus pas aan een volgende vorm van toetsafname toe als de voorgaande vorm om psychometrische overwegingen (betrouwbaarheid en validiteit) of zwaarwegende organisatorische redenen niet geschikt is.

4.3. Vormen om digitaal summatieve toetsen af te nemen

Locken of blokken van het device

Locken is het afsluiten van software en apps, of het beperken van functionaliteiten binnen software en

apps, zodat je geen gebruik kunt maken van digitale hulpmiddelen die tijdens de toets niet zijn toegestaan.
Blokken is het afsluiten en/of overnemen van specifieke onderdelen die toebehoren tot het device zoals camera, microfoon, touchfunctionaliteit, scherm etc. Dit betekent dat een leerling/student die functionaliteiten niet zelf kan inschakelen.

Inbreuk op de privacy van de leerling/student: matig

Voordelen:
- Frauderen door het gebruik van apparatuur en apps die niet zijn toegestaan wordt hiermee ondervangen.

Nadelen:
- Andere mogelijkheden tot frauderen worden hiermee niet ondervangen: studenten kunnen met elkaar of andere personen overleggen of een boek of spiekbriefje gebruiken. Surveilleren blijft dus noodzakelijk.

Aandachtspunten:
1. Ga na of deze vorm van toetsen een invulling is van het bestaande toets- of examenreglement of dat het nodig is om het reglement aan te passen. Ga ook na of de medezeggenschap (CSR) bij die aanpassing moet worden betrokken.
2. Er moet een verwerkersovereenkomst zijn afgesloten met de leverancier van de software die wordt gebruikt voor locking/blokken als er persoonsgegevens worden verwerkt door de leverancier.
3. Als de software wordt geïnstalleerd op het eigen device van de student is een duidelijke instructie nodig en een goede test vooraf en met ondersteuning (noodnummer o.i.d.) voor studenten die hiermee problemen ervaren.
4. Aan studenten die bezwaar hebben tegen het installeren van de software op hun eigen device moet er en een alternatief geboden worden, zoals een leenlaptop van de school.
5. Mochten studenten geen geschikt device tot hun beschikking hebben, dan moet er een alternatief kunnen worden geboden.
6. Studenten moeten kunnen beschikken over een goede en stabiele internetverbinding en een rustige ruimte om in te kunnen werken.
7. Tot slot moet er ook een goede instructie zijn voor het (automatisch) verwijderen van de software na afloop van de toets, zodat het device van de leerling/student niet langer gelockt/geblokt is dan noodzakelijk.

Naast locken en blokken bestaan ook mogelijkheden om te studenten te monitoren. Onder monitoren verstaan we de verschillende surveillance-opties of door de docent of geautomatiseerd door ‘het systeem’ (proctoring): kijken of de student niet spiekt of fraudeert. Dat kan “live” in het klaslokaal door een rondlopende docent of surveillant, maar ook online. Op dit vlak onderscheiden we drie opties:
1. live monitoring,
2. monitoring door opname, opslag en controle achteraf,
3. automatische proctoring.

Alle vormen van online monitoring hebben een grote impact op de privacy van de student. Vanwege het doel (fraude tegengaan) kan een student niet de achtergrond blurren of vervangen door een plaatje. Een onderwijsinstelling moet zich daarom altijd eerst afvragen of een dergelijke grote inbreuk wel wenselijk en echt noodzakelijk is.

Live monitoring

Het online monitoren van de student gebeurt live door middel van beeld-/geluidsopname, toegang tot het scherm, een webcam en/of mobiele telefoon. De surveillant/docent kan de student direct corrigeren of ingrijpen indien van toepassing en gewenst.

Inbreuk op de privacy van de student: groot

Voordeel:
- De mogelijkheden voor de student om te frauderen worden hiermee grotendeels ondervangen.

Nadelen:
- Studenten kunnen andere tabbladen en programma's open hebben staan. Dit is niet zichtbaar voor de surveillant/docent. Dit kan worden ondervangen door live monitoring te combineren met locken.
- Een surveillant/docent kan maar een beperkt aantal studenten tegelijk monitoren.

