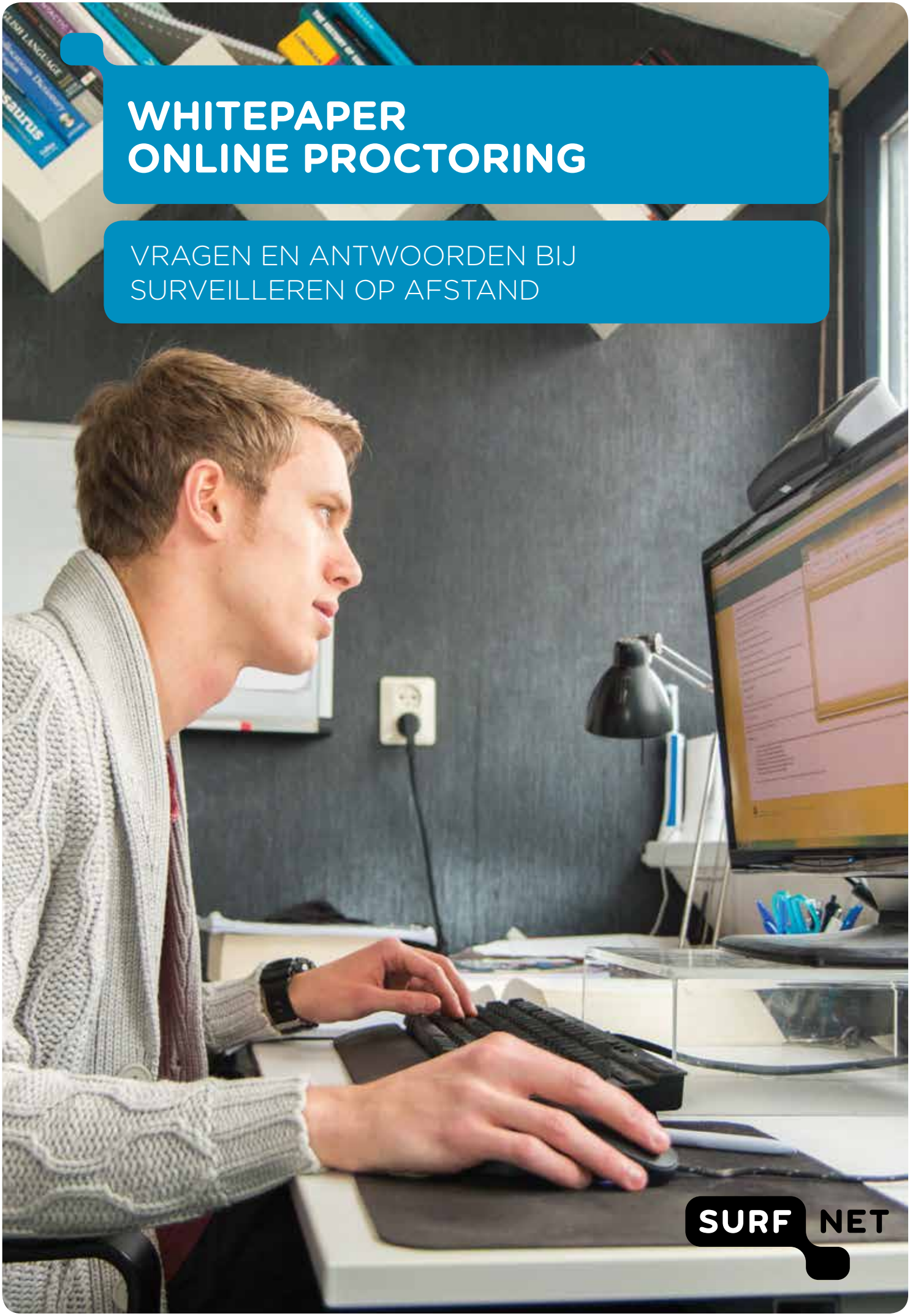
WHITEPAPER ONLINE PROCTORING

VRAGEN EN ANTWOORDEN BIJ SURVEILLEREN OP AFSTAND



SURF NET

VOORWOORD

In het Nederlandse (hoger) onderwijs is online proctoring in opkomst. Deze vorm van online surveilleren biedt de mogelijkheid om studenten veilig en betrouwbaar op afstand (plaatsonafhankelijk[1]) te kunnen toetsen. In veel situaties kan dit een ideale oplossing zijn.

Voorbeelden zijn MOOC's, studenten die in het buitenland stage lopen en toch in Nederland een tentamen willen doen, 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 onbeantwoorde 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 onderzoekstudies is het lastig een goed beeld te krijgen van online proctoring. Daarmee is het voor 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 SURFnet 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 het nu gebruikt wordt. Ook wordt ingegaan op de achtergronden van proctoring. Hoofdstuk 3 behandelt de belangrijkste vraagstukken bij gebruik van online proctoring (privacybescherming, veiligheid en fraudebestrijding, kosten). 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. In hoofdstuk 5 is ook een door SURFnet ontwikkeld Keuzemodel toetsveiligheid opgenomen op basis waarvan examencommissies kunnen beoordelen welk toetsmiddel geschikt is voor hun eigen situatie.

De verschillende leveranciers van online proctoring zijn in deze whitepaper met opzet niet met elkaar vergeleken. 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[2].

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, *lex.sietses@surfnet.nl*

1. De proctorsoftware wordt ook met enige regelmaat ingezet binnen de instelling zelf. In dat geval is het echter geen 'online' proctoring maar eerder van een Bring Your Own Device (BYOD) oplossing of een computerzaal van de instelling zelf. Deze whitepaper richt zich alleen op online proctoring waarbij het examen buiten de eigen instelling wordt afgenomen.
2. Zie bijvoorbeeld Eduventures: *http://www.eduventures.com/2015/08/the-developing-market-for-online-proctoring/#watched* of het Nederlandse *https://proctorexam.com/* (controleer wel of het de laatste versie is).

INHOUDSOPGAVE

SAMENVATTING

Online proctoring – surveilleren op afstand – is in opkomst. In de VS wordt het al regelmatig toegepast en steeds vaker experimenteren Nederlandse instellingen er mee. Online proctoring biedt kansen voor internationaal en flexibel onderwijs, maar er is – zeker in Nederland – nog 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 toepassen in hun opleiding. Zij worstelen onder meer met vragen rond privacy en fraudebestendigheid.

In deze whitepaper concludeert SURFnet dat online proctoring voor specifieke situaties veel toegevoegde waarde biedt. Tegelijk is de privacy-impact bij grootschalige invoering van online proctoring groot. Dit roept vragen op over de wenselijkheid en of een grootschalig toepassing past binnen de wettelijke kaders. Daarnaast brengt tentaminering buiten de eigen (gecontroleerde) omgeving van de instelling fraudevraagstukken met zich mee. Hieronder de belangrijkste conclusies op een rij.

Mogelijkheden van online proctoring

Online proctoring biedt uitkomst voor specifieke situaties. De Wageningen Universiteit 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 toch thuis tentamen doen.

In het algemeen maakt online proctoring plaats- en tijd onafhankelijk toetsen eenvoudiger. Studenten de mogelijkheid bieden op ieder moment een tentamen te doen wordt door instellingen nu als onrealistisch gezien. Online proctoring maakt dit gemakkelijker. Uiteraard vereisen dit soort oplossingen wel dat iedere student een uniek tentamen krijgt. Bijvoorbeeld op basis van een itemdatabank met veel tentamenvragen.

Privacy bij online proctoring

Een belangrijke afweging bij de verwerking van persoonsgegevens is of het middel in verhouding staat tot het doel (proportionaliteit). De privacy-impact van online proctoring is zeer groot. Camerabeelden vallen in een aparte categorie binnen de Wet bescherming persoonsgegevens: bijzondere persoonsgegevens. Op basis van camerabeelden worden bijvoorbeeld medische gegevens (bijvoorbeeld ‘draagt een bril’), ras en etniciteit bijgehouden. Deze proportionaliteitsafweging moet per geval worden gemaakt, maar online proctoring grootschalig inzetten voor alle tentamens aan alle studenten is vrijwel zeker niet proportioneel.

Daar komt bij dat toestemming van de student de meest voor de hand liggende grondslag is waarop de gegevens mogen worden verwerkt. Deze toestemming moet in vrijheid gegeven worden; de student moet dus kunnen weigeren zonder dat daar voor hem negatieve consequenties aan verbonden zijn. Als een student afhankelijk is van zijn onderwijsinstelling, dan is geen sprake meer van ‘in vrijheid’ gegeven toestemming. Instellingen moeten hier zeer zorgvuldig in zijn en mogen op geen enkele manier consequenties of gevolgen verbinden aan het weigeren van toestemming. Online proctoring kan dus ook niet verplicht worden en de instelling moet de student altijd een (kosteloos) alternatief aanbieden.

Daarnaast moeten instellingen ook zorgen voor een glasheldere toestemmingsvraag die aangeeft welke data worden verwerkt, waarvoor de data worden verwerkt, wie die de data kunnen

inzien, hoe lang die data worden bewaard en wat er verder met de data gebeurt. Dit moet helder geformuleerd zijn en staan op de plek waar de student toestemming geeft. Het mag niet verstopt staan, ook niet in een privacystatement. Tot slot moeten instellingen rekening houden met strenge eisen aan opslag en verwerking van de persoonsgegevens. Let op dat bij de opslag en verwerking van camerabeelden er nog strengere eisen van toepassing zijn.

