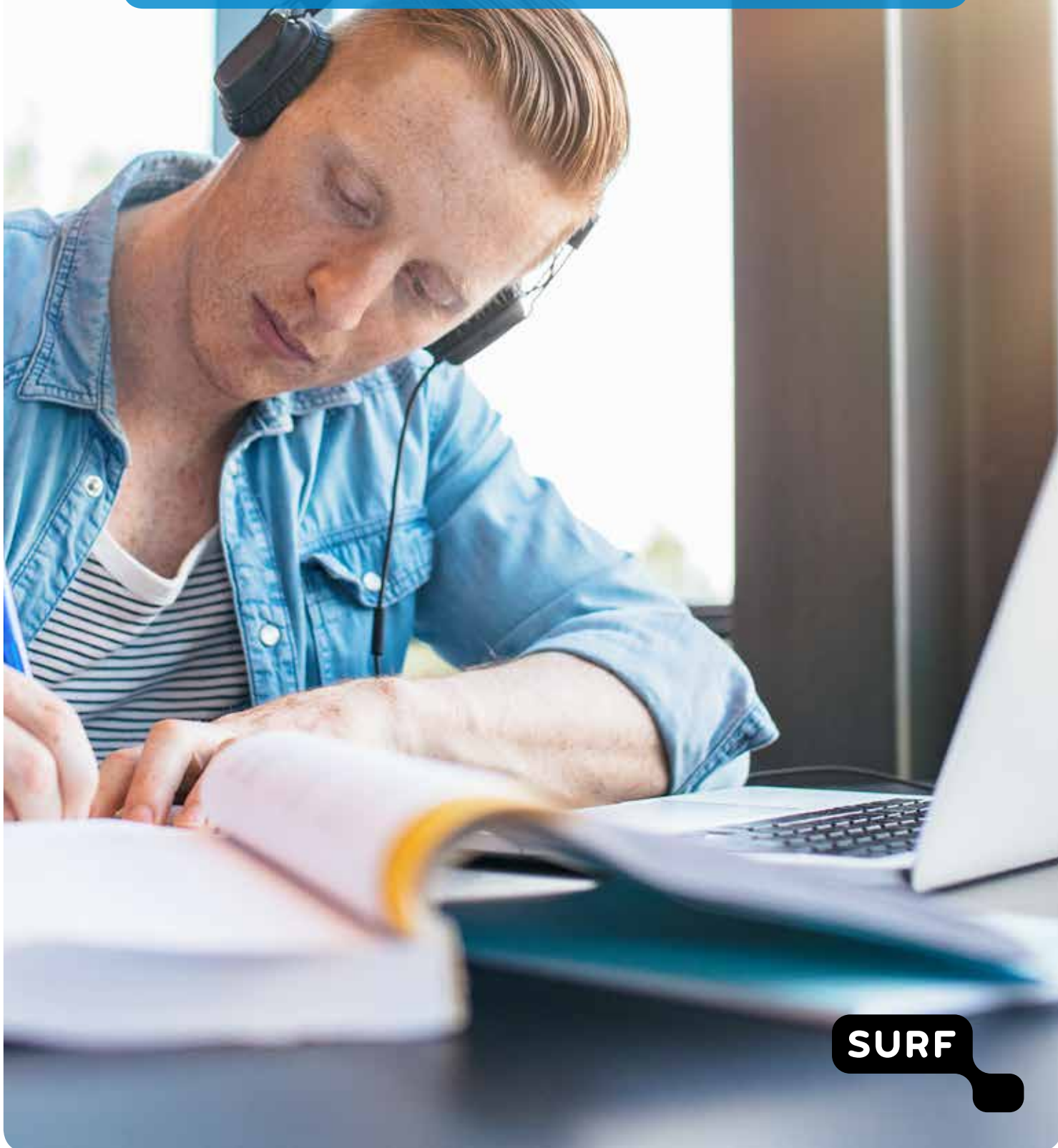


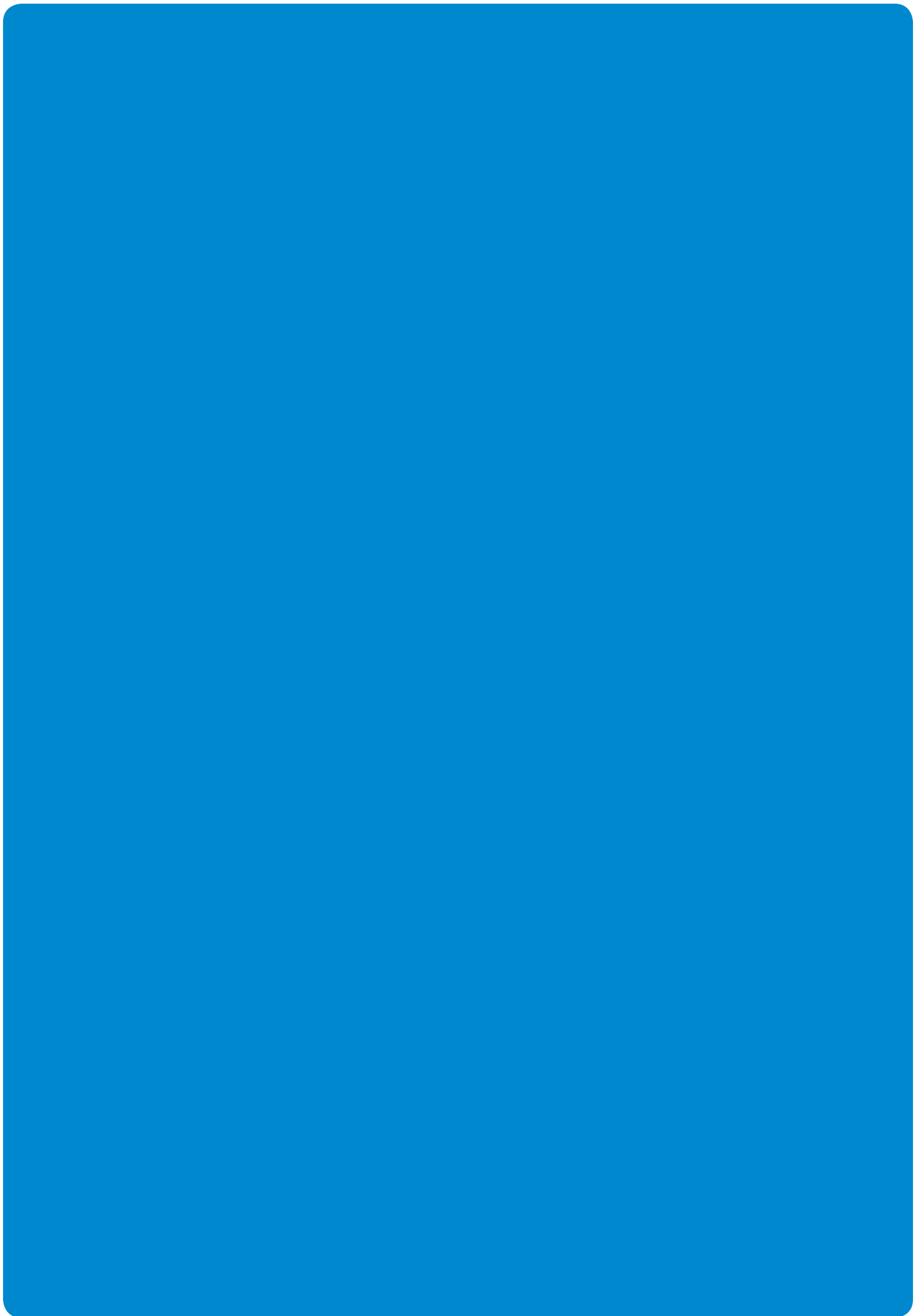
WHITEPAPER ONLINE PROCTORING

VRAGEN EN ANTWOORDEN BIJ
SURVEILLEREN OP AFSTAND

Update, april 2020



SURF



VOORWOORD

In het Nederlandse (hoger) onderwijs is online proctoring in opkomst. Deze vorm van online surveilleren biedt de mogelijkheid om studenten onder beveiligde condities op afstand (plaatsonafhankelijk) te toetsen. In veel situaties is dit een ideale oplossing.

Voorbeelden zijn de accreditatie van MOOC's of selectietoetsen voor Nederlandse en internationale hoger onderwijs studies, tentamens van Nederlandse studenten die tijdelijk in het buitenland studeren en toch in Nederland een tentamen willen doen, buitenlandse studenten die tijdelijk in Nederland hebben gestudeerd maar weer terug naar hun land van herkomst zijn, of buitenlandse pre-masterstudenten die worden toegelaten op basis van een toets. Online proctoring kan dus worden ingezet om het onderwijs flexibeler in te vullen.

Aan de andere kant zijn er nog veel te beantwoorden vragen, bijvoorbeeld op het gebied van privacy en de fraudebestendigheid van de verschillende proctorsystemen. Er is nauwelijks wetenschappelijk onderzoek naar gedaan en praktijkervaring is vooral opgedaan in kleinschalige experimenten. Door de snel veranderende markt en het gebrek aan stevige onderzoekstudies is het lastig een goed beeld te krijgen van online proctoring. Daarmee is het voor studentgeledingen, opleidingsmanagement en toets- en examencommissies moeilijk in te schatten of het een geschikt middel is voor een specifieke situatie binnen de eigen opleiding.

Met deze whitepaper wil SURF meer inzicht geven in online proctoring en de vraagstukken die daarbij een rol spelen. De whitepaper bestaat uit drie delen. Het eerste deel (hoofdstukken 1, 2 en 3) is van algemene aard. In hoofdstukken 1 en 2 beschrijven we welke vormen er bestaan en in welke situaties online proctoring nu gebruikt wordt. Ook gaan we in op de achtergronden ervan. Hoofdstuk 3 behandelt de belangrijkste vraagstukken bij gebruik van online proctoring (privacybescherming, veiligheid en fraudebestrijding, kosten). De delen twee en drie van deze whitepaper bieden verdieping. Hoofdstuk 4 gaat dieper in op privacybescherming en hoofdstuk 5 gaat uitgebreid in op veiligheid en fraudebestrijding.

We hebben dit whitepaper geüpdatet naar aanleiding van de coronacrisis: is het meer gerechtvaardigd en opportuun om online proctoring in te zetten als het niet mogelijk is om fysiek bij elkaar te komen om toetsen te maken? Een aantal keren melden we als een maatregel of stellingname specifiek betrekking heeft op crises als de coronacrisis.

Daarnaast zijn in de loop der jaren ook nieuwe inzichten ontstaan, mede als gevolg van uitspraken van de Autoriteit Persoonsgegevens. Zo worden camerabeelden niet meer per definitie als bijzondere persoonsgegevens beschouwd, maar alleen als sprake is van een identificatiedoel.

De verschillende leveranciers van online proctoring zijn in deze whitepaper met opzet niet met elkaar vergeleken, maar de recente eigenschappen van hun systemen wel. De markt ontwikkelt zich snel en leveranciers passen hun producten constant aan, dus iedere vergelijking zou al snel achterhaald zijn. Gelukkig zijn er online genoeg overzichten van leveranciers en hun producten te vinden.¹

Meer informatie over digitaal toetsen en online proctoring is te vinden op de [website van SURF](#). [SURFacademy](#) organiseert regelmatig bijeenkomsten over deze onderwerpen. Voor specifieke vragen over de in deze whitepaper besproken onderwerpen kunt u contact opnemen met [Lex Sietses](#).

1. Zie bijvoorbeeld <https://www.onlineproctoring.eu/en/online-proctoring-providers/>

INHOUDSOPGAVE

VOORWOORD	3
SAMENVATTING	5
DEEL 1 - IN VOGELVLUCHT	9
1. WAT IS ONLINE PROCTORING?	10
1.1 Live toezicht met conferencing software	10
1.2 Live proctoring met proctoring software	12
1.3 Opslag en controle achteraf met proctoring software	12
1.4 Geautomatiseerde review	13
2. MOGELIJKHEDEN VAN ONLINE PROCTORING	14
2.1 Internationaal onderwijs	14
2.2 Flexibilisering van tijd	15
2.3 Flexibilisering van plaats	15
2.4 Verschillende toetsvormen	15
3. VRAAGSTUKKEN BIJ ONLINE PROCTORING	18
3.1 Privacybescherming	18
3.2 Veiligheid en fraudebestrijding	19
3.3 Kosten	21
3.4 False positives	22
3.5 Borging	22
3.6 Studentervaring	22
3.7 Informatieverstrekking	23
3.8 Uitdagingen bij opschaling	24
DEEL 2 - VERDIEPING: ONLINE PROCTORING EN PRIVACY	25
4. PRIVACYBESCHERMING	26
4.1 Wat zijn persoonsgegevens?	26
4.2 Grondslagen voor verwerking van persoonsgegevens	27
4.3 Informatieverstrekking onder de AVG	29
4.4 Beveiliging van persoonsgegevens	29
4.5 Rechten van betrokkenen	30
4.6 Geautomatiseerde besluitvorming en proctoring	31
4.7 Diensten van derden	31
4.8 Verwerkingen in andere landen	32
4.9 Uitvoering Data protection impact assessment (DPIA)	32
4.10 Handhaving van de wet	32
4.11 Alternatieven voor online proctoring	33
4.12 Concrete aanbevelingen	34
DEEL 3 - VERDIEPING: FRAUDEBESTRIJDING	35
5. VEILIGHEID EN FRAUDEBESTRIJDING	36
5.1 Fraude voorkomen	36
5.2 Risicofactoren bij online proctoring	37
5.3 Wat betekent dit dan?	39
5.4 Keuzemodel	40

SAMENVATTING

Online proctoring – surveilleren op afstand – is in opkomst. In de VS wordt het al regelmatig toegepast en steeds vaker experimenteren Nederlandse instellingen ermee. Online proctoring biedt kansen voor internationaal en flexibel onderwijs, maar er is – zeker in Nederland – betrekkelijk weinig ervaring mee. Daardoor vinden examencommissies en anderen binnen de opleiding het lastig om te besluiten of, en zo ja op welke manier, zij online proctoring kunnen toepassen in hun opleiding. Zij worstelen onder meer met vragen over privacy en fraudebestendigheid.

In deze whitepaper concludeert SURF dat online proctoring voor specifieke situaties veel toegevoegde waarde biedt en voor verschillende toets toepassingen geschikt is. Tegelijk is de privacy-impact bij grootschalige invoering van online proctoring groot. Bij het updaten van deze whitepaper (2020) speelt de coronacrisis een grote factor in onze samenleving. Dat heeft veel invloed op het maken van afwegingen over privacy, ook op het gebied van online proctoring. Als tentamens niet gemaakt kunnen worden in grote toetszalen, dan is online proctoring eerder het minst ingrijpende middel. De balans tussen de rechten en vrijheden van de studenten (privacy) en het gerechtvaardigd belang van de instelling (veilige tentamens afnemen) slaat sneller door naar een toepassing van online proctoring op basis van gerechtvaardigd belang. Voor grootschalige toepassing in 'normale' tijden is toepassing van online proctoring waarschijnlijk nog slechts mogelijk met toestemming van de student.

Natuurlijk brengt tentaminering buiten de eigen (gecontroleerde) omgeving van de instelling fraudevraagstukken met zich mee. Op basis van een typologie van vormen van proctoring en het belang van toetsen kan echter wel een matrix worden gepresenteerd met een overzicht van toepassingen (zie paragraaf 5.4). Hieronder de belangrijkste conclusies op een rij.

Mogelijkheden van online proctoring

Online proctoring biedt uitkomst in specifieke situaties. Wageningen University & Research kan door online proctoring bijvoorbeeld een volledig online masterprogramma aanbieden, waarbij studenten van over de hele wereld hun tentamens kunnen doen. Ook biedt online proctoring topsporters de mogelijkheid tentamens te doen vanuit hun trainingskamp en kan een ernstig zieke student thuis tentamen doen.

In het algemeen maakt online proctoring plaats- en tijdonafhankelijk toetsen eenvoudiger. Dit argument heeft sinds het uitbreken van de coronacrisis sterk aan kracht gewonnen. Betrokken partijen in het onderwijs bepleiten in toenemende mate om online proctoring op grotere schaal toe te passen. Het zou in deze crisis een uitkomst kunnen bieden als toetsen geheel plaats- en tijdonafhankelijk kunnen worden afgenomen.

Voor volledige vrijheid in tijd is het echter wel nodig dat iedere student een uniek tentamen krijgt. Dat kan door studenten een unieke casus voor te leggen (zoals bij mondelinge toetsen of take-home exams) of door een grote itemdatabank met veel tentamenvragen in te zetten. Unieke opgaven zijn noodzakelijk omdat anders opdrachten en toetsvragen bekend zijn en de waarde van de toetsing verloren gaat. Instellingen voor hoger onderwijs zien het als weinig realistisch om studenten de mogelijkheid te bieden op ieder moment een tentamen te maken, met name omdat dit niet past binnen het huidige stelsel voor bekostigd hoger onderwijs.

Maar online proctoring kan in ieder geval wel plaatsafhankelijk toetsen gemakkelijker maken. Studenten kunnen een online geproctorde toets op elke willekeurige locatie maken, als de toets maar zo is opgezet dat de student niet wordt gestoord en er een goede internetverbinding is.

Het verschilt per leverancier of het mogelijk is om online toetsen en proctoring aan te bieden waarbij grote groepen studenten op exact hetzelfde tijdstip een toets moeten starten. Sommige leveranciers kennen de nodige uitdagingen ten aanzien van de performance van systemen.

Online proctoring vraagt soms wel om aanpassing van de toetsvorm. Bijvoorbeeld omdat studenten tijdens het tentamen niet naar het toilet kunnen. Zo is het aan te raden tentamens te beperken tot 90 minuten, of ze te splitsen in twee delen (van maximaal 90 minuten per tentamen).

Privacy bij online proctoring

Een belangrijke afweging bij de verwerking van persoonsgegevens is of het middel in verhouding staat tot het doel (proportionaliteit) en of het doel niet op een andere, minder ingrijpende manier kan worden bereikt (subsidiariteit). De privacy-impact van online proctoring is zeer groot, bijvoorbeeld door de inzet van camerabeelden en door de complete monitoring (in meerdere of mindere mate) van iemands computer. Ook worden opnamen gemaakt van iemands gedrag achter een computer om fraude te detecteren. Een ander doel van opnamen is het vaststellen van de identiteit. Het gaat dus mogelijk om het verwerken van bijzondere persoonsgegevens en in elk geval van gevoelige persoonsgegevens. Ten aanzien van de proportionaliteit en subsidiariteit moet bovendien eigenlijk per geval (bij het ontwerpen van de toets) een afweging worden gemaakt.

Tot op heden leek het daarom niet proportioneel om online proctoring voor tentaminering in het hoger onderwijs op grote schaal in te zetten. Dit komt vooral omdat er voldoende mogelijkheden zijn om toetsen op de campus af te nemen zonder dat het nodig is dit soort persoonsgegevens te verwerken. In de context van de coronacrisis is deze afweging uiteraard anders dan normaal. Waar grote toetszalen altijd een goed alternatief waren, is dat in de coronacrisis niet het geval. Privacy-afwegingen tijdens deze crisis zijn dan ook niet 1-op-1 te gebruiken voor de periode hierna. Er zal – na de coronacrisis – een nieuwe privacy-afweging gemaakt moeten worden. Het is aannemelijk dat deze afweging dan leidt tot een beperkter gebruik van online proctoring.

Een andere belangrijke afweging voor privacy bij online proctoring is de grondslag voor verwerking: een verwerking is alleen rechtmatig als één van de wettelijke grondslagen van toepassing is. Het is aan de instellingen om hierover een afweging en een keuze te maken. Grondslagen waar je bij online proctoring aan kan denken, zijn: toestemming, de noodzaak om gegevens te verwerken om een taak van algemeen belang uit te voeren of omdat het verwerken noodzakelijk is in het kader van een gerechtvaardigd belang.

Over het algemeen geldt door de aard van de te verwerken gegevens dat de grondslag 'toestemming' het meest geëigend lijkt. Dat betekent echter wel dat de student in volledige vrijheid toestemming moet kunnen verlenen, dat weigeren geen gevolgen heeft voor de student en dat er alternatieven moeten worden aangeboden buiten online proctoring. Omstandigheden zoals de onmogelijkheid om in een fysiek klaslokaal een tentamen af te nemen (zoals tijdens de coronacrisis) of de deelname van studenten in het buitenland spelen daardoor zeker mee in de afweging over de grondslag.

