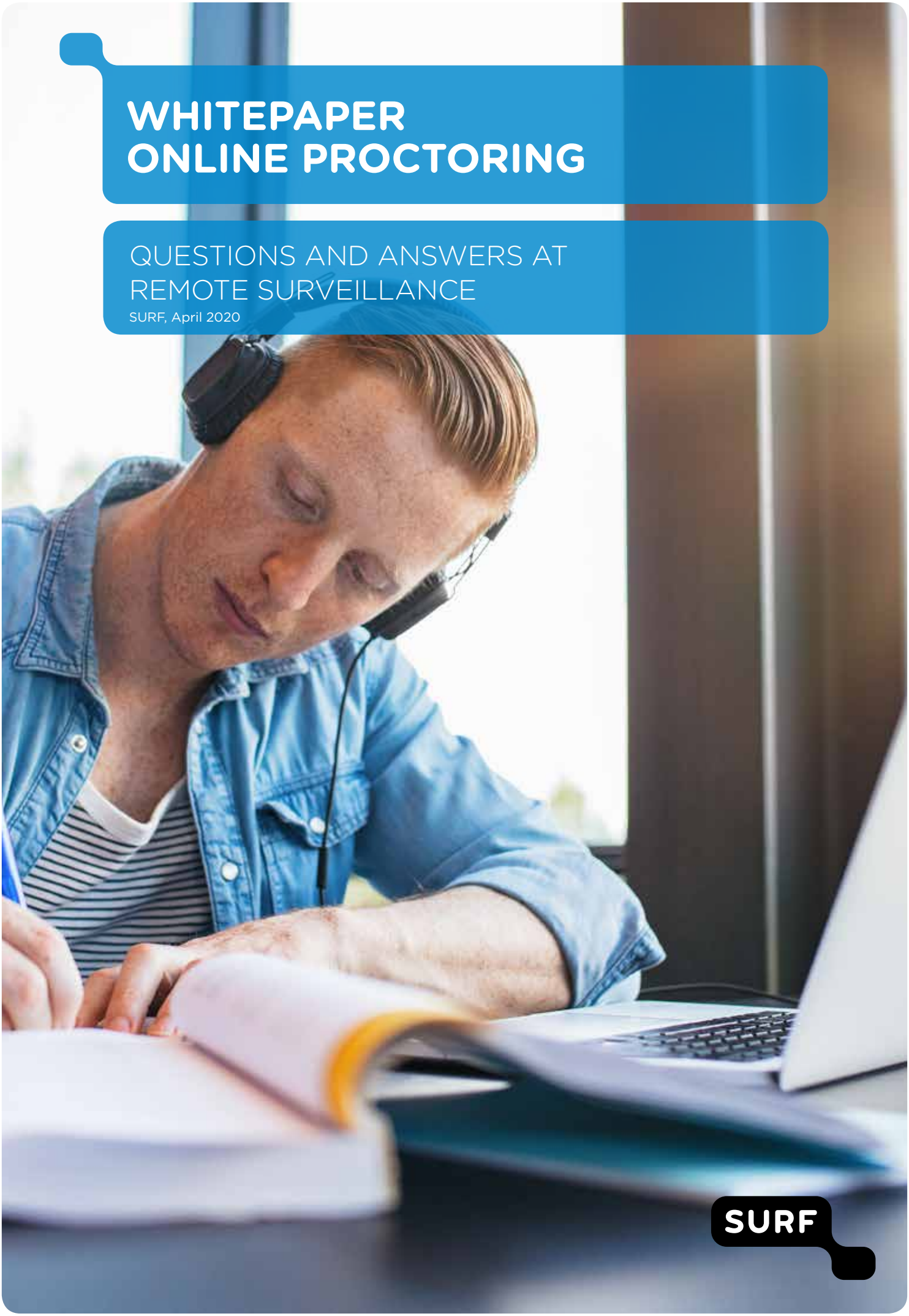
WHITEPAPER ONLINE PROCTORING

QUESTIONS AND ANSWERS AT REMOTE SURVEILLANCE

SURF, April 2020



FOREWORD

Online proctoring – or online invigilation – is increasingly being used in education (including higher education) in the Netherlands. This form of online invigilation makes it possible to test students remotely (from any location) in secure conditions. This is an ideal solution in many situations.

Examples are the accreditation of MOOCs or selection tests for Dutch and international higher education studies, exams of Dutch students who are studying abroad temporarily and still want to sit exams in the Netherlands, foreign students who have studied temporarily in the Netherlands but are back in their country of origin, and foreign pre-Master's students who are being admitted based on an assessment. Online proctoring can therefore be used to make the education process more flexible.

However, there are still many unanswered questions, for example relating to privacy and the resilience of the various proctoring systems against fraud. Scarcely any scholarly research has been done on these issues, and any practical experience has primarily been gained through small-scale experiments. Because of the rapidly changing market and the lack of solid research, it is difficult to gain a clear understanding of online proctoring. This makes it difficult for student groups, programme management and exam boards to assess whether or not it is a suitable resource to meet specific needs within their courses.

With this white paper, SURF wishes to provide a greater understanding of online proctoring and the issues that it raises. The white paper has three parts. The first part (sections 1, 2 and 3) is general in nature. Sections 1 and 2 describe what forms of online proctoring exist and in which situations online proctoring is currently used. We will also look at its backgrounds. Section 3 covers the key issues that emerge in the use of online proctoring (privacy protection, security, anti-fraud measures and costs). Sections two and three of this white paper provide greater detail. Section 4 takes a close look at privacy protection, while section 5 looks more closely at security and anti-fraud measures.

We have updated this white paper in response to the coronavirus crisis: is it more justified and appropriate to use online proctoring if it is not possible to meet physically for assessments? We report a number of times if a measure or statement specifically relates to crises such as the corona crisis.
New insights have also emerged over the years, partly as a result of decisions made by the Data Protection Authority (DPA). For example, camera images are no longer regarded as special category personal data by definition. Camera images are only regarded as special personal data if they have an identification purpose.
This white paper deliberately does not compare the various suppliers of online proctoring, but it does compare the recent properties of their systems. The market is developing rapidly and suppliers are constantly adapting their products, which would quickly render any comparison out of date. Fortunately, there are plenty of overviews of suppliers and their offerings to be found online.[1]

More information on digital assessment and online proctoring can be found on the SURF website. SURFacademy regularly organises meetings about these issues. If you have any specific questions about the topics covered in this white paper, please contact Lex Sietses.

1 See for instance https://www.onlineproctoring.eu/en/online-proctoring-providers/

CONTENTS

SUMMARY

Online proctoring – or remote surveillance of exams – is on the rise. It is already in regular use in the USA, and Dutch education institutions are also increasingly experimenting with it. Online proctoring offers opportunities for flexible education and on an international level, but there is still a lack of experience with it – especially in the Netherlands. Because of this, exam boards and other stakeholders within study programmes find it difficult to decide whether to use online proctoring in their courses and, if so, how. They struggle with issues relating to fraud prevention and privacy.

In this white paper, SURF concludes that online proctoring offers considerable added value in specific situations and is suitable for various assessment applications. At the same time, the large-scale introduction of online proctoring would have a major impact on privacy. The coronavirus crisis is currently playing a major role in our society as this white paper is updated (2020). This has a major impact on privacy considerations, which include online proctoring. If exams cannot be taken in large exam halls, online proctoring is the least drastic tool. The balance between students' rights and freedoms (privacy) and the legitimate interest of the institution (the organisation of safe exams) tends to favour the application of online proctoring based on a legitimate interest. For large-scale use in 'normal' times, the use of online proctoring is probably only possible with the student's consent.

Of course, holding exams outside the controlled environment of one's own institution introduces fraud issues. However, a matrix with an overview of applications can be presented based on a typology of proctoring forms and the importance of testing (see section 5.4). The key conclusions are set out below.

The possibilities of online proctoring

Online proctoring offers solutions in specific situations. For example, online proctoring allows Wageningen University & Research to offer an entirely online Master's programme in which students can take their exams from anywhere in the world. Online proctoring also allows elite athletes to take exams while based at their training camp, and seriously ill students can take exams from home.

In general, online proctoring makes it easier to hold exams flexibly in terms of time and location. This argument has gained considerable momentum since the start of the coronavirus crisis. Education stakeholders are increasingly advocating the use of online proctoring on a larger scale. During this crisis, one solution could be to organise tests in an entirely time-independent and location-independent way.

However, if students are given complete freedom in terms of the time the test is taken, each student must be given a unique exam. This can be done by presenting students with a unique case study (as for verbal tests or take-home final exams) or by using a large item database with many exam questions. Unique tasks are necessary, because otherwise assignments and assessment questions are known and the value of the assessment is lost. Higher education institutions feel it is unrealistic to offer students the opportunity to sit exams at any time, particularly as this is not in line with the current system of funded higher education.

However, online proctoring may make location-independent assessment easier. Students can take an online proctored test at any location if the test is set up to ensure that the student is not disturbed and has a good internet connection.

It depends on the supplier whether it is possible to offer online assessments and proctoring to large groups of students, starting at exactly the same time. Some suppliers have experienced system performance challenges.

Online proctoring sometimes requires the adjustment of the assessment format. For example, because students can't go to the toilet during the exam. It is recommended to limit exams to 90 minutes, or to split exams into two parts (of up to 90 minutes per exam).

Privacy and online proctoring

An important consideration when processing personal data is whether the means are in proportion to the ends (proportionality) and whether the ends can't be achieved in another, less drastic way (subsidiarity). Online proctoring has a huge impact on privacy, for example because of the use of camera images and the complete monitoring (to a greater or lesser extent) of a person's computer. A person's behaviour at the computer is also recorded in order to detect fraud. Another purpose of recordings is to establish identity. It is therefore possible to process special category personal data, and in any case sensitive personal data. Considerations in terms of proportionality and subsidiarity must also be made on a case-by-case basis (when designing the assessment).

That is why so far it has seemed disproportionate to use online proctoring for exams in higher education on a large scale. This is mainly because there were sufficient opportunities to organise assessments on campus without having to process this type of personal data.
In the context of the coronavirus crisis, these considerations are obviously different from normal. In the past, large exam halls were always a good alternative, but this is no longer the case during the coronavirus crisis. The privacy considerations during this crisis are therefore *not* to be extended automatically to the subsequent period. After the coronavirus crisis, the privacy aspects will have to be reviewed. It is likely that this review will then lead to a more limited use of online proctoring.

Another important privacy consideration for online proctoring is the basis for all processing: processing is only lawful if one of the legal bases applies. It is up to the institutions to make such a consideration and choice in this regard. The basic principles that can be considered for online proctoring are: consent and the necessity to process data in order to carry out a task that is in the public interest or in order to satisfy a legitimate interest.
In general, due to the nature of the data to be processed, the 'consent' basis seems to be the most appropriate. However, this does mean that students must be able to give their consent freely, that refusal has no consequences for them and that alternatives must be offered to online proctoring. Circumstances such as the impossibility of taking an exam in a physical classroom (such as during the coronavirus crisis) or the participation of students abroad will certainly help in the consideration of the basis.

The administrative and logistical process for testing may also become more complex if online proctoring is used. This means that consent is not always a feasible basis for the use of online proctoring for large groups of students, especially when an alternative is not realistic. The basis of a 'legitimate interest' may be found applicable. For example, this applies during the coronavirus crisis when students are not allowed to go on campus.[2] If less drastic alternatives become available again after the coronavirus crisis (such as exams in exam halls), the 'legitimate interest' basis can no longer be used.

In view of the special and sensitive nature of the personal data, institutions must take into account strict requirements, such as the storage, security, access and retention periods of the personal data. The setup of the online proctoring process must therefore be as privacy-friendly as possible, based on the principles of 'privacy by design'. For example, requesting an ID card is not an option. Student cards must be used for identification.

2 Please note that the coronavirus crisis does not automatically result in a legitimate interest. The institution must first look for privacy-friendly alternatives, including other forms of assessment that do not require proctoring. Students must also be explicitly informed of the right to object. The consideration of interests in any individual case may still mean that the institution is not permitted to make online proctoring mandatory. Ultimately, the institution itself must make these considerations on a case-by-case basis.