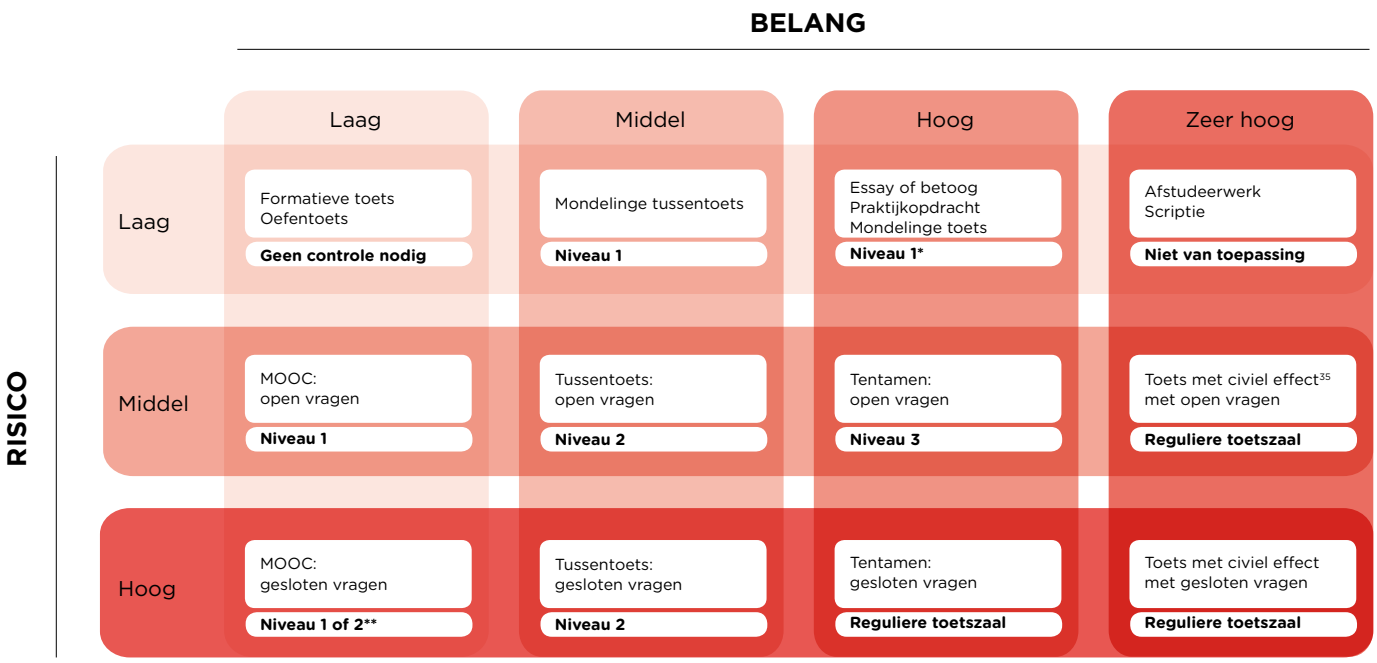
Fraudebestendigheid van online proctoring

Zolang de onderwijsinstelling geen controle heeft over de locatie waar het tentamen wordt afgenomen (en dat is de kern van online proctoring) dan is online proctoring onvoldoende fraudebestendig. Zeker bij meerkeuzevragen zijn er te veel mogelijkheden om te frauderen. SURFnet heeft daarom een keuzemodel ontwikkeld dat helpt te bepalen bij welke tentamenmomenten online proctoring passend is. De inschatting of online proctoring voor een specifiek tentamenmoment 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 tentamenmoment en de maatschappelijke waarde die aan een beoordeling hangt. Zo is een wekelijkse tussentoets minder belangrijk dan het afrondende tentamen van een vak. Fraude op een tussentoets heeft immers veel minder effect dan als het eindcijfer van een vak met fraude wordt behaald. Het risico hangt vooral van de toetsvorm af. Frauderen is simpelweg eenvoudiger bij meerkeuzententamens dan bij een tentamen met open vragen of bij een mondeling examen.

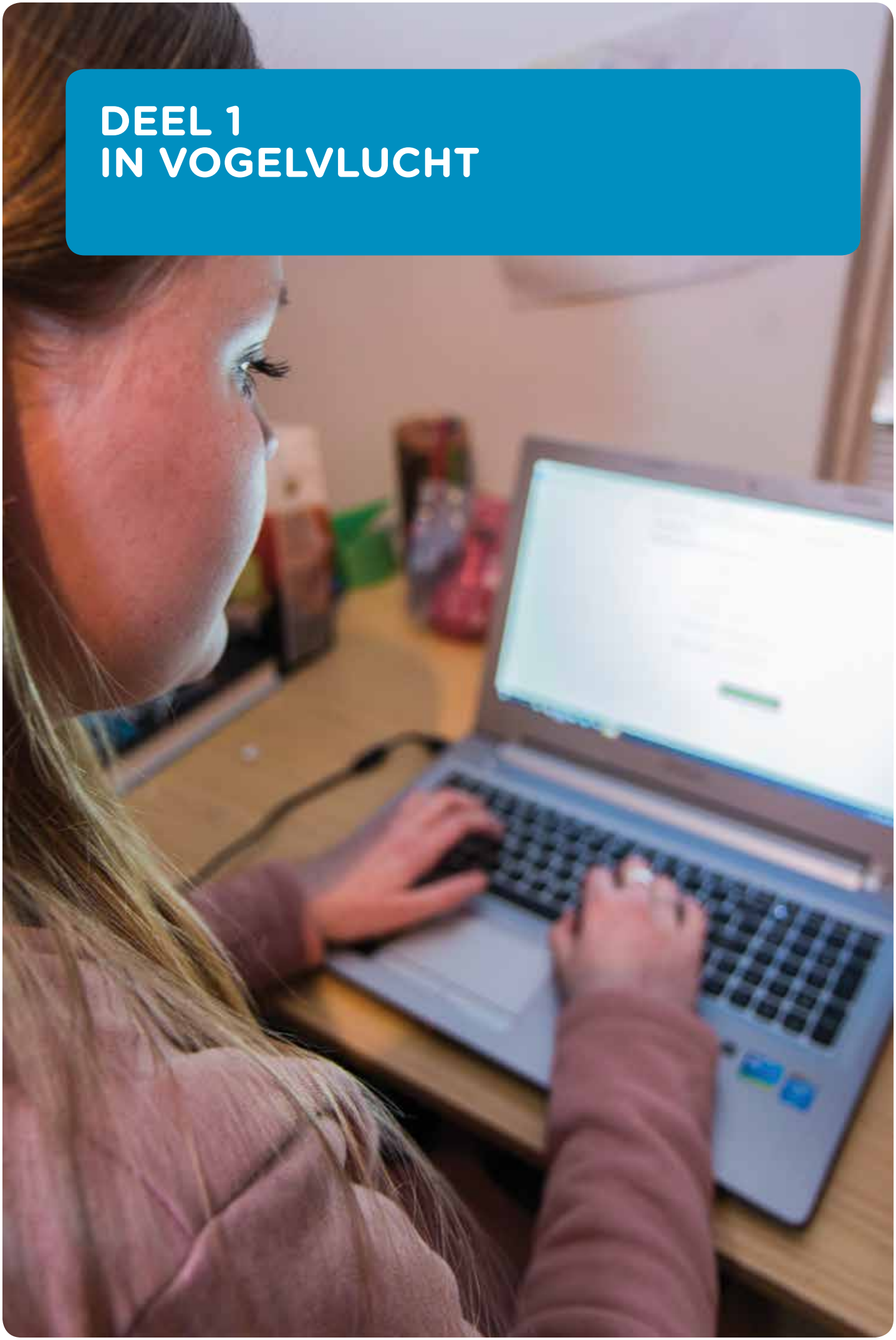
In het geval van online proctoring worden drie niveaus onderscheiden:
- *niveau 1:* screencapture en één camera;
- *niveau 2:* screencapture en twee camera's;
- *niveau 3:* volledige logging, screencapture, twee camera's en alleen live meekijken of een opname maken.

Deze insteek resulteert in onderstaand model.

Keuzemodel veilige toetsafname



* Online proctoring is uiteraard niet geschikt voor essays en ander werk met een lange doorlooptijd. Het is vooral geschikt voor bijvoorbeeld mondelinge examens.
** In geval van een MOOC is het afhankelijk van de waarde die aan de MOOC wordt gehecht.



DEEL 1
IN VOGELVLUCHT

1. WAT IS ONLINE PROCTORING?

Online proctoring is een vorm van digitale toetsafname waarmee een examen plaatsonafhankelijk kan worden afgenomen. De belofte van online proctorsoftware is dat studenten en cursisten hun examens overal (bijvoorbeeld thuis) veilig en betrouwbaar kunnen maken. Controlesoftware, videobeelden en meekijken op het scherm van de student moet voorkomen dat hij of zij fraudeert.

De exacte vorm van online proctoring verschilt per leverancier, maar er zijn drie hoofdcategorieën te onderscheiden: live proctoring waarbij iemand tijdens het examen meekijkt, het op een later tijdstip bekijken van ieder afgenomen examen, op basis van beelden en logs, en geautomatiseerde proctoring waarbij de software een deel van de detectie overneemt. Per categorie worden de belangrijkste voor- en nadelen benoemd.

1.1 Live proctoring

Live proctoring is de oudste en meest bekende vorm van online proctoring. Dit lijkt nog het meest op de analoge examenzaal: een proctor (surveillant) kijkt op afstand mee. Het aantal examens dat één surveillant kan volgen verschilt nogal per gekozen methode. Hoe meer schermen een proctor moet volgen, hoe minder examens er tegelijkertijd bekeken worden. De proctor kan tijdens het examen ingrijpen, net zoals een surveillant dat in een examenzaal kan doen. Hij kan bijvoorbeeld bij een openboekexamen 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.

De grootste nadelen van deze variant is de beperkte schaalbaarheid en het vereiste een examen vooraf te moeten plannen. De student kan niet zomaar inloggen en direct beginnen als hij er klaar voor denkt te zijn, maar moet enkele dagen van tevoren een moment prikken zodat er een proctor beschikbaar is. Het aantal beschikbare proctors bepaalt de capaciteit van het systeem.