Ook kan het administratieve en logistieke proces rondom toetsing ingewikkelder worden als gebruik gemaakt wordt van online proctoring. Dat maakt toestemming lang niet altijd een uitvoerbare grondslag voor het gebruik van online proctoring voor grote groepen studenten. Zeker wanneer een alternatief niet realistisch is, kan mogelijk de grondslag 'gerechtvaardigd belang' van toepassing worden verklaard. Dit geldt bijvoorbeeld gedurende de coronacrisis waarbij studenten niet op de campus mogen komen.² Als er na deze coronacrisis weer minder ingrijpende alternatieven beschikbaar zijn (zoals tentamens in toetszalen), dan is de grondslag 'gerechtvaardigd belang' niet meer te gebruiken.

Gegeven de bijzondere en gevoelige aard van de persoonsgegevens moeten instellingen rekening houden met strenge eisen aan bijvoorbeeld opslag, beveiliging, toegang en bewaartermijnen van de persoonsgegevens. Richt het proces rond online proctoring daarom zo privacyvriendelijk mogelijk in, aan de hand van de principes van 'privacy by design'. Zo is het vragen naar een ID-bewijs geen optie, gebruik daarom de studentenkaart voor identificatie.

2. Let op dat de coronacrisis niet automatisch een gerechtvaardigd belang geeft. De instelling moet eerst zoeken naar privacy-vriendelijke alternatieven, incl. bv. andere toetsvormen die geen proctoring vereisen. Ook moet de student expliciet op het recht op bezwaar worden gewezen en kan de belangenafweging voor een individueel geval dan alsnog tot gevolg hebben dat de instelling online proctoring niet verplicht mag stellen. Dit zijn uiteindelijk afwegingen die de instelling zelf per geval moet maken.

Fraudebestendigheid van online proctoring

Net als de bestaande tentamenzalen is online proctoring niet 100% in staat om fraude tegen te gaan of detecteren. Met sommige methoden lijkt het mogelijk om ongezien fraude te plegen, maar met de meer geavanceerde versies van online proctoring (bijvoorbeeld met tweede camera en detectie van software) is dat ook niet eenvoudig.

Voor online proctoring speelt echter wel een extra risico. Als online proctoring langdurig en vooral op grote schaal wordt toegepast, dan is de kans groot dat er software ontwikkeld wordt waarmee online proctoring omzeild kan worden. Als studenten weten dat deze software bestaat en gebruikt kan worden, dan maakt dit frauderen eenvoudiger.

Zoals gezegd is geen enkele vorm van toezicht 100% fraudebestendig. Ook in een campus-situatie met surveillanten die 50 studenten tegelijk in de gaten moeten houden, zijn er mogelijkheden voor studenten om te frauderen. Kortom, een instelling of opleiding moet per tentamen afwegen voor welke vorm van toezicht ze kiest.

Aanvullend geldt dat de kans op het succesvol detecteren van fraude afhankelijk is van de vorm en uitvoering van de gebruikte online proctoring-techniek (bijvoorbeeld live proctoring versus achteraf bekijken van beelden; zogenoemd 'record en review'). Mogelijk dat bij meerkeuzevragen de kans om te kunnen frauderen hoger is gezien de beperkte hoeveelheid informatie die uitgewisseld hoeft te worden. Aan de andere kant zitten studenten juist bij multiplechoicetoetsen bijna altijd stil achter het beeldscherm en vallen afwijkingen van gedrag sneller op. Of kleine bewegingen dan weer voldoende bewijs opleveren voor fraude is aan de examencommissies om te beoordelen.³

Hier staat tegenover dat in tegenstelling tot toezicht door surveillanten in een campus-setting, bij online proctoring alle gegevens (tijdelijk) bewaard blijven. Daardoor is er veel meer data waarop de instelling besluitvorming kan baseren.

Al met al brengen zowel online proctoring als campustoezicht risico's met zich mee. Daarbij speelt ook sterk mee voor welke vorm van online proctoring gekozen wordt. Zo is het gebruik van een tweede camera veiliger dan alleen meekijken via de webcam, maar ook ingrijpender voor de privacy van de student. De examencommissie zal per tentamen moeten afwegen welke vorm van proctoring past bij het af te nemen examen.

SURF heeft vanwege de verschillende mogelijkheden van (online) toezicht een keuzemodel ontwikkeld dat helpt te bepalen bij welke tentamens online proctoring passend is. De inschatting of online proctoring voor een specifiek tentamen geschikt is hangt hierbij van twee factoren af: het belang dat aan het tentamen wordt gehecht en het risico op fraude. Het model treft u hieronder met een korte toelichting, meer toelichting is te vinden in hoofdstuk 5.4

Het belang wordt bepaald door het (directe) effect van dat tentamen en de maatschappelijke waarde die aan een beoordeling is verbonden. Zo is een wekelijkse tussentoets minder belangrijk dan het afrondende tentamen van een vak. Fraude op een tussentoets heeft immers veel minder effect dan fraude die van invloed is op het eindcijfer van een vak. Het risico hangt tevens van de toetsvorm af. Frauderen is naar verwachting eenvoudiger bij meerkeuzententamens dan bij een tentamen met open vragen of bij een mondeling examen.

In het geval van online proctoring worden vier niveaus onderscheiden:

- *Niveau 0*: Online conferencing software met max 10 studenten;
- *Niveau 1*: Record & review, screen capture, één camera en logging websites;
- *Niveau 2*: Record & review, screen capture, één camera, lock-down mogelijkheden van de computer en logging van websites & applicaties;
- *Niveau 3*: Live proctoring met lock-down mogelijkheden van de computer en volledige logging van activiteit op de computer⁴, of record & review inclusief een tweede camera en verder zelfde features.

3. De bewijslast zal een stuk eenvoudiger zijn als gebruikt wordt van twee camera's, met slechts beeld van de webcam is het bewijs voor fraude waarschijnlijk al snel lastig. Sommige opleidingen kiezen er voor specifiek gedrag (bv. een ander in de ruimte) op zichzelf grond te maken voor het ongeldig verklaren van een tentamen. Daarvoor kan de bewijslast lager zijn dan fraude. Het risico daarvan is wel dat tentamens ongeldig worden verklaard zonder dat er daadwerkelijk spraken was van fraude.

4. Inclusief logging van websites, applicaties en achtergrondprocessen op de computer.

Voor een deel van het onderwijs (met zowel hoge risico's als een hoog of zeer hoog belang) geldt dat de veiligheid van online proctoring ook bij de keuze voor live proctoring nog grote risico's met zich meebrengt. Om het frauderisico te beperken zou in die gevallen een andere toetsmethode bekeken kunnen worden. Bijvoorbeeld een goed ingerichte eigen computerzaal, of mogelijk een veilige vorm van BYOD-tentamens in de eigen toetszaal⁵.

Daarnaast kan altijd worden teruggevallen op het allerhoogste beveiligingsniveau: een toetszaal met papieren toetsen. Let daarbij op, ook een toetszaal is niet 100% fraudebestendig en niet iedere toetszaal is hetzelfde. Een slechte toetszaal met te weinig surveillanten is mogelijk minder fraudebestendig dan goede online proctoring. Voor de beste vergelijking zouden we ook verschillende niveaus van toetszalen moeten definiëren. Dat is echter niet de expertise van SURF en de uitwerking hiervan is aan de onderwijsinstellingen. Het keuzemodel stelt daarom niet dat iedere toetszaal veiliger is dan online proctoring, maar dat het *maximale* veiligheidsniveau van online proctoring inherent lager ligt dan het *maximale* veiligheidsniveau van een toetszaal.

Tijdens de coronacrisis kan blijken dat het onmogelijk is om de toetszalen te gebruiken. In dat geval zal de examencommissie een inschatting moeten maken welke toetsvorm wat hen betreft passend is. Dat kan bijvoorbeeld live proctoring zijn, de meest fraudebestendige vorm van online proctoring, maar ook het aanpassen van de toetsvorm is een mogelijkheid: bijvoorbeeld van multiplechoice-vragen naar open vragen. Hetzelfde geldt voor de keuze van het veiligheidsniveau van proctoring. Uitvoerbaarheid, technische mogelijkheden en andere praktische argumenten kunnen zorgen dat de gewenste vorm van online proctoring niet beschikbaar is. De onderwijsinstelling kan er dan voor kiezen een lichtere vorm van proctoring in te zetten, zodat het tentamen wel doorgang kan vinden.

Onderwijsinstellingen zullen zich in zo'n geval ervan bewust moeten zijn dat zij meer risico nemen. Dit risico wordt groter naarmate online proctoring langduriger en op grote schaal wordt toegepast, aangezien de kans dan toeneemt dat software ontwikkeld en verspreid wordt om online proctoring te omzeilen.

Tot slot is het belangrijk te beseffen dat er veel meer factoren meespelen in het bepalen van zowel risico als belang van een tentamen. Denk aan tijdsdruk, maar ook of tentamenstof in een volgend tentamen weer getoetst wordt.⁶ Uiteindelijk moet een toets- of examencommissie deze afweging per geval maken.

Keuzemodel veilige toetsafname

		BELANG			
		Low	Medium	High	Very High
RISICO	Low	Formatieve toets Oefentoets Geen controle nodig	Mondelinge tussentoets Niveau 0	Essay of betoog Praktijkopdracht Mondelinge toets Niveau 1*	Afstudeerwerk Scriptie Niet van toepassing
	Medium	MOOC: open vragen Geen controle, of niveau 1**	Tussentoets: open vragen Niveau 1	Tentamen: open vragen Niveau 3	Toets met civiel effect? met open vragen Reguliere toetszaal***
	High	MOOC: gesloten vragen Geen controle, of niveau 1**	Tussentoets: gesloten vragen Niveau 2	Tentamen: gesloten vragen Reguliere toetszaal***	Toets met civiel effect met gesloten vragen Reguliere toetszaal***

* Online proctoring is uiteraard niet geschikt voor essays en ander werk met een lange doorlooptijd. Het is vooral geschikt voor bijvoorbeeld mondelinge examens met een beperkte tijdsduur (tot bijv. max 3 uur).

** In geval van een MOOC is het afhankelijk van de waarde die aan de MOOC wordt gehecht.

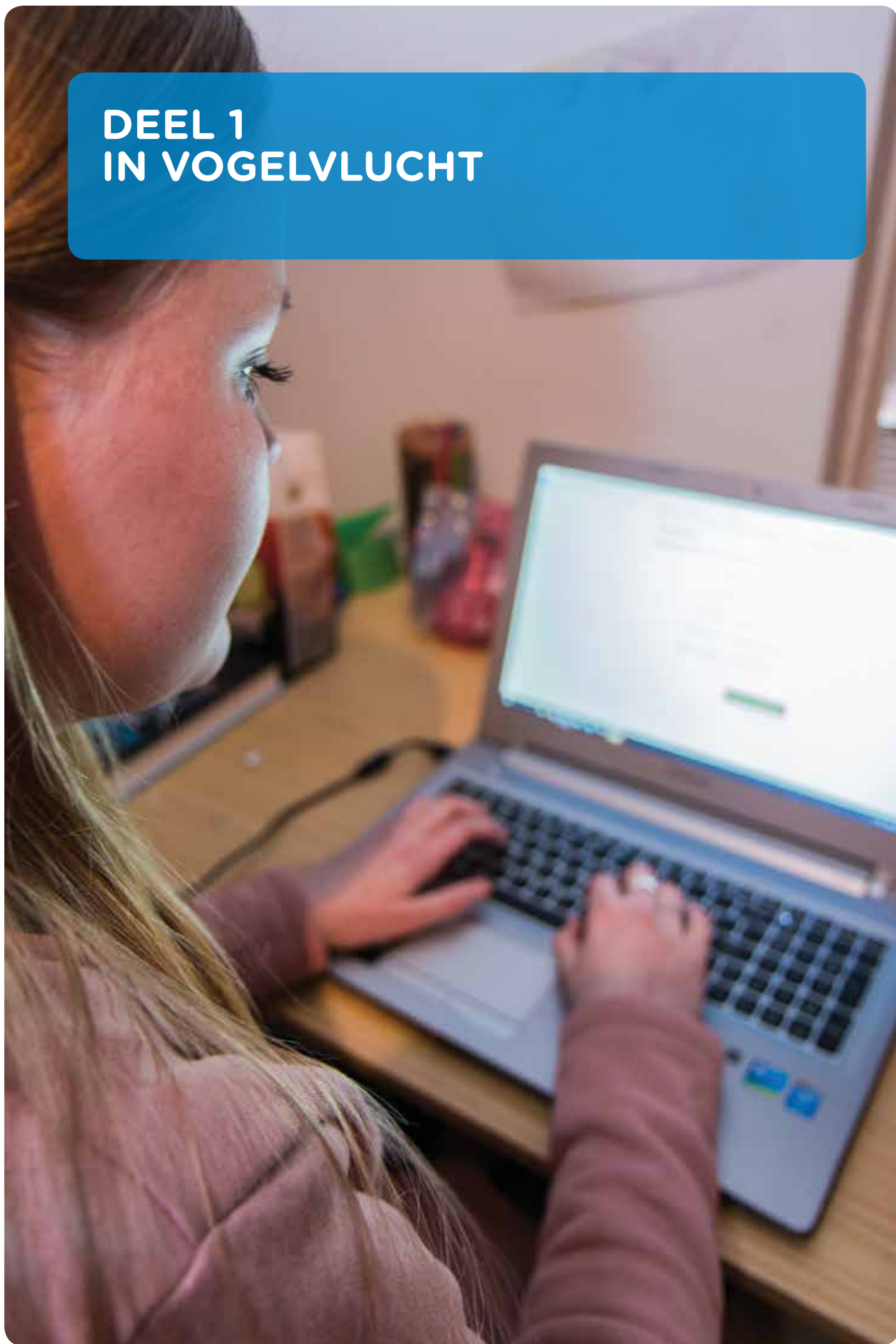
*** Tijdens de coronacrisis, als toetszalen niet beschikbaar zijn, is niveau 3 hier mogelijk een oplossing. Het is dan aan de examencommissie om het frauderisico af te wegen.

5. Voor deze whitepaper is geen onderzoek gedaan naar de mogelijkheden en veiligheid van BYOD-oplossingen of van de bestaande computerzalen. Maar in die gevallen heeft de onderwijsinstelling wel controle over de omgeving (het zwakke punt bij online proctoring). Daarom zijn deze oplossingen waarschijnlijk veiliger te maken dan met online proctoring ooit kan worden bereikt.

6. Er zijn opleidingen waar bv. calculus 1, 2 en 3 wordt gegeven als drie opbouwende vakken. Daarbij herhaalt het tentamen van calculus 3 ook de kennis uit calculus 1 en 2. In dat geval is het belang van de toetsing van calculus 1 en 2 *mogelijk* lager dan bij een vak waar kennis slechts eenmalig wordt getoetst.

7. Bijvoorbeeld om te kunnen werken als advocaat of in de rechterlijke macht.

DEEL 1 IN VOGELVLUCHT



1. WAT IS ONLINE PROCTORING?

Online proctoring is een vorm van plaatsonafhankelijke digitale toetsafname. Je surveilleert online, met behulp van speciale software. De belofte van online proctorsoftware is dat studenten en cursisten hun examens overal (bijvoorbeeld thuis) onder fraudebestendige omstandigheden c.q. gecontroleerd op fraude kunnen maken. Controlesoftware, videobeelden en meekijken op het scherm van de student moeten voorkomen dat hij of zij fraudeert.

De exacte vorm van online proctoring verschilt per leverancier, maar er zijn vier categorieën te onderscheiden: (1) live toezicht met conferencing software, (2) live proctoring (met speciale software) waarbij iemand tijdens het tentamen meekijkt en kan ingrijpen, (3) het handmatig op een later tijdstip bekijken van ieder afgenomen examen, op basis van beelden en logs, en (4) het geautomatiseerd reviewen (waarbij de rapportage achteraf wordt gecontroleerd). De hoeveelheid en aard van de verzamelde gegevens kan per categorie verschillen. Per categorie benoemen we de belangrijkste voor- en nadelen. Daarnaast behandelen we enkele alternatieven indien het niet mogelijk is om toetsen op locatie te maken.

Bij alle categorieën van proctoring bestaat het proces uit ongeveer dezelfde stappen.

- In de eerste stap wordt de technische werking van het proctoringsysteem getest, opdat alle gegevens technisch correct kunnen worden doorgegeven en verzameld. Na deze stap wordt aan de student meegedeeld dat alle gegevens vanaf dat punt worden opgeslagen.
- In de tweede stap start het proces om de student te identificeren. Daartoe wordt meestal een foto van de student via de webcam gemaakt en moet de student een identificatiemiddel via de webcam tonen. Meestal is dat laatste een studentenkaart, omdat het niet is toegestaan naar een ID-bewijs te vragen.
- In de derde stap wordt aan de student gevraagd om de ruimte te filmen waarin hij of zij zich bevindt. Via gedetailleerde stappen kan de student worden gevraagd om een 360-graden opname te maken van de ruimte, voor en achter de computer te filmen, onder het toetsenbord te filmen, het plafond te filmen en onder de tafel te filmen. Bij sommige systemen wordt eveneens gevraagd om de oren te filmen om te beoordelen of daar geen ongeoorloofde oortelefoons inzitten. Afhankelijk van de condities van de toets kan ook worden gevraagd om eventuele boeken, papieren of andere hulpmiddelen die de student op de tafel heeft liggen te filmen.

Als deze drie stappen zijn doorlopen kan de student pas de echte toets opstarten.

In alle gevallen is het van belang dat de procedure geborgd is in de examenregeling. Proctoring zal ook moeten plaatsvinden voordat een cijfer wordt toegekend.

Nu onderwijsinstellingen vanwege de coronacrisis vaak versneld overgaan tot het toepassen van online proctoring, is het belangrijk om keuzes adequaat te documenteren.

1.1 Live toezicht met conferencing software

Bij deze optie gebruikt de docent zelf reguliere conferencing software en kijkt direct mee met de studenten terwijl zij de toets maken. De docent kan de studenten via de webcam zien en ze gedurende de toets vragen om identificatie te laten zien. De docent kan echter niet de beeld-

schermen van de studenten zien. Let wel op, deze tools zijn uitdrukkelijk niet bedoeld voor online proctoring, ze vragen zorgvuldig werken van docenten (bijvoorbeeld om beelden op te slaan) en ze geven al snel schijnveiligheid.

In de praktijk wordt deze aanpak al gebruikt in combinatie met bijvoorbeeld een aanvullende beperking zoals beperkte tijd of open vragen in plaats van gesloten vragen. Deze vorm wordt in de praktijk zelfs ingezet waarbij studenten uitwerkingen maken op papier (zeker voor toepassingen waarbij studenten formules en berekeningen moeten laten zien) waarna de studenten hun uitwerking laten zien voor de camera. Daarna fotograferen ze hun uitwerking met hun mobiele telefoon en mailen deze aan de docent, of ze uploaden de uitwerking naar het leermanagementsysteem of toetsstelsel.⁸

Het spreekt voor zich dat bij deze vorm van online proctoring allerlei technische complicaties kunnen optreden. Het risico op fraude is bij deze categorie het grootste van alle vier de categorieën die we hier bespreken. Desalniettemin wordt deze vorm toegepast. De groepsgrootte moet bij voorkeur beperkt worden tot maximaal 5-10 studenten om enige vorm van controle te kunnen uitvoeren die verder gaat dan alleen de student via de webcam bekijken en van instructies voorzien.

Tijdens de coronacrisis is deze vorm ook toegepast bij grote groepen, voornamelijk zonder noemenswaardige technische problemen. Het is de vraag hoe fraudebestendig die methode is geweest. Gezien de crisissituatie hebben de betreffende opleidingen besloten dat het risico geaccepteerd moest worden.

SURF doet uitdrukkelijk geen uitspraak over de privacyvoorwaarden van conferencingssoftware. Omdat deze tools niet gemaakt zijn voor toezicht tijdens tentamens is dit aspect vaak niet eenvoudig te regelen. Ook het sluiten van een specifieke verwerkersovereenkomst is vaak niet of lastiger mogelijk.



Met online proctoring kan één surveillant meerdere studenten in de gaten houden

8. Deze vorm wordt overigens ook bij andere vormen van online proctoring ingezet. Doordat de student de uitwerking eerst op camera laat zien en daarna uploadt, is te controleren dat het geüploade document echt door die student is gemaakt.