Online proctoring fraud prevention

Like the existing exam halls, online proctoring is not 100% guaranteed to prevent or detect fraud. With some methods it seems to be possible to commit fraud without being detected, but the more advanced versions of online proctoring (for example, with a second camera and software detection) certainly make this very difficult.

However, there is certainly an additional risk associated with online proctoring. If online proctoring is used for a long time, particularly on a large scale, there is a significant chance that software will be developed to circumvent the online proctoring. If students know that this software exists and is ready to use, it makes fraud easier.

As mentioned above, no type of supervision is 100% fraud-resistant. Students can also commit fraud in a campus setting with invigilators who have to keep an eye on 50 students at the same time. It is therefore up to the institution or programme to choose its form of supervision for each exam.

The likelihood of successful fraud detection also depends on the type of online proctoring technique and its execution (for example live proctoring versus retrospective viewing of images, which is referred to as 'record and review'). Multiple choice questions may be associated with a higher fraud risk due to the limited amount of information that needs to be exchanged. However, during multiple choice tests, students almost always sit still at the screen, so it is easy to spot any behavioural deviations. It is up to the exam boards to assess whether small movements are sufficient evidence of fraud.[3]

Unlike surveillance by invigilators in a campus setting, online proctoring has all the data (temporarily) stored. This means that far more data is available on which the institution can base its decision.

All in all, both online proctoring and campus supervision are associated with risks. It is also very important which form of online proctoring is chosen. For example, the use of a second camera is more secure than simply watching students on their webcam, but it is also a more drastic approach in terms of student privacy. The exam committee will have to consider which form of proctoring is appropriate for each exam to be taken.

Because of the various options for (online) supervision, SURF has developed a selection model that helps to determine which online proctoring methods are appropriate for which exams. The assessment of whether online proctoring is suitable for a specific exam depends on two factors: the importance that is attached to the exam and the risk of fraud. The model is set out below with a brief explanation; further details are provided in section 5.4.

The importance is determined by the (immediate) effect of a particular exam and the value society attaches to the assessment. For instance, a weekly interim assessment is less important than a final exam for a module. The effect of fraud during an interim assessment is far less than the effect of fraud affecting the final score of a module. The risk also depends on the test format. Fraud is expected to be far easier during multiple choice exams than during oral exams or exams asking open-ended questions.

In online proctoring, four levels have been identified:

- Level 0: Online conferencing software with up to 10 students;
- Level 1: Record & review, screen capture, one camera and logging websites;
- Level 2: Record & review, screen capture, one camera, computer lock-down capabilities and website & application logging;
- Level 3: Live proctoring with computer lock-down capabilities and full computer activity logging[4], or record & review that includes a second camera and the same features.

3 The burden of proof is considerably easier when two cameras are used. If only a webcam is used, proving any type of fraud is likely to be difficult. Some training courses opt to make specific behaviours (for example the presence of someone else in the room) sufficient grounds to declare an exam invalid. In that case, the burden of proof may be less than fraud. However, the risk of this is that some exams are declared invalid even if no actual fraud has been committed.

4 Including computer logging of websites, applications and background processes.

In some areas of education (associated with both high risks and a high or very high level of importance), the security of online proctoring still carries major risks even where live proctoring is selected. In such cases, a different assessment method could be considered in order to reduce the risk of fraud. This may be a well-equipped computer lab at the institution, or a secure form of BYOD exam in the institution's own exam hall.[5]

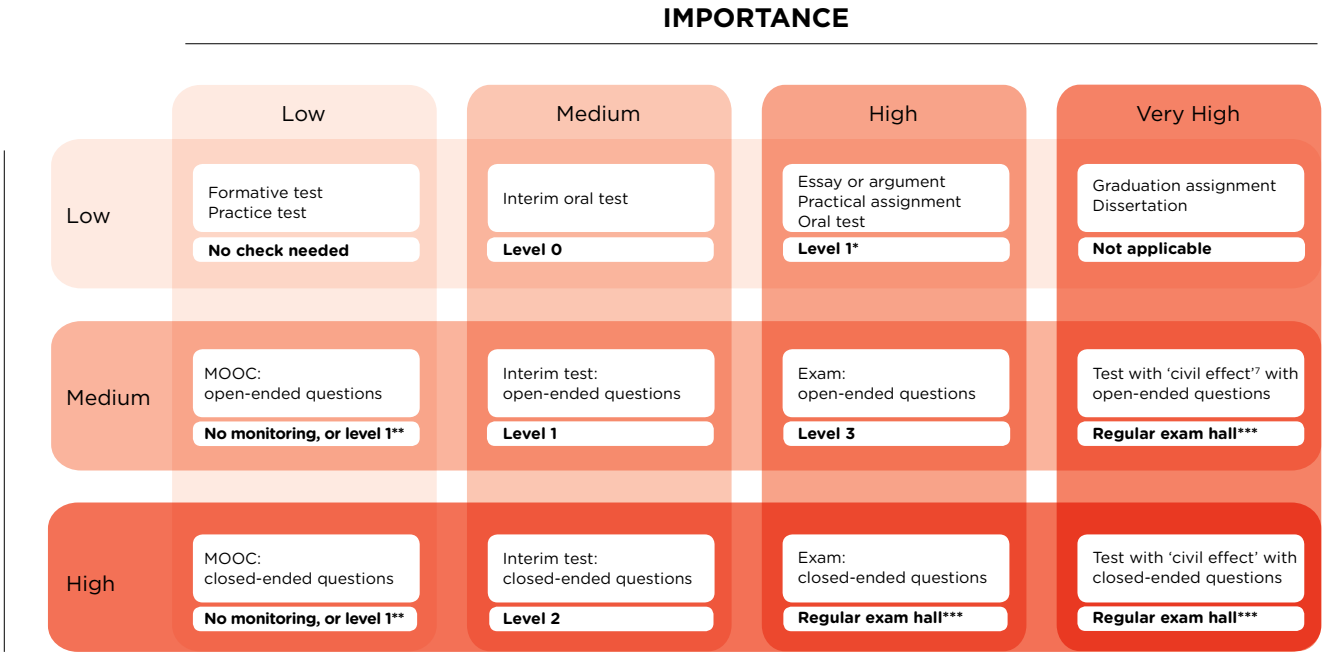
Institutions can also always fall back on the highest level of security: an exam hall with paper assessments. Please note that an exam hall is not 100% fraud-proof either, and not every exam hall is the same. A bad exam hall with too few invigilators may be less fraud-proof than good online proctoring. For the best comparison, we should also define different levels of exam halls. However, that is not SURF's expertise. It is up to the education institutions to develop this. The selection model therefore does not state that all exam halls are more secure than online proctoring. It states that the *maximum* security level of online proctoring is inherently lower than the *maximum* security level of an exam hall.

The coronavirus crisis may make the use of exam halls impossible. In that case, the exam committee will have to estimate which form of assessment is appropriate in their opinion. This could be live proctoring – the most fraud-resistant form of online proctoring – or an adjustment of the assessment format: for example open-ended questions instead of multiple choice questions. The same applies to the choice of security level for proctoring. The desired form of online proctoring may not be available based on feasibility, technical possibilities and other practical factors. The education institution may then choose to use a lighter form of proctoring to ensure that the exam can go ahead.

In that case, education institutions will have to be aware that they are taking a greater risk. This risk increases as online proctoring is applied for a longer period and on a large scale, because then it becomes more likely that software is developed and distributed to circumvent online proctoring.

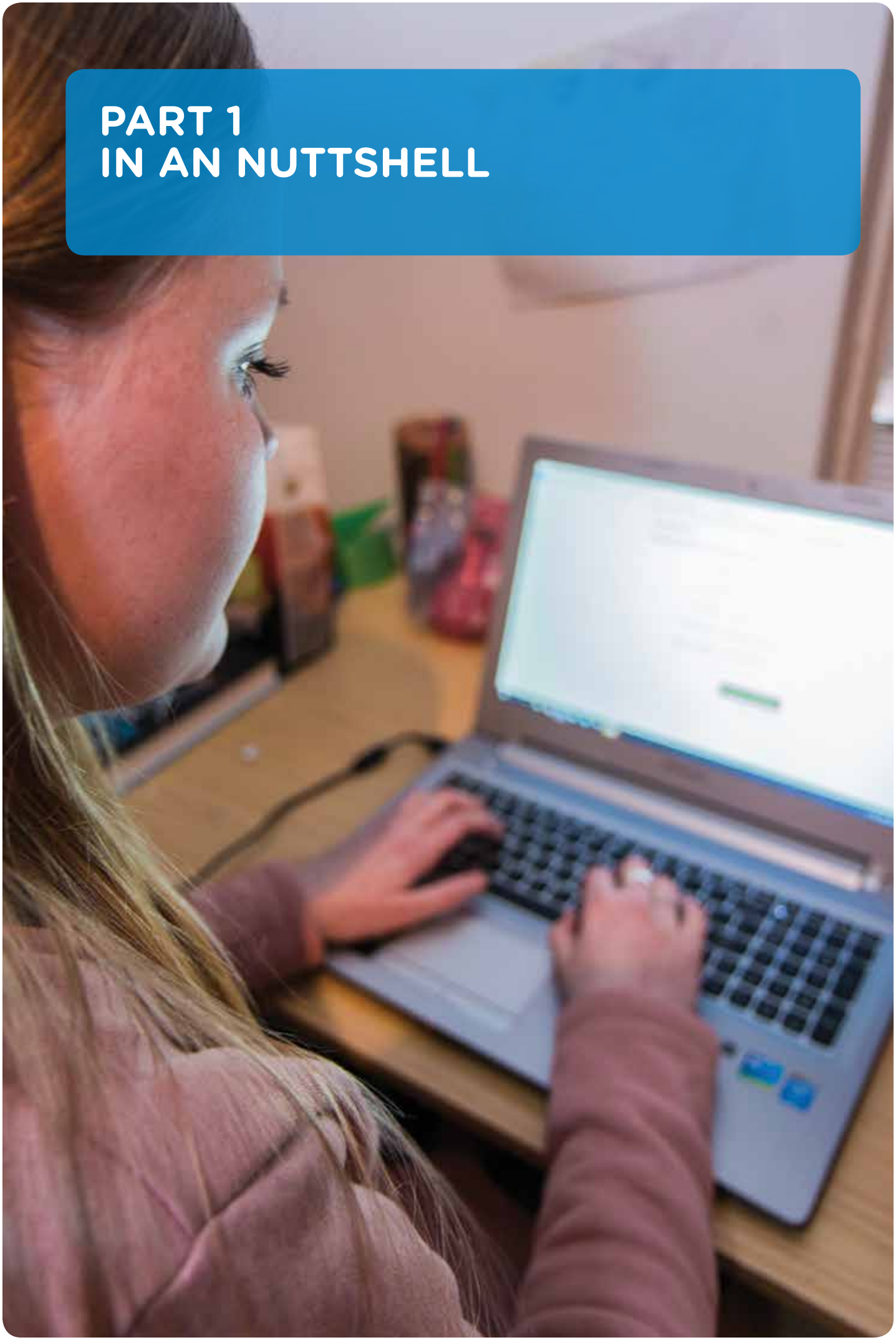
Finally, it is important to realise that the risk and the importance of an exam are determined by many more factors. One example is time pressure. Another is whether the exam content will be assessed again in a subsequent exam.[6] Ultimately, an assessment or exam committee must consider this on a case-by-case basis.

Model of choice for safe assessments



* Naturally, online proctoring is unsuitable for essays and work performed over long periods of time. It is particularly suitable for verbal exams with a limited duration (for example up to 3 hours).
** For MOOCs, this depends on the value placed on the MOOC.
*** During the coronavirus crisis, level 3 may be a solution if exam halls are not available. It is then up to the exam committee to consider the risk of fraud.

5 The possibilities and security of BYOD solutions or existing computer labs were not examined for the purposes of this white paper. However, in those cases the education institution does control the environment, which is a weakness of online proctoring. It is therefore likely that those solutions can be made more secure than anything that could be achieved with online proctoring.
6 For example, some programmes teach Calculus 1, 2 and 3 as three constructive modules. The exam of Calculus 3 therefore also refers to the knowledge gained from Calculus 1 and 2. In that case, the importance of the Calculus 1 and 2 assessments *may* be lower than assessments for modules that are only assessed once.
7 For instance, authorisation to enter professional practice as a lawyer or in the judicial system.