1.2 Opslag en controle achteraf

Deze veel voorkomende vorm van online proctoring slaat de camerabeelden en logs op, waarna proctors die achteraf (versneld) terugkijken. Op basis van de beelden beoordelen zij of er tijdens het examenfraude is gepleegd of niet. Het grootste voordeel van deze variant is dat studenten het examen kunnen doen wanneer zij er klaar voor zijn. Ze kunnen direct inloggen en een examen starten, zonder iets vooraf te hoeven inplannen. Een ander voordeel is dat deze variant goed schaalbaar is en examens met grote aantallen studenten tegelijk aan kan. Grote aantallen studenten kunnen op hetzelfde moment hun examen doen, waarna de proctors die over een langere periode beoordelen. Dat kan niet met live proctoring.

Het nadeel is dat een proctor tijdens het tentamen niet kan ingrijpen en de student er dus niet op kan wijzen dat iets niet mag. Ook kan niet worden ingegrepen als de camera verkeerd staat opgesteld en de proctor niet het hele bureau kan zien. Tijdens live proctoring zou dit geen probleem zijn; bij terugkijken achteraf moet een examen in dat geval mogelijk ongeldig worden verklaard.

1.3 Geautomatiseerde proctoring

Bij geautomatiseerde proctoring – een variant die steeds meer opkomt – kijken proctors niet meer het hele examen (terug) maar signaleert de software momenten waarop mogelijk sprake is van fraude. Bijvoorbeeld wanneer andere software wordt opgestart, de student wegkijkt of omdat er iemand anders in de ruimte wordt gedetecteerd. De proctor krijgt hiervan een melding. Hij kan die specifieke momenten terugkijken en beoordelen of er inderdaad spraken is van fraude.

Geautomatiseerde proctoring maakt proctoring een stuk efficiënter en bespaart veel tijd, omdat niet alle beelden en logs teruggekeken hoeven te worden. Dit maakt het ook een zeer goed schaalbare oplossing. Een van de nadelen is dat als studenten weten hoe de software werkt, ze de fraudepreventiemaatregelen makkelijker kunnen omzeilen. Een menselijke proctor blijft voor de student daarentegen onvoorspelbaar omdat nooit zeker is waar die op dat moment op let. Een ander nadeel is dat de software al snel *false positives* geeft (ten onrechte iets aanziet voor potentiële fraude).

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

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 redenen om online proctoring toe te passen. Vervolgens worden in de volgende hoofdstukken enkele vraagstukken verder uitgediept.

2.1 Internationaal onderwijs

Steeds meer onderwijsinstellingen introduceren open en online courses die wereldwijd worden gevolgd. Dit varieert van een kleine online cursus tot een volledig masterprogramma. Studenten of cursisten voor ieder tentamen naar Nederland laten vliegen is uiteraard geen optie. Voor het afnemen van tentamens in het buitenland kunnen instellingen wel 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 4-jarige parttime online master leidt op voor hetzelfde diploma als de reguliere 2-jarige 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 dit mogelijk te maken. Dit past ook goed in reguliere toetsproces. 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, en hebben we plannen voor studenten die voor stage in het buitenland zitten of topsporters die op trainingsckamp moeten."
Rolf Marteijn, Wageningen Universiteit

2.2 Flexibilisering van tijd

Steeds meer instellingen hebben de ambitie om de student centraal te stellen bij het aanbieden van onderwijs, in plaats van een vaststaand curriculum als uitgangspunt te nemen. Dat is ook een wens van studenten.[3] 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 examens aanbieden is met papieren examens onuitvoerbaar, dan zouden er immers op ieder moment van de dag tentamenzalen met surveillanten beschikbaar moeten zijn. Online proctoring biedt hier wel mogelijkheden voor en zo kan de student examen doen wanneer hij daar klaar voor is.

3. *http://www.lsvb.nl/actueel/rapport/lsvb-introduceert-de-flexstudent*

2.3 Flexibilisering van plaats

Instellingen willen steeds vaker niet alleen tijd- maar ook plaatsonafhankelijk onderwijs kunnen aanbieden. Die wens geldt het sterkst voor internationaal onderwijs[4], 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 zijn te vinden.

2.4 Verschillende toetsvormen

Een vaak gehoord misverstand is dat online proctoring vooral of zelfs alleen geschikt zou zijn voor multiplechoicetentamens. Die aanname is onterecht, online proctoring kan iedere digitale tentamenvorm ondersteunen. Het gebruik van webcams biedt daarnaast andere 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 examinator de ingescande versie beoordeelt.

Studenten over online proctoring

"Voor Landelijke Studentenvakbond (LSVb) is online proctoring een interessante ontwikkeling. Deze vorm van toetsen biedt nieuwe kansen en maakt onderwijs mondiaal toegankelijk. In een wereld waar internationalisering een steeds grotere rol speelt en onderwijs ook op afstand plaatsvindt, zijn technologische ontwikkelingen onvermijdbaar. Het experimenteren met deze vorm van toetsing gaat echter ook gepaard met een aantal risico's. De fraudegevoeligheid van de toetsingsvorm blijft een groot risico, dat zelfs met alle bedachte maatregelen niet volledig kan worden uitgesloten.

Ook de beoordeling van het videomateriaal geschiedt door een andere partij, waardoor de rol van de examencommissie ingeperkt lijkt te worden. De vraag rijst hiermee of de controle gewaarborgd kan worden en welk toezicht hier op is. Als laatste staat voor de LSVb altijd voorop dat digitalisering additioneel dient te zijn aan het primaire klassikale onderwijs. Interactie tussen studenten onderling en tussen student en docent zijn essentieel in het hoger onderwijs."
Stefan Wirken, Landelijke Studentenvakbond

"Het ISO vindt tijd- en plaatsonafhankelijk leren en toetsen erg belangrijk. Proctoring is een goede methode is om een student thuis een tentamen te laten maken en maakt het makkelijker studenten zelf te laten beslissen wanneer ze het tentamen maken. Doordat een student niet een halfjaar op hun tentamen hoeft te wachten, voorkomt dit ook studievertraging. Het is wel van belang dat hierbij goede begeleiding is richting de student en dat studenten nog altijd samenkomen zodat er een studentencommunity blijft bestaan.

Ondanks de voordelen zitten er wel een aantal risico's aan het gebruikmaken van online proctoring, namelijk privacy en fraudegevoeligheid. Er komt nog meer privacygevoelige informatie van de student bij de instelling te liggen. Op het moment dat deze informatie verkeerd wordt gebruikt of op straat komt te liggen hebben zowel student als instelling een groot probleem. Een ander risico is dat het fraudegevoelig kan zijn. Frauderen in de eigen studentenkamer is immers gemakkelijker dan in een tentamenzaal. Het ISO vindt het dus een interessante ontwikkeling en ziet mogelijkheden om dit via pilots uit te proberen. Het is dan ook vooral een goede toevoeging zijn voor studenten die hier behoefte aan hebben en geen universele oplossing."
Simon Theeuwes, Interstedelijk Studenten Overleg

4. Hier worden studies bedoeld waarbij de studenten zich over de gehele wereld bevinden en (dus) op afstand onderwijs volgen, waarbij het examen laten doen binnen de eigen instelling onrealistisch is.

3. VRAAGSTUKKEN BIJ ONLINE PROCTORING

In dit hoofdstuk wordt ingegaan op de belangrijkste vraagstukken over online proctoring: privacybescherming, beveiliging en fraudebestrijding, en de kosten ervan.

3.1 Privacybescherming

Bij online proctoring worden persoonsgegevens verwerkt: gegevens die direct of indirect iets zeggen over studenten. De Wet bescherming persoonsgegevens (Wbp) stelt strenge eisen aan de verwerking van deze gegevens, bijvoorbeeld bij het vragen van toestemming, 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.

Hoofdstuk 4
Wat zegt de wet over privacy?

De belangrijkste punten uit de Wbp zijn:

- **Toestemming**
  Voor het verwerken van persoonsgegevens is een wettelijke grondslag (een basis die het recht op verwerking geeft) nodig. In het geval van online proctoring is dat bijna altijd toestemming. Deze toestemming moet de student 'in vrijheid' kunnen geven, wat inhoudt dat hij toestemming zonder consequenties moet kunnen weigeren. In het geval van regulier onderwijs[5] kan online proctoring dus niet worden verplicht; er moet altijd een kosteloos alternatief worden geboden.

- **Informatieplicht**
  Voordat een student om toestemming wordt gevraagd, moet die goed weten waarvoor hij precies toestemming geeft. Een vinkje laten plaatsen voor een algemene zinsnede zoals: "Ik geef toestemming voor online proctoring" is onvoldoende, ook als er een privacystatement is waarin meer uitleg staat. De tekst waarop akkoord gegeven wordt moet specifiek genoeg zijn. Een voorbeeld van zo'n tekst is zijn "Ik geef toestemming voor het maken van videoopnamen, het bijhouden van mijn toetsaanslagen en het maken van schermafbeeldingen van mijn pc. Deze beelden worden voor een periode van ## weken bewaard. De proctor van <bedrijf X> en mijn examinator krijgen deze data om te beoordelen of ik het tentamen volgens de regels heb afgelegd. Zie voor meer uitleg hierover ons privacyreglement."[6]

- **Doelbinding**
  Persoonsgegevens mogen alleen worden gebruikt voor het doel waarvoor ze zijn verkregen en waarvoor men een grondslag (meestal toestemming) heeft. Daardoor kan data uit het online proctorsysteem bijvoorbeeld niet worden gebruikt voor learning analytics.

- **Bijzondere persoonsgegevens**
  Met het begrip 'bijzondere persoonsgegevens' worden zaken zoals iemands gezondheid, etniciteit, seksuele en politieke voorkeur en godsdienst bedoeld. Deze gegevens mogen niet worden verzameld of gebruikt zonder uitdrukkelijke toestemming én alleen als dit niet anders kan.
  In het geval van online proctoring worden vrijwel altijd bijzondere persoonsgegevens verwerkt zoals herkenbare afkomst of etniciteit. Een ander bekend probleem is op beeld opnemen van identiteitsbewijzen, daarbij mag het BSN niet zichtbaar zijn. Hierdoor gelden zwaardere eisen aan het verkrijgen van toestemming en aan de opslag van deze gegevens.