1.2 Live proctoring met proctoring software

Live proctoring is de oudste en meest bekende vorm van online proctoring. Deze vorm lijkt nog het meest op de fysieke examenzaal: een proctor (surveillant) kijkt real-time op afstand mee. Het aantal studenten dat één proctor kan volgen, bedraagt tussen de 7 en 10. Hoe meer schermen een proctor moet volgen, hoe minder examens hij tegelijkertijd kan bekijken. De proctor zorgt dat het autoriseren en legitimeren correct verloopt en kan de check accorderen. Ook kan de proctor aangeven dat de kamer onvoldoende verlicht is. De proctor bekijkt real-time wat de student op het scherm en achter het scherm doet. De proctor kan tijdens het tentamen ingrijpen, net zoals een surveillant dat in een examenzaal kan doen. Hij kan bijvoorbeeld bij een openboek-examen de student vragen het boek uit te schudden of te laten zien om te bewijzen dat er geen aantekeningen in staan of briefjes in verstopt zitten. Ook kan de proctor aan de student vragen om de alt-tab toets in te drukken om te kijken welke applicaties draaien.⁹ Daarnaast kan de proctor tussendoor controlevragen stellen en vragen om nogmaals te laten zien wat er zich in de kamer van de student afspeelt. Verder kan de proctor de student vragen om met een spiegel voor de webcam de randen van het beeldscherm te filmen. Als er indicatie is dat een student opgaven illegaal overneemt (bijvoorbeeld door een foto van het scherm te maken) kan de proctor ingrijpen. Als er een indicatie is dat de student fraudeert, kan de proctor het tentamen voortijdig afbreken.

De grootste nadelen van deze variant zijn de beperkte schaalbaarheid (maximaal 7-10 studenten tegelijkertijd) en de eis dat een tentamen vooraf moet worden gepland. Bij proctoringbedrijven kunnen studenten echter zelf hun eigen tijdslot reserveren. Dat vraagt uiteraard wel unieke examens per student (bijvoorbeeld op basis van een itembank of geparametriseerde vragen). Proctoringbedrijven hebben inmiddels een schaalgrootte waardoor inplannen van toetsen op dit moment meestal tot een paar uur van tevoren mogelijk is. Of dit ook het geval is als de behoefte aan deze vorm van online proctoring op korte termijn zal verveelvoudigen, moet worden afgewacht.

Live proctoring wordt ook vaak ingezet in combinatie met digitaal toetsen waarbij studenten fysiek aanwezig zijn bij de onderwijsinstelling. Deze combinatie is uiteraard niet mogelijk als de gebouwen van de onderwijsinstellingen gesloten zijn (zoals tijdens de coronacrisis).

Live proctoring kan ook worden gecombineerd met het opslaan van de beelden om eventuele controle achteraf ook nog mogelijk te maken. Live proctoring, zeker in combinatie met bijvoorbeeld uitgebreide logging- en lockdown-mogelijkheden, is de meest fraudebestendige vorm van online proctoring.

1.3 Opslag en controle achteraf met proctoring software

Bij de meest voorkomende vorm van online proctoring kijkt de proctor niet real-time mee, maar worden de camerabeelden en logs opgeslagen, waarna reviewers de beelden achteraf gaan bekijken (human intervention). Dit wordt vaak 'record and review' genoemd. Op basis van de beelden beoordelen reviewers of er tijdens het tentamen mogelijk fraude is gepleegd.

Het grootste voordeel van opslag en controle achteraf is dat deze variant goed schaalbaar is en gebruikt kan worden bij grote tentamens die op hetzelfde moment starten. Grote aantallen studenten kunnen op hetzelfde moment het tentamen doen, waarna de reviewers die over een langere periode beoordelen.

In de praktijk van het hoger onderwijs vindt de reviewing in meerdere rondes plaats. In de eerste ronde wordt een algemene integrale review gedaan waarin allerlei afwijkend gedrag wordt gerapporteerd. In de tweede ronde gaan (gecertificeerde) surveillanten de beelden beoordelen om daadwerkelijke vermoedens van fraude te identificeren. In de derde ronde worden de studenten, waar een vermoeden van fraude is, gezamenlijk met bijvoorbeeld de examinator of de examencommissie beoordeeld.

In de praktijk blijkt dat er vaak twee verschillende soorten afwijkingen optreden. De eerste soort is dat studenten zich (per ongeluk) niet aan alle kleine detailregels houden (er klinkt geluid, er loopt per ongeluk iemand door het beeld, er valt kortstondig videobeeld weg). Deze afwijkingen zijn niet direct als fraude te typeren. De tweede soort afwijking is dat studenten

9. Let op dat er eenvoudige methodes zijn om applicaties te verbergen die daardoor wel draaien, maar met dit soort methodes niet zichtbaar worden.

daadwerkelijk proberen worden om op niet-geoorloofde wijze de toetsopdrachten te maken. Het nadeel van deze methode is dat de proctor niet real-time meekijkt tijdens het tentamen en dus niet kan ingrijpen en de student er niet op kan wijzen dat iets niet mag. Deze methode is bovendien arbeidsintensief en heeft een lange doorlooptijd. Ook kan de proctor niet ingrijpen als de camera verkeerd staat opgesteld en het bureau bijvoorbeeld niet goed zichtbaar is. Verder kan niet ingegrepen worden als de student bijvoorbeeld de toetsvragen illegaal kopieert (maar dan kan achteraf natuurlijk wel een sanctie worden opgelegd). Tijdens live proctoring is dit geen probleem; bij terugkijken achteraf moet een tentamen in dat geval mogelijk ongeldig worden verklaard.

1.4 Geautomatiseerde reviewing

Bij geautomatiseerde reviewondersteuning – een variant die steeds meer opkomt – kijken reviewers niet meer het hele tentamen (terug), maar signaleert de software momenten waarop mogelijk sprake is van afwijkend gedrag. Bij het configureren van de software wordt per tentamen vooraf aangegeven wat verdacht gedrag is. Mag de student bijvoorbeeld wel of geen naslagwerk gebruiken tijdens het tentamen, of andere software opstarten? Afwijkend gedrag is bijvoorbeeld als de student wegloopt of wegstijgt, of als er iemand anders in de ruimte wordt gedetecteerd. De reviewer krijgt hiervan een melding via een rapportage die automatisch wordt gegenereerd op basis van gedrag dat vooraf als ‘verdacht’ is gedefinieerd. De reviewer kan die specifieke momenten terugkijken en beoordelen of er inderdaad sprake is van een vermoeden van fraude. Deze variant is dankzij ontwikkelingen op het gebied van artificiële intelligentie sterk in opkomst.

Geautomatiseerde reviewondersteuning maakt proctoring een stuk efficiënter en bespaart veel tijd, omdat niet alle beelden en logs teruggekeken hoeven te worden door menselijke reviewers. Dit maakt het ook een zeer goed schaalbare oplossing. Eén van de nadelen van de methode kan zijn dat als studenten weten hoe de software werkt, ze de fraudepreventiemaatregelen makkelijker kunnen omzeilen. Dat is ook een risico in de huidige tentamenzaal, ook daar proberen studenten misbruik te maken van de feilbaarheid van de surveillanten. Een menselijke reviewer blijft voor de student wel moeilijker te misleiden, omdat het menselijk vermogen om afwijkingen te detecteren (nog) groter is dan dat van een computeranalyse. Ook zijn menselijke surveillanten onvoorspelbaar, in tegenstelling tot software. Zodra studenten een werkende methode ontdekken om software te misleiden, dan werkt die altijd.

Een ander nadeel is dat de software mogelijk veel *false positives* geeft (ten onrechte iets aanziet voor potentiële fraude) waardoor de tweede reviewronde nog relatief veel tijd kan kosten. De ervaringen in welke mate dit effect optreedt zijn nog beperkt.

2. MOGELIJKHEDEN VAN ONLINE PROCTORING

Online proctoring biedt – zeker voor online en internationaal onderwijs – de potentie om onderwijs toegankelijker en flexibeler in te richten. Tegelijkertijd kleven er risico's en twijfels aan het gebruik ervan. Dit hoofdstuk beschrijft de belangrijkste achtergronden van online proctoring. Vervolgens worden in de volgende hoofdstukken enkele vraagstukken verder uitgediept.

2.1 Internationaal onderwijs

Steeds meer onderwijsinstellingen introduceren open en online cursussen die wereldwijd worden gevolgd. Ze variëren van een kleine online cursus tot een volledig masterprogramma. Het is uiteraard niet mogelijk om studenten of cursisten voor ieder tentamen naar Nederland te laten vliegen. Voor het afnemen van tentamens in het buitenland kunnen instellingen samenwerken met internationale testcentrums of Nederlandse ambassades. Echt ideaal is dit niet. Het is soms erg duur, slecht schaalbaar en lang niet in alle landen een even geschikte oplossing. Juist in deze internationale context, waarbij studenten op allerlei verschillende plaatsen (en landen) wonen, kan online proctoring een uitkomst zijn.

Een volledig internationale masterspecialisatie

“Op dit moment volgen 25 studenten de masterspecialisatie ‘Nutritional Epidemiology and Public Health’ volledig online. Deze vierjarige parttime online master leidt op voor hetzelfde diploma als de reguliere tweejarige fulltime on-campus master.

Bij zo'n volledig online vorm past het natuurlijk niet als studenten voor hun tentamens naar Nederland zouden moeten komen. Daarom gebruiken wij online proctoring om de tentaminering mogelijk te maken. Dit past ook goed in reguliere toetsprocessen. Waar een docent normaal de pc-zaal laat inrichten voor een tentamen, wordt nu de online omgeving ter beschikking gesteld.

We zien online proctoring niet als vervanging voor alle on-campus tentamens, maar wel als een hele mooie oplossing voor specifieke situaties. Naast deze master wordt het bijvoorbeeld ook nu al ingezet voor de decentrale selectie op de Nederlandse Antillen. Ook hebben we plannen voor studenten die voor stage in het buitenland zitten of topsporters die op trainingskamp moeten.”

Rolf Martelijn, Wageningen University & Research

2.2 Flexibilisering van tijd

Steeds meer instellingen stellen de student centraal bij het aanbieden van onderwijs, in plaats van een vaststaand curriculum als uitgangspunt te nemen. Dat is ook een wens van studenten¹⁰. Daarnaast is niet iedere student op hetzelfde moment klaar voor een examen. Waar de een de stof na de helft van de tijd al beheerst heeft de ander juist meer tijd nodig. Tijdonafhankelijk papieren examens aanbieden is praktisch onuitvoerbaar, dan zouden er immers op ieder moment van de dag tentamenzalen met surveillanten beschikbaar moeten zijn. Met online proctoring is dit wel mogelijk; hiermee kan de student tentamen doen wanneer hij daar klaar voor is.

2.3 Flexibilisering van plaats

Instellingen willen steeds vaker niet alleen tijd- maar ook plaatsafhankelijk onderwijs kunnen aanbieden. Eén van de redenen is dat toetslocaties relatief zeer dure ruimten zijn. Die wens geldt het sterkst voor internationaal onderwijs, maar komt ook steeds meer op voor onderwijs binnen Nederland. Zeker bij deeltijd- en duaal onderwijs is dit van toepassing, omdat deze studenten veel minder op de locatie van de instelling aanwezig zijn. Door de coronacrisis geldt deze reden extra sterk.

2.4 Verschillende toetsvormen

Een vaak gehoord misverstand is dat online proctoring vooral of zelfs alleen geschikt zou zijn voor meerkeuzetentamens. Die aanname is onterecht. Online proctoring kan iedere digitale tentamenvorm ondersteunen. Het gebruik van webcams biedt daarnaast aanvullende mogelijkheden, bijvoorbeeld om papieren aantekeningen te laten meetellen bij de beoordeling van een tentamen. De student kan die voor de webcam laten zien, waarna de examiner de ingescande versie beoordeelt. Zie ook paragraaf 1.2.

10. In 2016 heeft de landelijke studentenvakbond een rapport over de 'flexstudent' gepubliceerd.

Studenten over online proctoring

Voor de Landelijke Studentenvakbond (LSVb) is het gebruik van online proctoring erg dubbel. Aan de ene kant biedt online proctoring een uitkomst voor toetsen op afstand, waardoor het onderwijs toegankelijker wordt. Hierdoor kunnen studenten die niet fysiek bij een tentamen kunnen zijn door bijvoorbeeld verblijf in het buitenland of ziekte alsnog deelnemen aan het bestaande tentamen. Zo lopen zij geen studievertraging op. Ook hebben we gezien dat online proctoring een snelle oplossing kan zijn in tijden van crisis, zoals bij de uitbraak van het COVID-19 virus. Hierdoor kunnen vakken die al begonnen zijn alsnog afgesloten worden, door te surveilleren op afstand.

Aan de andere kant zijn er wel grote gevolgen voor de privacy van studenten door het gebruik van de verschillende vormen van online proctoring. De Landelijke Studentenvakbond vindt dat daarom altijd eerst gezocht moet worden naar alternatieve manieren van toetsen. Zelfs als een toets met behulp van online proctoring de beste optie blijkt voor het afnemen van een tentamen moet het voor studenten altijd mogelijk zijn om online proctoring te weigeren en een alternatieve opdracht aangeboden te krijgen, zonder studievertraging te riskeren. Niet voor elke student is het prettig en/of mogelijk om bijvoorbeeld hun kamer te filmen en op een rustige manier een toets af te nemen. Studenten moeten hierover van tevoren voldoende en helder worden voorgelicht over de manier van toetsen, wat er met hun gegevens gebeurt, en wat hun rechten zijn, om hierover een beslissing te kunnen nemen.

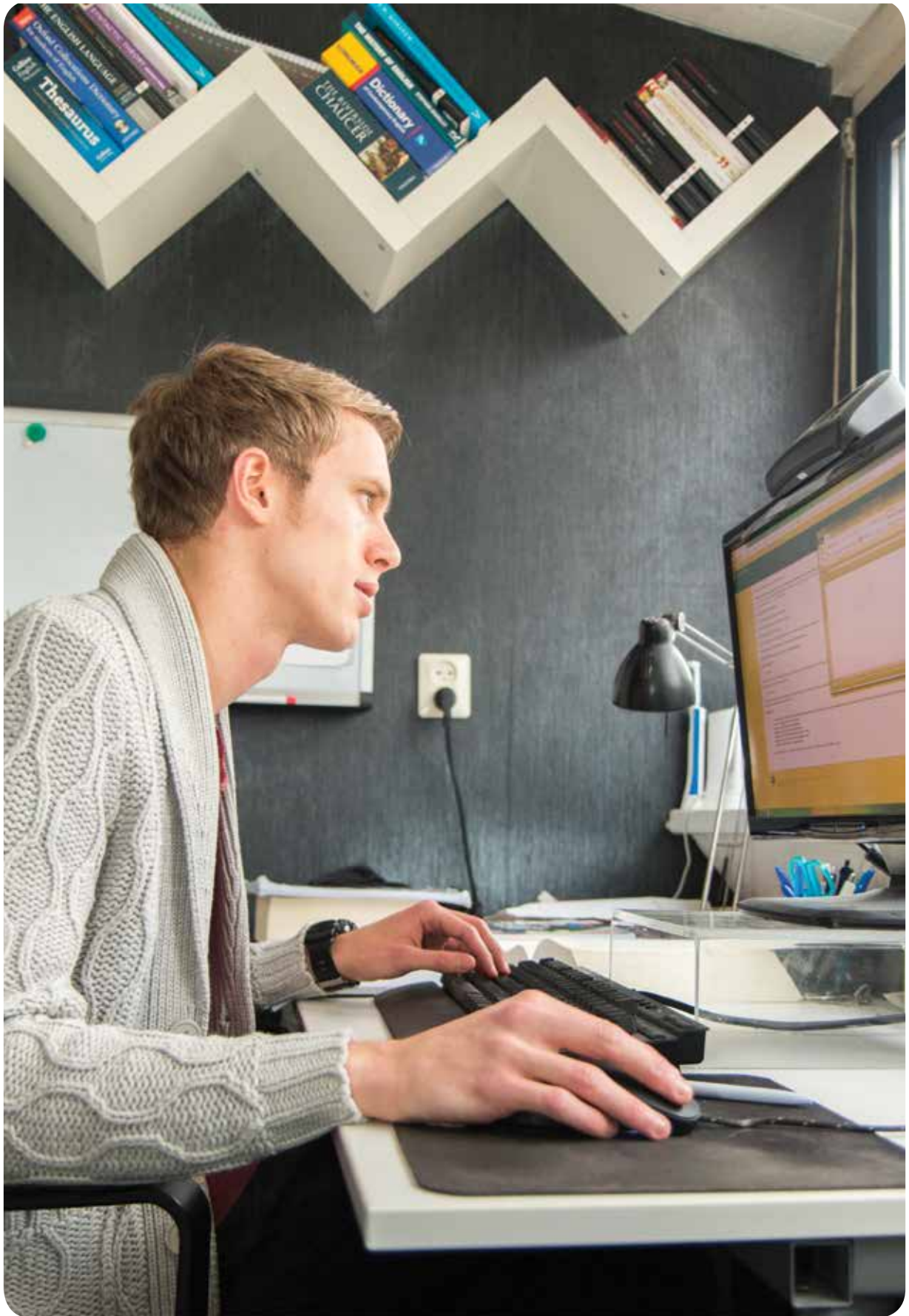
Online proctoring biedt dus een goed alternatief in situaties waarbij een bestaande toets op afstand gemaakt moet worden, en vergroot daarmee te toegankelijkheid van het onderwijs. Er zijn echter te veel ethische en privacy gerelateerde bezwaren om online proctoring ook op grote schaal in te zetten.

Roos van Leeuwen, Landelijke Studentenvakbond

“Het ISO vindt de mogelijkheid tot tijd- en plaatsonafhankelijk studeren en toetsen belangrijk om het onderwijs flexibeler in te richten en op die manier onderwijs beter te kunnen inrichten naar de behoeftes van de student. De optie van tijd- en plaatsonafhankelijk onderwijs kan ook bijdragen aan de toegankelijkheid van het onderwijs. Zo is tentamineren op afstand bijvoorbeeld een uitkomst voor studenten die door ziekte niet fysiek in de collegebanken kunnen zitten en is tijdsafhankelijk onderwijs een uitkomst voor studerende topsporters die hun studie combineren met strakke sportroosters. In crisissituaties waarin onderwijs noodgedwongen op afstand wordt ingericht, zoals op dit moment door het coronavirus het geval is, is tentamineren op afstand een uitkomst om studievertraging te voorkomen. Echter betekent toetsing op afstand volgens het ISO niet direct de stap naar online proctoring. Aan online proctoring kleven immers ook risico's, bijvoorbeeld op het gebied van privacy en ethische vraagstukken. Bovendien kan het idee van een toezien oog dat meekijkt via de camera ook de concentratie van studenten beïnvloeden. Volgens het ISO zou eerst moeten worden gekeken naar alternatieve manieren van toetsen op afstand, voordat over wordt gegaan op online proctoring.

Wanneer blijkt dat online proctoring echt noodzakelijk is en er geen goede alternatieve toetsvormen voorhanden zijn, is het belangrijk dat er goed met deze privacygevoelige data wordt omgegaan en hierover duidelijk naar studenten wordt gecommuniceerd. Studenten moeten worden ingelicht over hun rechten, bijvoorbeeld om te vragen naar een alternatief. Daarnaast moet het voor studenten duidelijk zijn wat er met de beelden wordt gedaan en hoe lang deze bij wie in het beheer zijn. Daarnaast vindt het ISO het belangrijk dat privacy protocollen op instellingen samen met de studenten tot stand komen. De studenten in de medezeggenschap zouden vanaf het begin moeten worden meegenomen in het opstellen van privacy protocollen, om op die manier te waarborgen dat de student meebeslist over wat er met zijn/haar data gebeurt.”

Eline van Hove, Interstedelijk Studenten Overleg



3. VRAAGSTUKKEN BIJ ONLINE PROCTORING

In dit hoofdstuk wordt dieper ingegaan op belangrijke voorwaardelijke vraagstukken over online proctoring: privacybescherming, beveiliging en fraudebestrijding, en de kosten ervan. Dit hoofdstuk gaat ook in op uitdagingen om online proctoring op te schalen. Dat is nu actueel omdat het vanwege de coronacrisis voorlopig niet mogelijk is om bij een onderwijsinstelling een toets te maken.

3.1 Privacybescherming

Bij online proctoring worden persoonsgegevens verwerkt: gegevens die direct of indirect iets zeggen over studenten. De Algemene Verordening Gegevensbescherming (AVG) stelt strenge eisen aan de verwerking van deze gegevens, bijvoorbeeld bij het bepalen van de grondslag, het informeren van studenten en de beveiliging van de opgeslagen gegevens. Hoofdstuk 4 gaat hier uitgebreider op in en biedt handvatten waarmee instellingen passende instrumenten kunnen ontwikkelen.