PART 1
IN AN NUTTSHELL

1. WHAT IS ONLINE PROCTORING?

Online proctoring is a form of location-independent digital assessment. The invigilation takes place online using special software. Online proctoring software promises to allow students and course participants to sit their exams anywhere (for example at home) in fraud-resistant conditions and/or with invigilation against fraud. Monitoring software, video images and the monitoring of students' screens should prevent them from engaging in fraud.

The exact form of online proctoring varies from supplier to supplier, but we can identify four categories: (1) Live supervision with conferencing software, (2) live proctoring (with special software) that allows someone to watch and intervene during the exam, (3) the option to manually watch each exam again at a later stage based on images and logs, and (4) an automated review (including subsequent monitoring of the report). The amount and nature of the data collected may vary from category to category. We list the main advantages and disadvantages for each category. We will also discuss a few alternatives if it is not possible to take the tests on site.

In all categories of proctoring, the process consists of approximately the same steps.

- The first step is to test the technical operation of the proctoring system to ensure that all data is transferred and collected in a technically correct manner. After this step, the student is informed that all data will be stored from that moment onwards.

- In the second step, the student identification process commences. A photo of the student is usually taken with the webcam and the student must show proof of identification to the webcam. The latter is usually a student card, as requesting an ID card is not permitted.

- In the third step, the student is asked to film the current environment. Via detailed steps students may be asked to make a 360-degree recording of the room, film in front of and behind the computer, film under the keyboard, film the ceiling and film under the table. Some systems also ask the student to film their ears to make sure that no unauthorised earphones are being used. Depending on the conditions of the assessment, the student may also be asked to film any books, papers or other aids on the table.

Once those three steps have been completed, the student can begin the actual assessment.

In all cases, it is important that the procedure is guaranteed in the exam regulations. Proctoring must also take place before a score is given.
As educational institutions often accelerate the use of online proctoring due to the coronary crisis, it is important to adequately document choices.

1.1 Live supervision with conferencing software

With this option, lecturers themselves use regular conferencing software and they take a closer look at the students during the assessment. The lecturer can see the students with the webcam and ask them to show identification during the assessment. However, the lecturer can't see the students' screens.

Please note that these tools are very clearly not intended for online proctoring. They require lecturers to take great care as they follow the process (for example to store images) and they often create a false sense of security.

In the field this approach is already used in combination with an additional restriction, such as limited time or open-ended questions instead of closed-ended questions. In practice, this form is also used in cases where students write down their work on a piece of paper (especially in applications that require students to show certain formulas and calculations), and then show their work to the camera. They then photograph their work with their mobile phone and email it to the lecturer, or upload it to the learning management system or assessment system.[8]

It goes without saying that all kinds of technical complications may occur during this type of online proctoring. In this category, the risk of fraud is the highest out of all the four categories discussed here. Nevertheless, this format is used. The group size is preferably limited to a maximum of 5-10 students in order to enable some form of monitoring that goes beyond watching and instructing the student via the webcam.

During the coronavirus crisis, this format has also been applied in large groups. This has not yet caused any significant technical problems. The question is how fraud-proof this method has been. In view of the current crisis situation, the programmes in question decided that the risk had to be accepted.

SURF makes no explicit statement about the privacy conditions of conferencing software. As these tools were not designed for supervision during exams, this aspect is often not very easy to control. It is also often impossible or more difficult to enter into a specific processor agreement.

One supervisor can monitor multiple students with online proctoring

8 This format is also used for other types of online proctoring. Because the student first shows the work to a camera and then uploads it, it can be checked that the uploaded document was actually written by that student.

1.2 Live proctoring with proctoring software

Live proctoring is the oldest and best-known form of online proctoring. This method is the most similar to an actual physical exam hall: a proctor (invigilator) is watching the proceedings remotely in real time. The number of students that one proctor can monitor is between 7 and 10. The more screens a proctor has to monitor, the fewer exams he can see at the same time. The proctor ensures that authorisation and authentication are performed correctly and can approve the check. The proctor can also indicate that the room is insufficiently lit.
The proctor checks what the student is doing on the screen and in front of the screen in real time. The proctor can intervene during the exam, just like an invigilator can in an exam hall. For instance, during an open-book exam, the proctor can ask students to shake or show their books to prove that no notes or crib sheets are hidden inside. The proctor can also ask students to press the alt-tab keys to see which applications are running.[9] The proctor can also ask verification questions during the exam and request that the student shows what is happening in the room again. The proctor can also ask the student to film the edges of the screen with a mirror in front of the webcam. If there is any indication that the student is recording assignments illegally (for example by taking a photo of the screen), the proctor may intervene. If there is any indication that the student is committing fraud, the proctor may end the exam prematurely.

The main drawbacks of this variant are the limited scalability (a maximum of 7-10 students at the same time) and the requirement that exams must be scheduled in advance. However, when proctoring companies are used, students can reserve their own time slot. Of course this does require unique exams for each student (based on an item database or parameterised questions, for example). Proctoring companies are now operating on a scale that allows assessment scheduling up to a few hours in advance. Whether this will also be the case if demand for this form of online proctoring rockets in the short term is yet to be seen.

Live proctoring is also often used in combination with digital assessment with students physically attending the education institution. Naturally, this combination is impossible if the education institutions' buildings are closed (as they have been during the coronavirus crisis).

Live proctoring can also be combined with storage of the footage to allow subsequent verification. Live proctoring, particularly in combination with extensive logging and lockdown opportunities, is the most fraud-proof form of online proctoring.

1.3 Subsequent storage and verification with proctoring software

In the most common form of online proctoring, the proctor does not watch the footage in real time. Instead the camera footage and logs are saved and reviewers watch the footage afterwards (human intervention). This is often referred to as' record and review '. Reviewers use the footage to assess whether fraud may have occurred during the exam.

The main advantage of storage and subsequent verification is that this variant is easily scalable and can be used for large simultaneous exams. Large numbers of students can sit their exams at the same time, and the proctors can then assess them over a longer period.

In higher education, reviewing consists of several rounds. In the first round, a general integrated review is carried out that reports on all kinds of abnormal behaviour. In the second round, (certified) invigilators assess the footage to identify actual suspicions of fraud. In the third round, students under suspicion of fraud are assessed jointly, for example by the examiner or the exam committee.

In practice, two different types of deviations are often found. The first type is when students (accidentally) fail to comply with all the detailed regulations (a sound is heard, someone accidentally walks into the background, the video image is briefly lost). These deviations cannot be immediately identified as fraud. The second type of deviation is when students try to carry out the assessment assignments in an unauthorised manner.

9 Please note that there are simple methods to hide applications that are running, but are not visible using these methods.

The disadvantage of this method is that the proctor does not monitor things in real time during the exam and therefore cannot intervene and point out to the student that what they are doing is not permitted. This method is also labour-intensive and has a long lead time. The proctor is also unable to intervene if the camera is positioned incorrectly or the desk is not sufficiently visible, for example. No action can be taken if the student copies the assessment questions illegally (although a sanction may be imposed afterwards, of course). This is not a problem during live proctoring, in which case an exam may have to be declared invalid when it is viewed again afterwards.

1.4 Automated proctoring

In automated proctoring – which is becoming more and more popular – proctors no longer monitor (or review) the entire exam. Instead, the software identifies specific moments of potential fraud. Suspicious behaviour is specified in advance for each exam when the software is configured. For example, is the student permitted to use reference materials during the exam or start up other software? An example of deviating behaviour is when the student walks or looks away, or when someone else is detected in the room. If this happens, the reviewer receives a notification in a report that is automatically generated, based on behaviour that has been previously defined as “suspicious”. The reviewer can then watch those specific moments again to assess whether this is a case of suspected fraud. Thanks to new developments in artificial intelligence, this variant is now very much on the rise.

Automated proctoring makes the proctoring process far more efficient and saves a lot of time, as not all footage and logs have to be watched again by human reviewers. This also makes it a very scalable solution. One of the disadvantages of the method may be that if students know how the software works, they will be able to evade the fraud prevention measures more easily. This is also a risk in the current exam hall situation, where some students also try to exploit the invigilators’ flaws. However, a human reviewer is still more difficult for students to mislead, because the human ability to detect deviations is (still) greater than that of computer analysis. Unlike software, human invigilators are also unpredictable. Once students have discovered a working method to mislead software, it will always work.

Another disadvantage is that the software may give a lot of *false positives* (the incorrect identification of something as potential fraud), which means that the second round of reviews may still take a relatively long time. Experience of the extent to which this effect occurs is still limited.

2. THE POSSIBILITIES OF ONLINE PROCTORING

Online proctoring has the potential to make education more accessible and more flexible – particularly for online and international education. However, there are also risks and doubts about its use. This section describes the main backgrounds to online proctoring. The following sections then take a closer look at some of the issues involved.

2.1 International education

Increasing numbers of education institutions are introducing open and online courses that can be followed from anywhere in the world. They vary from short online courses to entire Master's degree programmes. Of course, it is impossible for students or course participants to fly to the Netherlands for every exam. Institutions could work with international assessment centres or Dutch embassies to organise exams abroad. However, this is not ideal. It can be very expensive, it is not easily scalable and it is not always a suitable solution in all countries. Online proctoring may offer a solution in an international context of students living in all kinds of different locations (and countries).

A fully international Master's specialisation

"25 students are currently following the Master's specialisation in Nutritional Epidemiology and Public Health entirely online. This 4-year part-time online Master's programme leads to the same degree as the regular 2-year full-time on-campus Master's programme.

When offering such a programme entirely online, it would not be appropriate to force students to come to the Netherlands to sit their exams. That is why we use online proctoring for the exams. It also works well for the regular assessment process. Where a lecturer would normally set the computer lab up for an exam, we now make an online environment available.

We see online proctoring not as a replacement for all on-campus exams, but as a great solution for specific situations. In addition to this Master's degree, online proctoring is also being used for decentralised selection in the Netherlands Antilles, for example. We are also evolving plans for students on a work placement abroad or elite athletes attending training camps."
Rolf Marteijn, Wageningen University & Research

2.2 Flexibility in terms of time

More and more institutions put students at the centre of their educational offerings rather than base themselves on a fixed curriculum. This is also what students themselves want[10]. Furthermore, students are not always ready to take their exams at the same time. Whereas one student may master the content in half the available time, another student may actually need additional time. Offering paper-based exams at any time is unfeasible, because exam halls and proctors would have to be available at every moment of the day. However, this is possible with online proctoring, as it allows students to sit exams when they are ready.

2.3 Flexibility in terms of location

Institutions want to be able to offer education not just at any time, but also in any location. One of the reasons for this is that assessment locations are relatively expensive spaces. This impulse is strongest at international level, but is also occurring more frequently in domestic education within the Netherlands. This is particularly true for part-time studies and work-study programmes, because students taking this type of course will spend less time on campus. This is especially true during the coronavirus crisis.

2.4 Different exam types

A common misunderstanding is that online proctoring is primarily or even only suitable for multiple choice exams. This assumption is incorrect. Online proctoring can be used to support any digital exam format. The use of webcams also offers complementary options, for example allowing handwritten notes to be taken into account when marking exams. The student can show them to the webcam and the examiner can then assess the scanned version. See also section 1.2.