5. Dit geldt het strengst voor bekostigd, publiek onderwijs. Voor bijvoorbeeld MOOC's en keuzevakken geldt dat de student ervoor kan kiezen dit vak of de cursus niet te volgen.
6. Let op dat hiernaast aparte toestemming wordt gevraagd voor de bijzondere persoonsgegevens die met de camerabeelden worden verkregen.

Privacy in de Delftse praktijk

"De Wbp vereist dat we onze studenten voorafgaand aan het inschrijven voor een vak om toestemming moeten vragen om online proctoring te kunnen gebruiken. Omdat we nog bezig zijn met de opbouw van ons online onderwijs, waarbij soms de exacte vorm van toetsing nog niet is bepaald, gaan we alle online studenten om vragen om in te stemmen met het gebruik van online proctoring. Ongeacht of het voor dat specifieke vak uiteindelijk zal worden toegepast.

Docenten die online proctoring willen gebruiken en de betrokken examencommissies moeten goed geïnformeerd zijn over de wettelijke vereisten: de docenten moeten namelijk een alternatieve toets- of surveillance vorm aanbieden. Dit alternatief moet op zijn beurt voldoen aan vereisten van de examencommissie. Er moet dus een goed plan B worden opgesteld."
Meta Keijzer-de Ruijter, TU Delft

3.2 Veiligheid en fraudebestrijding

Fraudebestrijding is een belangrijk thema waarvoor veel maatschappelijke aandacht bestaat. Examencommissies willen volledig achter ieder door hen afgegeven diploma kunnen staan. In een reguliere tentamenzaal is fraudebestrijding al een uitdaging; het wordt nog veel ingewikkelder met digitale toetsmiddelen zoals online proctoring wordt ingezet.

Hoofdstuk 5
Hoe betrouwbaar is online proctoring?

Het is algemeen bekend dat een reguliere tentamenzaal niet 100% veilig is. Onderwijsinstellingen en examencommissies hebben wel veel ervaring met het gebruik van die reguliere tentamenzaal en kunnen daardoor redelijk goed inschatten welke risico's daarbij komen kijken.

Bij online proctoring bestaat die ervaring nog niet. Veel instellingen die met online proctoring aan de slag willen, moeten steeds zelf een inschatting maken hoe veilig het door hen gewenste middel is. Een complicerende factor is dat iedere leverancier weer net andere methodes en technieken gebruikt en de ervaringen van de ene instelling niet altijd direct bruikbaar zijn voor een andere.

Studenten voerden een security audit uit

"Bij de UvA hebben we al ruim achthonderd tentamens afgenomen met het gebruik online proctorsoftware. Hier waren we zeer tevreden over. In navolging daarvan 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, of studenten (gemakkelijk) kunnen frauderen en of de privacy van de studenten gewaarborgd is. Wij hebben hiervoor een opdracht uitgezet bij vier informatica studenten, 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 hoofdstuk 5 wordt uitgebreid ingegaan op mogelijke manieren van fraude en hoe proctoringsoftware die probeert te voorkomen. Op basis daarvan kunnen de volgende conclusies worden getrokken:

- Fraude waarbij de hardware of software wordt gemanipuleerd is *meestal* te detecteren. Dit heeft echter al snel 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 totaal anders in een reguliere tentamenzaal, waar fraude (bijna[7]) altijd een individuele actie is.
- Wanneer de onderwijsinstelling geen controle heeft over de ruimte waar een tentamen wordt afgenomen, dan kan op veel (vrijwel) niet te detecteren manieren worden gefraudeerd.
- Met een beetje creativiteit is de lijst vrijwel onuitputtelijk.[8] In hoofdstuk 5 wordt een selectie van mogelijke fraudemogelijkheden 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 inherente grenzen. Juist het voordeel dat een examen niet meer plaatsgebonden is, maakt ook dat de onderwijsinstelling de omgeving waarin het examen wordt afgenomen niet kan controleren. Controlemechanismes zoals webcams maken dit risico wel kleiner, maar nemen het niet weg.

Maakt dat online proctoring een onbruikbaar middel om tentamens af te nemen? Nee, online proctoring is als hulpmiddel bij afname van digitale tentamens in bepaalde situaties zeker bruikbaar. 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 wordt uitgebreider ingegaan op de mogelijke manieren van fraude en de wijze waarop online proctoring hier bescherming tegen kan bieden. Daarnaast is er door SURFnet een keuzemodel toetsveiligheid ontwikkeld, waarmee examen- of toetscommissies kunnen inschatten welke methode voor de afname van digitale toetsen voor een specifieke situatie geschikt is. Dit model is in hoofdstuk 5.4 te vinden.

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'[9] uitgevoerd. Hoewel die zich primair richtte op de digitale toets en dus niet op online proctoring, is er wel een aantal interessante punten die hier het herhalen waard zijn. Daarnaast is het nuttig op te merken dat instellingen online proctoring niet alleen willen inzetten bij het maken van bestaande digitale toetsen, maar ook willen aangrijpen om bestaande papieren toetsen over te zetten naar digitale.

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

- De verdeling over de diverse kostenposten verschilt behoorlijk tussen de instellingen. 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.

7. 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.
8. Zie bijvoorbeeld: *http://madebyknight.com/knuckle-scanners-cheating-how-to-bypass-proctortrack/*
9. SURF, Quickscan 'Kosten en baten van digitaal toetsen', februari 2013, te vinden op *https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/Quickscan+Kosten+en+baten+van+digitaal+toetsen.pdf*

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 nu eigenaar is van grote toetszalen en deze niet kan of wil afstoten, dan blijven veel vaste kosten (vaak verrekend in de prijs per vierkante meter) bestaan, ook als een bepaalde opleiding die niet meer doorbelast krijgt.
- De prijzen voor online proctoring verschillen zowel per aanbieder als per methode. Hoe meer schermen (één per camera plus de screencapture) de proctor moet volgen, hoe minder studenten hij kan controleren. Het kan rendabel zijn om een tentamenzaal te gebruiken waarbij studenten op eigen hardware tentamen doen, en de proctor alleen een screencapture ontvangt. Het inzetten van eigen surveillanten voor de fysieke controle in de tentamenzaal is wellicht goedkoper (en veiliger) dan online proctoring in een oncontroleerbare thuissituatie.

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 Marteijn, Universiteit Wageningen

- Het komt voor dat onderwijsinstellingen extra kosten voor onderwijs en examens willen doorbelasten aan studenten[10]. Ook voor online proctoring wordt dit wel eens geopperd. Dit is niet toegestaan in het geval van regulier, Nederlands bekostigd onderwijs. Een onderwijsinstelling mag studenten namelijk niet weigeren en moet hen toegang bieden tot het onderwijs. Daarbij hoort de verplichting dit te realiseren voor het wettelijk of instellingscollegegeld. Een bijdrage vragen aan de student is alleen toegestaan bij vrijwillige keuzevakken en als er een gratis alternatief wordt geboden en bij niet-bekostigd onderwijs.

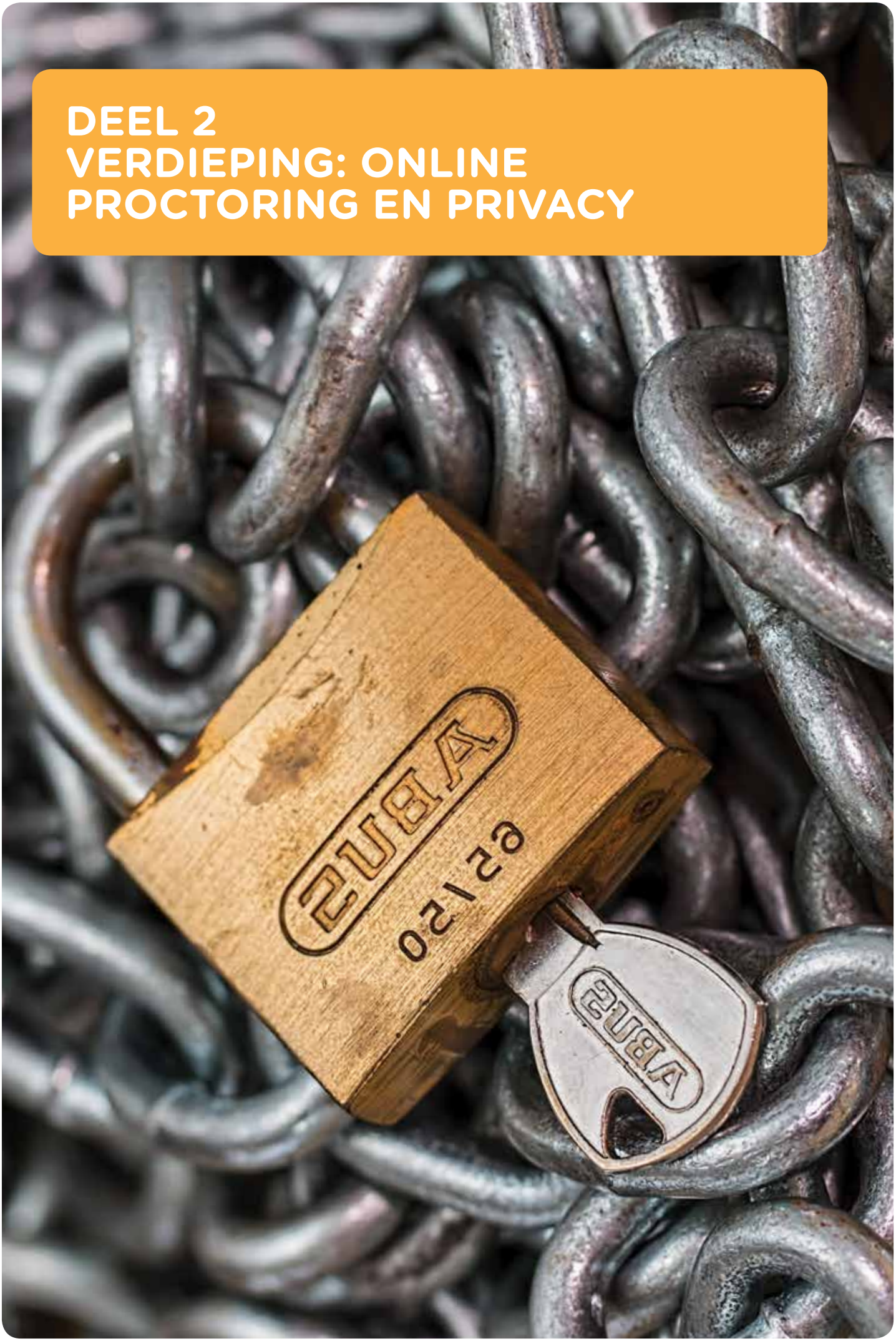
3.4 False positives

Het ten onrechte detecteren van potentiële fraude is een probleem bij iedere vorm van online proctoring. Dat komt bijvoorbeeld omdat sommige leveranciers iedere vorm van wegkijken al rapporteren. Zo schreef 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."[11]