Belangrijke punten uit de AVG zijn:

• Grondslag

Voor het verwerken van persoonsgegevens is een wettelijke grondslag nodig (een basis die het recht op verwerking geeft). Grondslagen bij online proctoring zijn bijvoorbeeld: (1) toestemming, (2) de noodzaak om gegevens te verwerken om een taak van algemeen belang of openbaar gezag uit te oefenen, en (3) de noodzaak om gegevens te verwerken in het kader van een gerechtvaardigd belang. In de context van de coronacrisis kan gerechtvaardigd belang als grondslag voor online proctoring worden gebruikt (zie kader met een voorbeeld van de Vrije Universiteit). Zodra examens in toetszalen weer een goed alternatief zijn, zal deze grondslag waarschijnlijk vervallen aangezien er dan een privacyvriendelijker alternatief is voor online proctoring.

Voor de grondslag 'toestemming' geldt dat toestemming door een student in vrijheid gegeven moet kunnen worden, weigeren geen gevolgen heeft voor de student en/of er een alternatief is buiten online proctoring. Dat maakt toestemming bij online proctoring op grote schaal vaak lastig toe te passen. Toestemming kan mogelijk wel gebruikt worden voor studenten die vanuit het buitenland tentamen willen doen, of voor studenten die zelf aangeven liever thuis (in rust) tentamen te doen.

• Informatieplicht

In alle gevallen geldt dat de studenten (en de ouders wanneer de student jonger is dan 16 jaar) onder andere geïnformeerd moeten worden over wat de verwerking behelst, welke gegevens worden verzameld, hoe lang deze worden bewaard, en wat de grondslag is. Als de grondslag is gebaseerd op gerechtvaardigd belang, moeten de studenten ook geïnformeerd worden over de wijze waarop dat belang is afgewogen tegen het belang van de student.

• Doelbinding

Persoonsgegevens mogen alleen worden gebruikt voor het doel waarvoor ze zijn verkregen en waarvoor men een grondslag heeft. De gegevens mogen vervolgens niet verder worden verwerkt op een manier die niet verenigbaar is met die doeleinden.

Voor meer details over de AVG en online proctoring verwijzen we naar **hoofdstuk 4**.

VU: online proctoring onder het gerechtvaardigd belang

In tijden van de coronacrisis is bij de Vrije Universiteit (VU) de eerste boodschap: *'Zorg dat je een andere toetsvorm vindt dan de klassieke eindtoets. Als het echt niet anders kan, dan komt de klassieke eindtoets wellicht in aanmerking voor online proctoring.'* Per toets bepaalt de Examencommissie - in overleg met de examinatoren - welke alternatieve toetsvorm wenselijk en noodzakelijk is.

Wanneer online proctoring ingezet wordt, kiest de VU (als niet publiekrechtelijke instelling) daarbij voor de grondslag 'gerechtvaardigd belang'.

De VU geeft aan dat online proctoring bij de betreffende toets op afstand noodzakelijk is om:

- a. te controleren wie de persoon is die de toets maakt;
- b. vast te stellen dat geen fraude is gepleegd tijdens het maken van de toets;
- c. vast te stellen dat de toets binnen het gegeven tijds kader is gemaakt; en
- d. de werkwijze wordt gevolgd zoals beschreven in de privacyverklaring.

Er is dan sprake van een noodzakelijk, gerechtvaardigd belang van de VU, dat zwaarder weegt dan de rechten en vrijheden van de betrokkenen (art. 6.1 f AVG).

Deze afweging zal van geval tot geval moeten worden beoordeeld. De VU heeft een uitgebreide privacyverklaring opgesteld waarin wordt beschreven hoe de privacy van studenten wordt gewaarborgd. Hierin wordt vermeld dat studenten bezwaar kunnen maken via de Functionaris Gegevensbescherming.

Zie: <https://communities.surf.nl/artikel/vu-online-proctoring-onder-het-gerechtvaardigd-belang>

3.2 Veiligheid en fraudebestrijding

Fraudebestrijding is een belangrijk thema waarvoor veel maatschappelijke aandacht bestaat. Examencommissies willen volledig achter ieder diploma kunnen staan dat zij afgeven. In een reguliere tentamenzaal is fraudebestrijding al een uitdaging; het kan nog veel ingewikkelder worden als digitale toetsmiddelen zoals online proctoring worden ingezet.

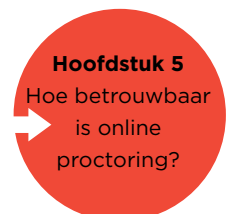
Het is algemeen bekend dat een reguliere tentamenzaal niet 100% veilig is. Onderwijsinstellingen en examencommissies hebben echter wel veel ervaring met het gebruik van die reguliere tentamenzaal en kunnen daardoor redelijk goed inschatten welke risico's daarbij komen kijken: er is sprake van een zekere mate van 'common understanding' zonder dat precies bekend is hoeveel fraude er nu eigenlijk gepleegd wordt.

Bij online proctoring is die ervaring nog beperkt. Veel instellingen die met online proctoring aan de slag willen, moeten steeds zelf al doende inschattingen leren maken hoe veilig het middel is dat ze willen inzetten. Vaak wordt het gesprek door docenten en examencommissies ook met een verkeerde vraag ingezet: *"is online proctoring 100% veilig?"* Deze vraag is niet reëel aangezien geen enkele manier van tentamineren 100% veilig is.

Een complicerende factor is dat iedere leverancier weer net andere methodes en technieken gebruikt. Hierdoor zijn de ervaringen van de ene instelling niet altijd direct bruikbaar voor een andere.

Het tegengaan van fraude is gebaseerd op drie componenten.

- **Preventie:** Duidelijke voorlichting geven en vermelden wat verdacht gedrag is, studenten ontmoedigen om fraude te plegen. Deze component is de belangrijkste component om fraude tegen te gaan.
- **Detectie:** Gegevens heel goed vastleggen tijdens de identificatie en toetsafname en borgen dat onreglementair gedrag snel en goed geïdentificeerd wordt.
- **Sanctie:** Duidelijk maken dat onreglementair gedrag en fraude zal leiden tot zwaarwegende consequenties.



Studenten voerden een security audit uit

“Bij de UvA hebben we al ruim achthonderd tentamens afgenomen met het gebruik van online proctorsoftware. Hier waren we zeer tevreden over. Als vervolg daarop wilden we onderzoeken op welke manieren deze software ingezet kon worden in het regulier onderwijs, daarom zijn we het SURFnet-project ‘Surveilleren op afstand’ gestart.

In dit project onderzoeken wij de veiligheid van de software en gaan we na of studenten (gemakkelijk) kunnen frauderen en of de privacy van de studenten gewaarborgd is. Wij hebben hiervoor een opdracht uitgezet bij vier informaticastudenten, die gespecialiseerd zijn in het hacken van systemen. Deze studenten hebben een kleinschalige security audit uitgevoerd om te beoordelen of studenten kunnen frauderen en of er privacy-kwesties aan het licht komen. Zij hebben hierbij verschillende problemen gevonden die er inderdaad op wijzen dat er veiligheids- en privacy-issues zijn. Er is met de leverancier afgesproken dat zij met een aantal van deze problemen aan de slag gaan en dat er een tweede security audit zal worden uitgevoerd, om te kijken of de problemen zijn opgelost.

Niet voor alle problemen zal waarschijnlijk een oplossing zijn. Als UvA moeten wij nu beoordelen of die risico's voor ons acceptabel zijn, wetende dat ook de reguliere toetszaal niet 100% fraudevrij is.”

Guusje Smit, Universiteit van Amsterdam (in 2016)

In hoofdstuk 5 wordt uitgebreid ingegaan op mogelijke manieren van fraude en hoe proctoringsoftware die probeert te voorkomen. Op basis daarvan kunnen de volgende constatering worden gedaan:

- Fraude waarbij de hardware of software wordt gemanipuleerd is meestal te detecteren. Dit heeft echter al snel een vergaande impact op de privacy van studenten.
- Zodra een student software heeft ontwikkeld die frauderen mogelijk maakt, kan hij deze in een oogwenk onder een grote groep studenten verspreiden. Deze schaalbaarheid is anders dan in een reguliere tentamenzaal, waar fraude meestal een individuele¹¹ actie is.
- Wanneer de onderwijsinstelling geen controle heeft over de fysieke ruimte waar een tentamen wordt afgenomen, dan kan op veel (vrijwel) niet te detecteren manieren worden gefraudeerd.
- Met een beetje creativiteit lijken er veel mogelijkheden te zijn.¹² In hoofdstuk 5 wordt een selectie van de mogelijke vormen van fraude besproken.

Zowel aan online proctoring als aan toezicht in de reguliere tentamenzaal kleven risico's. In beide gevallen kan worden gefraudeerd. Maar er zijn wel verschillen. Een reguliere tentamenzaal biedt altijd een hoger *maximaal* veiligheidsniveau. Online proctoring heeft door de aard van het systeem inherent beperktere grenzen. Juist het voordeel dat een tentamen niet plaatsgebonden is, maakt ook dat de onderwijsinstelling de omgeving waarin het tentamen wordt afgenomen beperkter kan controleren.

Maken die nadelen online proctoring een onbruikbaar middel om tentamens af te nemen? Nee, online proctoring is als hulpmiddel bij afname van digitale tentamens zeker bruikbaar en de preventieve werking om fraude tegen te gaan moet niet onderschat worden. Wel is het maken van een goede afweging belangrijk, waarbij zowel het belang als het risico van een specifiek tentamen worden meegewogen en naast de voordelen worden gezet.

In hoofdstuk 5 gaan we uitgebreider in op vormen van fraude en de wijze waarop online proctoring hiertegen bescherming kan bieden. Daarnaast is er in hoofdstuk 5.4 een door SURF ontwikkeld keuzemodel toetsveiligheid opgenomen. Aan de hand hiervan kunnen examen- of toetscommissies inschatten welke methode voor de afname van digitale toetsen voor een specifieke situatie geschikt is.

11. Er zijn uiteraard gevallen waarbij de tentamenvragen gestolen worden, maar bij fraude in een reguliere tentamenzaal betreft het meestal een individuele student die spiekt, antwoorden doorgeeft of op een andere individuele manier fraudeert.

12. Zie deze link uit 2015: <https://jakebinstein.com/blog/on-knuckle-scanners-and-cheating-how-to-bypass-proctortrack/> - op basis van de comments zoeken studenten ook in 2020 actief naar manieren om online proctoring te omzeilen.

3.3 Kosten

Een argument voor proctoring dat – zeker door proctoraanbieders – vaak wordt genoemd, is de kostenbesparing. De indruk wordt gewekt dat proctoring (vrijwel) altijd goedkoper is dan een tentamenzaal. In de praktijk ligt dat genuanceerder. Er spelen veel extra factoren een rol waardoor de situatie per instelling en zelfs per opleiding kan verschillen.

In 2013 heeft SURF een quickscan ‘Kosten en baten van digitaal toetsen’¹³ uitgevoerd. Hoewel die zich primair richtte op de digitale toets en dus niet op online proctoring, bevat deze quickscan wel een aantal interessante punten die hier het herhalen waard zijn. Daarnaast is het van belang dat instellingen online proctoring niet alleen willen inzetten bij het maken van bestaande digitale toetsen, maar ook willen aangrijpen om bestaande papieren toetsen om te zetten in digitale toetsen.

Naar aanleiding van de quickscan in 2013 zijn de volgende punten interessant:

- De verdeling over de diverse kostenposten verschilt behoorlijk per instelling. Per instelling is de situatie uniek en één uniform antwoord is dus niet te geven.
- De baten van digitaal toetsen waren in 2013 vooral kwalitatief, bijvoorbeeld dat vaardigheden kunnen worden getoetst die op papier slecht te toetsen zijn.

Kostenbesparing moet dus niet worden gezien als een zelfstandig doel bij online proctoring of digitaal toetsen in het algemeen. Niet de financiële besparingen, maar het verbeteren van toetskwaliteit en didactische voordelen moeten de business case sluitend maken.

Dat neemt niet weg dat voor de invoering en het gebruik van online proctoring een financiële inschatting moet worden gemaakt. Enkele aandachtspunten hierbij zijn:

- Wees kritisch of een kostenbesparing echt te realiseren is. Wanneer bijvoorbeeld tentamenzalen extern worden gehuurd, dan kunnen die kosten door gebruik te maken van online proctoring daadwerkelijk worden bespaard. Maar als een instelling zelf eigenaar is van grote toetszalen en deze niet kan of wil afstoten, dan blijven veel vaste kosten (vaak verrekend in de m2-prijs) bestaan, ook als een bepaalde opleiding die niet meer doorbelast krijgt.
- De prijzen voor online proctoring verschillen zowel per aanbieder als per methode. Er zijn modellen waarbij gewerkt wordt met een vaste voet en een instellingslicentie en modellen waarbij gewerkt wordt met de hoeveelheid afgenomen toetsen en de hoeveelheid gereviewde toetsen.
- Om onreglementair gedrag en fraude vast te stellen, zal altijd gewerkt moeten worden met (gecertificeerde) surveillanten. Zij moeten de kritische momenten die geïdentificeerd zijn tijdens een eerste review nogmaals controleren. De kosten daarvan kunnen ook aanzienlijk zijn. De inschattingen op dit moment zijn dat het de surveillanten gemiddeld tussen 3-5 minuten per student kost om achteraf een proces-verbaal op te stellen.
- Het inzetten van eigen surveillanten voor de fysieke controle in de tentamenzaal is wellicht goedkoper (en veiliger) dan online proctoring in een oncontroleerbare thuissituatie.
- Het komt voor dat onderwijsinstellingen extra kosten voor onderwijs en examens willen doorbelasten aan studenten¹⁴. Ook voor online proctoring wordt dit wel eens geopperd. Dit is niet toegestaan in het geval van regulier bekostigd onderwijs in Nederland. Een onderwijsinstelling mag studenten namelijk niet weigeren en moet hen toegang bieden tot het onderwijs. Daarbij hoort de verplichting het onderwijs te realiseren voor het wettelijke collegegeld. Een bijdrage vragen aan de student is alleen toegestaan bij vrijwillige keuzevakken en als er een gratis alternatief wordt geboden.

Kosten en baten aan de WUR

“Wij zien dat op dit moment online proctoring iets duurder is dan onze reguliere toetszalen. Voor het reguliere papieren tentamen gebruiken we de gymzalen die overdag toch leeg staan. Daar moeten dan alleen wat stoeltjes en tafels in gezet worden en dat zijn de grote kosten niet. Omdat wij nog standaard computerzalen hebben voor ons onderwijs geldt hetzelfde voor digitale tentamens, dat kunnen we on-campus goedkoper dan met online proctoring.”

Rolf Marteijs, Wageningen University & Research

13. SURFnet (2014). Whitepaper De businesscase van digitaal toetsen: <https://www.surf.nl/whitepaper-de-businesscase-van-digitaal-toetsen>

14. Zie bijvoorbeeld <https://www.iso.nl/2014/03/zwartboek-van-extra-kosten-naast-collegegeld-online/>

3.4 False positives

Het ten onrechte detecteren van potentiële fraude is een probleem bij iedere vorm van proctoring. Dat komt bijvoorbeeld doordat sommige leveranciers iedere vorm van wegstijgen al rapporteren. Zo schrijft *The Chronicle of Higher Education* in 2013 over Software Secure: “The company’s subcontractor in India, Sameva Global, said it notes ‘minor suspicions’ in 50 percent of exams; ‘intermediate’ suspicions in 20 to 30 percent; and ‘major’ incidents in 2 to 5 percent.”¹⁵

Het probleem van *false positives* is waarschijnlijk het grootst bij geautomatiseerde reviewing en het kleinst bij live proctoring. Bij live proctoring kan een proctor bijvoorbeeld vragen de webcam te richten op de plek waar een student zijn ogen naar liet afdwalen; bij opnames blijft altijd onzeker of een student probeerde te spieken, of gewoon even wegkeek van het scherm. Kortom, het is van groot belang om geconstateerd afwijkend gedrag achteraf met verstand van zaken te interpreteren. Het trainen van surveillanten moet een integraal onderdeel vormen van het online proctoringproces.

3.5. Borging

Examencommissies zijn verantwoordelijk voor het borgen van de kwaliteit van de toetsing en staan garant voor de kwaliteit van examens en diploma’s. Zij moeten dan ook nauw betrokken worden bij de invoering van online proctoring. Examencommissies zijn afhankelijk van anderen als het gaat om het ontwerp van de procedure voor online proctoring, en om de communicatie richting docenten en studenten. Zorg er daarom voor dat een team binnen de onderwijsinstelling ondersteuning biedt op dit gebied, ook aan examencommissies.

Belangrijke elementen van de borging zijn:

- Beargumenteer waarom is gekozen voor online proctoring (en niet voor andere alternatieven).
- Beargumenteer voor welk type online proctoring is gekozen.
- Informeer docenten over wat er komt kijken bij online proctoring¹⁶.
- Test de werking van de digitale toets.
- Configureer de instellingen van online proctoring (geef bijvoorbeeld aan welke tools gebruikt mogen worden en welk gedrag van studenten is toegestaan, zoals naar het toilet gaan).
- Informeer studenten over de procedure (zoals systemcheck en identificatie).
- Informeer studenten over borging van de privacy (bijvoorbeeld waar data opgeslagen worden en wie er toegang toe heeft).
- Informeer studenten wie voor welk aspect van de technische infrastructuur verantwoordelijk is.
- Beschrijf procedures over wat er gedaan wordt als specifieke vormen van fraude wordt geconstateerd.

Zie verder de aanbevelingen in 4.10.

De instelling is verplicht om in de onderwijs- en examenregeling informatie op te nemen over hoe tentamens worden afgelegd.

3.6 Studentervaring

In 2016 waren studentorganisaties relatief positief over online proctoring. Uit ervaringen vanuit het Europese OP4RE project is gebleken¹⁷ dat studenten die ervaring hebben met online proctoring, hierover in het algemeen licht positief zijn ten opzichte van toetsen op de campus. De redenen daarvoor zijn dat studenten niet hoeven te reizen, dat ze met een voor hun bekend apparaat de toetsen kunnen maken en menen dat ze het comfort van hun eigen huis prefereren boven een drukke en onpersoonlijke tentamenhal.

Nu er meer ervaring met online proctoring is, noemen de studenten ook meer specifieke bezwaren. De bezwaren hebben betrekking op¹⁸:

- De vraag waarom een onderwijsinstelling niet kiest voor alternatieve vormen van toetsen.
- Consequenties indien technische problemen bij online proctoring optreden.
- Het huis van studenten leent zich naar hun mening niet altijd voor het maken van tentamens. Niet elke student heeft de beschikking over een ruimte waarin hij of zij in alle rust een tentamen kan maken.

15. Steve Kolowich, ‘Behind the Webcam’s Watchful Eye, Online Proctoring Takes Hold’, 15 april 2013, te vinden op <http://chronicle.com/article/Behind-the-Webcams-Watchful/138505/>

16. De VU heeft hiervoor bijvoorbeeld een speciale website ingericht: <https://canvas.vu.nl/courses/47759/pages/online-proctoring-information-for-teachers>

17. OP4RE project via <https://onlineproctoring.eu>

18. Zie: <https://www.dub.uu.nl/nl/opinie/bedank-voor-online-proctoring>

- De vraag of er zomaar opnames kunnen worden gemaakt van de privésfeer van studenten. Studenten hebben immers meestal niet de beschikking over een aparte werkkamer.
- De vraag hoe omgegaan wordt met het registreren van bijzondere persoonsgegevens.
- Welke zekerheden er zijn wat er met de beelden gebeurt?
- Studenten kunnen zich bekeken voelen. Dat is anders dan in een toetszaal. In welke mate beïnvloedt dit het resultaat?

Voorts blijkt dat als studenten toetsen maken via online proctoring, ze zich ook zorgen maken over hoe zij hulp kunnen krijgen als er iets misgaat, als opdrachten niet duidelijk zijn of wanneer er sprake is van verdacht gedrag.

De genoemde bezwaren moeten niet gebagatelliseerd worden, maar ze zijn op zich geen reden om online proctoring niet toe te passen of studenten nooit de mogelijkheid te bieden er gebruik van te maken.