Aandachtspunten:
1. Ga na of deze vorm van toetsen een invulling is van het bestaande toets- of examenreglement of dat het nodig is om het reglement aan te passen en ga na of de medezeggenschap (CSR) bij die aanpassing moet worden betrokken.
2. Er moet een verwerkersovereenkomst zijn afgesloten met de leverancier van de software die wordt gebruikt voor monitoring.
3. De privacy-impact van live monitoring is groot. Een docent of surveillant krijgt veel informatie te zien over de privé-omgeving van de leerling/student. Het is goed om van te voren in gedragsregels voor docenten vast te leggen hoe een docent moet omgaan met deze informatie. Bijvoorbeeld in welke gevallen een verdenking op fraude ontstaat, wat een docent in dat geval doet (direct ingrijpen of achteraf rapporteren), of een docent een /student mag aanspreken op zijn/haar privésituatie die in beeld komt etc.
4. Studenten moeten vooraf goed geïnformeerd worden over het doel van de monitoring, de wijze waarop monitoring plaatsvindt, welke signalen leiden tot een vermoeden van fraude en wat er met de informatie wordt gedaan die docenten te zien krijgen.
5. Als er aparte software geïnstalleerd moet worden op het eigen device van de studenten is een duidelijke instructie nodig en een goede test vooraf en met ondersteuning (noodnummer o.i.d.) voor studenten die hiermee problemen ervaren. Dit is niet nodig als monitoring via bijvoorbeeld Teams plaatsvindt en de student daarmee al bekend is via de digitale lessen.
6. Aan studenten die bezwaar hebben tegen het installeren van aparte software op hun eigen device moet er en een alternatief geboden worden, zoals een leenlaptop van de school.
7. Mochten studenten geen geschikt device tot hun beschikking hebben, dan moet er een alternatief kunnen worden geboden.
8. Studenten moeten kunnen beschikken over een goede en stabiele internetverbinding en een rustige ruimte om in te kunnen werken. Als zij dat niet hebben moet er een alternatief geboden worden, bijvoorbeeld om de toets op school af te nemen.
9. Mocht er aparte software geïnstalleerd worden dan moet er ook een goede instructie zijn voor het (automatisch) verwijderen van de software na afloop van de toets, zodat er niet langer kan worden meegekeken met het device van de student dan noodzakelijk.

Monitoring door opname, opslag & controle achteraf

De afname van de toets wordt in beeld en geluid opgenomen. Nadat de toets heeft plaatsgevonden, kan de docent het complete toetsmoment terugkijken. De docent ziet zowel een opname van het computerscherm als de omstandigheden waarin de student de toets maakt. Denk bijvoorbeeld aan de ruimte waarin de student zit, de omgevingsgeluiden en/of het gedrag van de student.

Inbreuk op de privacy van de student: groot tot zeer groot

Voordelen:
- de mogelijkheden tot frauderen worden hiermee grotendeels ondervangen.
- docenten hoeven niet *live* mee te kijken.

Nadelen:

- de mogelijkheden tot frauderen zijn niet uitgesloten. Studenten kunnen andere tabbladen en programma's open hebben staan. Dit is niet zichtbaar voor de docent. Dit kan worden ondervangen door live monitoring te combineren met locken.
- Het is veel werk voor de docent om alle opnames achteraf te bekijken.

Aandachtspunten:

1. Voordat wordt overgegaan tot monitoring door opname, opslag en controle achteraf moet een DPIA van de gegevensverwerking en - zo nodig – van nieuwe software worden uitgevoerd.
2. Ga na of deze vorm van toetsen een invulling is van het bestaande toets- of examenreglement of dat het nodig is om het reglement aan te passen en ga na of de medezeggenschap (CSR) bij die aanpassing moet worden betrokken.
3. Er moet een verwerkersovereenkomst zijn afgesloten met de leverancier van de software die wordt gebruikt voor monitoring. Monitoring door middel van opname, opslag en controle achteraf moet daarin zijn meegenomen in de bijlagen als aparte verwerking van persoonsgegevens.
4. De privacy-impact van monitoring door middel van opname, opslag en controle achteraf is groot tot zeer groot. Een docent krijgt veel informatie te zien over de privé-omgeving van de student. Die informatie wordt bovendien opgenomen en opgeslagen. Het is goed om van te voren gedragsregels voor docenten op te stellen over hoe een docent omgaat met deze informatie. Bijvoorbeeld in welke gevallen een verdenking op fraude ontstaat, wat een docent in dat geval doet (direct ingrijpen of achteraf rapporteren), of een docent een leerling/student mag aanspreken op zijn/haar privésituatie die in beeld komt etc.
5. Een protocol is noodzakelijk waarin wordt vastgelegd waar de opnames op beveiligde wijze worden opgeslagen, wie toegang hebben tot de opnames, het verbod op maken van kopieën van de opnames en wanneer de opnames worden vernietigd (= zo snel mogelijk nadat het resultaat is vastgesteld en daar geen bezwaar of beroep meer tegen mogelijk is).
6. Studenten moeten vooraf goed geïnformeerd worden over het doel van de monitoring, de wijze waarop monitoring plaatsvindt, welke signalen leiden tot een vermoeden van fraude, wat er met de informatie wordt gedaan die docenten te zien krijgen, wie de opnames kunnen zien, hoelang ze worden bewaard etc.
7. Als er aparte software geïnstalleerd moet worden op het eigen device van de leerling is een duidelijke instructie nodig en een goede test vooraf en met ondersteuning (noodnummer o.i.d.) voor studenten die hiermee problemen ervaren. Dit is niet nodig als monitoring via bijvoorbeeld Teams plaatsvindt en de student daarmee al bekend is via de digitale lessen.
8. Aan studenten die bezwaar hebben tegen het installeren van aparte software op hun eigen device moet er en een alternatief geboden worden, zoals een leenlaptop van de school.
9. Mochten studenten geen geschikt device tot hun beschikking hebben, dan moet er een alternatief kunnen worden geboden.
10. Studenten moeten kunnen beschikken over een goede en stabiele internetverbinding en een rustige ruimte om in te kunnen werken. Als zij dat niet hebben moet er een alternatief geboden worden, bijvoorbeeld om de toets op school af te nemen.
11. Mocht er aparte software geïnstalleerd worden dan moet er ook een goede instructie zijn voor het (automatisch) verwijderen van de software na afloop van de toets, zodat er niet langer kan opnames kunnen worden gemaakt met het device van de leerling/student dan noodzakelijk.