Het probleem van *false positives* is het grootst bij geautomatiseerde proctoring 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. Alleen een '360 graden webcam zou hier een oplossing kunnen bieden maar daarvan is de resolutie vaak laag en het werkt voor de proctor verwarrend. Kortom, hier is zonder live proctor geen goede oplossing voor.

10. Zie bijvoorbeeld *http://www.iso.nl/website/wp-content/uploads/2014/03/Zwartboek-extra-kosten-naast-collegegeld.pdf*
11. 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/*

DEEL 2
VERDIEPING: ONLINE PROCTORING EN PRIVACY



4. WAT ZEGT DE WET OVER PRIVACY?

Wanneer een instantie persoonsgegevens verwerkt, is daarop de Wet bescherming persoonsgegevens (Wbp) van toepassing. Wat betekent de Wbp voor online proctoring? Op die vraag zijn geen pasklare antwoorden te geven omdat per situatie een inschatting gemaakt moet worden.

Duidelijk is wel dat voldoen aan de wet geen kwestie is van het laten ondertekenen van een standaard toestemmingsformulier en het aanbieden van een privacyverklaring op de website. De Wbp stelt hoge eisen aan de toestemmingsvraag en informatievoorziening, maar ook de beveiliging en opslag van persoonsgegevens. De toestemmingsvraag en informatievoorziening moeten op maat zijn opgesteld, gezien de specifieke tools die worden ingezet.

Dit hoofdstuk, deels gebaseerd op de 'Handreiking Learning analytics onder de Wet bescherming persoonsgegevens'[12] van SURFnet, biedt handvatten waarmee instellingen passende instrumenten kunnen ontwikkelen.

4.1 Wat zijn persoonsgegevens?

Persoonsgegevens zijn onder de Wbp 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. Als gegevens op een of andere manier tot een persoon te herleiden zijn, zijn het persoonsgegevens. Het gaat dus niet alleen om namen, adressen, camerabeelden of contactgegevens.

Slechts wanneer de koppeling feitelijk onmogelijk is, bijvoorbeeld omdat willekeurige nummers zijn toegekend en de lijst met naam-nummerkoppeling vernietigd is, zijn de gegevens (meestal) niet langer persoonsgegevens te noemen. Ook bij een 'anonieme' verzameling kan er toch sprake zijn van persoonsgegevens bijvoorbeeld door het maken van een combinatie met een andere (openbare) bron. Alleen als ook dat niet mogelijk is dan is geen spraken meer van persoonsgegevens.

Aggregeren

Indien een instelling de data uit proctorsoftware ook voor andere doelen wil gebruiken (bijvoorbeeld voor learning analytics of roostering), dan kan het zinvol zijn de persoonsgegevens te aggregeren tot uitspraken over meer dan één persoon. Daarmee verliezen de gegevens status van persoonsgegevens en vanaf dat moment gelden de beperkingen uit de Wbp niet meer. Hiervoor is het de eis dat gegevens op geen enkele manier te herleiden zijn tot individuele personen. Ook niet met behulp van andere bronnen en gegevens.

Let ook op dat gegevens alleen gebruikt mogen worden voor het doel waar ze voor verkregen zijn. Dat betekent dat een student expliciet toestemming moet hebben gegeven om zijn persoonsgegevens ook voor learning analytics of betere roostering te gebruiken.[13]

12. SURFnet, 'Handreiking Learning analytics onder de Wet bescherming persoonsgegevens', november 2015. Te vinden op *https://www.surf.nl/kennisbank/2015/learning-analytics-onder-de-wet-bescherming-persoonsgegevens.html.* Omdat de WBp voor zowel learning analytics als online proctoring grotendeels hetzelfde zegt zijn in dit hoofdstuk grote delen van de tekst uit de handreiking overgenomen. Om de vertaalslag naar online proctoring te maken en correcte voorbeelden te geven zijn aanpassingen zijn gedaan.
13. Op het moment dat de gegevens verkregen worden zijn het immers nog persoonsgegevens. Het voordeel ontstaat na aggregeren omdat verwerking, opslag en beveiliging daarna niet meer aan de eisen uit de Wbp is gebonden.

Bijzondere persoonsgegevens
Bijzondere persoonsgegevens zoals iemands gezondheid, politieke voorkeur of godsdienst mogen niet worden verzameld of gebruikt, tenzij de wet dat verplicht, of met uitdrukkelijke aparte toestemming. In dat laatste geval alleen mag het alleen in gevallen die de wet specifiek toestaat. Uitdrukkelijke toestemming wil zeggen dat er apart wordt gevraagd naar dit gegeven, voorzien van aparte uitleg waarom (en de mogelijkheid om nee te zeggen).

Camerabeelden bevatten bijvoorbeeld vrijwel altijd bijzondere persoonsgegevens, zoals etniciteit (bv. door de vorm van de ogen) en godsdienst (iemand draagt een kruisje of keppeltje). Zodra camerabeelden bedoeld zijn ter identificatie van personen dan zijn dit altijd bijzondere persoonsgegevens.[14] Wanneer een opname wordt gemaakt van een identiteitsbewijs is een leesbaar burgerservicenummer ook een bijzonder persoonsgegeven. Voor een BSN gelden nog zwaardere eisen, dit mag alleen worden opgeslagen als de wet daar expliciet toestemming voor geeft. In het geval van online proctoring is dat niet het geval en het opslaan van (camerabeelden van) het BSN is dus strikt verboden.

Met online proctoring worden bijzondere persoonsgegevens verwerkt en dit is vooraf te verwachten. Daardoor gelden niet alleen zwaardere eisen aan het verkrijgen van toestemming, maar ook aan de een zorgvuldige omgang (bijvoorbeeld opslag) van de gegevens.

4.2 Grondslagen voor verwerking van persoonsgegevens

Ieder gebruik van persoonsgegevens wordt in de Wbp 'verwerken' genoemd. Het verwerken van persoonsgegevens is alleen toegestaan wanneer dit op één van de in de wet genoemde grondslagen gebeurt. Er kunnen meerdere grondslagen tegelijk gelden, maar als er geen enkele grond is aan te wijzen, dan is de verwerking niet toegestaan, ongeacht hoe handig, nuttig, bewezen effectief of wenselijk de verwerking zou zijn. Verder geldt bij verwerking een aantal randvoorwaarden (grondslagen), te weten:

- toestemming
- uitvoering overeenkomst
- wettelijke plicht
- vrijwaring vitaal belang
- uitvoering overheidstaak
- noodzakelijk voor gerechtvaardigd belang van de instelling

De voor online proctoring meest relevante grondslagen zijn 'toestemming' en 'uitvoering overeenkomst'.

Toestemming
Hoofdregel in de Wbp is dat persoonsgegevens alleen mogen worden verwerkt met toestemming van de persoon over wie het gaat. Maar toestemming krijg je niet zomaar: je moet wel eerst precies uitleggen wát je gaat doen en waarom, en pas dan kun je aan iemand vragen of hij dat wel wil.

Toestemming moet in vrijheid worden gegeven. Dat wil zeggen dat iemand vrij kan kiezen om 'ja' of 'nee' te zeggen. Het 'nee' zeggen mag geen significante gevolgen hebben, zoals het niet mee kunnen doen aan een examen. Ook niet toegestaan is de toestemming pas na inschrijving van het vak te vragen, bijvoorbeeld bij de eerste keer dat iemand een tentamen doet. Een student kan dan realistisch gezien niet meer weigeren, omdat hij al is ingeschreven voor het vak.

Toestemming moet specifiek zijn. Niet specifiek is: "Ik geef toestemming voor online proctoring". De term 'online proctoring' is immers nog onvoldoende ingeburgerd om zonder nadere toelichting te gebruiken. Ook teksten als "Ik geef toestemming voor surveillance op afstand tijdens mijn tentamen" zijn niet specifiek genoeg. Wie monitort er, om wat voor gegevens gaat het en wat gebeurt daarmee? Een meer adequate toestemmingszin zou zijn "Ik geef toestemming voor het maken van video-opnamen, het bijhouden van mijn toetsaanslagen en het maken van schermafbeeldingen van mijn pc. Deze beelden worden voor een periode van ## weken bewaard. De proctor van <bedrijf X> en mijn examinator krijgen deze data om te beoordelen of ik het tentamen volgens de regels heb afgelegd. Zie voor meer uitleg hierover ons privacyreglement." Daarnaast moet apart toestemming worden gevraagd voor de bijzondere persoonsgegevens die verkregen worden op basis van de camerabeelden.