3.7 Informatieverstrekking

In een aantal gevallen kan het een direct gerechtvaardigd belang zijn van de instelling om online proctoring toe te passen (bijvoorbeeld tijdens de coronacrisis of voor studenten die in het buitenland zijn). Immers, het is goed mogelijk om te onderbouwen waarom deze vorm van toetsing wordt toegepast en het is mogelijk om voldoende waarborgen te bieden waardoor eventuele negatieve gevolgen van deze vorm van toetsing niet optreden.

Als de instelling ervoor kiest om online proctoring toe te passen, moet die instelling heel goed uitleggen waarom online proctoring wordt toegepast en hoe het precies in zijn werk gaat.

In de eerste plaats moet de instelling door middel van een privacyverklaring duidelijk maken hoe de keuze voor online geproctorde toetsen tot stand komt. In die verklaring moet bijvoorbeeld duidelijk aangegeven worden dat er géén alternatief is (we verwijzen hier ook naar hoofdstuk 4), welke mogelijkheden er zijn voor bezwaar en eventuele alternatieven, van welke systeemleveranciers gebruik wordt gemaakt en welke afspraken zijn gemaakt over wie er toegang heeft tot de gegevens, hoe ze beveiligd zijn en wanneer ze verwijderd worden. Ook moet duidelijk worden gemaakt dat de student géén bijzondere persoonsgegevens hoeft te geven. De instructies moeten duidelijk maken dat studenten voorwerpen die verwijzen naar een bijzonder persoonsgegeven af moeten dekken of uit zicht moeten plaatsen als ze die gegevens niet willen delen. Denk aan een menora, koran of wijwaterbakje, een verwijzing naar hun seksuele geaardheid of een medische conditie. Verder mag een ID-bewijs nooit worden gevraagd voor de identificatie.

Als studenten bezwaar maken, is het nodig dat een functionaris gegevensbescherming of een commissie de bezwaren afweegt tegen de belangen van de instelling. Hiervoor kunnen bezwaren gelden vanuit privacyoptiek, maar ook specifieke uitzonderingen zoals een onveilige situatie thuis. Een ander bezwaar kan zijn dat de student thuis of in zijn/haar omgeving echt geen gelegenheid heeft om een geproctorde toets te doen. Bij sommige instellingen wordt daarbij het advies van de studieadviseur gevraagd. Vervolgens beslist de functionaris gegevensbescherming of een commissie of een bezwaar gegrond is en of een uitzondering van toepassing is.

Ten tweede is het maken en ter beschikking stellen van duidelijke instructies heel belangrijk. De beste optie is om met een video precies uit te leggen hoe het proces in zijn werk gaat en wat er allemaal vereist wordt. Daarnaast is een uitgebreide lijst met Frequently Asked Questions van belang, evenals bijvoorbeeld een chatomgeving waar de studenten terecht kunnen als ze er niet uitkomen.

Ten derde is het van belang dat studenten kunnen oefenen met de online proctoring software. Daarmee kunnen studenten namelijk in de eerste plaats testen of hun apparatuur geschikt is (en kunnen ze eventuele technische problemen oplossen vóórdat de echte toets is). In de tweede plaats kunnen ze de procedure testen zodat ze precies weten wat er gaat gebeuren tijdens een echte toets. De ervaring in Nederland leert tot nu toe dat, ondanks deze voorbereidingen, tussen de 5% en 10% van de studenten bij de eerste online geproctorde toets nog een inlogprobleem ervaart. Bij een tweede geproctorde toets neemt dit percentage echter snel af. Het is zelfs mogelijk om de oefensessie met de proctoring software voor studenten te verplichten als onderdeel van de totale toets. Daarmee kan bovendien ook achteraf duidelijker worden bepaald wie voor een eventueel technische probleem verantwoordelijk is.

In de communicatie met de student moet erop gewezen worden dat het de verantwoordelijkheid van de student is dat de eigen apparatuur werkt. Mochten er problemen optreden, stel dan als instelling zeker dat gemonitord en gelogd wordt dat het proctoringsysteem als geheel functioneert opdat duidelijk is dat het probleem niet aan het systeem heeft gelegen. Het is dan waarschijnlijker dat het aan de voorbereiding of apparatuur van de student heeft gelegen. Als het proctoringsysteem zelf haperingen vertoont, moeten natuurlijk andere procedures worden bewandeld. De situatie is dan vergelijkbaar met het mislukken van een papieren toets, waarbij bijvoorbeeld is gebleken dat de verkeerde toets was geprint. Meestal volgt dan een algehele herkansing.

Vanuit de praktijk is overigens op het moment van schrijven gebleken dat de groep studenten met onoverkomelijke bezwaren tegen online proctoring, gegeven de maatregelen die hierboven zijn beschreven, tot dusver beperkt is.

3.8. Uitdagingen bij opschaling

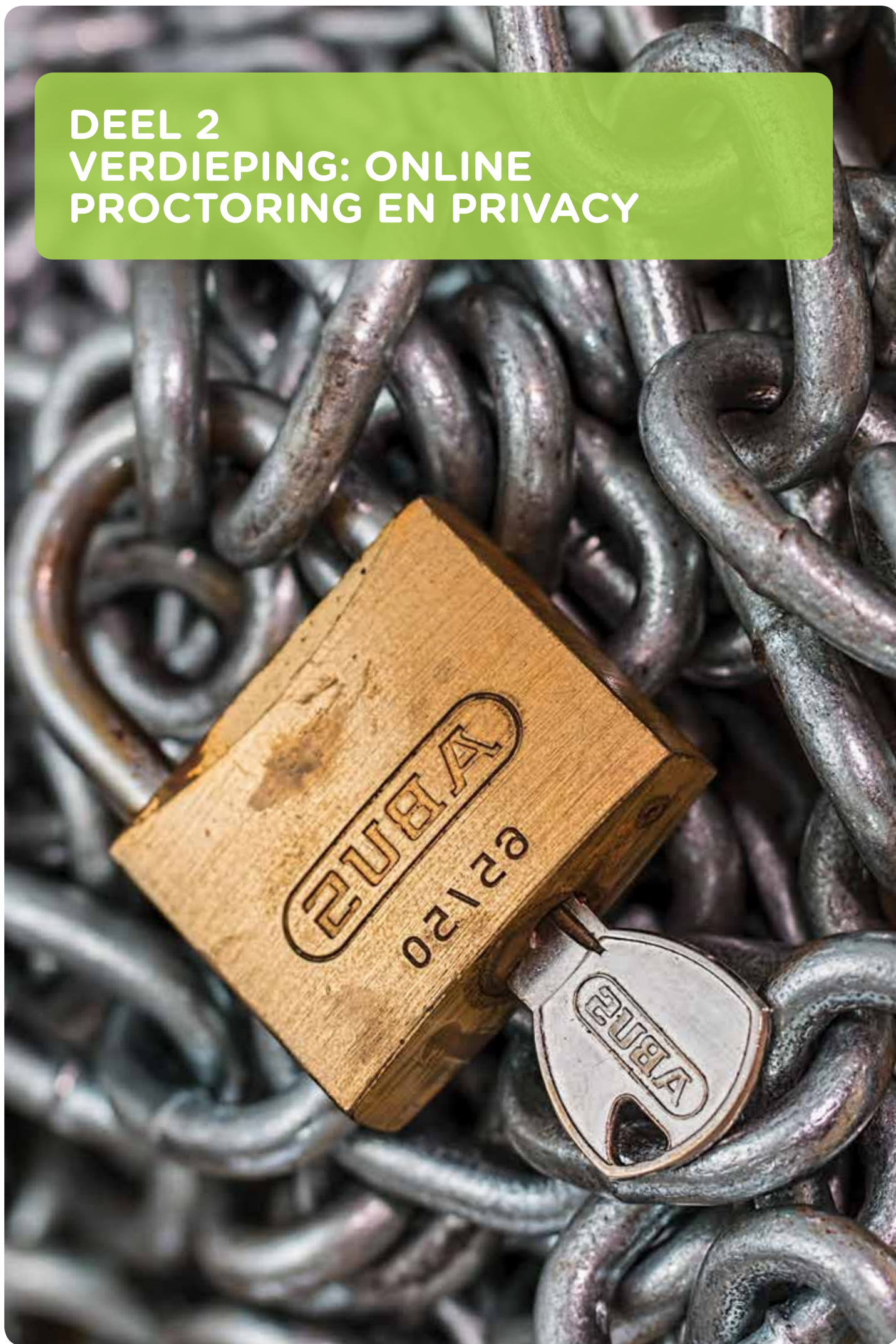
De coronacrisis heeft de belangstelling voor online proctoring sterk vergroot. Het opschalen van online proctoring leidt echter ook tot de nodige uitdagingen.

- Onderwijsinstellingen moeten de nodige voorbereidende werkzaamheden uitvoeren, voordat zij online proctoring kunnen toepassen (zie bijvoorbeeld 4.10).
- Live proctoring is zeker niet geschikt voor het hoger onderwijs gezien de schaalgrootte. Het is de vraag of online proctoring, waarbij opnames opgeslagen en (semi-automatisch) gereviewd worden, in korte tijd kunnen worden opgeschaald. Hebben leveranciers voldoende capaciteit om online proctoring in korte tijd bij tal van onderwijsinstellingen organisatiebreed in te voeren?
- Kunnen de systemen en netwerken van de leveranciers een sterke toename van online proctoring aan? Of krijgen we te maken met technische problemen, met een negatieve impact op de kwaliteit van het toetsen? In dat geval kan de rechtmatigheid van toetsing minder worden gewaarborgd¹⁹.
- Hebben alle studenten de beschikking over passende faciliteiten om te participeren in online proctoring? Denk daarbij aan studenten die gebruikmaken van een laptop van een werkgever waarop zij niets kunnen installeren of waarbij zij geen gebruik kunnen maken van een webcam. Of aan studenten die een laptop delen met een gezinslid, waardoor zij niet altijd de beschikking hebben over de laptop. Normaliter hebben deze studenten een keuze om wel of niet aan online proctoring te participeren.
- Het is de vraag of leveranciers op eventuele technische problemen anticiperen en bijvoorbeeld bepaalde functionaliteiten, zoals het gebruik van een tweede camera, uitschakelen om de 'performance' van het systeem goed te houden bij een grotere belasting. Dit gaat wellicht ten koste van de betrouwbaarheid van online proctoring.
- Online proctoring biedt een groot risico op schaalbaar en 'exporteerbaar' frauderen. Indien online proctoring intensiever en op grotere schaal wordt toegepast, neemt de kans toe dat software ontwikkeld wordt waarmee de werking van proctorsoftware omzeild kan worden.

Deze software zal dan snel worden verspreid. Je kunt dit vergelijken met software die nu ontwikkeld wordt om vals te spelen bij videogames. Ondanks de vele miljoenen die ontwikkelaars van videogames investeren in mogelijkheden om deze 'sabotagesoftware' te detecteren en te bestrijden, weten ze dit probleem niet uit te bannen. Het is de vraag of leveranciers van online proctoring software ook in staat zijn tot zulke grote investeringen. Bovendien is het belang van frauderen bij een tentamen veel groter dan dat van valspelen in videogames. Op korte termijn speelt dit probleem niet. Maar op de wat langere termijn zal dit een reëel probleem worden, indien online proctoring voor veel tentamens en grote groepen studenten wereldwijd wordt toegepast.

19. Klinkenberg, S. (2020). Op afstand tentamineren? Het advies van de SIG Digitaal Toetsen. <https://communities.surf.nl/artikel/op-afstand-tentamineren-het-advies-van-de-sig-digitaal-toetsen>

DEEL 2 VERDIEPING: ONLINE PROCTORING EN PRIVACY



4. PRIVACYBESCHERMING

Wanneer een instantie persoonsgegevens verwerkt, is daarop de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Wat betekent de AVG voor online proctoring? Op die vraag zijn geen pasklare antwoorden te geven.

Duidelijk is wel dat het niet voldoende is om studenten een standaard toestemmingsformulier te laten ondertekenen en een privacyverklaring op de website aan te bieden. De AVG stelt hoge eisen aan zorgvuldige verzameling en verwerking van persoonsgegevens, maar ook aan de beveiliging en opslag van persoonsgegevens.

Dit hoofdstuk biedt handvatten waarmee instellingen passende instrumenten kunnen ontwikkelen.

4.1 Wat zijn persoonsgegevens?

Persoonsgegevens zijn onder de AVG alle gegevens die direct of indirect herleidbaar zijn tot een persoon. Iemands naam of adres is een persoonsgegeven, maar ook gegevens over iemands gedrag vallen hieronder. Bijhouden wat iemand tijdens een tentamen doet, is dus een vorm van persoonsgegevens verzamelen. Ook als gegevens die tot een persoon te herleiden zijn, zijn persoonsgegevens. Het gaat dus niet alleen om namen, adressen, camerabeelden of contactgegevens.

Ook bij een verzameling van gegevens die op het eerste gezicht anoniem zijn, kan er toch sprake zijn van persoonsgegevens, bijvoorbeeld als het mogelijk is de gegevens te combineren met een andere (openbare) bron. Alleen als het ook na de combinatie niet mogelijk is de gegevens te herleiden tot een persoon, is er geen sprake van persoonsgegevens. Vaak is het wel mogelijk om gegevens te herleiden naar personen en van 'geanonimiseerde' gegevens is dan ook niet snel sprake.

Let ook op dat persoonsgegevens alleen gebruikt mogen worden voor het doel waarvoor ze verkregen zijn. Indien een instelling de data uit proctorsoftware ook voor andere doelen wil gebruiken (bijvoorbeeld voor learning analytics of roostering), dan kan het nodig zijn de persoonsgegevens te aggregeren tot uitspraken over meer dan één persoon. Als gegevens echt niet meer te herleiden zijn tot een individu (en aggregatie dus niet ongedaan gemaakt kan worden), dan zijn het geen persoonsgegevens meer. Deze geaggregeerde data zijn daarna vrij te gebruiken. Let wel op dat de persoonsgegevens aggregeren ook een verwerking is en alleen mag als dat verenigbaar is met een van de vooraf gespecificeerde en gecommuniceerde doeleinden.

Een andere optie is persoonsgegevens pseudonimiseren. Dit is een beveiligingsmaatregel, omdat de impact van bijvoorbeeld een datalek beperkt wordt. Doordat de persoonsgegevens toch herleidbaar zijn tot individuen is de AVG nog steeds van toepassing. Bij geanonimiseerde persoonsgegevens mogen de gegevens op geen enkele manier (terug) te herleiden zijn tot individuele personen; ook niet met behulp van andere bronnen en gegevens. Meer informatie over Learning Analytics is te vinden in het document ['Learning analytics in 5 stappen: een handreiking voor de AVG'](#).

Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zoals iemands gezondheid, politieke voorkeur of godsdienst mogen in principe niet worden verzameld of gebruikt. Dit mag alleen als de wet dat verplicht, met uitdrukkelijke toestemming of als een van de andere uitzonderingen onder de AVG van toepassing is. Uitdrukkelijke toestemming mag alleen gebruikt worden wanneer de persoon vrij, dus zonder druk, deze toestemming kan geven. Uitdrukkelijke toestemming wil zeggen dat er apart wordt gevraagd naar dit gegeven, voorzien van een uitleg waarom (en de mogelijkheid om nee te zeggen). De persoon die de toestemming geeft moet hiervoor een actieve handeling uitvoeren.

Gevoelige persoonsgegevens

Gevoelige persoonsgegevens zijn gegevens die stigmatiserend kunnen werken. Voorbeelden van gevoelige gegevens zijn financiële gegevens, informatie over relatieproblemen en informatie over school- en studieprestaties. Als gevolg van deze gevoeligheid is er extra voorzichtigheid geboden bij het gebruik ervan.

Met online proctoring worden er gevoelige persoonsgegevens verwerkt over studenten. Daarnaast wordt de student met online proctoring ook gemonitord en opgenomen. In het bijzonder moet ook rekening worden gehouden met de uitkomsten en resultaten van de online proctoring-software. De detectie van afwijkend gedrag tijdens een online geproctorde toets kan een indicatie zijn van frauduleus handelen.

Vaak worden er bij online proctoring camerabeelden verwerkt en mogelijk in sommige gevallen ook opgeslagen (en vervolgens weer verwijderd). Hoewel camerabeelden meestal niet als bijzonder persoonsgegeven worden aangemerkt (tenzij de beelden bedoeld zijn voor identificatie) kunnen de beelden wel veel zeggen over een student. Het zijn dus sowieso gevoelige persoonsgegevens. Doordat identificatie onderdeel van online proctoring is, is het de vraag of camerabeelden in dit geval niet alsnog geclassificeerd moeten worden als bijzondere persoonsgegevens.²⁰ Bij de update van deze whitepaper is daar geen sluitend antwoord op te geven, dus zal iedere instelling deze afweging zelf (per geval) moeten maken.

4.2 Grondslagen voor verwerking van persoonsgegevens

Ieder gebruik van persoonsgegevens wordt in de AVG 'verwerken' genoemd. Het verwerken van persoonsgegevens is alleen toegestaan wanneer dit gebeurt op basis van een grondslag die in de wet genoemd is. Bij het gebruik van online proctoring-software bij toetsing en examinering worden persoonsgegevens van studenten verwerkt. Hiervoor is dus een juridische grondslag nodig. Er kunnen meerdere grondslagen tegelijk gelden voor verschillende onderdelen van het proces, maar als er geen enkele grond is aan te wijzen, dan is de verwerking niet toegestaan. Het maakt daarbij niet uit hoe handig, nuttig, effectief of wenselijk de verwerking zou zijn. Onder de AVG bestaan de volgende grondslagen:

- toestemming
- uitvoering overeenkomst
- wettelijke plicht
- vitaal belang
- uitvoering van een taak van algemeen belang
- noodzakelijk voor het gerechtvaardigd belang van de instelling

Bij gebruikmaking van (online) proctoring software is belangrijk dat er een legitieme grondslag voor het verwerken van de persoonsgegevens is. Het doel van online proctoring is het controleren van studenten op het rechtmatig afleggen van toetsen en examens. Vanwege de afhankelijkheidsrelatie tussen studenten en instelling is het niet mogelijk om toestemming te vragen aan de studenten (of hun ouders of vertegenwoordigers). Door deze afhankelijkheid kan de toestemming niet 'vrij' gegeven worden. Een vrij gegeven toestemming onder de AVG betekent namelijk dat de studenten ook moeten kunnen weigeren, zonder dat dit negatieve consequenties heeft en dat er een alternatief wordt geboden.

20. Zie ook <https://autoriteitpersoonsgegevens.nl/nl/nieuws/autoriteit-persoonsgegevens-publiceert-beleidsregels-cameratoezicht>

De grondslag 'toestemming' kan mogelijk wel geschikt zijn voor kleine groepen en specifieke uitzonderingssituaties. Bijvoorbeeld topsporters in een hoogtekamp, een buitenlandstage of omdat studenten zelf aangegeven liever thuis tentamen te doen, omdat ze last hebben van de drukke tentamenzaal of lange reistijd. Maar zoals gezegd moet het dan echt een vrijwillig gegeven toestemming zijn. Ook de afhankelijkheidsrelatie tussen de studenten en de instelling speelt mee en (sociale) druk van de instelling kan door de Autoriteit Persoonsgegevens gezien worden als reden waarom toestemming niet meer vrij gegeven is.

Tijdens de coronacrisis lijken 'het uitvoeren van een taak van algemeen belang' en 'gerechtvaardigd belang' de meest voor de hand liggende grondslagen. Dit komt doordat de coronacrisis de context fundamenteel verandert. Waar de tentamenzaal normaal gesproken een realistisch alternatief is, geldt dat tijdens deze crisis niet. Het is goed mogelijk dat na de crisissituatie weer een privacy-vriendelijker alternatief is; dan vervalt vanaf dat moment ook de grondslag voor online proctoring die tijdens de crisis gold. Daardoor is buiten coronatijden de grondslag 'toestemming' mogelijk de enige optie.

Wet op het hoger onderwijs

Op grond van de Wet op het hoger onderwijs is de instelling verplicht voor elk onderwijsinstelling een tentamen af te nemen en voor elke opleiding een examen²¹. De instelling (het instellingsbestuur) is verantwoordelijk voor de praktische organisatie van examens²². Hoe exact invulling wordt gegeven aan de organisatie voor de examens is aan de instelling. Het afnemen van tentamens en examens voor de instelling is een publiek taak die uitgevoerd moet worden door de instelling.