10 The national student union published a report on ‘flex students’ in 2016.

What students think of online proctoring

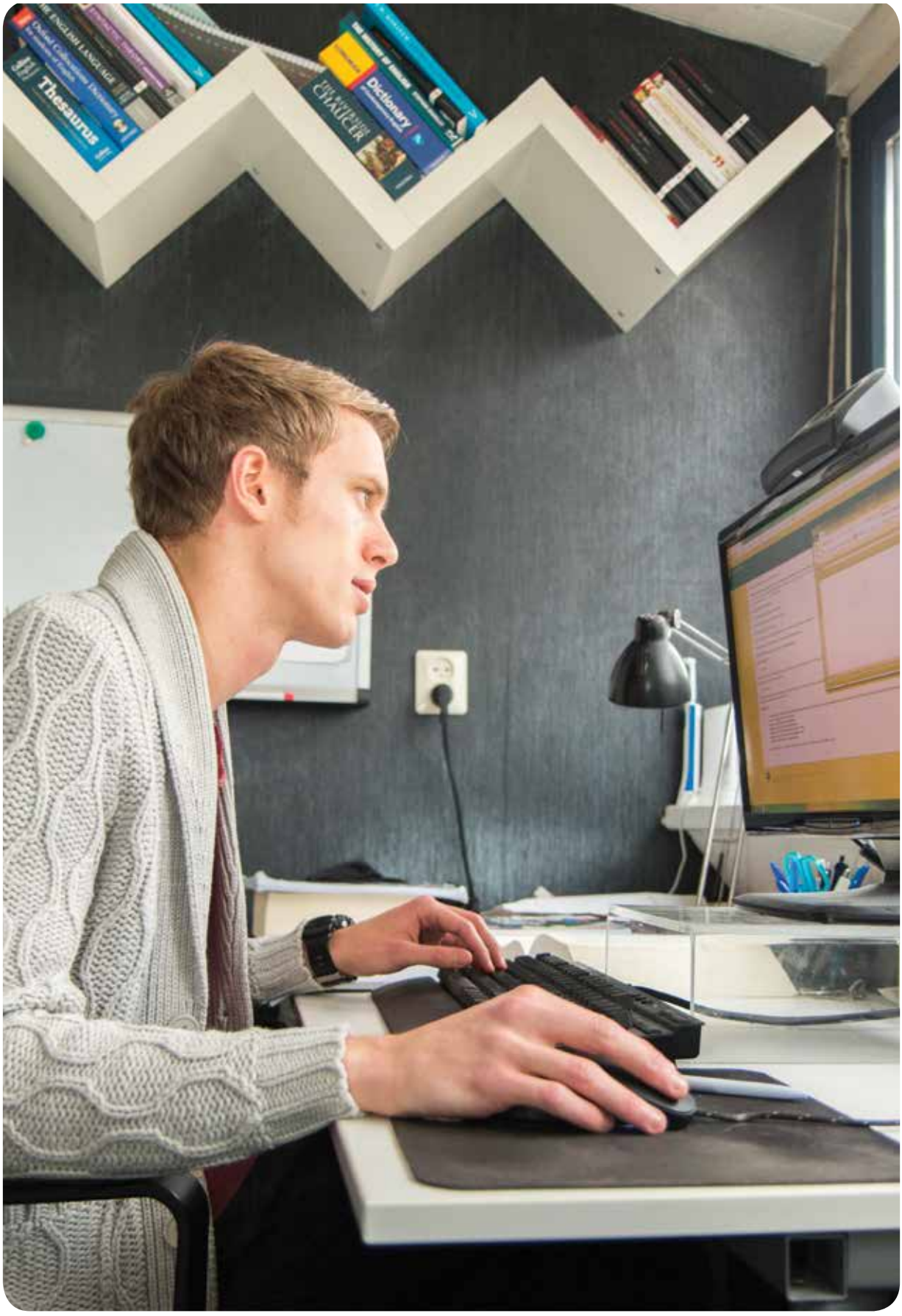
As far as the National Student Union LSVb is concerned, the use of online proctoring is a double-edged sword. On the one hand, online proctoring offers a solution for remote assessment, which makes education more accessible. This means that students who cannot be physically take part in an exam because they are ill or staying abroad can still take part in the existing exam. They will not experience any delay in their studies as a result. We have also seen that online proctoring can offer a quick solution in times of crisis, such as the outbreak of the COVID-19 virus. This means that students can still complete modules that have already started thanks to remote invigilation.

On the other hand, the various forms of online proctoring have major consequences for students' privacy. The National Student Union therefore believes that alternative assessment methods should always be sought first. Even if an assessment based on online proctoring proves to be the best option for an exam, students should always be able to refuse online proctoring in favour of an alternative assignment without the risk of delaying their studies. It is not convenient and/or possible for all students to film their room and take a test in a quiet environment, for example. Students must be adequately and clearly informed in advance about the assessment method, their rights and about what will happen to their data. They can then make a decision based on that information.

Online proctoring therefore offers a good alternative in situations where an existing assessment must be carried out remotely and it therefore increases the accessibility of education. However, there are too many ethical and privacy-related objections to the implementation of online proctoring on a large scale.
Roos van Leeuwen, National Student Union

"The Dutch National Students Association feels it is important to organise studies and assessments in a way that is time and location independent to make education more flexible and more adaptable to students' needs. The option of time and location independent education may also make education more accessible. For example, remote exams offer a solution to students who cannot physically attend the education institution due to illness, and time-independent education offers a solution to students who are combining their studies with demanding sports schedules. In crisis situations in which education must be set up remotely, as is currently the case with coronavirus, remote exams are a solution to prevent study delays. However, the Dutch National Students Association does not see remote assessments as a direct step towards online proctoring. Online proctoring is also associated with certain risks, for example in terms of privacy and ethical issues. The idea of a camera watching may also affect students' concentration. According to the Dutch National Students Association, alternative types of remote assessment should be considered first before proceeding with online proctoring.

If it turns out that online proctoring is really necessary and no good alternative assessment methods are available, it is important that all privacy-sensitive data is handled properly and that this is clearly communicated to students. Students must be informed of their rights. For example they must know that they are entitled to request an alternative. It must also be clear to students what the footage will be used for and for how long the footage will be managed by whom. The Dutch National Students Association also considers it important that privacy protocols for institutions are created together with the students. The students should be included in the preparation of the privacy protocols from the outset and they should have a say in them. This ensures that students are involved in the decisions about what will happen to their data."
Eline van Hove of the Dutch National Students Association ISO


Thesaurus
Dictionary
CHAUCER

3. ISSUES WITH ONLINE PROCTORING

This section examines important conditional issues relating to online proctoring: privacy protection, security and anti-fraud measures, and their costs. This section also addresses the challenges of scaling up online proctoring. This is currently topical because the coronavirus crisis is making it impossible to take a test at an education institution for the time being.

3.1 Privacy protection

For more details on GDPR and online proctoring, please refer to **section 4**.

Online proctoring involves the processing of personal data: data that says something directly or indirectly about students. The General Data Protection Regulation (GDPR) sets strict requirements for processing of this type of data, for example to determine the lawful basis, to inform students and to secure the stored data. Section 4 looks at this in closer detail and offers guidelines that institutions can use to develop suitable tools.

Important requirements in the GDPR are:

- **Lawful bases**
  Processing personal data requires a lawful basis (a condition that must be met in order for the data to be processed). The lawful bases for online proctoring are for example: (1) consent, (2) the need to process data in order to perform a task that is in the public interest or under public authority, and (3) the need to process data in the context of a legitimate interest. In the context of the coronavirus crisis, a legitimate interest can be used as a basis for online proctoring (see box with an example from VU Amsterdam). Once exams in exam halls are a proper alternative again, this basis is likely to lapse, as there will be a more privacy-friendly alternative to online proctoring.

  As far as the basis for 'consent' is concerned, a student must be able to freely give consent, refusal must not have consequences for the student and/or there must be an alternative to online proctoring. This often makes it difficult to apply consent to online proctoring on a large scale. However, consent may be used for students who wish to take exams from abroad, or for students who have indicated that they prefer to take their exams at home (in a quiet environment).

- **Duty to provide information**
  In all cases, the students (and their parents if the students are less than 16 years of age) must be given certain information. For example, they must be told what the processing involves, what data is collected, how long this data is kept and what the legal basis is. If the legal basis is based on a legitimate interest, the students must also be informed about how that interest has been balanced against the student's interests.

- **Purpose limitation**
  Personal data may only be used for the purpose it was obtained for and for which there is a legal basis. The data shall not be processed further at a later stage in a manner that is incompatible with those purposes.

VU Amsterdam: online proctoring with a legitimate interest

In times of coronavirus crisis, VU Amsterdam's first message is: *'Make sure that you find a different form of assessment than the traditional final assessment. If this is not possible, the conventional final assessment may be eligible for online proctoring.'* When online proctoring is used, VU Amsterdam (as an institution governed by public law) chooses the basis of 'legitimate interest'.

VU Amsterdam indicates that online proctoring for the relevant remote assessment is necessary in order to:

a. check who is the person taking the test;
b. establish that no fraud was committed during the test;
c. establish that the assessment has been completed within the given timeframe; and
d. follow the working method as described in the privacy statement.

In that case, there is a need for a legitimate interest for VU Amsterdam that outweighs the rights and freedoms of the data subjects (Article 6.1 f GDPR).

This consideration will have to be assessed on a case-by-case basis. VU Amsterdam has drawn up an extensive privacy statement that describes how the privacy of students is guaranteed. It states that students can raise their objections to the Data Protection Officer.

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

3.2 Security and anti-fraud measures

Chapter 5 How reliable is online monitoring?

Combating fraud is an important topic that attracts a great deal of public interest. Examination committees want to be able to fully support every qualification they award. Combating fraud is already a challenge in a regular exam hall; it can become far more complicated when digital assessment tools such as online proctoring are used.

It is generally acknowledged that regular exam halls are not 100% secure. However, education institutions and exam boards have a great deal of experience with the use of a regular exam hall and can therefore assess the risks involved fairly accurately: there is a certain degree of 'common understanding' without knowing exactly how much fraud is actually committed.

In the case of online proctoring, this experience is still limited. Many institutions wanting to use online proctoring will have to make their own ongoing assessment of how secure the solution they want to use is. Lecturers and exam boards often start the conversation with the wrong question: *"Is online proctoring 100% secure?"* This question is not realistic, as no testing method is ever 100% secure.

A complicating factor is that each supplier uses different methods and techniques. This means that the experiences of one institution cannot always be used directly by another institution.

Combating fraud is based on three components.
- *Prevention*: provide clear information, mention what suspicious behaviour is, and discourage students from committing fraud. This component is the most important component in preventing fraud.
- *Detection*: record data very well during identification and assessment, and ensure that unreasonable behaviour is identified quickly and properly.
- *Sanction*: make it clear that non-compliant behaviour and fraud will lead to serious consequences.

Students carried out a security audit

"At the University of Amsterdam (UvA), we have already held around eight hundred exams using online proctoring software. We are very satisfied with the results. We wanted to follow this up by investigating how the software could be used in regular education, and so we decided to start the SURFnet 'Online Proctoring' project.

This project aims to investigate the security of the software and examines whether students can (easily) commit fraud, and whether the students' privacy is guaranteed. We gave the assignment to four IT students who specialise in hacking systems. These students carried out a small-scale security audit to assess whether students are able to commit fraud and whether any privacy issues emerged. They identified various problems that do indeed point to security and privacy issues. It was agreed with the supplier that they would start by tackling a number of these problems and that a second security audit would be performed to assess whether the problems have been solved.

It is likely that not all of the problems will have a solution. UvA now has to assess whether the risks are acceptable for UvA, bearing in mind that the regular exam hall is also not 100% fraud-free."
Guusje Smit of University of Amsterdam (in 2016)

Section 5 looks extensively at possible ways to commit fraud and how proctoring software attempts to prevent it. Based on this, the following conclusions can be drawn:

- Fraud involving manipulation of hardware or software can usually be detected. However, this often has far-reaching implications for student privacy.
- Once a student has developed software to make it possible to commit fraud, the student could pass it on to a large group of students in the blink of an eye. This scalability is not the same as in a regular exam hall, where fraud is usually an individual[11] action.
- If the education institution does not have any control over the physical space where an exam is held, fraud can be committed in ways that are (almost) impossible to detect.
- With a bit of creativity, there seem to be many opportunities.[12] Section 5 discusses a selection of possible forms of fraud.

Both online proctoring and proctoring in regular exam halls come with risks attached. Fraud is possible in both situations, but there are also differences. A regular exam hall always offers a higher maximum level of security. Online proctoring is inherently more limited due to the nature of the system. The very advantage that an exam is not location-dependent also means that the education institution's control of the exam environment is more limited.

Do those disadvantages mean that online proctoring is useless as a means of organising exams? No, online proctoring is certainly useful as a tool for taking digital exams, and the preventive measures to prevent fraud should not be underestimated. However, it is important to make a well-founded consideration that assesses both the importance and risk of a specific exam, and compares those with the benefits.

Section 5 takes a closer look at various forms of fraud and how online proctoring can protect against them. Section 5.4 also includes an assessment security selection model that was developed by SURF. Exam boards can use this to assess which method is suitable for taking digital assessments in a specific situation.