14. Zie voor meer informatie pagina 25 van de beleidsregels cameratoezicht van de Autoriteit Persoonsgegevens: *https://autoriteitpersoonsgegevens.nl/nl/nieuws/autoriteit-persoonsgegevens-publiceert-beleidsregels-cameratoezicht*

Toestemming mag op voorhand worden gegeven. Het is dus niet per se nodig om per tentamen toestemming te vragen. Brede toestemming zou al aan het begin van het jaar gevraagd kunnen worden. Daarbij moet de student dan wel uitgebreid geïnformeerd worden. Op welke vakken heeft de toestemming betrekking, hoe ver gaat per vak of tentamen de monitoring en wat zijn per vak of tentamen de gevolgen? Als de gekozen proctormethode voor alle vakken hetzelfde is, kan dit uiteraard relatief simpel worden uitgelegd. Het doorvoeren van een verandering in de monitoring tijdens het studiejaar kan echter niet. Omdat studenten daar geen toestemming voor hebben gegeven moet die opnieuw worden gevraagd.

Toestemming kan pas worden gegeven nadat adequate informatie is verstrekt: gedetailleerde uitleg wat men van plan is te doen. Wel is toegestaan om een korte uitleg (enkele zinnen) te geven met een aanklikbare verwijzing naar de privacyverklaring waarin meer informatie te lezen is.

Toestemming kan ook worden ingetrokken. Dit maakt eerder uitgevoerde verwerkingen niet ineens onrechtmatig, maar vanaf dat moment mogen die verwerkingen niet meer worden gedaan. Net als het kunnen weigeren van toestemming moet het intrekken van deze toestemming in vrijheid kunnen plaatsvinden. Het intrekken van toestemming mag dus geen significante gevolgen hebben, zoals het niet mee kunnen meedoen aan een examen. Het aanbieden van een andere vorm (bijvoorbeeld een schriftelijk tentamen) mag wel, maar het doorberekenen van kosten mag niet.
Intrekken van de toestemming kan op ieder moment en zonder opgaaf van redenen, tenzij het onredelijk is de toestemming in te trekken. Dat is echter niet snel het geval.

Uitvoering overeenkomst
De andere voor online proctoring relevante grondslag is ‘uitvoering overeenkomst’. Wanneer er een overeenkomst (contract) tussen twee partijen bestaat, mogen de contractpartijen elkaars persoonsgegevens verwerken zonder nog eens apart toestemming te vragen wanneer dat noodzakelijk is voor een goede uitvoering van die overeenkomst. Het verwerken van de gegevens moet wel noodzakelijk zijn. Dat is strenger dan ‘wenselijk’ of ‘handig’ of zelfs ‘het meest efficiënt voor iedereen’. Noodzakelijk impliceert dat er eigenlijk geen alternatief is; dat zonder het gebruik van deze persoonsgegevens de overeenkomst niet kan worden nagekomen. Hier wreekt zich het feit dat online proctoring heel nieuw is en daardoor al snel als ‘niet noodzakelijk’ zal worden gezien. De zienswijze kan zijn dat onderwijs ook prima zonder online proctoring kan worden gegeven. Samenvattend: op basis van de grondslag ‘uitvoering overeenkomst’ kan online proctoring op dit moment niet worden verantwoord.

4.3 Beveiliging van persoonsgegevens

Wie persoonsgegevens verwerkt[15], moet deze adequaat beveiligen. Dit betekent dat alle verkregen persoonsgegevens redelijkerwijs veilig moeten zijn tegen ongeautoriseerde kennisname of gebruik ervan. Daarbij moet uiteraard rekening worden gehouden met alle omstandigheden en de aard van de gegevens. Het gaat dan zowel om de gegevens die men eigenlijk wilde hebben, als om bijvangst of onbedoeld ontvangen persoonsgegevens.

Er is geen eis dat de beveiliging perfect moet zijn. Het kan voorkomen dat aan de wet wordt voldaan en desondanks persoonsgegevens worden misbruikt of ontvreemd. Uiteraard valt er dan wel wat uit te leggen en dient men dat meestal ook te melden als datalek (zie hieronder).

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 ‘Juridisch normenkader cloudservices hoger onderwijs’[16] en het ‘Normenkader informatiebeveiliging’[17] van SURF en de ISO-norm 27001[18] kunnen wel helpen bepalen of de beveiligd adequaat is.

15. 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.
16. Juridisch normenkader cloudservices hoger onderwijs: *https://www.surf.nl/kennis-en-innovatie/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html.*
17. SURFnet Normenkader informatiebeveiliging: *https://www.surf.nl/binaries/content/assets/surf/nl/2015/normenkader-informatiebeveiliging-ho-2015-v1.4.pdf.*
18. *https://nl.wikipedia.org/wiki/ISO/IEC_27001*

Aansprakelijkheid
Wanneer een instelling software of diensten van derden inzet, blijft de instelling zelf verantwoordelijk 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 uit te breiden voor gevallen waarin er schade door privacyschending ontstaat.

Datalekken
Sinds 1 januari 2016 bevat de Wbp aanvullende bepalingen omtrent datalekken. Daarbij wordt iedere inbreuk op de beveiliging van persoonsgegevens gezien als een datalek. Het gaat dus niet alleen om het grootschalig ontvreemden van persoonsgegevens door externe hackers; ook ongeautoriseerde toegang tot gegevens 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 worden gemeld. Hierdoor weten betrokkenen dat er een probleem is, en ook de toezichthouder kan dan optreden. Er zijn dan ook twee meldplichten vastgelegd in de Wbp:

1. *Melding aan de toezichthouder.*
   Een datalek moet worden gemeld wanneer deze "leidt tot de aanzienlijke kans op ernstige nadelige gevolgen" of wanneer deze daadwerkelijk die gevolgen heeft. Meldingen aan de toezichthouder zijn vertrouwelijk.
2. *Melding aan betrokkenen.*
   Betrokkenen (studenten, medewerkers, etc.) moeten worden geïnformeerd over een datalek dat hen aangaat wanneer dit lek "waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer".

4.4 Recht van inzage en verwijdering

In de Wbp zijn ook het recht van inzage en verwijdering vastgelegd.

Inzage
Doel van een inzageverzoek is de betrokkene op de hoogte te brengen van wat een instelling over hem weet. Dit betekent dus dat het volledige dossier en alle registraties van gegevens moeten worden verstrekt, dus niet alleen wat standaard via een online tool kan worden ingezien of wat zonder moeite kan worden aangeleverd. Het inzagerecht geldt dus bijvoorbeeld ook voor de camerabeelden en logbestanden. Ook aantekeningen en registraties in niet online beschikbare dossiers vallen in principe onder het inzagerecht.
Een verzoek om inzage in persoonsgegevens moet altijd worden gehonoreerd. Er zijn geen mogelijkheden om bijvoorbeeld inzage te weigeren op grond van 'bedrijfsgeheim' of auteursrecht van de leverancier van de tool. Ook het doel van de inzage doet er niet toe en een verzoek mag dus niet worden geweigerd omdat onduidelijk is wat de vrager met de gegevens van plan is.

Voor online proctoring kan het lastig zijn aan deze verplichting te voldoen als hier geen functionaliteit voor is ingebouwd. Er mag ten hoogste een vergoeding van 5 euro per inzageverzoek worden gevraagd.[19] Excessief veel verzoeken in korte tijd mogen worden geweigerd.

Het valt te verwachten dat studenten de gegevens van hun examen 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.

Verwijdering
Gegevens mogen niet langer worden bewaard dan nodig is voor de doelen waarvoor zij zijn verzameld. Voor online proctoring betekent dit concreet dat gegevens verwijderd moeten worden als het tentamen definitief is beoordeeld en er geen bezwaar of beroep meer mogelijk is. Daarnaast kan iemand verzoeken zijn of haar persoonsgegevens te verwijderen. Dit moet verzoek moet worden ingewilligd tenzij er zwaarwegende belangen zijn dat niet te doen. Wanneer van persoonsgegevens geaggregeerde combinaties zijn gemaakt, hoeven deze combinaties na een verwijderingsverzoek niet te worden gewist, omdat deze combinaties geen persoonsgegevens bevatten. Als de gegevens zich bevinden in bronbestanden voor wetenschappelijk onderzoek mogen deze worden behouden, maar alléén voor verificatie van dat onderzoek (dus niet voor ander onderzoek, ook niet als vervolg op het betreffende onderzoek).

19. Volgens het 'Besluit kostenvergoeding rechten betrokkene Wbp', te vinden op *http://wetten.overheid.nl/BWBR0012565/geldigheidsdatum_24-12-2015.*

Wanneer verwijdering technisch niet mogelijk is, bijvoorbeeld op back-ups die extern worden opgeslagen, heeft de betrokkene in ieder geval het recht ze te laten afschermen zodat ze nergens anders meer voor kunnen worden gebruikt. De relevante delen van deze back-ups moet de instelling vanaf dan dus niet meer ongebreideld kunnen inzetten. Anders zouden bij het terugzetten van deze back-up de verwijderde gegevens weer terug zijn.

4.5 Geautomatiseerde besluitvorming

De Wbp verbiedt volledig geautomatiseerde besluitvorming of het opleggen van sancties gebaseerd op een persoonlijkheidsprofiel. Onder zo'n profiel wordt verstaan een verzameling persoonsgegevens die "een beeld [geven] van bepaalde aspecten van zijn persoonlijkheid". Het gaat dan bijvoorbeeld om iemands kredietwaardigheid, betrouwbaarheid of gedrag.

Besluitvorming bij online proctoring

Volledig geautomatiseerde besluitvorming wordt door sommigen gezien als de toekomst van online proctoring, maar door de Wbp wordt dit verboden. Het is dus niet toegestaan om de software te laten besluiten dat een tentamen ongeldig is. Dat besluit zal altijd genomen moeten worden door een mens (een docent) en die moet daarvoor een eigen beoordeling uitvoeren. Een tentamen ongeldig verklaren "omdat het systeem te veel afwijkingen heeft geconstateerd" mag dus niet.