Geautomatiseerde proctoring

De toetsafname wordt opgenomen en er worden tijdens de afname controles uitgevoerd door detectiesoftware die automatisch incidenten signaleert zoals afwijkend gedrag, het openen of bekijken van bepaalde programma's op het device of geluiden uit de omgeving. De opnames en geregistreerde signalen worden opgeslagen. De docent kan op basis daarvan achteraf eventuele fraude vaststellen.

Inbreuk op de privacy van de student: zeer groot. Toepassing alleen bij hoge uitzondering en na uitvoering DPIA.

Voordelen:

- De mogelijkheden tot frauderen worden hiermee grotendeels ondervangen.
- Docenten/surveillanten hoeven niet *live* of alleen steekproefsgewijs *live* mee te kijken.
- Docenten hoeven achteraf niet de hele opname te bekijken maar alleen de geregistreerde signalen van afwijkingen (maar zie ook bij Nadelen).

Nadelen:

- De detectiesoftware bepaalt niet of er sprake is van fraude, maar signaleert afwijkend gedrag. Docenten moeten achteraf deze signalen bekijken om vast te stellen of er fraude is gepleegd. Dit kan om veel vals-positieve signalen gaan.

Aandachtspunten:

1. Voordat wordt overgegaan tot proctoring moet een DPIA worden uitgevoerd van de gegevensverwerking en - indien van toepassing - van nieuw software.
2. Er moet een verwerkersovereenkomst zijn afgesloten met de leverancier van de software die wordt gebruikt voor proctoring. Hierbij moet voldaan zijn aan de AVG wat bij een leverancier die buiten Europa gevestigd is lastiger is.
3. Ga na of deze vorm van toetsen een invulling is van het bestaande toets- of examenreglement of dat het nodig is om het reglement aan te passen en ga na of de medezeggenschap bij die aanpassing moet worden betrokken.
4. De privacy-impact van proctoring is zeer groot. Alle handelingen van studenten bij de afname van een toets worden opgenomen en opgeslagen. Een docent of surveillant kan bij signalen veel informatie te zien krijgen over de privé-omgeving van de student. Die informatie wordt bovendien opgenomen en opgeslagen. Het is goed om van te voren gedragsregels voor docenten op te stellen over hoe een docent omgaat met deze informatie. Bijvoorbeeld in welke gevallen een verdenking op fraude ontstaat, wat een docent in dat geval doet (direct ingrijpen of achteraf rapporteren), of een docent een student mag aanspreken op zijn/haar privésituatie die in beeld komt etc.
5. Er moet in een protocol worden vastgelegd waar de opnames op beveiligde wijze worden opgeslagen (binnen de EER), wie toegang hebben tot de opnames, het verbod op maken van kopieën van de opnames en wanneer de opnames worden vernietigd (= zo snel mogelijk nadat het resultaat is vastgesteld en daar geen bezwaar of beroep meer tegen mogelijk is).
6. Studenten moeten vooraf goed geïnformeerd worden over het doel van de proctoring, de wijze waarop proctoring plaatsvindt, welke signalen leiden tot een vermoeden van fraude, wat er met de informatie wordt gedaan die docenten te zien krijgen, wie de opnames kunnen zien, hoelang ze worden bewaard etc.
7. Als er aparte software geïnstalleerd moet worden op het eigen device van de student is een duidelijke instructie nodig en een goede test vooraf en met ondersteuning (noodnummer o.i.d.) voor studenten die hiermee problemen ervaren.
8. Aan studenten die bezwaar hebben tegen het installeren van de proctoring-software op hun eigen device moet er en een alternatief geboden worden, zoals een leenlaptop van de school.
9. Mochten studenten geen geschikt device tot hun beschikking hebben, dan moet er een alternatief kunnen worden geboden.
10. Studenten moeten kunnen beschikken over een goede en stabiele internetverbinding en een rustige ruimte om in te kunnen werken. Als zij dat niet hebben moet er een alternatief geboden worden, bijvoorbeeld om de toets op school af te nemen.
11. Er moet ook een goede instructie zijn voor het (automatisch) verwijderen van de software na afloop van de toets, zodat er niet langer dan noodzakelijk opnames kunnen worden gemaakt met het device van de student. Ook als op een later moment een andere toets met proctoring wordt afgenomen.