11 Naturally, there are cases where exam questions are stolen; however exam hall fraud usually involves an individual student copying another student's answers, passing answers to someone else, or carrying out some other form of individual fraud.
12 See this link from 2015: https://jakebinstein.com/blog/on-knuckle-scanners-and-cheating-how-to-bypass-proctortrack/ - based on the comments, students are also actively searching for ways to avoid online proctoring in 2020.

3.3 Costs

One argument often made in favour of online proctoring (especially by proctoring providers) is the cost saving. The impression is created that online proctoring is almost always less expensive than an exam hall. In practice, the situation is less clear-cut. There are many additional factors at play, which means that the situation can vary from institution to institution and even from study programme to study programme.

In 2013, SURF performed a quick scan of the 'Costs and benefits of digital assessment'[13]. Although this was primarily focused on digital assessment and not on online proctoring, this quick scan did produce a number of interesting points that are worth repeating here. Furthermore, it is important to note that institutions want to use online proctoring not just for existing digital assessments, but also for converting existing paper-based assessments to digital assessments.

Following the quick scan that took place in 2013, the following points are worth considering:

- The distribution over the different cost centres varies considerably depending on the institution. The situation is unique to each institution and there is no uniform answer.
- In 2013, the benefits of digital assessment were primarily qualitative – for instance, that it allows skills to be tested that are difficult to assess on paper.

Reduced costs should therefore not be regarded as a distinct goal for online proctoring or digital assessment in general. It is not the financial savings, but the improvement of assessment quality and educational benefits that should make the business case conclusive.
This does not detract from the fact that a financial appraisal must be made before the introduction and use of online proctoring. Some points worth noting:

- Be critical as to whether or not a cost saving is actually achievable. For instance, when exam halls are hired externally, these costs could be saved by using online proctoring. But if an institution itself is the owner of large exam halls and does not want to or is unable to divest them, many fixed expenses (often calculated as a price per m^2) will remain even if it is no longer charged to a particular study programme.
- The prices for online proctoring vary according to both the provider and the method. Some models use a fixed base and an institution licence. Other models use the number of assessments taken and the number of reviewed assessments.
- In order to establish non-compliant behaviour and fraud, (certified) invigilators must always be used. They must recheck the critical times identified during an initial review. The costs of this may also be considerable. The current estimates are that invigilators take an average of 3-5 minutes per student in order to draw up a report afterwards.
- The use of own invigilators for the physical monitoring in an exam hall is likely to be more cost-effective (and more secure) than online proctoring in an uncontrollable home situation.
- Sometimes, education institutions charge students for additional costs involved in teaching and exams[14], and this has also been suggested for online proctoring. However, this is not permitted for normal publicly funded education in the Netherlands. This is because education institutions may not turn students away and must offer them access to education. This includes the obligation to provide education for the statutory tuition fees. Asking students to make a financial contribution is only permitted in the case of voluntary optional modules and if a free alternative is offered.

Costs and benefits for Wageningen University & Research

"We are currently seeing that online proctoring is a little more expensive than our regular exam halls. For regular paper-based exams we use the gym halls, which are normally empty during the day anyway. We only have to move in some chairs and tables, and these are not so expensive. Because we still have standard computer labs for our education, the same applies to digital exams: it is cheaper to hold exams on-campus than to use online proctoring."
Rolf Marteijn of Wageningen University & Research

13 SURFnet (2014). White paper: De businesscase van digitaal toetsen: https://www.surf.nl/whitepaper-de-businesscase-van-digitaal-toetsen
14 See for instance https://www.iso.nl/2014/03/zwartboek-van-extra-kosten-naast-collegegeld-online

3.4 False positives

The incorrect detection of potential fraud is a problem for every form of proctoring. This might be because some providers report every instance of the user looking away from the screen, for example. In 2013 the *Chronicle of Higher Education* wrote the following about 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]

False positives occur most often with automated reviewing and occur least often with live proctoring. In live proctoring, for instance, a proctor can direct the webcam towards the place that the student let their eyes wander to. With recordings, it always remains uncertain whether a student tried to cheat, or simply looked away from the screen. In short, it is very important to interpret observed abnormal behaviour afterwards with a good understanding of the facts. The training of invigilators must be an integral part of the online proctoring process.

3.5. Guarantees

Examination committees are responsible for ensuring the quality of the assessment and guarantee the quality of exams and qualifications. They must therefore be closely involved in the introduction of online proctoring. Exam boards are dependent on others when it comes to designing the online proctoring procedure and communicating with lecturers and students. Make sure that a team within the education institution provides support in this area, including to the exam boards.

Important elements of the guarantees are:

- Explain why online proctoring was chosen (and not other alternatives).
- State which type of online proctoring has been chosen.
- Inform lecturers about what is involved in online proctoring[16].
- Test the operation of the digital assessment.
- Configure the settings of online proctoring (for example, indicate which tools may be used and which student behaviour is permitted, such as going to the toilet).
- Inform students about the procedure (such as system check and identification).
- Inform students about the privacy guarantee (for example where the data is stored and who has access to it).
- Inform students who is responsible for which aspect of the technical infrastructure.
- Describe the procedures for what will happen if specific forms of fraud are detected.

See also the recommendations in 4.10 below.

The institution must include information on how exams are conducted in the education and examination rules.

3.6 Student experience

In 2016, student organisations were relatively positive about online proctoring. The European OP4RE project has shown[17] that students who have experienced online proctoring are generally fairly positive about this in comparison with on campus assessments. The reasons for this are that students do not have to travel, they can take their tests with a well-known device and they prefer the comfort of their own home to a busy and impersonal exam hall.

Now that we have more experience with online proctoring, the students are also raising more specific objections. The objections relate to[18]:

- The question of why an educational institution does not opt for alternative forms of assessment.
- Consequences in the event of technical problems with online proctoring.

15 Steve Kolowich, 'Behind the Webcam's Watchful Eye, Online Proctoring Takes Hold', 15 April 2013, available on http://chronicle.com/article/Behind-the-Webcams-Watchful/138505/
16 VU Amsterdam has set up a special website for this purpose: https://canvas.vu.nl/courses/47759/pages/online-proctoring-information-for-teachers
17 OP4RE project via https://onlineproctoring.eu
18 See: https://www.dub.uu.nl/nl/opinie/bedank-voor-online-proctoring

- In the students' opinion, their homes are not always appropriate for taking exams. Not every student has access to a room where they can sit an exam in peace and quiet.
- The question of whether the students' private environments can be recorded. Students generally do not have a separate room to work in.
- How to deal with the registration of special category personal data.
- What certainties are there in terms of what happens to the footage?
- Students may feel they are being watched. This is different than in an exam hall. To what extent does this affect the result?

Students who take tests via online proctoring are also concerned about how to get help if something goes wrong, if assignments are unclear, or if there is any suspicious behaviour.

The objections mentioned should not be trivialised, but they are not in themselves grounds for not implementing online proctoring or for never allowing students to use it..

3.7 Information to be provided

In a number of cases, it may be in the institution's direct legitimate interest to implement online proctoring (for example during the coronavirus crisis or for students abroad). After all, it is possible to substantiate why this form of testing is used and sufficient guarantees can be provided to prevent any negative consequences of this form of testing.
If the institution chooses to apply online proctoring, it must explain very clearly why online proctoring is used and exactly how it works.

Firstly, the institution must make clear in a privacy statement how the choice of online proctored assessment is made. For example, this statement must clearly mention that there is no alternative (we also refer to section 4 in that regard), which options there are to raise objections and possible alternatives, which system suppliers are used and which agreements have been made on who has access to the data, how the data is protected and when it is deleted. It must also be made clear that the student does not have to provide any special category personal data. The instructions must make it clear that students must cover or position out of sight any objects referring to particular personal information if they do not wish to share that information. Examples are a menora, a Qur'an or holy water font and references to sexual orientation or a medical condition. Furthermore, no identity document must never be requested for identification.
If students object, a data protection officer or committee must balance the objections against the interests of the institution. This may include objections from a privacy point of view, but also specific exceptions, such as an unsafe situation at home. Another objection may be that the student does not really have the opportunity to take a proctored assessment at home or in his or her environment. Some institutions request the study advisor's advice in that regard. The data protection officer or a committee then decide whether an objection is well-founded and whether an exception applies.

Secondly, creating and providing clear instructions is very important. The best option is to use a video to explain exactly how the process works and what is required. An extensive list of Frequently Asked Questions is also important, as is a chat environment that students can visit if they do not know the solution.
Thirdly, it is important that students can practise using the online proctoring software. This allows students to first test the suitability of their equipment (and to solve any technical problems before the actual assessment). Secondly, they can test the procedure, so that they know exactly what is going to happen during the real test. Experience in the Netherlands has taught us that, despite these preparations, between 5% and 10% of students still experience login problems with the first online proctored test. However, this percentage decreases rapidly for the second proctored test. It is even possible to make the student trial session with the proctoring software mandatory as part of the total assessment. This also makes it easier to determine who is responsible for any technical problems afterwards.
During the communication with the student, it should be pointed out that it is the student's responsibility to ensure that their own equipment works. If any problems occur, the institution must make sure to monitor and log that the proctoring system as a whole is functioning, so that it is clear that the problem is not caused by the system. In that case, it is more likely that the student's preparation or equipment is the cause.

If the proctoring system itself shows any problems, other procedures must of course be followed. The situation is then similar to the failure of a paper test, which, for example, showed that the wrong test was printed. In most cases, the assessment is re-scheduled for a later date.

At the time of writing, experience has shown that the group of students with insurmountable objections to online proctoring has so far been limited under the measures described above.

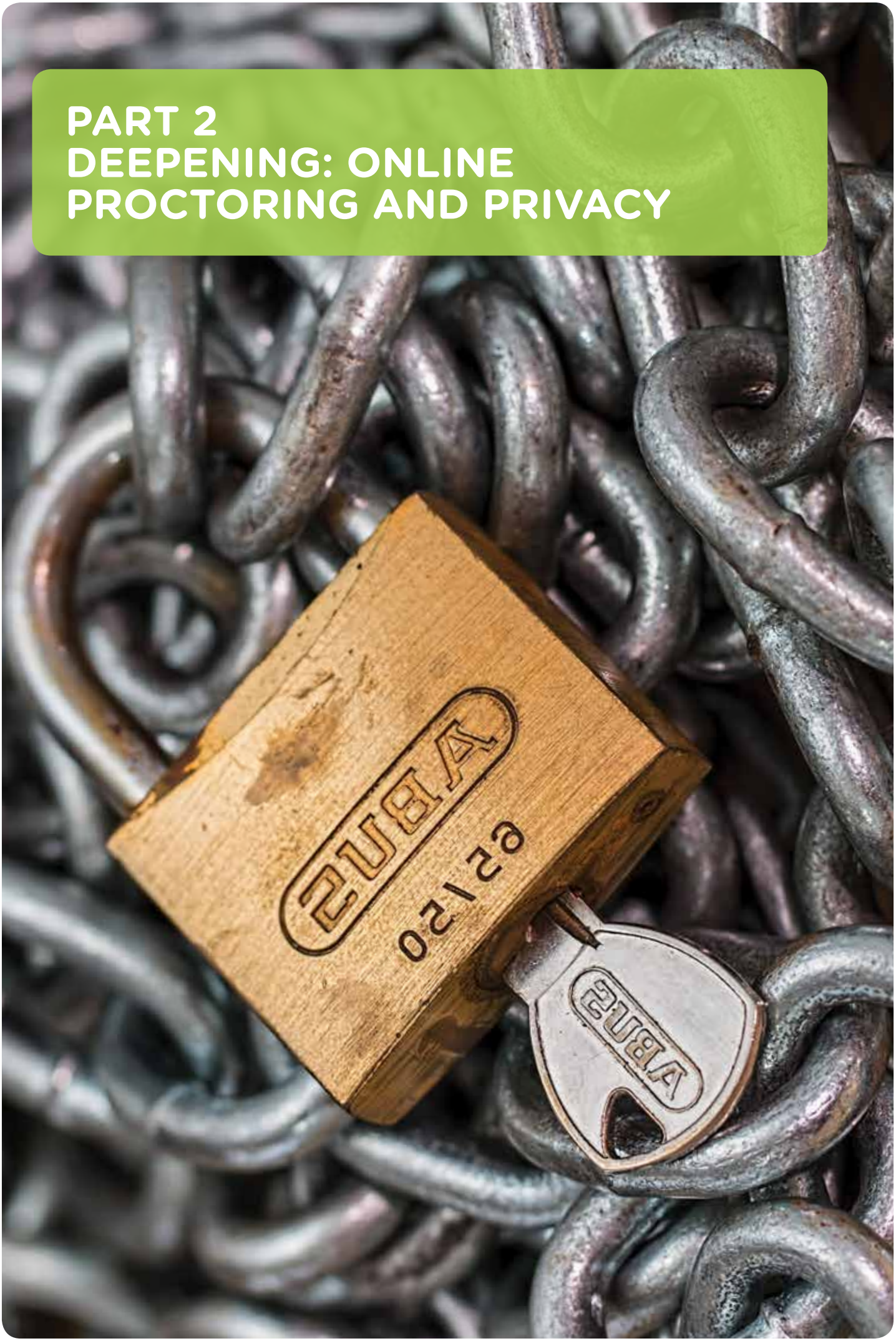
3.8. Challenges of upscaling

The corona crisis has considerably increased interest in online proctoring. However, scaling up online proctoring also has its challenges.