Gerechtvaardigd belang²³

De instelling is op basis van de Wet hoger onderwijs vrij om de praktische organisatie van examens in te vullen. Bij deze invulling moet altijd een afweging worden gemaakt tussen de belangen van de instelling en de impact op de privacy van de studenten. Deze afweging moet worden vastgelegd. De instelling moet de keuze voor online proctoring bij het afleggen van tentamens en examens dus onderbouwen, waarbij de belangen van de instellingen zwaarder moeten wegen dan de privacybelangen van de student, en mag de privacy van de student dus niet onevenredig worden geschaad.

In de belangenafweging voor de inzet van de online proctoring, moeten de volgende onderdelen aan bod komen:

- a. Het gerechtvaardigde belang van de instelling
- b. De mate waarin de verwerking *noodzakelijk* is voor de behartiging van het gerechtvaardigd belang. De noodzaak van deze verwerking kan vastgesteld worden aan de hand van de begrippen proportionaliteit en subsidiariteit.
 - *Proportionaliteit*
Proportionaliteit houdt in dat het doel van de verwerking van de persoonsgegevens voor de instelling in verhouding moet staan tot de inbreuk op de privacy van de student.
 - *Subsidiariteit*
Subsidiariteit houdt in dat het beoogde doel dat voor de verwerking is vastgesteld, niet op een minder ingrijpende manier en/of met minder ingrijpende middelen kan worden bereikt
- c. De mate waarin de belangen of de grondrechten of de fundamentele vrijheden van de student worden geschaad als gevolg van de verwerking
- d. De maatregelen die de instelling heeft genomen om de schade aan de belangen of de grondrechten en de fundamentele vrijheden van de student zo veel als mogelijk te beperken
- e. De weging tussen onderdeel a/b enerzijds en c/d anderzijds

De coronacrisis is sterk van invloed op de vraag of sprake is van een gerechtvaardigd belang, of online proctoring proportioneel is en op de vraag of het beoogde doel – het beoordelen van studenten – niet op een minder ingrijpende manier bereikt kan worden. Als het niet mogelijk is om tentamens op een fysieke locatie af te nemen, dan kan sprake zijn van een gerechtvaardigd belang en noodzakelijkheid. Als het weer mogelijk is om tentamens in een toetszaal te maken, dan is waarschijnlijk geen sprake meer van een gerechtvaardigd belang.

21. Artikel 7.3 Wet op Hoger onderwijs en wetenschappelijk onderzoek

22. Artikel 7.10 Wet op Hoger onderwijs en wetenschappelijk onderzoek

23. Let op: de grondslag gerechtvaardigd belang kan volgens de AVG niet van toepassing zijn op verwerkingen door overheidsinstanties in het kader van de uitvoering van hun taken. Een instelling die zich dus classificeert als een overheidsorganisatie heeft niet de optie om gerechtvaardigd belang als grondslag te gebruiken.

Daarnaast moet de instelling het gebruik van dergelijke software bij de afname van digitale toetsing ook opnemen in de onderwijs- en examenregeling, zodat duidelijk is op welke wijze en onder welke voorwaarden deze toetsing plaatsvindt. De instelling is verplicht om in de onderwijs- en examenregeling informatie op te nemen over de manier waarop tentamens worden afgelegd.²⁴

(Zie ook andere voorwaarden onder de AVG).

4.3 Informatieverstrekking onder de AVG

De AVG kent naast de grondslag nog enkele andere voorwaarden waaraan voldaan moet worden. Er moet sprake zijn van:

- Er moet sprake zijn van een uitdrukkelijk geformuleerd doel. Een voorbeeld hiervan is het garanderen van de integriteit van examens of toetsen, die niet op eigen locatie worden afgenomen, of het tegengaan van fraude bij digitale toetsen en examens.
- Daarnaast mogen alleen persoonsgegevens worden verwerkt die nodig zijn om het doel te bereiken (data-minimalisatie).
- De persoonsgegevens mogen niet langer worden bewaard dan voor het eventueel bewijs van rechtmatige toetsing noodzakelijk is. Als er onregelmatigheden tijdens het toetsen zijn geconstateerd, is het gelet op bewijs en eventuele bezwaren of klachtprocedures wel toegestaan de gegevens (langer) te bewaren, zolang de onderwijsinstelling deze nodig heeft voor de bewijsvoering.
- Een laatste voorwaarde is dat studenten (of hun ouders als ze onder de 16 jaar zijn) inzage moeten kunnen hebben in de gegevens die zijn vastgelegd door de proctoring-software. Daaronder vallen ook beeld- en geluidopnames.

4.4 Beveiliging van persoonsgegevens

Wie persoonsgegevens verwerkt²⁵, moet deze adequaat beveiligen, met gebruikmaking van de meest recente technieken. Dit betekent dat alle verkregen persoonsgegevens redelijkerwijs veilig moeten zijn tegen ongeautoriseerde kennisname, gebruik of verlies ervan. Hierbij gaat het niet alleen om technische, maar ook om organisatorische maatregelen. Daarbij moet uiteraard rekening worden gehouden met alle omstandigheden, zoals stand van de techniek, de kosten van de uitvoering van de maatregelen, de risico's voor studenten en de aard van de gegevens.

Er bestaat geen algemeen geldende norm of standaard waarmee in alle omstandigheden aan de wet wordt voldaan. Hoewel in bepaalde branches specifieke normen (zoals NEN 7510 in de zorg) als adequaat worden gezien, zijn deze er niet voor het onderwijs. Het 'SURF Juridisch normenkader (Cloud)services hoger onderwijs'²⁶ en het 'Normenkader informatiebeveiliging'²⁷ van SURF en de ISO-norm 27001²⁸ kunnen wel helpen bepalen of de beveiliging adequaat is.

Beveiliging van applicaties

Niet alleen de persoonsgegevens moeten adequaat beveiligd worden, dat geldt ook voor de applicatie(s). Dat betekent dat de infrastructuur waarop de applicatie draait, afdoende beschermd moet zijn. Bovendien moet er een adequate toegangsbeveiliging zijn waarmee vastgesteld kan worden dat de juiste persoon inlogt. Ook hiervoor geven de ISO27000-beveiligingstandaarden en het hiervan afgeleide normenkader informatiebeveiliging Hoger Onderwijs handreikingen. Technische oplossingen voor adequate beveiliging zijn er in vele soorten en maten. Het verdient de voorkeur om periodiek een audit te laten uitvoeren door een onafhankelijke externe partij die zowel de technische als de organisatorische beveiliging beoordeelt. Hierbij moet ook aandacht zijn voor afdoende beveiliging tegen sabotagevormen zoals DDOS.

Aansprakelijkheid

Wanneer een instelling software of diensten van derden inzet, blijft de instelling zelfverantwoordelijk en aansprakelijk voor de beveiliging daarvan. Dit geldt ook wanneer de leverancier zijn aansprakelijkheid heeft ingeperkt. Het is verstandig om zo'n beperking van aansprakelijkheid te weigeren of om de aansprakelijkheid uit te breiden voor gevallen waarin er schade door privacyschending ontstaat.

24. Artikel 7:13 lid 1 sub I Wet op Hoger onderwijs en wetenschappelijk onderzoek

25. Let op, de term 'verwerken' is hier breder dan misschien gedacht. Het gaat om elke handeling of geheel van handelingen met betrekking tot Persoonsgegevens, dus bijvoorbeeld ook de opslag of het doorsturen van gegevens zonder zelf wijzigingen aan te brengen.

26. SURF Juridisch normenkader (Cloud)services: <https://www.surf.nl/surf-juridisch-normenkader-cloudservices>

27. SURFnet Normenkader informatiebeveiliging: <https://wiki.surfnet.nl/display/SA/Normenkader+informatiebeveiliging>

28. https://nl.wikipedia.org/wiki/ISO/IEC_27001

Datalekken

Bij een datalek gaat het om ongeoorloofde of onbedoelde toegang tot persoonsgegevens. Maar ook het ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgegevens vallen hieronder. Het gaat dus niet alleen om grootschalige diefstal van persoonsgegevens door hackers; ook ongeautoriseerde toegang tot (een beperkte set) persoonsgegevens valt hieronder. Denk aan studenten die elkaars resultaten kunnen inzien of een docent die zonder reden toegang heeft tot persoonsgegevens van een student.

Datalekken moeten aan de Autoriteit Persoonsgegevens worden gemeld, tenzij het datalek waarschijnlijk geen risico inhoudt voor de rechten en vrijheden van de student. Hierdoor weten betrokkenen dat er een datalek heeft opgetreden (en kunnen betrokken zelf maatregelen treffen). Ook de toezichthouder kan optreden, mocht dit nodig zijn. Er zijn dan ook twee meldplichten vastgelegd in de AVG²⁹:

1. Melding aan de toezichthouder.

Een datalek moet worden gemeld “tenzij het onwaarschijnlijk is dat een inbreuk een risico voor de rechten en vrijheden van natuurlijke personen inhoudt”³⁰. Meldingen aan de toezichthouder zijn vertrouwelijk.

2. Melding aan betrokkenen.

Betrokkenen (studenten, medewerkers, et cetera) moeten worden geïnformeerd over een datalek dat hen aangaat wanneer dit lek “waarschijnlijk een hoog risico voor hun rechten en vrijheden oplevert”³¹.

4.5 Rechten van betrokkenen

In de AVG zijn er verschillende rechten die een betrokkene (student) heeft om de controle op zijn persoonsgegevens te houden. De vier rechten die het meest relevant zijn voor online proctoring zijn het recht van inzage, correctie, verwijdering en bezwaar. Deze worden hieronder kort besproken.

Inzage

Doel van een inzageverzoek is de betrokkene op de hoogte te brengen van welke gegevens een instelling over hem of haar heeft. Dit betekent dus dat de instelling het volledige dossier en alle registraties van gegevens moet verstrekken, dus niet alleen de standaard gegevens die via een online tool ingezien kunnen worden of de gegevens die zonder moeite aangeleverd kunnen worden. Het inzagerecht geldt dus bijvoorbeeld ook voor de camerabeelden en logbestanden. Ook aantekeningen in niet online beschikbare dossiers vallen in principe onder het inzagerecht. Wel kan het zo zijn dat een betrokkene een specifiek inzageverzoek doet waaraan de instelling makkelijker kan voldoen.

Voor online proctoring kan het lastig zijn aan deze verplichting te voldoen als hier geen functionaliteit voor is ingebouwd. De instelling mag in principe geen vergoeding aan de student vragen voor een inzageverzoek. In een uitzonderlijk geval is het wel mogelijk om administratiekosten in rekening te brengen, namelijk bij een verzoek om meerdere kopieën of herhaaldelijke verzoeken. Excessief veel verzoeken in korte tijd mogen worden geweigerd. Het valt te verwachten dat studenten de gegevens van hun tentamen willen inzien voor bijvoorbeeld bezwaar- en beroepsprocedures. Om aan deze verzoeken te kunnen voldoen, is het belangrijk een adequaat proces in te richten, of dit door de leverancier in de software te laten realiseren.

Correctie

Een betrokkene kan met het recht van inzage achterhalen of er persoonsgegevens van hem of haar worden verwerkt en zo ja, welke.

Een gevolg van een succesvol inzageverzoek kan zijn dat de student erachter komt dat de gegevens niet juist of onvolledig zijn. Dan komt het recht op rectificatie aan bod, waarmee een student onvolledigheden en/of fouten in zijn of haar persoonsgegevens kan laten corrigeren. De instelling dient alle redelijke maatregelen te nemen om ervoor te zorgen dat onjuiste persoonsgegevens worden gecorrigeerd of gewist. Let wel, het gaat hier om feitelijke onjuistheden. Een student kan het recht op correctie bijvoorbeeld niet gebruiken om een voor hem onwelgevallig cijfer te corrigeren.

29. Artikel 33 en 34 AVG

30. Zie: <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken#wanneer-hoef-ik-een-datalek-n%C3%ADet-te-melden-aan-de-ap-en-de-betrokken-personen-7333>

31. Zie <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken#wanneer-levert-een-datalek-een-hoog-risico-op-7331>

Verwijdering

Het recht van verwijdering geldt voor alle gegevens die niet correct, niet meer relevant of niet meer nodig zijn voor de doelen waarvoor zij zijn verzameld. Voor de persoonsgegevens die gebruikt en geanalyseerd zijn om online proctoring mogelijk te maken, betekent dit concreet dat gegevens verwijderd moeten worden als het tentamen definitief is beoordeeld en er geen bezwaar of beroep meer mogelijk is. Houd wel rekening met bewaartermijnen uit de Wet op het hoger onderwijs en wetenschappelijk onderzoek. Vergeet ook niet dat de partijen die deze gegevens namens de instelling verwerken (bijvoorbeeld datacenters waar back-ups staan opgeslagen), onder verantwoordelijkheid van de instelling vallen en dus betrokken moeten worden om aan de wet te voldoen.

Recht van bezwaar bij gerechtvaardigd belang en op basis van algemeen belang

De student heeft het recht om op grond van zijn bijzondere situatie bezwaar te maken tegen verwerkingen van de persoonsgegevens als deze worden verwerkt op basis van gerechtvaardigd belang of algemeen belang. Als de instelling dwingende en legitieme gronden voor de verwerking kan aantonen die zwaarder wegen dan die van de student, kan het bezwaar worden geweigerd.

4.6 Geautomatiseerde besluitvorming en proctoring

Bij online proctoring moet rekening worden gehouden met geautomatiseerde besluitvorming en profilering.³² Geautomatiseerde online proctoring om fraude te kunnen detecteren kan negatieve gevolgen hebben voor de student of de student in aanzienlijke mate treffen. Wanneer er door online proctoring een geautomatiseerd besluit wordt genomen, zonder menselijke tussenkomst, waardoor de student een sanctie of maatregel krijgt opgelegd zoals een negatief resultaat of schorsing, heeft dit negatieve gevolgen voor de student.

Een betrokkene heeft ook het recht om niet te worden onderworpen aan geautomatiseerde besluitvorming, zonder menselijke tussenkomst, wanneer er rechtsgevolgen zijn verbonden aan zo een geautomatiseerd besluit of wanneer het de betrokkene in aanmerkelijke mate treft. Het is een vereiste dat er bij zulke besluiten altijd nog een daadwerkelijke menselijke beoordeling door een persoon (surveillant, docent of examiner) plaatsvindt. Dit is op zich natuurlijk heel goed te organiseren en dus te borgen. In de beschrijving van het proces van proctoring door opslag en controle achteraf in hoofdstuk 2 is beschreven hoe dat in drie ronden vormgegeven zou moeten worden.

4.7 Diensten van derden

Vaak zal voor online proctoring gebruik worden gemaakt van diensten van derden. Dit kan al spelen wanneer men software inkoopt en deze bij de instelling inzet. Maar steeds vaker wordt ook de dienstverlening zelf (zoals de opslag van data of de inzet en training van menselijke proctors) aan derden uitbesteed.

Aandachtspunten

Bij het inzetten van software of diensten van derden gelden twee belangrijke aandachtspunten:

1. Voor de student is de instelling altijd zelf aansprakelijk voor de kwaliteit van en problemen bij de dienstverlening. Dit geldt dus ook wanneer de softwareleverancier zelf geen aansprakelijkheid wenst te dragen. De student kan deze aansprakelijkheid niet 'wegtekenen' via bijvoorbeeld een aansprakelijkheidsbeperking in de akkoordverklaring of een disclaimer bij het startscherm van de software.
2. Als de dienstverlener zelf ook persoonsgegevens verwerkt, zoals het geval is bij clouddiensten, dan moet de instelling aparte afspraken maken over wat de dienstverlener daarmee mag doen. De dienstverlener wordt dan een verwerker genoemd in de zin van de AVG.

De in het tweede punt bedoelde afspraken moeten worden vastgelegd in een zogeheten verwerkersovereenkomst.

Gebruik van data door de leverancier van proctoring software voor andere doeleinden

Het kan voorkomen dat de leverancier van de proctoring-software gebruik wil maken van persoonsgegevens of (geanonimiseerde) data voor eigen doelen, buiten de verwerkersovereenkomst om. Als er sprake is van een verwerkersovereenkomst, is het de leverancier niet toegestaan binnen die overeenkomst verkregen persoonsgegevens te gebruiken voor eigen doeleinden. Dit dient contractueel te worden uitgesloten. Eventueel kunnen wel tijdens het verwerken anonieme gegevens worden gegenereerd, die inzicht kunnen geven in het gebruik van de software. Dat is toegestaan als die gegevens alleen bedoeld zijn om de gebruikerservaring van de software te verbeteren of fouten of bugs in de software te verhelpen.

Algemeen geldt dat de leverancier zelfstandig verwerkingsverantwoordelijk is voor iedere verwerking van persoonsgegevens buiten de overeengekomen doeleinden uit de verwerkersovereenkomst. Daarbij moet de leverancier voor die verwerking zelfstandig een doel en rechtmatige grondslag hebben.

4.8 Verwerkingen in andere landen

De AVG is Europese regelgeving. In de Europese regels is opgenomen dat persoonsgegevens alleen mogen worden opgeslagen of verwerkt in landen waar een 'adequaate' niveau van bescherming bestaat. Dat wil zeggen dat het land regels moet hebben die vergelijkbaar zijn met de Europese regelgeving. Dit onder meer om ervoor te zorgen dat de persoonsgegevens op een vergelijkbaar niveau beschermd worden.

Buiten Europa

Er is geen verplichting om persoonsgegevens in Nederland op te slaan. Ieder land binnen de Europese Economische Ruimte (EER) heeft in principe een adequaat beschermingsniveau. Bij landen buiten de EER ligt dit moeilijker, omdat er vrij weinig landen zijn die voldoen aan de Europese eisen. Op dit moment geldt nog de EU-U.S. Privacy Shield. Naar verwachting volgt in de loop van 2020 nog een uitspraak van het Europees Hof over de adequaatheid van het beschermingsniveau van EU-U.S. Privacy Shield.

Europese dochter

Er ontstaat een bijzondere situatie wanneer persoonsgegevens worden opgeslagen in een datacenter in een Europees land dat wordt beheerd door een Amerikaanse partij of een dochtermaatschappij van een Amerikaanse partij. De Amerikaanse CLOUD ACT regelt de toegang tot elektronisch bewijs in strafzaken. Amerikaanse autoriteiten kunnen bij Amerikaanse cloud-dienstverleners gegevens vorderen die in een ander land zijn opgeslagen. Hieraan zijn wel de nodige waarborgen verbonden, namelijk dat er een bevel is van een Amerikaanse rechter. Een dergelijke informatievordering kan worden aangevochten door het betreffende bedrijf of de EU. Vervolgens zal de Amerikaanse rechter een belangenafweging moeten maken en beslissen of de AVG zwaarder moet wegen of juist de CLOUD ACT. Hoe een dergelijke vordering dan wel bezwaar zal uitpakken is op het moment van schrijven (april 2020) onbekend.

4.9 Uitvoering Data protection impact assessment (DPIA)

Gegevensbescherming begint bij het in kaart brengen van risico's voor betrokkenen. Een hulpmiddel daarvoor is de Data Protection Impact Assessment (DPIA) ofwel de beoordeling van de effecten van gegevensbescherming. Dit bij wet verplichte proces helpt bij het identificeren en minimaliseren van de risico's van een verwerking van persoonsgegevens. Deze risicobeoordeling moet worden uitgevoerd als een verwerking waarschijnlijk leidt tot een hoog risico voor de betrokkenen. Daarnaast kan er bij het gebruik van online proctoring sprake zijn van verwerking op grote schaal van (gevoelige) persoonsgegevens. Wanneer dit zo is, is het verplicht een DPIA uit te voeren.

4.10 Handhaving van de wet

De komst van de AVG heeft de handhaving van de privacywetgeving veranderd. De toezichthouder heeft nu de mogelijkheid zwaardere boetes op te leggen. De toezichthouder kan een boete opleggen wanneer een instelling geen adequate beveiliging heeft of een datalek niet meldt. Deze boete kan in theorie oplopen tot 10 miljoen euro of 2% van de jaaromzet. De toezichthouder heeft een beleid gepubliceerd over de hoogte van de boetes voor verschillende soorten overtredingen.

4.11 Alternatieven voor online proctoring³³

Dankzij de coronacrisis is het vooralsnog niet mogelijk om fysiek naar een onderwijsinstelling te gaan om een schriftelijke of digitale toets te maken. Zoals in dit hoofdstuk al beschreven kan online proctoring in deze situatie een proportioneel middel zijn, bijvoorbeeld op basis van gerechtvaardigd belang.

Echter, de instelling moet wel per toets aangeven dat er géén goed alternatief is voor het toetsen van de beoogde kennis en vaardigheden. Het is dus noodzakelijk eerst alternatieve oplossingen voor klassieke tentamens in ogenschouw te nemen. Hieronder sommen we een paar mogelijkheden.