4.4. Andere informatiebronnen digitaal toetsen

Meer informatie over digitaal toetsen is te vinden in de volgende bronnen:

Handreiking Verantwoord Diplomabesluit
Cito – Digitaal toetsen Tips&Tricks
Lesopafstand – Toetsen op afstand
Lesopafstand – Tips van docenten
Autoriteit Persoonsgegevens
SURF over Online Proctoring (filmpje)

5. Tips AVG en digitaal onderwijs

5.1. Algemene handreiking voor faciliteren van thuiswerken

- Zorg dat de docenten veilig thuis kunnen werken.
- Geef de docenten advies en instructies om thuis te kunnen zorgen voor een veilige internetverbinding / wifi-wachtwoord.
- Bied een VPN-verbinding aan (eduVPN bijvoorbeeld).
- Wijs docenten op het clear-desk/clear-screen-beleid, ook thuis: voorkom dat huisgenoten meekijken/lezen/luisteren.
- Geef uitleg hoe docenten hun achtergrond kunnen vervagen of kunnen voorzien van een plaatje.
- Zorg er centraal voor dat de instellingen in de omgeving waarin online les wordt gegeven aan de studenten zo min mogelijk rechten (bijv. maken van opnames, elkaar verwijderen of muten) zijn toegekend. Kan dit niet centraal worden ingesteld voorzie de docenten dan van heldere instructies.
- Wijs docenten erop dat gegevens in principe niet op lokale/verwijderbare devices mogen worden opgeslagen maar alleen in de digitale omgeving van de onderwijsinstelling. Als het echt niet anders kan, dan moeten gegevens in ieder geval versleuteld zijn en het device voorzien van een wachtwoord.
- Breid de instructie/ondersteuning door IM/IT uit naar de thuissituatie van de medewerkers.
- Instrueer medewerkers over het gebruik van applicaties en geef daarbij aan dat in principe alleen applicaties mogen worden gebruikt die de onderwijsinstelling aanbiedt. Wil een docent toch een andere applicatie gebruiken dan moet eerst contact worden opgenomen met de IBP-functionaris en/of IT.
- Zorg dat in de gedragscode voor medewerkers is vastgelegd hoe medewerkers moeten omgaan met informatie over de privé-situatie van studenten die zij door digitaal onderwijs mogelijk te zien krijgen.
- Zorg dat in de gedragscode voor studenten is vastgelegd aan welke regels zij zich dienen te houden bij digitaal onderwijs, bijvoorbeeld dat zij geen opnames mogen maken van online onderwijs. Geef daarbij ook aan welke disciplinaire maatregelen/sancties op overtreding van de regels staan. Voorzie docenten van een bondige samenvatting van de regels, zodat zij die aan het begin van de les kunnen laten zien aan en bespreken met de studenten.
- Zorg dat voor docenten duidelijk is waar zij terecht kunnen met hun eigen vragen of klachten, en waar zij met vragen of klachten van studenten en hun ouders terecht kunnen.

5.2. Handreiking thuiswerken, gericht op docenten

- Zorg voor een veilige en rustige thuiswerkplek.
- Pas de *clear desk*- en *clear screen*-regels toe.
- Zet je eigen achtergrond van de online omgeving uit en zorg voor een rustige andere achtergrond.
- Bespreek met jouw studenten altijd bij de start van de les de gedragsregels.
    - Het maken van opnames van de digitale les is verboden
    - Let zelf op wat er in beeld komt: je kunt een andere achtergrond instellen of de achtergrond blurren.
    - Zet je geluid uit, zet het alleen aan als de docent daar om vraagt.
    - Zet je camera aan bij het begin van de les in verband met de aanwezigheidsregistratie, de camera *mag* daarna uit en wordt op verzoek van de

docent weer aangezet, de docent bepaalt afhankelijk van de vorm van onderwijs wat noodzakelijk is.
    - Online les is gewoon les, de regels van school gelden nu ook.
    - Geen ongewenst gedrag, zoals het verwijderen van andere studenten of het dempen van microfoons.
- Dit ongewenste gedrag kan je ook voorkomen door jezelf in te stellen als presentator.
- Verwijder een student na herhaaldelijk ongewenst gedrag uit de les en maak hiervan intern melding via de gebruikelijke procedures.