- Education institutions must carry out the necessary preparatory work before they can implement online proctoring (for example see 4.10).
- Live proctoring is certainly not suitable for higher education in view of its scale. The question is whether online proctoring, during which recordings are stored and reviewed (semi-automatically), can be scaled up in a short period of time. Do suppliers have sufficient capacity to introduce online proctoring across a wide range of education institutions in a short period of time?
- Can the suppliers' systems and networks cope with a sharp increase in online proctoring? Or are we facing technical problems that will have a negative impact on the quality of the tests? In that case, the legality of the assessment cannot be guaranteed to the same extent[19].
- Do all students have the appropriate facilities to participate in online proctoring? For example, students may be using an employer's laptop that does not allow them to install anything or use the webcam. Or students may be sharing a laptop with a family member, which means they do not always have access to the laptop. Normally, these students have a choice of whether or not to participate in online proctoring.
- The question is whether the suppliers are anticipating any technical problems and are switching off certain functionalities – such as the use of a second camera – in order to maintain the system's performance during more intensive use. This would probably compromise the reliability of the online proctoring.
- Online proctoring is associated with a high risk of scalable and 'exportable' fraud. If online proctoring is used more intensively and on a larger scale, there is a greater chance that software will be developed to circumvent the operation of the proctoring software. This software will then be distributed quickly. This is comparable to the software that is now being developed to cheat in video games. Despite the many millions that video game developers are investing in ways to detect and combat this' sabotage software ', they are not able to eliminate this problem. The question is whether suppliers of online proctoring software can also make such large investments. In addition, fraud is far more important in exams than in video games. This is not a problem in the short term. In the somewhat longer term, however, this will become a real issue if online proctoring is used for many exams and large groups of students worldwide.

19 Klinkenberg, S. (2020). Remote examinations? The recommendations of the SIG Digitaal Toetsen. https://communities.surf.nl/artikel/op-afstand-tentamineren-het-advies-van-de-sig-digitaal-toetsen

PART 2
DEEPENING: ONLINE PROCTORING AND PRIVACY



4. PRIVACY PROTECTION

When an institution processes personal data, the General Data Protection Regulation (GDPR) applies. What does the GDPR mean for online proctoring? There are no ready-made answers to this question.

It is clear, however, that it is not enough to have students sign a standard consent form and provide a privacy statement on the website. The GDPR sets high standards for the careful collection and processing of personal data, but also for the security and storage of personal data.

This section provides guidance on how institutions can develop the appropriate tools.

4.1 What is personal data?

Under the GDPR, personal data refers to any data that can be used to identify a person, either directly or indirectly. Names and addresses constitute personal data, as does data about a person's behaviour. Keeping track of what someone is doing during an exam is therefore also a form of collecting personal data. Data that can be traced back to a person is also regarded as personal data. This therefore refers to more than just names, addresses, camera footage or contact details.

Even when data is gathered that seems anonymous at first glance, personal data may still be involved, for example if it is possible to combine the data with another (public) source. Only if the data can't be traced back to a person after combining it with other data, can we rule out the presence of any personal data. Data can often be traced back to individuals and anonymised data is therefore not readily available.

Please also note that personal data may only be used for the purpose for which it was obtained. If an institution wants to use data from the proctoring software for other purposes (for example for learning analytics or timetabling), it may be useful to aggregate the personal data into conclusions about more than one person. If it is absolutely impossible to trace back the data to an individual (and the aggregation can therefore not be undone), it is no longer personal data. The aggregated data can then be used freely. Please note that aggregation of personal data is also a processing operation and is only permitted if it is compatible with one of the previously specified and communicated purposes.

Another option is the pseudonymisation of personal data. This is a security measure, for example because it limits the impact of a data leak. Because the personal data can still be traced back to individuals, the GDPR still applies. In the case of anonymised personal data, it must be impossible to trace back the data to any individuals in any way, even when other sources and data are used. More information about Learning Analytics can be found in the document 'Learning analytics in 5 steps: a guide to the GDPR'.

Special category data
In principle, special category personal data about areas such as a person's health, political preference or religion must not be collected or used. Such data can only be collected if it is required by law, with explicit consent or if one of the other exceptions under the GDPR applies.

Explicit consent may only be used if the person can freely give consent without any pressure. Explicit consent means that a separate request is made for this data, accompanied by a separate explanation of the reason why (and the option to refuse). The person giving consent must take a specific action for this purpose.

Sensitive personal data
Sensitive personal data is data that may have a stigmatising effect. Examples of sensitive data are financial data, information about relationship problems and information about school and study performance. As a result of this sensitivity, extra care must be taken when using such data.

Online proctoring processes sensitive personal data about students. Online proctoring also involves the monitoring and recording of the student. In particular, the outcome and results of the online proctoring software should also be taken into account. The detection of deviating behaviour during an online proctored test may be an indication of fraudulent actions.

Camera images are often processed in online proctoring. In some cases, the images may also be stored (and then deleted). Although camera images or footage is usually not regarded as special category personal data (unless it is intended for identification), images can say a lot about a student. It is therefore always considered as sensitive personal data. Because identification is part of online proctoring, the question is whether we should still classify camera images as special category personal data in this case.[20] As we are updating this white paper, we have no clear answer to this, so every institution will have to make this assessment itself (on a case-by-case basis).

4.2 The legal basis for personal data processing

The GDPR considers any use of personal data to be processing. The processing of personal data is only permitted in accordance with a basis that is stated in the law. If assessments and exams use online proctoring, this involves the processing of students' personal data. A legal basis is therefore required. Several legal bases may apply to different parts of the process simultaneously, but if no legal basis can be identified, processing is not permitted. It does not matter how convenient, useful, effective or desirable the processing would be. Under the GDPR, the following legal bases exist:

- consent
- performance of a contract
- legal obligation
- vital interests
- performance of a task of public interest
- necessary for the legitimate interests of the institution

When using (online) proctoring software, it is important to have a legal basis for processing the personal data. The purpose of online proctoring is to monitor students with regard to the lawful completion of assessments and exams. Due to the relationship of dependence between the students and the institution, it is not possible to request the consent of the students (or their parents or representatives). Because of this dependence, the consent cannot be given 'freely'. Consent that is given freely under the GDPR means that students must also be able to refuse without any negative consequences and that an alternative must be offered.

However, the basis for 'consent' may be suitable for small groups and specific exceptional situations. Examples are elite athletes participating in a high-altitude training camp, an international work experience and students who indicate that they prefer to sit their exams at home, because they find a busy exam hall or long travel times difficult. But as mentioned above, the consent must be truly voluntary. The relationship of dependence between the students and the institution also plays a role, and the Data Protection Authority may see (social) pressure from the institution as the reason why consent is not given freely.

20 See also https://autoriteitpersoonsgegevens.nl/nl/nieuws/autoriteit-persoonsgegevens-publiceert-beleidsregels-cameratoezicht

During the coronavirus crisis, 'performing a task of public interest' and 'legitimate interest' seem to be the most obvious bases. This is because the coronavirus crisis has fundamentally changed the context. Whereas an exam hall is normally a realistic alternative, this is not the case during this crisis. A more privacy-friendly alternative may be possible again after this crisis situation. In that case, the basis for online proctoring that applied during the crisis will immediately expire. Outside the coronavirus crisis, 'consent' may therefore be the only option.

Higher education law
Under the higher education law, the institution is obliged to organise an exam for each unit of study and a final exam for each course.[21] The institution administration is responsible for the practical organisation of exams[22]. The institution will determine the exact details of how the exams are organised. The organisation of exams and final exams is a public task that must be carried out by the institution.

Legitimate interest[23]
Based on the higher education law, the institution is free to organise the practicalities of the exams. In this context, a balance must always be struck between the interests of the institution and the impact on the students' privacy. This balanced consideration must be documented. The institution must therefore support the choice of online proctoring when organising assessments and exams, and the interests of the institutions must outweigh the privacy interests of the students, and must therefore not adversely affect those privacy interests.

When considering the interests of online proctoring, the following aspects must be discussed:

a. The legitimate interest of the institution.
b. The extent to which the processing is necessary to defend the legitimate interest. The need for this processing can be established with the concepts of proportionality and subsidiarity.

   Proportionality
   Proportionality means that the purpose of processing the personal data for the institution must be in proportion to the breach of the student's privacy.
   Subsidiarity
   Subsidiarity means that it must not be possible to achieve the intended purpose that was set for the processing in a way that is less drastic and/or with less drastic means.

c. The extent to which the interests, fundamental rights or freedoms of the student are compromised as a result of the processing.
d. The measures taken by the institution to compromise the interests, fundamental rights or freedoms of the student as little as possible.
e. The balancing of items a/b on the one hand and c/d on the other hand.

The coronavirus crisis strongly affects whether or not there is a legitimate interest, whether or not online proctoring is proportionate and whether or not the intended objective of assessing students can be achieved in a less drastic manner. If it is not possible to organise exams at a physical location, there may be a legitimate interest and necessity. As soon as it is possible to organise exams in an exam hall again, there is probably no longer a legitimate interest.

In addition, the institution must include the use of such software for digital assessment in the education and exam rules, so that it is clear how this assessment is carried out and under what conditions. The institution must include information on how exams are conducted in the education and examination rules.[24]
(See also other GDPR conditions).

21 Article 7.3 Law on higher education and scientific research
22 Article 7.10 Law on higher education and scientific research
23 Please note that according to the GDPR, the legitimate interest basis may not apply to processing carried out by public authorities as part of their tasks. An institution that classifies itself as a government organisation therefore does not have the option to use legitimate interest as a basis.
24 Article 7.13 (1) (l) Law on higher education and scientific research

4.3 Information to be provided under the GDPR

In addition to the bases, the GDPR also sets a number of other conditions that must be met. The following must be considered:

- There must be an explicitly described purpose. An example of this is the guaranteed integrity of exams or assessments not taken at one's own location, and the prevention of fraud in digital assessments and exams.
- In addition, only personal data that is necessary to achieve the purpose are allowed to be processed (data minimisation).
- Personal data must not be retained for longer than is necessary for the possible verification of the assessment's compliance. If any irregularities are detected during the assessment, it is permitted to keep the data (longer) in view of any evidence and objections or complaints procedures, provided that the education institution needs the data for the purposes of providing evidence.
- A final condition is that students (or their parents if the students are less than 16 years of age) must be able to consult the data that was recorded by the proctoring software. This includes image and sound recordings.

4.4 Personal data security

Anyone who processes personal data[25] must ensure that it is adequately secured by using the most recent techniques. This means that all personal data gathered must be reasonably secured against unauthorised access or use. This involves not just technical measures, but also organisational measures. Of course all circumstances, such as current technical developments, the costs of implementing the measures, the risks to students and the type of data, must be taken into account.

There is no generally applicable norm or standard that can offer full compliance with the law in all circumstances. Although certain standards are regarded as adequate in some sectors (such as NEN 7510 in the Dutch care sector), there are none available for the education sector. The 'SURF legal standards framework for (cloud) services in higher education'[26] and the 'SURF standards framework for information security'[27] and ISO 27001[28] may help you decide whether your security arrangements are adequate.