- De toets vervalt. Op een later moment wordt getoetst of studenten de betreffende leerstof beheersen. Dit kan wellicht leiden tot piekbelasting bij studenten omdat op een later moment meer leerstof getoetst zal worden. Dit is echter ook afhankelijk van de vraag of studenten in hun onderwijs regelmatig oefenen met de leerstof.
- De toets wordt uitgesteld totdat het mogelijk is toetsen bij de onderwijsinstelling te maken. Hierdoor hoeft de onderwijsinstelling op korte termijn geen actie te ondernemen. Deze oplossing leidt wel tot een piekbelasting bij docenten en studenten, op een later moment. Verder loopt de student mogelijk studievertraging op.
- De toets wordt meer formatief ingezet en er worden andere toetsvormen toegepast tijdens de uitvoering van het onderwijs. De instelling past de wijze van beoordelen aan waarbij meer gekeken wordt naar inspanning en progressie van de student dan naar het behaald niveau. Er kan wel worden gemonitord of studenten leerstof hebben begrepen en weten hoe zij de leerstof kunnen toepassen. Op een later moment beoordeelt de docent dan op een andere manier of studenten de leerstof daadwerkelijk kunnen toepassen en het niveau dat wordt behaald. Dit alternatief is in lijn met de adviezen die toetsexperts als Dominique Sluijsmans al jaren geven. Formatief toetsen biedt nog géén antwoord op het borgen van de kwaliteit van het gerealiseerde eindniveau van de student. De onderwijsinstelling zal later nog een geborgde toetsprocedure moeten realiseren.
- De toets wordt op een locatie uitgevoerd waarbij studenten en docenten minimaal anderhalve meter van elkaar verwijderd zijn. Dit alternatief vraagt om een besluit om voor het maken van een tentamen fysiek bij elkaar te komen. Je zult ook de logistiek van het uitreiken en inleveren van tentamens hierop moeten inrichten. Dit zal vooral bij kleine groepen studenten een alternatief kunnen zijn, maar voor grote groepen is dit vermoedelijk niet uitvoerbaar.
- De toets wordt vervangen door een alternatieve vorm van beoordelen die niet vraagt om separaat online toezicht. Voorbeelden zijn een opdracht (bijvoorbeeld studenten toetsvragen met antwoorden laten ontwikkelen), een 'take-home' toets, een open boek-tentamen of een mondeling tentamen. Vanuit het perspectief van examencommissies lijkt deze optie aantrekkelijk omdat het niveau van de toetsing waarschijnlijk meer verschuift van reproductie van kennis naar productie van kennis. Dat is op zich een aantrekkelijk alternatief omdat het 'niveau' van het onderwijs en de toetsing niet daalt. Dit vergt echter wel de nodige inspanningen van examinatoren en docenten. De uitvoerbaarheid is vooral afhankelijk van het aantal studenten dat een toets afneemt en of er bijvoorbeeld al gewerkt werd aan een andere toetsvorm. Tegelijkertijd wordt van studenten in deze opzet naar verwachting een andere inspanning vereist.
- De toets wordt niet veranderd, maar wel online afgenomen, maar zonder online proctoring. Deze vorm betekent eigenlijk dat je er als docent op vertrouwt dat de student de toets maakt zonder te frauderen. Dit is natuurlijk weinig fraude-preventief. Maar er zijn aanvullende mogelijkheden:
 - Er kan aan de studenten worden gevraagd om een Academic Integrity Statement in te vullen dat ze niet frauderen. Het is niet bewezen welk effect dit heeft.
 - De online toets wordt voorzien van een strakke begin- en eindtijd om de toegang te beperken.
 - Een grote eindtoets wordt in meerdere kleine toetsen gesplitst opdat de impact van fraude verkleind wordt.
 - De vragen worden uit een grote itembank getrokken of geparametriseerd zodat iedere student andere vragen heeft.
 - Als de student een antwoord heeft gegeven op een vraag (gesloten of open) kan deze niet meer worden veranderd zodra de volgende vraag in beeld komt.
 - De tijd per toetsvraag wordt beperkt. Hierbij is echter de vraag of tijdsdruk niet een te grote invloed heeft op het resultaat.
 - Er wordt gekozen voor open vragen in plaats van gesloten vragen die achteraf ook op plagiaat worden gecheckt.

33. De informatie uit deze paragraaf is grotendeels gebaseerd op het Adviesdocument inzake het op afstand veilig, betrouwbaar en valide afnemen van summatieve kennistoetsen van de Werkgroep DKT-FOL van Fontys Hogescholen (27-3-2020).

Het is in elk geval belangrijk je te realiseren dat het toepassen van online proctoring één van de alternatieven is nu instellingen dankzij de coronacrisis niet in staat zijn op locatie groot-schalig tentamens af te nemen. Mogelijk dat een combinatie van een aantal alternatieven én online proctoring de oplossing biedt. Bijvoorbeeld het laten vervallen of formatief maken van wekelijkse voortgangstoetsen, het uitstellen van enkele examens met een zeer groot (civiel) belang en de rest van de examens via online proctoring.

Avans Hogescholen heeft een '[Beslisboom Toetsen op afstand](#)' samengesteld die helpt bij het maken van een weloverwogen keuze met betrekking tot de aanpassing van toetsen: Zie ook de [toelichting](#).

4.12 Concrete aanbevelingen

Op basis van de privacyaspecten die in dit hoofdstuk zijn beschreven, is voor onderwijsinstellingen een aantal best practices op het gebied van online proctoring opgesteld.

1. Stel een aparte privacyverklaring op voor online proctoring en leg daarin het doel vast. Maak duidelijk welke gegevens worden verzameld en wat daarmee gebeurt.
2. Leg hierin ook vast dat gegevens direct worden vernietigd als deze niet meer noodzakelijk zijn. Zorg ervoor dat zowel de instelling als de leverancier deze bewaartermijnen strak handhaven.
3. Als gekozen wordt voor de grondslag gerechtvaardigd belang, zorg dan voor een goed onderbouwde belangenafweging van het gerechtvaardigd belang voor de inzet van de online proctoring, waarbij de volgende onderdelen aan bod komen:
 - a. Het gerechtvaardigde belang van de instelling.
 - b. De mate waarin de verwerking nodig is om het gerechtvaardigd belang te behartigen;
 - c. De mate waarin de belangen of de grondrechten of de fundamentele vrijheden van de betrokkenen worden geschaad als gevolg van de verwerking.
 - d. De maatregelen die de instelling heeft genomen om de schade aan de belangen of de grondrechten of de fundamentele vrijheden van de betrokkenen zo veel als mogelijk te beperken.
 - e. De weging tussen onderdeel a/b enerzijds en c/d anderzijds.
 - f. Let hierbij op dat de grondslag gerechtvaardigd belang alleen gebruikt kan worden als er geen privacy-vriendelijkere alternatieven zijn. Onderbouw dus ook waarom die niet beschikbaar zijn.
4. Spreek af met de leverancier dat deze gedetailleerde uitleg verstrekt, ook bij updates van de tool, zodat deze in de privacyverklaring kan worden opgenomen.
5. Houd toezicht op gebruik van de gegevens, zorg dat alleen die mensen toegang hebben die dit voor de uitoefening van hun werk echt nodig hebben (bijvoorbeeld de surveillant, bij voorkeur hebben examinatoren en leden van examencommissies géén rechtstreekse toegang, toegang wordt alleen gegeven via de surveillant).
6. Stel een mogelijkheid beschikbaar om online proctoring gegevens te downloaden (inzageverzoek) en desgewenst te corrigeren (bij evidente fouten).
7. Ga na welke tools geautomatiseerd beslissingen nemen die studenten in aanmerkelijke mate raken. Richt het proces zo in dat uiteindelijk een mens het besluit neemt (dat rechtsgevolgen heeft voor de student) en biedt altijd een duidelijke bezwaarmogelijkheid aan.
8. Sluit verwerkersovereenkomsten met de leveranciers van online proctoring tools.
9. Controleer regelmatig de beveiligingsaudits en rapporten van de leverancier om te verifiëren of de leverancier nog aan de beveiligingsnormen voldoet.
10. Stel beleid op tegen datalekken en schendingen van de beveiliging.
11. Reageer positief op privacyzorgen en -bezwaren van studenten en zorg voor alternatieven waarmee deze zorgen kunnen worden weggenomen.
12. Zorg dat er een DPIA wordt uitgevoerd wanneer de verwerking een hoog risico inhoudt voor de betrokkenen of wanneer de verwerking inhoudt dat dat persoonsgegevens op grote schaal verwerkt worden.

DEEL 3 VERDIEPING: FRAUDEBESTRIJDING



5. VEILIGHEID EN FRAUDEBESTRIJDING

Voor veiligheid en fraudebestrijding bestaat veel maatschappelijke aandacht, maar tegelijkertijd zijn het lastige onderwerpen. Hoe hoger de eisen aan de veiligheid van een tentamenafname, hoe duurder en onpraktischer het vaak wordt en hoe groter de impact op de privacy van studenten. Zelfs afname in een reguliere tentamenzaal is niet 100% veilig, maar doordat onderwijsinstellingen en examencommissies daar wel veel ervaring mee hebben, zijn zij in de veronderstelling dat zij de risico's goed kennen en dat fraude op een acceptabele manier wordt tegengegaan.

Dit hoofdstuk beschrijft de verschillende oplossingen die online proctoring software biedt om fraude te voorkomen. Ook komen de manieren aan bod waarop studenten kunnen proberen te frauderen. Een examen- en toetscommissie kan op basis hiervan en met het keuzemodel toetsveiligheid in paragraaf 5.4 inschatten of online proctoring geschikt is voor bepaalde toetsen of examens.

5.1 Fraude voorkomen

Preventieve werking van online proctoring

Online proctoring biedt diverse middelen om de veiligheid te vergroten en fraude te voorkomen. Alleen al de aankondiging dat er online toezicht plaatsvindt, zal de eventuele neiging om te frauderen verminderen. In die aankondiging worden allerlei methoden en maatregelen opgesomd om het frauderen zoveel mogelijk te ontmoedigen. Want hoe meer maatregelen getroffen worden, hoe meer moeite een student zal moeten doen om toch ongezien te frauderen. Hoe meer moeite nodig is, hoe minder fraude zal voorkomen is de redenering. Deze vorm van fraudepreventie is vrijwel gelijk aan de klassieke preventie bij toetsing op locatie.

Tegelijkertijd worden er in de praktijk al methoden ingezet voor toetsing waarbij het toezicht in feite beperkt is, soms vanwege een gebrek aan alternatieven. Denk hier aan het gebruik van videoconferencingtools voor toezicht. Tijdens de coronacrisis worden deze soms toch als acceptabel beoordeeld, simpelweg omdat de instelling geen alternatief voorhanden heeft.

Het preventieve aspect van online proctoring wordt vaak niet ingebracht in de discussie rondom online proctoring. Pleitbezorgers van online proctoring menen dat hierdoor geen valide discussie over dit onderwerp wordt gevoerd.

Camera('s) en microfoon

Bij vrijwel alle proctorsoftware kan een proctor of reviewer meekijken via de webcam van de student. Er zijn ook varianten met twee webcams. Voor de tweede webcam wordt dan vaak gebruik gemaakt van een telefoon of tablet die achter de student geplaatst moet worden. Daardoor is een groter deel van de ruimte zichtbaar en heeft de proctor of reviewer ook zicht op het beeldscherm en toetsenbord van de student. De tweede webcam kan ook worden gebruikt om te controleren of de student bijvoorbeeld geen oortjes in heeft.

Gezichtsherkenningstechnologie

Sommige leveranciers van proctorsoftware maken gebruik van gezichtsherkenningstechnologie om studenten te autoriseren. We komen dan op het terrein van geautomatiseerde verwerking van biometrische data, vergelijkbaar met vingerafdrukherkenning. Met gezichtsherkenningstechnologie kan met grote zekerheid worden geverifieerd of een student waar-

van de biometrische gegevens bekend zijn in een systeem ook daadwerkelijk achter het beeldscherm zit tijdens een toets. Deze technologie is omstreden en het is een zwaar middel om in te zetten, met vergaande gevolgen voor de privacy.

Hetzelfde geldt voor keystroke dynamics. Niet alleen wat een gebruiker tikt (een wachtwoord) kan iemand identificeren, maar ook de *manier waarop* iemand dat doet^{34 35}. Dit is dus ook een vorm van geautomatiseerde biometrische identificatie en daarmee ook een zwaar middel³⁶. Zowel de gezichtsherkenningstechnologie als de keystroke dynamics technologie worden om redenen van 'privacy impact reductie' niet toegepast in de systemen die gebruikt worden in het Nederlands hoger onderwijs.

Een vorm van omgevings-, gezichts- en houdingsherkenningstechnologie die echter wél wordt toegepast is gebaseerd op herkenning *zonder* identificatie of autorisatie. De software 'neemt alleen waar' dat er een persoon in beeld is, maar weet niet welke persoon dit is. Deze technologie heeft dus veel minder vergaande impact op de privacy en het is de vraag of dit als verwerking van biometrische data moet worden gezien. Op basis van vergelijking van de beelden met andere beelden van personen die de toets maken, kan bijvoorbeeld afwijkend gedrag worden geconstateerd; vervolgens kan het systeem deze afwijking rapporteren.

Screencapture

Een andere methode die vrijwel alle leveranciers gebruiken, is dat de surveillant via screen-capture kan nagaan wat zich op het scherm van de student afspeelt. De surveillant kan daardoor zien welke programma's open staan en of de student niet stiekem verboden bronnen opent.

Lockdown browser

De 'lockdown browser' is een functie die niet alleen bij online proctoring wordt gebruikt, maar ook in andere vormen van digitaal toetsen. Hierdoor kunnen alleen de tentamenomgeving en specifieke, toegestane applicaties worden gebruikt. De mogelijkheden kunnen per leverancier nogal verschillen. Het is belangrijk deze functie niet te overschatten. Het feit dat iemand geen andere applicaties kan starten, wil niet zeggen dat die applicaties niet op de achtergrond kunnen draaien. Met voldoende ICT-kennis zijn de lockdown browsers (op een eigen device) bovendien wel te omzeilen. Dat maakt ze zeker niet zinloos, maar bij online proctoring moeten ze vooral worden gezien als aanvulling op screencapture, logging van geraadpleegde bronnen en systemen en camerabeelden. Let ook op dat één student met voldoende ICT-kennis software kan ontwikkelen die daarna wereldwijd door vele duizenden studenten gebruikt kan worden. Kortom, niet iedere individuele fraudeur heeft per definitie een hoge mate van ICT-kennis nodig.

Logging van de pc zelf

Sommige proctorleveranciers maken het mogelijk om tot in zeker detail te zien wat er op de computer van de student gebeurt. Hoe ver dit gaat verschilt per leverancier, maar de mogelijkheden zijn groot. Zo kunnen lopende processen³⁷ worden gescand en kunnen delen van het geheugen worden uitgelezen. Daartoe moet de software toegang krijgen tot bepaalde onderdelen van het systeem van de pc. Omdat dit vaak de privé-laptop van een student is, krijgt de software daarmee ook toegang tot veel niet relevante persoonsgegevens van de student. Daarmee is dit eveneens een zwaar middel om in te zetten en moet heel duidelijk gemaakt worden in bijvoorbeeld de privacyverklaring welke data wordt verzameld en wat daarmee gebeurt. Indien de leverancier voldoende transparant is over de werking van de logging kan inzet van dit middel acceptabel zijn, geredeneerd vanuit het doel van de dataverwerking.

5.2 Risicofactoren bij online proctoring

Een student kan op verschillende manieren proberen te frauderen. Onderstaande lijst is zeker niet uitputtend, maar geeft wel een beeld van de mogelijkheden. Per fraudemethode wordt aangegeven of en zo ja op welke manier online proctoring de fraude bestrijdt.

34. Jiexun L., Rong Z. en Hsinchun C. (2006). 'From fingerprint to writeprint'. Communications of the ACM, Volume 49 Issue 4. Te vinden op <http://www.disciplineoforganizing.org/wp-content/uploads/2013/01/FingerprintToWriteprint.pdf>

35. Bijvoorbeeld het tempo waarin iemand tikt, bij welke letters of cijfers iemand vertraagt en hoe lang iemand een toets ingedrukt houdt. Voor meer achtergrondinformatie zie: https://en.wikipedia.org/wiki/Keystroke_dynamics

36. Met 'keystroke dynamics' kan iemand overigens nog niet met zekerheid worden herkend, maar wel steeds beter dat iemand het niet is. Wanneer de keystroke dynamics van een student bekend zijn, kan de software een seintje geven als degene die het tentamen maakt *waarschijnlijk niet* de student is die het tentamen zou moeten doen. Dat kan aanleiding zijn de camerabeelden nog een keer goed te bekijken.

37. Dit zijn bijvoorbeeld applicaties die aan staan (ook als dat op de achtergrond is).

De hardware en software

Bij online proctoring maakt de student gebruik van de eigen pc of laptop. Hiermee zou op verschillende manieren fraude kunnen worden gepleegd.

- *Er worden aparte programma's ontwikkeld waarmee proctorsoftware wordt omzeild.*
In de game-industrie hebben ontwikkelaars er veel last van dat software wordt ontwikkeld die het mogelijk maakt om vals te spelen. Naarmate online proctoring op grotere schaal wordt toegepast, zal er een markt ontstaan voor vergelijkbare software die online proctoring probeert te omzeilen.
 - Dit impliceert dat leveranciers van online proctoring software detectiesoftware moeten ontwikkelen, die door kwaadwillenden vervolgens weer omzeild zal worden.
 - Ondanks miljoeneninvesteringen hebben game-ontwikkelaars deze strijd nog steeds niet gewonnen. Het is dus de vraag of dit voor online proctoring (waar het belang bij fraude veel groter is) wel gaat lukken.

- *Een extra browser of tabblad*
Misschien wel de bekendste methode om te frauderen is om tijdens het tentamen antwoorden proberen op te zoeken op internet.
 - *Tegenmaatregel:* deze vorm van fraude is gemakkelijk tegen te gaan. Screenshots en een extra webcam lossen dit sowieso op. Ook een goede 'lockdown browser' is vaak voldoende.

- *Een tweede persoon die meekijkt of de pc bestuurt.*
Net zoals een online proctor kan meekijken, kan een student ook iemand anders op afstand toegang geven tot zijn pc. Die ander kan dan meekijken en zelfs het toetsenbord en de muis besturen en zo het tentamen doen terwijl de student zelf achter de pc zit.
 - *Tegenmaatregel 1:* als de proctor de muis en het toetsenbord van de student kan zien, dan zou dit te detecteren zijn doordat de bewegingen niet overeenkomen met wat op het scherm gebeurt. De kans dat een proctor dit ziet is echter niet zo groot.³⁸
 - *Tegenmaatregel 2:* als een student een uur lang moet 'faken' dat hij/zij daadwerkelijk een tentamen maakt zal snel afwijkend gedrag kunnen worden geconstateerd.
 - *Tegenmaatregel 3:* eigenlijk kan alleen goede loggingsoftware dit tegengaan. Deze software kan in detail zien welke softwareprocessen op een pc draaien en welke externe verbindingen er gemaakt worden.

- *Software die antwoorden geeft*
De student kan software installeren die de vragen op het scherm scant en de antwoorden daarvan opzoekt. Die antwoorden zou de software op het scherm kunnen laten zien, en eventueel zelfs direct kunnen invullen.
 - *Tegenmaatregel 1:* als het antwoord zichtbaar op het scherm wordt getoond, valt dit gemakkelijk te detecteren met screenshots.
 - *Tegenmaatregel 2:* lastiger wordt het als de software het antwoord meteen invult. In dat geval is eigenlijk alleen goede loggingsoftware een geschikte oplossing.

- *Een virtuele pc*
Met een virtuele pc simuleert de student een extra pc binnen zijn reguliere omgeving. Als het tentamen hierbinnen wordt afgenomen, zal de proctorsoftware alleen dat scherm zien en is onzichtbaar welke software op de hoofd-pc draait. Dat maakt veel van de eerdergenoemde opgeloste fraudeopties opeens weer mogelijk.
 - *Tegenmaatregel 1:* als het gebruik van een virtuele pc tijdens het tentamen verboden is, dan is het mogelijk deze toch te detecteren met vergaande software. Dit lukt echter niet op alle hardware en met alle virtualisatiesoftware en het valt niet te detecteren met proctorsoftware die in een browser draait.
 - *Tegenmaatregel 2:* een tweede camera achter de student helpt ook omdat het scherm dan alsnog in zijn geheel bekeken wordt. Dit voorkomt een deel van de fraude, zoals het open hebben van extra schermen. Software die volledig op de achtergrond werkt kan hiermee niet worden gedetecteerd.