Profielinformatie

Voor het verbod op automatische besluitvorming moet het gaan om profielinformatie. Het is dus wél gewoon toegestaan om een student volautomatisch een onvoldoende te geven op basis van het aantal gemaakte fouten. Maar iemand op basis van een geschiedenis met zware onvoldoendes uitsluiten als fraudeur omdat hij nu ineens een 9,5 haalt, mag niet. Hetzelfde geldt als software constateert dat de toetsaanslagen van een student aantonen dat hij niet zelf tikt maar iemand anders. Dit mag op zichzelf niet de reden zijn te concluderen dat er fraude is gepleegd

Bezwaar

Wanneer een besluit of maatregel een persoon "in aanmerkelijke mate treft" en gebaseerd is op zo'n persoonlijkheidsprofiel, dan dient altijd de mogelijkheid van bezwaar open te staan. Het is in de praktijk verdedigbaar dat deze optie wordt geboden nadat de maatregel is opgelegd, zolang er nog tijd is om het negatieve gevolg te corrigeren. Dat kan bijvoorbeeld via de toevoeging "Ben je het hier niet mee eens? Neem dan binnen 4 weken contact op met de examencommissie" bij de mededeling dat men een extra vak moet doen.

4.6 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. Richting de student is de instelling altijd zelf aansprakelijk voor de kwaliteit 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 ontvangt, 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 bewerker genoemd in de zin van de Wbp.

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

4.7 Verwerkingen in andere landen

De Wbp is gebaseerd op Europese regels. Deze zijn de strengste ter wereld; Europa loopt ver voorop met de bescherming van persoonsgegevens. In de Europese regels is opgenomen dat persoonsgegevens alleen mogen worden opgeslagen of verwerkt in landen waar een 'adequaat' niveau van bescherming bestaat. Dat wil zeggen dat het land net zulke strenge regels heeft als Europa zelf. Dit met onder meer als doel andere landen te dwingen ook regelgeving over persoonsgegevens aan te nemen.

Een nadere uitwerking hiervan is te vinden in het 'Juridisch Normenkader cloudservices hoger onderwijs'.[20] Dit document stelt normen voor het hoger onderwijs in Nederland op het gebied van vertrouwelijkheid, privacy, eigendom en beschikbaarheid ten aanzien van cloudleveranciers.

Buiten Europa

Er is geen verplichting om persoonsgegevens in Nederland op te slaan. Ieder land binnen de Europese Economische Ruimte (EER) is in principe adequaat. Bij landen buiten EER ligt dit moeilijker, omdat er vrij weinig landen zijn die voldoen aan de Europese eisen. De Verenigde Staten voldoen hieraan in ieder geval niet, blijkt uit een recente uitspraak van het Europese Hof. Het gebruik maken van Amerikaanse leveranciers is hiermee op het moment van schrijven lastig. De meest up-to-date informatie is te vinden op de website van SURF.

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. Hoewel die partij dan onder Europees recht valt, lijkt het erop dat de Amerikaanse overheid zich ook bevoegd acht om bij dat Europese datacenter persoonsgegevens op te vragen onder de Patriot Act of andere Amerikaanse wetgeving. Op het moment van schrijven (eind 2015) loopt hierover een rechtszaak tegen Microsoft. Wanneer in hoger beroep definitief wordt beslist dat de Amerikaanse justitie gegevens mag vorderen uit Europese datacenters van dochterbedrijven van een Amerikaans bedrijf, wordt het onmogelijk dergelijke datacenters te gebruiken voor het opslaan van persoonsgegevens.

4.8 Handhaving van de wet

Handhaving van de Wbp is in Nederland altijd een beetje een ondergeschoven kindje gebleven. De reden hiervoor lag met name in de zeer beperkte boetebevoegdheid van het College Bescherming Persoonsgegevens. Een wetswijziging per 1 januari 2016 heeft hier verandering in gebracht: op overtreding van vrijwel elke plicht uit de Wbp komt nu een boete te staan. Dit geldt ook voor het niet hebben van een adequate beveiliging en voor het niet melden wanneer men daartoe verplicht was. Deze boete kan in theorie oplopen tot 810.000 euro, de hoogste categorie uit het bestuursrecht. De toezichthouder zal wel eerst beleid moeten publiceren over welke soort boetes worden gesteld op welke soorten overtredingen.

In principe kunnen overtredingen pas worden beboet nadat een bindende aanwijzing is opgelegd die niet wordt opgevolgd. Een bindende aanwijzing is een last (art. 5:2 Awb) die is opgelegd na een overtreding, bijvoorbeeld hoe de beveiliging moet worden aangescherpt. Wanneer de overtreding opzettelijk is begaan of het gevolg is van "ernstig verwijtbare nalatigheid", mag de toezichthouder echter direct een boete opleggen. Het is nog niet duidelijk wanneer hiervan sprake is. Zolang een organisatie geen beleid heeft voor het signaleren en melden van datalekken zal er al snel sprake zijn van ernstig verwijtbare nalatigheid.

4.9 Concrete aanbevelingen

Op basis van de privacyaspecten die in dit hoofdstuk zijn beschreven, is voor onderwijsinstellingen een aantal adviezen 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 nadat het tentamenresultaat definitief is geworden. Zorg er voor dat zowel de instelling als de leverancier deze bewaartermijnen strak handhaven.

20. *https://www.surf.nl/kennis-en-innovatie/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html*

3. Vraag om toestemming:
   a. op een moment dat de student deze nog zonder gevolgen kan weigeren;
   b. nadat duidelijke toelichting is verstrekt;
   c. en bied een optie om gewoon door te gaan als toestemming wordt geweigerd (weiger een student dus niet voor het examen, maar zorg voor een alternatief).
4. Formuleer toestemmingsvragen expliciet als ja/nee-vragen, waarbij uit de zin zelf duidelijk is waarvoor toestemming wordt gevraagd.
5. Spreek af met de leverancier dat deze gedetailleerde uitleg verstrekt, ook bij updates van de tool, zodat deze in de privacyverklaring kan worden opgenomen.
6. 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 examinator en examencommissie).
7. Stel een mogelijkheid beschikbaar om online proctoring gegevens te downloaden (inzage-verzoek) en desgewenst te corrigeren (bij evidente fouten).
8. 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 en biedt altijd een duidelijke bezwaarmogelijkheid aan.
9. Sluit bewerkersovereenkomsten met de leveranciers van online proctoring tools. Bepaal daarin:
   a. dat zij aansprakelijk zijn voor datalekken;
   b. dat zij de gegevens niet voor eigen doeleinden mogen gebruiken;
   c. dat zij gedetailleerde informatie aanleveren aan studenten over hoe de tools werken.
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 vermeden.

DEEL 3
VERDIEPING:
FRAUDEBESTRIJDING

5. HOE BETROUWBAAR IS ONLINE PROCTORING?

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 een bepaalde plek in het curriculum.

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, kunnen zij de risico's goed inschatten en tot een voor hen acceptabel niveau beperken.

5.1 Fraude voorkomen

Online proctoring biedt diverse middelen om de veiligheid te vergroten en fraude te voorkomen.

Camera('s) en microfoon

Bij vrijwel alle proctorsoftware kan een proctor 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 ook zicht op het beeldscherm en toetsenbord van de student.

Screencapture

Een andere methode die vrijwel alle leveranciers gebruiken, is dat de proctor via screencapture rechtstreeks mee kan kijken op het scherm van de student. De proctor kan daardoor zien welke programma's open staan en of de student niet verboden bronnen opent.

Lock-down browser

De 'lock-down browser' is een functie die niet alleen bij online proctoring wordt gebruikt maar ook bij 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 niet op de achtergrond kunnen draaien en met voldoende ICT-kennis zijn de meeste lock-down browser (op een eigen device) wel te omzeilen. Dat maakt ze zeker niet zinloos, maar bij online proctoring moeten ze vooral worden gezien als aanvulling op screencapture en camerabeelden.

Logging van de pc zelf

Sommige proctorleveranciers maken het mogelijk om tot in 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 processen[21] worden gescand en kan het geheugen worden uitgelezen. Daartoe moet de software volledige toegang krijgen tot de pc. Daarmee is dit een zeer zwaar middel om in te zetten met vergaande gevolgen voor de privacy.

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

Keystroke dynamics
Niet alleen wat een gebruiker tikt (een wachtwoord) kan iemand identificeren, maar ook de manier waarop iemand dat doet.[22] Met 'keystroke dynamics' kan iemand 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 examen maakt waarschijnlijk niet de student is die het examen zou moeten doen. Dat kan aanleiding zijn de camerabeelden nog een keer goed te bekijken. Belangrijk is te beseffen dat keystroke dynamics gevoelige persoonsgegevens zijn, vergelijkbaar met bijvoorbeeld een vingerafdruk.[23]

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 goed beeld van de mogelijkheden. Per fraudemethode wordt aangegeven of en zo ja op welke manier online proctoring de fraude bestrijdt.

De hardware en software
Bij online proctoring maakt de student gebruik van de eigen pc of laptop.[24] Dit betekent dat er verschillende manieren zijn om tijdens een tentamen te frauderen.

- *Een extra browser of tabblad*
  Misschien wel de bekendste methode om te frauderen is als de student tijdens het tentamen antwoorden probeert op te zoeken door gebruik te maken van internet.
  ⦸ *Tegenmaatregel:* deze manier is gemakkelijk tegen te gaan. Screencaptures en een extra webcam zorgen ervoor dat de student 'betrapt' wordt. Ook een goede 'lock-down 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 examen 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 klein.[25]
  ⦸ *Tegenmaatregel 2:* 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.
  ⦸ *Tegenmaatregel 3:* in gevallen waar het tentamen langere antwoorden verlangt, is gebruik van keystroke dynamics een goede oplossing om te herkennen wie de tekst schrijft.