Application Security
Besides personal data, applications also need to be adequately secured. This means that the infrastructure on which the application runs must be adequately protected. There must also be adequate access security to ensure that the right person logs in. The ISO 27000 security standards and the standards framework for information security in higher education offer guidance on this. Technical solutions for adequate security come in many shapes and sizes. It is preferable to have a periodic audit carried out by an independent external party that assesses both technical and organisational security. Attention must also be paid to adequate protection against forms of sabotage, such as DDOS.

Liability
Even when an institution uses third-party software or services, the institution itself remains responsible and liable for the security of the software or services. This applies even if the supplier has limited their own liability. It makes sense to refuse any limitation of liability or to expand the liability to allow for cases where harm is caused as a result of a privacy breach.

Data breaches
A data breach involves unauthorised or unintentional access to personal data. However, it also includes the unwanted destruction, loss, alteration and provision of personal data. This is therefore not just about large-scale theft of personal data by hackers, but can also be about unauthorised access to (a limited set of) personal data. For example, students may be able to see each other's results or a lecturer may be able to access a student's personal data without due cause.

25 Please note that the term 'process' is used here in a broader sense than usual. It refers to any action or set of actions performed with the personal data, including the storage or forwarding of data, even if no changes are made to the data.
26 SURF legal standards framework for (cloud) services: https://www.surf.nl/surf-juridisch-normenkader-cloudservices.
27 SURFnet standards framework for information security: https://wiki.surfnet.nl/display/SA/Normenkader+informatiebeveiliging
28 https://nl.wikipedia.org/wiki/ISO/IEC_27001

Data breaches must be reported to the Data Protection Authority, unless the data breach is likely to pose no risks to the rights and freedoms of the student. This lets the data subjects know that a data breach has occurred (and the data subjects can take measures themselves). The regulator may also act if necessary. The GDPR includes two separate reporting obligations:[29]

1. *Reporting to the Data Protection Authority.*
   A data breach must be reported *"unless it is unlikely that a breach will endanger the rights and freedoms of natural persons"*.[30] Reports made to the Data Protection Authority are confidential.
2. *Reporting to the data subjects.*
   Data subjects (students, employees and so on) must be informed of a data breach affecting them if this breach "probably poses a high risk to their rights and freedoms".[31]

4.5 Rights of data subjects

GDPR states that data subjects (students) have several rights that allow them to remain in control of their personal data. The four most relevant rights for online proctoring are the rights of access, rectification, erasure and objection. These are briefly discussed below.

Access
The purpose of an access request is to allow data subjects to find out what data an institution holds about them. This means that the institution must provide the complete file and all data registrations, not just the standard data that can be accessed with an online tool or the data that can be supplied without effort. The right of access therefore also applies to camera images and log files. Notes made in offline files are normally also covered by the right of access. However, a data subject may make a specific request for access that the institution can fulfil more easily.

With online proctoring, it can be difficult to be fully compliant with this obligation if the necessary functionality has not been built in. In principle, the institution is not permitted to request compensation if the student requests access. In exceptional cases, it is possible to charge an administrative fee if several copies are requested or repeated requests are made. An excessive amount of requests in a short period of time may be refused.

It is expected that students may wish to access their exam data in the context of an appeal or objection procedure, for example. In order to honour these requests, it is important to establish an adequate process or to have the supplier to build one into the software.

Rectification
A data subject may use the right to access to ascertain whether personal data relating to him or her is being processed and, if so, what data exactly.

A successful request for access may mean that the student finds out that the data are incorrect or incomplete. In that case, the right to rectification becomes relevant. This right allows students to have their incomplete and/or incorrect personal data corrected.
The institution must take all reasonable steps to ensure that any inaccurate personal data is corrected or erased. Please note that this is about factual inaccuracies. For example, a student cannot use the right to rectification in order to correct a grade that does not suit the student.

29 Articles 33 and 34 of the GDPR
30 See: 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 See: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken#wanneer-levert-een-datalek-een-hoog-risico-op-7331

Erasure
The right to erasure applies to all data that is incorrect, no longer relevant or no longer necessary for the purposes for which the data was collected. For personal data used and analysed to enable online proctoring, this specifically means that data must be deleted once the assessment has been confirmed and an objection or appeal is no longer possible. Do take into account the retention periods stated in the law on higher education and scientific research. Also bear in mind that the parties that are processing this data on behalf of the institution (for example data centres that store back-ups) are the responsibility of the institution and must therefore be involved in order to comply with the law.

Right to object in the event of a legitimate interest and based on the public interest
Students have the right to object to the processing of their personal data based on their particular situation, if that data is processed based on a legitimate interest or public interest. If the institution can demonstrate compelling and legitimate processing grounds outweighing the student's, the objection may be refused.

4.6 Automated decision-making and proctoring

Online proctoring must take into account automated decision-making and profiling.[32] Automated online proctoring aimed at detecting fraud can have negative consequences for the student or significantly affect the student. An automated decision taken by means of online proctoring without human intervention may result in a sanction or measure for the student, such as a negative score or suspension. This has a negative effect on the student.

A data subject also has the right not to be subjected to automated decision-making without human intervention, if this is associated with legal consequences or if this significantly affects the data subject. It is a requirement that such decisions always involve an actual human assessment by an invigilator, lecturer or examiner. This is naturally quite easy to organise and to guarantee. Chapter 2 describes the process of proctoring through storage and subsequent verification and states how this should be designed in three rounds.

4.7 Third-party services

Online proctoring will often involve the use of third-party services. This role can even commence when the software is purchased and commissioned by the institution. However the provision of the service itself (such as data storage or the deployment and training of human proctors) is also increasingly being outsourced to third parties.

Focus areas
When using third-party software or services, there are two important points to consider:

1. The institution itself is always responsible for the quality of the service and for any problems vis-à-vis the student. This will also be the case when the software supplier does not wish to accept any liability. The student cannot release the institution from this liability through a limitation of liability in the acceptance statement or a disclaimer in the software's splash screen (for example).
2. If the service provider also processes personal data, as is the case with cloud services, then the institution must agree separate arrangements regarding what the service provider may do with it. The service provider then becomes a processor under the GDPR.

The arrangements referred to in the second point must be set out in a processing agreement.

32 Article 22 of the General Data Protection Regulation.

Data use by the proctoring software supplier for other purposes
The supplier of the proctoring software may wish to use personal data or (anonymised) data for its own purposes outside the processing agreement. In the case of a data processing agreement, the supplier is not permitted to use personal data obtained under that agreement for its own purposes. This should be excluded contractually. However, it may be possible to generate anonymous data during processing, which may provide insight into the use of the software. This is permitted if this data is only intended to improve the user experience of software, or to rectify errors or bugs in the software.

As a general rule, the supplier is independently responsible for any processing of personal data outside the agreed purposes of the processor agreement. The supplier must have an independent purpose and legitimate basis for such processing.

4.8 Processing in other countries

The GDPR is a European regulation. The European rules state that personal data may only be stored or processed in countries that have an 'adequate' level of protection. This means that the country must have rules similar to the European regulations. One of the reasons for this is to ensure that personal data is protected at a similar level.

Outside Europe
There is no obligation to store personal data in the Netherlands. In principle, every country within the European Economic Area (EEA) offers an adequate level of protection. The situation is more difficult in countries outside the EEA, because there are very few countries that meet the European requirements. At the moment, the EU-U.S. Privacy Shield applies. A decision by the European Court of Justice on the adequacy of the level of protection provided by the EU-U.S. Privacy Shield is expected during the course of 2020.

European subsidiary
A special situation arises when personal data is stored in a European country in a data centre that is managed by a US company or the subsidiary of a US company. The U.S. CLOUD ACT regulates access to electronic evidence in criminal proceedings. The U.S. authorities may request U.S. cloud service providers to provide data that is stored in another country. However, certain guarantees apply in this regard, namely that there is an order issued by an American court. Such an information claim may be challenged by the relevant company or the EU. Subsequently, the U.S. court must consider the interests and decide whether the GDPR or the CLOUD ACT should prevail. At the time of writing (April 2020), it is unknown how such a claim or objection will work.

4.9 Execution of Data Protection Impact Assessment (DPIA)

Data protection starts by identifying the risks to the data subjects. The Data Protection Impact Assessment (DPIA) is a tool which does this. It assesses the effects of data protection. This process, which is required by law, helps to identify and minimise the risks of processing personal data. This risk assessment must be carried out if processing is likely to result in a high risk to the data subjects. The use of online proctoring may also involve the processing of (sensitive) personal data on a large scale. If this is the case, undertaking a DPIA is mandatory.

4.10 Law enforcement

The arrival of the GDPR has changed the enforcement of the privacy legislation. The regulator now has the option of imposing higher fines. The supervisor may impose a fine if an institution does not have adequate security or does not report a data breach. In theory, this fine can be as high as 10 million euros or 2% of annual turnover. The regulator has published a policy on the level of the fines for different types of violations.

4.11 Alternatives to online proctoring[33]

Due to the coronavirus crisis, it is not yet possible to physically go to an education institution to undertake a written or digital assessment. As already outlined in this section, online proctoring can be a proportional tool in this situation, for example on the basis of legitimate interest.

However, the institution must indicate *for each assessment* that there is no suitable alternative for assessing the intended knowledge and skills. It is therefore necessary to first consider alternative solutions to conventional exams. A few options are outlined below.

- The assessment is cancelled. Whether students have mastered the relevant subject matter will be assessed at a later date. This could lead to peak workloads for students, as more of the subject matter will be tested at a later stage. However, this also depends on whether students regularly practise the subject matter during their education.
- The assessment is postponed until it is possible to organise assessments at the education institution. This means that the education institution does not need to take any action in the short term. This solution does, however, result in peak workloads for lecturers and students at a later stage. Students may also experience a delay in their studies.
- The assessment is used in a more formative way and other types of assessment are used during the education itself. The institution adjusts the assessment method to look more closely at the student's efforts and progress rather than at the level achieved. However, whether students have understood the subject matter and how they can apply the subject matter can be monitored. At a later stage, the lecturer will then use a different method to assess whether students can actually apply the subject matter and what level they have achieved. This alternative is in line with the advice that assessment experts such as Dominique Sluijsmans have been issuing for years. Formal testing still does not guarantee the quality of the final level achieved by the student. The education institution will need to implement another guaranteed assessment procedure at a later stage.
- The assessment is carried out at a location where students and lecturers can stay at least one and a half metres apart. This alternative requires a decision to meet physically in order to complete the exam. You will also need to arrange the logistics for distributing and submitting the exams. This could be an alternative for small groups of students in particular, but this is unlikely to be feasible for large groups.
- The test will be replaced by an alternative form of assessment that does not require separate online monitoring. Examples are an assignment (for example, allowing students to develop assessment questions with the answers), a 'take-home' test, an open book exam or an oral exam. From the viewpoint of the exam boards, this option seems attractive because the assessment level is likely to shift more from knowledge reproduction to knowledge production. This is an attractive alternative in itself, because the 'level' of the education and assessment remains the same. However, this does require the efforts of examiners and lecturers. The feasibility depends mainly on the number of students taking a test and, for example, whether another form of assessment is already in the process of being developed. At the same time, the design is expected to require a different type of effort from students.
- The assessment does not change, but it is organised online, without online proctoring. This type of assessment means that lecturers rely on students to take the test without committing fraud. This obviously does not prevent fraud in any way. But there are additional options:
  - Students may be asked to complete an Academic Integrity Statement saying that they will not commit fraud. The effect of this has not been proved.
  - The online assessment has strict start and end times in order to restrict access.
  - A large final assessment is split into several small tests to reduce the impact of fraud.
  - The questions are retrieved from a large item bank or are parameterised so that every student is given different questions.
  - If the student has answered a (closed-ended or open-ended) question, it cannot be changed once the next question is displayed.
  - The time for each assessment question is limited. However, the question here is whether time pressure will not affect the results too much.
  - Open-ended questions are chosen instead of closed-ended questions. These are then checked for plagiarism afterwards.

33 The information in this paragraph is largely based on the guidance document on the safe, reliable and valid completion of summative knowledge assessments by the DKT-FOL Working Group of the Fontys University of Applied Sciences (27-03-2020).

In any case, it is important to realise that the use of online proctoring is one of the alternatives when institutions are unable to organise large-scale exams on-site due to the coronavirus crisis. The solution may be a combination of online proctoring with some alternatives. For example, you can cancel the weekly progress tests or make them formative, you can postpone some exams with a very high (civil) interest, and you can organise the rest of the exams with online proctoring.