38. Het is mogelijk het lokale toetsenbord tijdelijk uit te schakelen waardoor de student antwoorden kan intikken zonder dat er iets op het scherm gebeurt. Als hij dat ongeveer tegelijk doet met de persoon die voor hem de antwoorden invult, zal dit nauwelijks opvallen.

Hulp in de omgeving

- *Een andere persoon in de ruimte*

Als er iemand anders in de ruimte is zou er overleg kunnen plaatsvinden met degene die tentamen doet (zowel pratend als met gebaren).

- ⊘ *Tegenmaatregel 1:* een microfoon kan dit voor een deel opvangen, als er tenminste gesproken wordt. Dat maakt overleg tussen de student en een ander relatief ingewikkeld. Dit is overigens standaardpraktijk bij alle proctoring software.
- ⊘ *Tegenmaatregel 2:* uiteraard helpt hier het gebruik van camera's. Vaak moet de student voor het tentamen begint de hele ruimte even laten zien. Maar zeker bij gebruik van één camera kan een tweede persoon zich steeds buiten beeld verstoppen. Deze kan instructies geven door middel van gebaren of briefjes.³⁹

- *Iemand anders zit achter de pc*

Er wordt – net als in een reguliere tentamenzaal – soms geprobeerd een ander het tentamen te laten maken.

- ⊘ *Tegenmaatregel:* iemand vragen zich te legitimeren met een collegekaart of ID-bewijs door deze via de webcam te laten zien. Dit is in feite standaardpraktijk en dit risico speelt dus geen rol.

- *Verstopte spiekbrieftjes*

In de reguliere tentamenzaal worden regelmatig spiekbrieftjes gebruikt. Dat zal als de student thuis tentamen doet eerder toe- dan afnemen.

- ⊘ *Tegenmaatregel 1:* spiekbrieftjes zijn maar gedeeltelijk te voorkomen. Camerabeelden kunnen hierbij wel helpen, zeker als voorafgaand aan het tentamen een goede en zorgvuldige check van de hele kamer wordt gedaan. Tijdens het tentamen zal de kamer nooit volledig zichtbaar zijn en is het verstoppen van een briefje mogelijk.⁴⁰
- ⊘ *Tegenmaatregel 2:* de student vragen om met een handspiegel via de webcam de rand van het beeldscherm te laten zien (om opgeplakte post-it briefjes te kunnen waarnemen).

- *Iemand kijkt op afstand mee*

Eerder is al de mogelijkheid besproken hoe gedetecteerd kan worden dat iemand door middel van software op de pc meekijkt. Er zijn echter ook andere manieren om mee te kijken, bijvoorbeeld door een aparte camera (een telefoon of tablet) achter de student te plaatsen of met een zogenaamde buttoncamera op de kleding. Ook het splitsen/aftappen van de beeldschermkabel is mogelijk.⁴¹

- *Geen tegenmaatregel mogelijk:* dit valt dat niet te detecteren wanneer het goed wordt uitgevoerd (een kleine camera is gemakkelijk tussen een stel boeken te verstoppen). De uitdaging voor de student is daarna om ervoor te zorgen dat iemand anders de antwoorden kan doorsturen. Hiervoor geldt hetzelfde als voor de spiekbrieftjes: dit is altijd wel te verbergen, omdat nooit de gehele ruimte zichtbaar is. Vooral bij multiplechoice-examens is deze vorm van fraude heel eenvoudig, omdat maar weinig informatie hoeft te worden doorgegeven (het nummer van het antwoord)⁴². Deze fraude kan wel bemoeilijkt worden door de antwoorden te randomiseren.
- Het effect van deze vorm van fraude kan echter weer tegengegaan worden door niet voor multiplechoicevragen te kiezen maar open vragen met relatief lange antwoorden. Er kan een aanvullende combinatie met een open boek tentamenvorm worden toegepast. Immers, hoe langer en uitgebreider de antwoorden zijn die moeten worden gegeven, hoe lastiger deze vorm van fraude wordt.

5.3 Wat betekent dit dan?

Met een beetje creativiteit is de lijst met fraudemogelijkheden bij online proctoring aanzienlijk.⁴³ Op basis van de voorbeelden in dit hoofdstuk valt een aantal conclusies te trekken:

39 Dit wordt het makkelijkste als de tweede persoon het scherm kan zien, maar zelfs als dat niet kan zou de student af en toe hardop kunnen praten. Dat is moeilijk te verbieden want sommige mensen denken hardop.

40 Er zijn meerdere manieren denkbaar waarop het briefje niet zichtbaar is tijdens de check van de kamer maar wel tijdens het tentamen. Bijvoorbeeld door er iets voor te hangen dat met een dun touwtje verwijderd kan worden. Zolang die plek buiten beeld blijft tijdens het tentamen is dit bijna niet te detecteren.

41 Dit kan met een klein kastje dat tussen de pc en de monitor zit en door de pc niet te detecteren is. Het signaal kan op die manier zowel met een kabel als draadloos naar iemand anders worden doorgestuurd.

42 Voorbeeld: een student kan vier kleine lampjes in zijn kamer verbergen die aangestuurd worden door de persoon die meekijkt. Ieder lampje staat dan voor 1 antwoord (A, B, C of D). Zo zijn er tientallen manieren van subtiele communicatie denkbaar die niet of nauwelijks gedetecteerd kunnen worden.

43 Zie bijvoorbeeld: <http://madebyknight.com/knuckle-scanners-cheating-how-to-bypass-proctortrack/>

- Fraude waarbij de hardware of software wordt gemanipuleerd, is meestal te detecteren. Wel betekent dit al snel een grotere impact op de privacy van studenten, maar dit kan noodzakelijk zijn als er geen goed alternatief te realiseren is (zoals tijdens de coronacrisis het geval kan zijn).
- Zolang de onderwijsinstelling geen controle heeft over de ruimte waar het tentamen wordt afgenomen en de computer van de student, zijn er manieren te bedenken waarop gefraudeerd kan worden zonder dat detectie direct mogelijk is. In theorie zijn alle andere factoren in een tentamenzaal na te bootsen met tentamens op PC's van de instelling inclusief online proctoring. Daarom is de *maximale* fraudebestendigheid van online proctoring altijd lager dan de maximale fraudebestendigheid van tentamenafname in een toetszaal.

Desondanks is online proctoring als hulpmiddel bij de afname van digitale tentamens in bepaalde situaties zeker bruikbaar. Wel is belangrijk een goede afweging te maken waarbij zowel het belang als het risico van een specifiek tentamen worden meegewogen en naast de voordelen worden gezet.

Om examen- of toetscommissies per situatie bij die afweging te ondersteunen, heeft SURF een keuzemodel toetsveiligheid ontwikkeld. De volgende paragraaf beschrijft dit keuzemodel.

5.4 Keuzemodel

Bij het bepalen van een geschikte methode voor de afname van digitale toetsen – van 'bring your own device' (BYOD) tot online proctoring of het gebruik van eigen computerzalen – wordt meestal gekeken naar het belang ('stakes') dat aan een specifieke toets wordt gehecht. Vaak kent men slechts twee niveaus: 'high stakes'- en 'low stakes'-tentamens. Daardoor wordt veel nuance gemist:

- 1) Alle summatieve toetsen (zowel tussen- als eindtoetsen) worden gezien als 'high stakes'-toets.
- 2) Er wordt geen onderscheid gemaakt in toetsvormen (meerkeuze, schriftelijk, mondeling of een essay), terwijl de toetsvorm grote invloed heeft op de geschiktheid van verschillende methodes voor toetsafname.⁴⁴

Om een meer genuanceerde afweging te kunnen maken, heeft SURF een model ontwikkeld waarbij zowel het risico op fraude als het belang van het toetsresultaat wordt meegewogen. Dit model is niet alleen geschikt voor online proctoring, maar is breed inzetbaar: het kan examen- en toetscommissies ondersteunen bij het vaststellen of de beoogde afnamesituatie voldoet, of om te zien welke methodes voor toetsafname binnen het curriculum geschikt zijn.

5.4.1 Belang van de toets

Het keuzemodel onderscheidt vier niveaus om het belang van een toets aan te geven:

- *Low*
Dit zijn formatieve toetsen en tentamens of online courses waaraan geen grote maatschappelijke waarde wordt gehecht. Denk aan MOOC's zoals de cursussen van Coursera of programma's van de Universiteit van Nederland.
- *Medium*
In dit geval gaat het om toetsen die niet direct (significant) bijdragen aan de cijferlijst, maar waar wel enige consequenties aan vastzitten. Voorbeelden zijn kleine wekelijkse tussentoetsen die samen één extra punt kunnen opleveren, of toetsen die studenten toegang geven tot een vak, een tentamen of een stage.
- *High*
Het gaat hier om tentamens die direct significante invloed hebben op het behalen van studiepunten. Dus in ieder geval alle tentamens voor vakken waarvoor studiepunten gegeven worden, maar bijvoorbeeld ook deexamens die samen tot het eindcijfer leiden.
- *Very high*
In deze categorie vallen specifieke vakken of toetsmomenten waarbij door de aard van het vak of bepaalde (juridische) consequenties nog hogere eisen gesteld worden⁴⁵ aan fraudepreventie. Bijvoorbeeld toetsen om te kunnen werken als advocaat of in de rechterlijke macht (civiel effect), of voor het halen van een BIG-registratie. Het kan ook gaan om

⁴⁴ Het risico op fraude is immers veel groter bij een meerkeuzetoets dan bij een mondeling tentamen.

⁴⁵ Dit kunnen eisen zijn die de examencommissie oplegt, maar kunnen ook voortkomen uit een algemeen maatschappelijke wens of wet- en regelgeving. De uiteindelijke inschatting ligt echter altijd bij de examencommissie.

tentamens waaraan om andere maatschappelijke redenen extra zwaar wordt getild, zoals de CITO-toets, eindexamens op de middelbare school of taal- en rekentoetsen op de PABO. Verder vallen hieronder afstudeerwerken, die immers doorslaggevend zijn voor het al dan niet verstrekken van een diploma.

5.4.2 Risico op fraude

Het keuzemodel onderscheidt drie niveaus om het risico op fraude bij een bepaald tentamen aan te geven:

- *Low*
Dit is een tentamen waarbij de student volledig uniek werk inlevert, zoals scripties, essays en mondelinge examens, maar ook praktijkopdrachten vallen hieronder. Bij fraudepreventie gaat het hierbij vooral om het detecteren van plagiaat en de mogelijkheid vast te stellen dat de student het werk zelf heeft gemaakt.
- *Medium*
Een tentamen waarbij de antwoorden uniek zijn, maar waarbij het geen volledig eigen werk betreft zoals bij een scriptie of essay. Denk hierbij aan een schriftelijke toets met open vragen waarbij de antwoorden van voldoende lengte zijn om per student uniek te zijn. Bijvoorbeeld een toets met uitgebreide wiskundige uitwerkingen op papier, of waar antwoorden uitgebreid tekstueel onderbouwd dienen te worden.
- *High*
Tentamens waarbij slechts één antwoord mogelijk is en studenten per vraag dus nauwelijks unieke antwoorden zullen geven. Dit gaat dus om alle gesloten vragen inclusief meerkeuzevragen.

5.4.3 Het keuzemodel

De basis voor het keuzemodel is de indeling naar risico en belang zoals hiervoor is beschreven. Het model hieronder is al gedeeltelijk ingevuld om een beeld te geven hoe het gebruikt kan worden. Iedere examen- of toetscommissie kan het voor de eigen context aanpassen. Daarbij moet ook de samenhang in het curriculum worden meegewogen. Als bijvoorbeeld bepaalde kennis meerdere keren in een opleiding wordt getoetst, dan kan een examencommissie oordelen dat aan een eerdere toets een lager belang wordt gehecht dan aan een latere. De kennis wordt immers nogmaals getoetst en een eventueel frauderende student zal dan alsnog door de mand vallen.

Per combinatie van belang en risico wordt in het model aangegeven welk beveiligingsniveau daarbij hoort. Dit kan bijvoorbeeld betekenen dat gekozen wordt tussen verschillende vormen van online proctoring, of dat er een afweging wordt gemaakt tussen BYOD en een vaste opstelling voor digitaal toetsen.

In het geval van online proctoring worden vier niveaus onderscheiden:

- *Niveau 0*: Online conferencing software met max 10 studenten;
- *Niveau 1*: Record & review, screen capture, één camera en logging websites;
- *Niveau 2*: Record & review, screen capture, één camera, lock-down mogelijkheden van de computer en logging van websites & applicaties;
- *Niveau 3*: Live proctoring met lock-down mogelijkheden van de computer en volledige logging van activiteit op de computer⁴⁷, of record & review inclusief een tweede camera en verder zelfde features.

Voor een deel van het onderwijs (met zowel hoge risico's als een hoog of zeer hoog belang) heeft de veiligheid van online proctoring ook bij de methode van live proctoring nog grote risico's. Om het frauderisico te beperken zou in deze gevallen een andere toetsmethode gekozen kunnen worden. Bijvoorbeeld een goed ingerichte eigen computerzaal, of mogelijk een veilige vorm van BYOD-tentamens binnen de eigen toetszaal⁴⁸.

⁴⁶ Het register waarin medewerkers in de gezondheidszorg geregistreerd staan. Alleen personen die zijn geregistreerd mogen dit beroep uitoefenen, zie ook: <https://nl.wikipedia.org/wiki/BIG-register>

⁴⁷ Inclusief logging van websites, applicaties en achtergrondprocessen op de computer

⁴⁸ Voor deze whitepaper is geen onderzoek gedaan naar de mogelijkheden en veiligheid van BYOD-oplossingen of van de bestaande computerzalen. Echter, daarbij heeft de onderwijsinstelling wel controle over de omgeving (het zwakke punt bij online proctoring) en is dit waarschijnlijk veiliger te krijgen dan online proctoring ooit zou kunnen.

Daarnaast kan altijd worden teruggevallen op het allerhoogste beveiligingsniveau: een toetszaal met papieren toetsen. Let daarbij op, ook een toetszaal is niet 100% fraudebestendig en niet iedere toetszaal is hetzelfde. Een slechte toetszaal met te weinig surveillanten is mogelijk minder fraudebestendig dan goede online proctoring. Voor de beste vergelijking zouden we ook verschillende niveaus van toetszalen moeten definiëren. Dat is echter niet de expertise van SURF en de uitwerking hiervan is aan de onderwijsinstellingen. Het keuzemodel stelt daarom niet dat iedere toetszaal veiliger is dan online proctoring, maar dat het *maximale* veiligheidsniveau van online proctoring inherent lager ligt dan het maximale veiligheidsniveau van een toetszaal.

Tijdens de coronacrisis kan blijken dat het onmogelijk is om de toetszalen te gebruiken. In dat geval zal de examencommissie een inschatting moeten maken welke toetsvorm wat hen betreft passend is. Dat kan bijvoorbeeld live proctoring zijn, de meest fraudebestendige vorm van online proctoring, maar ook het aanpassen van de toetsvorm is een mogelijkheid: bijvoorbeeld van multiplechoice-vragen naar open vragen. Hetzelfde geldt voor de keuze van het veiligheidsniveau van proctoring. Uitvoerbaarheid, technische mogelijkheden en andere praktische argumenten kunnen zorgen dat de gewenste vorm van online proctoring niet beschikbaar is. De onderwijsinstelling kan er dan voor kiezen een lichtere vorm van proctoring in te zetten, zodat het tentamen wel doorgang kan vinden. Dat kan bijvoorbeeld live proctoring zijn, de meest fraudebestendige vorm van online proctoring, maar ook het aanpassen van de toetsvorm (bijvoorbeeld van meerkeuzevragen naar open vragen).

Eenzelfde soort afweging geldt voor het niveau van proctoring. Uitvoerbaarheid, technische mogelijkheden en andere praktische argumenten kunnen zorgen dat de gewenste vorm van online proctoring niet beschikbaar is. De onderwijsinstelling kan er dan voor kiezen een lichtere vorm in te zetten, omdat het tentamen daarmee wel doorgang kan vinden. Onderwijsinstellingen zullen zich dan bewust moeten zijn dat zij meer risico nemen. Dit risico wordt groter naarmate online proctoring langduriger en op grote schaal wordt toegepast, aangezien de kans toeneemt dat software ontwikkeld en verspreid wordt om online proctoring te omzeilen.

Er zal echter ook gekeken moeten worden naar alternatieve vormen van tentamineren met een lage impact op privacy en met beperkter risico op fraude. Verder zal rekening moeten worden gehouden met de technische mogelijkheden van de student en van de leveranciers van de toetsapplicatie en proctoringsoftware.

Als het echter niet mogelijk is om bijvoorbeeld een tentamen met gesloten vragen te vervangen door een open boek tentamen, dan zal in elk geval gewerkt moeten worden met een zo hoog mogelijk niveau aan beveiliging.

BELANG

	Low	Medium	High	Very high
Low	Formatieve toets Oefentoets Geen controle nodig	Mondelinge tussentoets Niveau 0	Essay of betoog Praktijkopdracht Mondelinge toets Niveau 1*	Afstudeerwerk Scriptie Niet van toepassing
Medium	MOOC: open vragen Geen controle of niveau 1**	Tussentoets: open vragen Niveau 1	Tentamen: open vragen Niveau 3	Toets met civiel effect ⁴⁹ met open vragen Reguliere toetszaal***
High	MOOC: gesloten vragen Geen controle of niveau 1**	Tussentoets: gesloten vragen Niveau 2	Tentamen: gesloten vragen Reguliere toetszaal***	Toets met civiel effect met gesloten vragen Reguliere toetszaal***

* Online proctoring is uiteraard niet geschikt voor essays en ander werk met een lange doorlooptijd. Het is vooral geschikt voor bijvoorbeeld mondelinge examens met een beperkte tijdsduur (tot bijv. max 3 uur).

** In geval van een MOOC is het afhankelijk van de waarde die aan de MOOC wordt gehecht.

*** Tijdens de coronacrisis, als toetszalen niet beschikbaar zijn, is niveau 4 hier mogelijk een oplossing. Het is dan aan de examencommissie om het frauderisico af te wegen.

COLOFON

Auteur

Lex Sietses (SURF)

Bijgedragen aan samenstelling en inhoud

Cora Arts (Privacy Company)
Willem Brouwer (Hogeschool van Amsterdam)
Natasa Brouwer-Zupancic (Universiteit van Amsterdam)
Silvester Draaijer (Vrije Universiteit)
Gerard Folkerts (Wageningen University and Research)
Michiel van Geloven (SURF)
Eline van Hove (Interstedelijk Studenten Overleg)
Iris Huis in 't Veld (SURF)
Evelijn Jeunink (SURF)
Vincent Kalis (Tilburg University)
Meta Keijzer-de Ruijter (TU Delft)
Sharon Klinkenberg (Universiteit van Amsterdam)
Anne Martine Koetsier (Privacy Company)
Roos van Leeuwen (Landelijke Studentenvakbond)
Rolf Marteiijn (Wageningen Universiteit)
Alf Moens (SURF)
Annette Peet (SURF)
Wilfred Rubens (namens SURF)
Guusje Smit (Universiteit van Amsterdam)
Sebas Veeke (SURF)
Marja Verstelle (Universiteit Leiden)
Jenny de Werk (SURF)
Ulrike Wild (Wageningen University and Research)

Tekstredactie

Erik van der Spek

Ontwerp

De Hondsdagen, Bunnik

Foto's

IStock
Lars van Rooijen Fotografie
Yuri Samoilov www.flickr.com/photos/yusamoilov/13334048894
Steve Buissinne <https://pixabay.com/nl/users/stevepb-282134/>

SURF

info@surf.nl

www.surf.nl



2020

Deze uitgave is gepubliceerd onder Creative Commons-licentie 4.0 Internationaal.
Internationaal. <https://creativecommons.org/licenses/by/4.0/deed.nl>.
De afbeelding op de cover valt niet onder CC BY 4.0.

Disclaimer

De informatie in deze publicatie is met de grootst mogelijke zorg samengesteld, desondanks kunnen aan deze publicatie geen rechten worden ontleend.

April 2020

SURF

SURF

Kantoren Hoog Overborch (Hoog Catharijne)
Moreelsepark 48

Postbus 19035
3501 DA Utrecht

+31 (0)30 887 873 000

info@surf.nl
www.surf.nl