- *Software die antwoorden geeft*
  De student kan software installeren die de vragen op het scherm scant en de antwoorden daarvan opzoekt. Die zou hij op het scherm kunnen laten zien, en eventueel zelfs direct kunnen invullen.
  ⦸ *Tegenmaatregel 1:* als het antwoord zichtbaar op het scherm wordt getoond dan valt dit gemakkelijk te detecteren met screencaptures.
  ⦸ *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 examen hierbinnen wordt afgenomen dan zal de proctorsoftware alleen dat scherm zien en is onzichtbaar welke software er op de hoofd-pc draait. Dat maakt veel van de eerder genoemde opgeloste fraudeopties opeens weer mogelijk. Een bijkomend probleem is dat er goede redenen kunnen zijn dat de student een virtuele pc gebruikt. Als de tentamen- of proctorsoftware bijvoorbeeld alleen op iOS (Apple) en Windows draait en de student regulier Linux gebruikt dan kan hij niet anders.
  ⦸ *Tegenmaatregel 1:* ervan uitgaande dat 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.

22. 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.*
23. 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.*
24. Indien proctorsoftware wordt ingezet binnen de eigen tentamenzaal, op PC's van de instelling dan geldt dit hoofdstuk uiteraard niet.
25. 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 dan zal dit nauwelijks opvallen.

⦸ *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.

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.

⦸ *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.[26] Kortom, maatregelen kunnen deze fraudemethode lastig maken maar hij is niet helemaal te voorkomen.

• *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. Let op: als een ID-bewijs gevraagd wordt mag het BSN niet zichtbaar zijn.

• *Verstopte spiekbriefjes*

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

⦸ *Tegenmaatregel:* spiekbriefjes 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.[27]

• *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. Ook het splitsen/aftappen van de beeldschermkabel is mogelijk.[28]

⊗ *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). Uitdaging voor de student is ervoor te zorgen dat de ander antwoorden kan doorsturen. Hiervoor geldt hetzelfde als voor de spiekbriefjes: dit is altijd wel te verbergen, omdat nooit de hele ruimte zichtbaar is. Hoe langer en uitgebreider de antwoorden, hoe lastiger deze vorm van fraude wordt. Vooral bij multiplechoice-examens is dit heel eenvoudig omdat maar een geringe hoeveelheid informatie hoeft te worden gecommuniceerd (het nummer van het antwoord).[29]

5.3 Wat betekent dit dan?

Met een beetje creativiteit is de lijst met fraudemogelijkheden bij online proctoring vrijwel onuitputtelijk.[30] Op basis van de voorbeelden in dit hoofdstuk valt een aantal conclusies te trekken:

- Fraude waarbij de hardware of software wordt gemanipuleerd, is meestal te detecteren. Wel betekent dit al snel vérgaande impact op de privacy van studenten.
- Zolang de onderwijsinstelling geen controle heeft over de ruimte waar het tentamen wordt afgenomen, zijn er teveel (vrijwel) niet te detecteren manieren waarop gefraudeerd kan worden. Daarom kan online proctoring nooit zo veilig zijn als tentamenafname in een toetszaal.

26. 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.
27. 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.
28. 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.
29. 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.
30. Zie bijvoorbeeld: *http://madebyknight.com/knuckle-scanners-cheating-how-to-bypass-proctortrack/.*

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 SURFnet een keuzemodel toetsveiligheid ontwikkeld. De volgende paragraaf beschrijft dit keuzemodel.

5.4 Keuzemodel veilige toetsafname

Bij het bepalen van een geschikte methode voor digitale toetsafname wordt op dit moment vooral gekeken naar het belang ('stakes') dat aan een specifieke toets wordt gehecht. Vaak onderscheidt men daarbij 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.[31]

Om een meer genuanceerde afweging te kunnen maken, heeft SURFnet 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:

- *Laag*
  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 Kahn Academy of open courseware.
- *Middel*
  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 toegang verschaffen tot een vak, het doen van tentamen of het op stage mogen gaan.
- *Hoog*
  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 deelexamens die samen tot het eindcijfer leiden.
- *Zeer hoog*
  In deze categorie vallen specifieke vakken of toetsmomenten waarbij door de aard van het vak of bepaalde (juridische) consequenties nog hogere eisen gesteld worden[32] 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.[33] Het kan ook gaan om 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:

- *Laag*
  Dit is een tentamen waarbij de student volledig uniek werk inlevert, zoals scripties, essays en mondelinge examens, maar ook aan praktijkopdrachten. Bij fraudepreventie gaat het hier vooral om het detecteren van plagiaat en de mogelijkheid vast te stellen dat de student het werk zelf heeft gemaakt.

31. Het risico op fraude is immers veel groter bij een meerkeuzetoets dan bij een mondeling tentamen.
32. 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.
33. 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*

• *Middel*
Een tentamen waarbij de antwoorden uniek zijn, maar 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.
• *Hoog*
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.

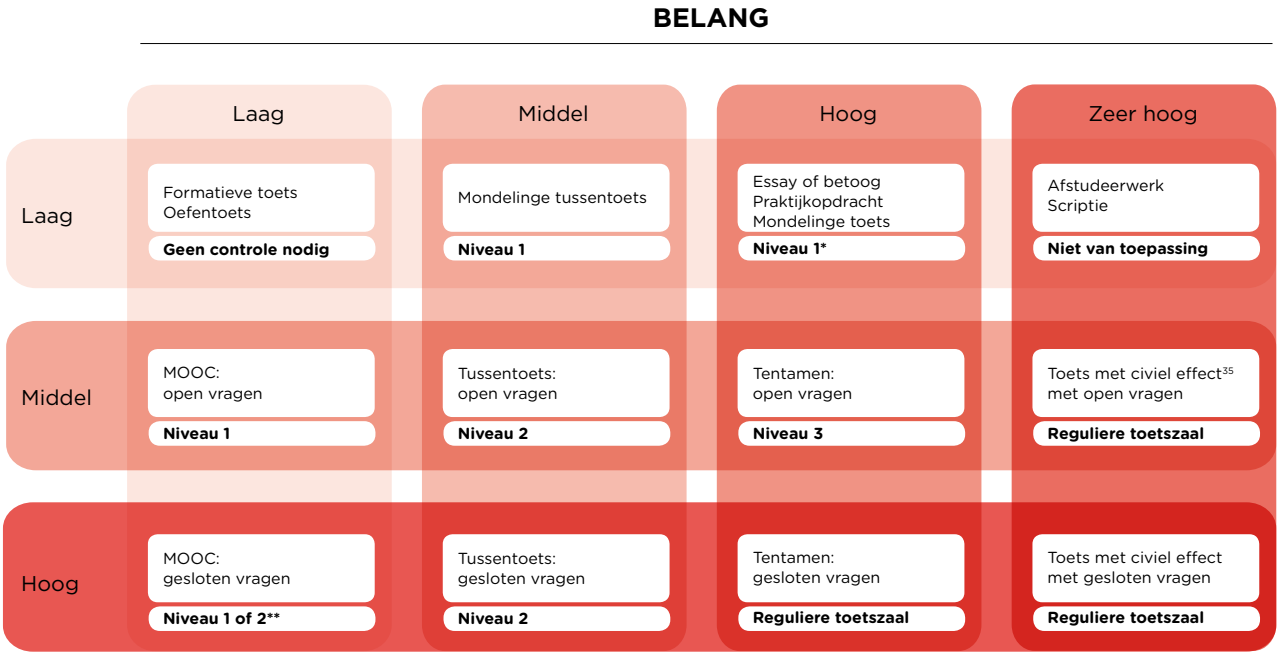
5.4.3 Het keuzemodel

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 drie niveaus onderscheiden:
• *niveau 1:* screencapture en één camera;
• *niveau 2:* screencapture en twee camera's;
• *niveau 3:* volledige logging, screencapture, twee camera's en alleen live meekijken of een opname maken.

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 op dit moment nog ontoereikend is. Om het frauderisico te beperken zou een andere toetsmethode bekeken kunnen worden. Bijvoorbeeld een goed ingerichte eigen computerzaal, of mogelijk een veilige vorm van BYOD-tentamens binnen de eigen toetszaal. Daarnaast kan altijd worden teruggevallen op de reguliere toetszaal[34] met papieren toetsen.



* Online proctoring is uiteraard niet geschikt voor essays en ander werk met een lange doorlooptijd. Het is vooral geschikt voor bijvoorbeeld mondelinge examens.
** In geval van een MOOC is het afhankelijk van de waarde die aan de MOOC wordt gehecht.

34. 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.
35. Bijvoorbeeld om te kunnen werken als advocaat of in de rechterlijke macht.

COLOFON

Auteur
Lex Sietses (SURFnet)

Bijgedragen aan samenstelling en inhoud
Willem Brouwer (Hogeschool van Amsterdam)
Natasa Brouwer-Zupancic (Universiteit van Amsterdam)
Michiel van Geloven (SURFnet)
Evelijn Jeunink (SURFnet)
Meta Keijzer-de Ruijter (TU Delft)
Rolf Marteijn (Wageningen Universiteit)
Alf Moens (SURFnet)
Annette Peet (SURFnet)
Guusje Smit (Universiteit van Amsterdam)
Simon Theeuwes (Interstedelijk Studenten Overleg)
Sebas Veeke (SURFnet)
Josephine Verstappen (Landelijke Studentenvakbond)
Marja Verstelle (Universiteit Leiden)
Jenny de Werk (SURFnet)
Stefan Wirken (Landelijke Studentenvakbond)

Tekstredactie
Daphne Riksen - Ediction

Ontwerp
De Hondsdagen, Bunnik

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

SURFnet
admin@surfnet.nl
www.surf.nl/surfnet

Maart 2016

SURFnet
Kantoren Hoog Overborch (Hoog Catharijne)
Moreelsepark 48

Postbus 19035
3501 DA Utrecht

+31 (0)30 887 873 000

admin@surfnet.nl
www.surf.nl/surfnet