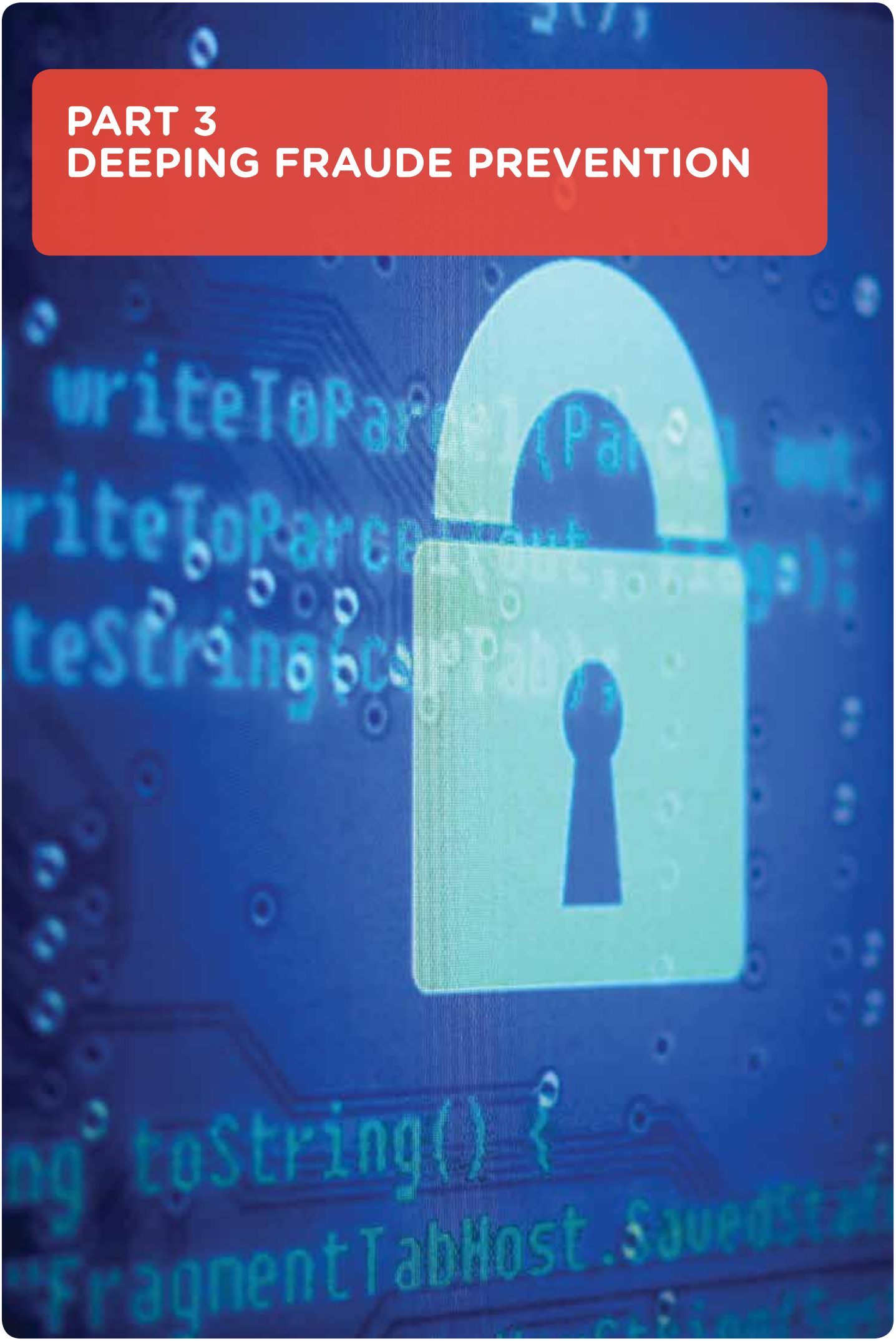
Avans University of Applied Sciences has set up a 'Remote Assessment Decision Tree' that helps to make a well-considered choice in terms of the adjustment of assessments: See also the explanation.

4.12 Specific recommendations

Based on the privacy aspects described in this section, a number of online proctoring best practices have been prepared for institutions:

1. Draft a separate privacy statement for online proctoring and state the purpose in it. Make clear what data will be collected and what will happen to that data.
2. Also state here that data is immediately destroyed if it is no longer necessary. Ensure that both the institution and the supplier strictly adhere to these retention limits.
3. If a legitimate interest is chosen as the legal basis, ensure a well-founded assessment of the legitimate interest in the use of online proctoring, covering the following areas:
   a. The legitimate interest of the institution
   b. The extent to which processing is necessary to protect the legitimate interest;
   c. The extent to which the data subjects' interests or fundamental rights or freedoms are compromised as a result of the processing.
   d. The measures taken by the institution to minimise the damage to the interests or fundamental rights or freedoms of data subjects.
   e. The balancing of items a/b on the one hand and c/d on the other hand.
   f. Please note that the legitimate interest can only be used if there are no privacy-friendly alternatives. You should therefore also explain why these are not available.
4. Agree with the software supplier that it will provide detailed information, even for updates to the tool, so that this can be included in the privacy statement.
5. Supervise the use of the data, ensure that the only people who have access to it are the people who require it for the performance of their duties (for instance the invigilator; it is preferred that the examiners and members of the exam board do not have direct access, access is only granted via the invigilator).
6. Make an option available to download online proctoring data (access request) and, where appropriate, to correct it (in the case of obvious errors).
7. Find out which tools make automated decisions that have a considerable impact on students. Design the process so that the ultimate decision (with legal consequences for the student) is made by a human, and always offer a clear opportunity to raise an objection.
8. Conclude data processing agreements with the suppliers of online proctoring tools.
9. Regularly check the supplier's security audits and reports to ensure that the supplier still complies with the security standards.
10. Prepare a policy to prevent data and security breaches.
11. Respond positively to personal data protection concerns and objections from students, and provide alternatives that will take away those concerns.
12. Ensure that a DPIA is carried out if the processing involves a high risk to the data subjects or if personal data is processed on a large scale.

PART 3
DEEPING FRAUDE PREVENTION



5. SECURITY AND ANTI-FRAUD MEASURES

Security and fraud prevention attract a great deal of public interest, but at the same time they are difficult subjects. The higher the security requirements of an examination, the more expensive and more impractical it will often become, and the greater the impact will be on the privacy of students. Even a regular exam hall is not 100% secure, but since education institutions and exam boards have a lot of experience with this, they assume that they know the risks well and that fraud is being countered in an acceptable manner.

This section describes the various solutions that online proctoring software offers to prevent fraud. It also looks at the ways in which students may try to commit fraud. Based on this and together with the assessment security selection model in section 5.4, an exam board can assess whether online proctoring is suitable for particular assessments or exams.

5.1 Preventing fraud

Preventive effect of online proctoring
Online proctoring offers various means to increase security and prevent fraud. Just the announcement that online monitoring is taking place will reduce any tendency to commit fraud. This announcement lists all kinds of methods and measures to discourage fraud as much as possible. After all, the more measures are taken, the more effort a student will have to make to secretly commit fraud. The reasoning is that the more effort it takes, the less fraud will happen. This form of fraud prevention is almost identical to conventional prevention when testing on site.

At the same time, certain testing methods are already being used in the field where supervision is in fact limited, sometimes due to a lack of alternatives. Consider the use of video conferencing tools for supervision. During the coronavirus crisis, these are sometimes assessed as acceptable, simply because the institution has no alternative available.

The preventive aspect of online proctoring is often not included in the discussion about online proctoring. Advocators of online proctoring believe that this does not give rise to a valid discussion on this subject.

Cameras and microphones
Almost all proctoring software allows the proctor to watch over the exam via the student's webcam. There are also variants that use two webcams. The second webcam is often provided by a phone or tablet that must be placed behind the student. This ensures that a larger part of the space is visible and gives the proctor or reviewer a view of the student's screen and keyboard. The second webcam can also be used to check that the student is not wearing earbuds, for example.

Facial recognition technology
Some proctoring software providers use facial recognition technology to authorise students. That takes us into the field of automated processing of biometric data, similar to fingerprint recognition. Facial recognition technology can be used to verify with high certainty that the student whose biometric data is known in the system is actually sitting in front of the screen during an exam. This technology is controversial. It is a very potent tool to deploy, with far-reaching consequences in terms of privacy.
The same applies to keystroke dynamics. It is not only what a user types (a password) that can identify someone, but also the way in which they type it[34] [35]. This is also a form of automated biometric identification and therefore a very powerful tool[36]. Neither facial recognition technology nor keystroke dynamics technology are used in higher education systems in the Netherlands for reasons of 'privacy impact reduction'.

One form of environmental, visual and postural recognition technology that is applied uses recognition *without* identification or authorisation. The software only "detects" that a person is in the picture, but does not know which person this is. This technology therefore has a far less far-reaching impact on privacy, and it is questionable whether this should be considered as the processing of biometric data. For example, comparing those images with other images of persons who are taking the test allows deviating behaviour to be observed and the system to report this deviation.

Screen capture
Another method that almost all suppliers use is that the invigilator can use screen capture to check what is happening on the student's screen. The invigilator can then see what programs are open and whether the student is secretly using any prohibited sources.

Lockdown browser
The 'lockdown browser' is a feature that is not only used for online proctoring, but also in other forms of digital assessment. Only the assessment environment and specific, authorised applications can be used. The options can vary from one supplier to the next.
It is important not to overestimate this feature. The fact that someone can't start other applications does not mean that they cannot run them in the background. With sufficient ICT knowledge, lockdown browsers (on own devices) can also be bypassed. This does not make it completely useless, but for online proctoring it should be seen as complementary to screen capture, the logging of consulted sources and systems and camera images. Please also note that one student with sufficient ICT knowledge can develop software that can then be used by thousands of students worldwide. In short, not every individual fraudster needs a high level of ICT knowledge by definition.

PC logging
Some proctoring suppliers allow you to see in quite some detail what is happening on the student's computer. The extent varies from one supplier to the next, but the potential is huge. This allows current processes to[37] be scanned and parts of the memory to be read. This requires access to certain components of the PC's system. As the computer used is often the student's private laptop, the software also gains access to many of the student's irrelevant personal data. As a result, this is also considered overkill. It must be made very clear in a document such as the privacy statement which data is being collected and what is done with it. If the supplier is sufficiently transparent about the operation of the logging, the use of this method may be acceptable, according to the basis for the data processing.

5.2 Online proctoring risk factors

A student can attempt to commit fraud in a variety of ways. The list below is certainly not exhaustive, but gives an indication of the possibilities. For each fraud method, we indicate whether it can be combated by online proctoring and, if so, how.

34 Jiexun L., Rong Z. and Hsinchun C. (2006). 'From fingerprint to writeprint'. Communications of the ACM, Volume 49 Issue 4. Available at http://www.disciplineoforganizing.org/wp-content/uploads/2013/01/FingerprintToWriteprint.pdf.
35 This might include the speed at which the person types, the letters that slow them down and how long they hold down keys. For more background information, see: https://en.wikipedia.org/wiki/Keystroke_dynamics.
36 'Keystroke dynamics' does not mean that someone can be recognised with absolute certainty. It is, however, getting better and better at detecting *someone else* at the keyboard. If the student's keystroke dynamics are known, the software can issue an alert that the person sitting the exam is *probably* not the student who should be sitting the exam. This could prompt a thorough review of the camera images.
37 These might be applications that remain open, even if only in the background.

Hardware and software

In online proctoring, students use their own PC or laptop. This could be used to commit fraud in various ways.

- *Separate programs are developed to bypass the proctoring software.*
  In the gaming industry, developers are experiencing huge problems with software that is developed to make it possible to cheat. As online proctoring is applied on a larger scale, a market will emerge for similar software seeking to circumvent online proctoring.
  - That means that suppliers of online proctoring software must develop detection software, which will then be circumvented again by the malicious parties.
  - Despite investing millions, game developers have still not won this battle. The question is therefore whether this will ever be successful for online proctoring (as the importance of the fraud is much greater there).

- *An extra browser or tab*
  Perhaps the best known method of fraud is to try to find answers on the internet during the exam.
  - Countermeasure: this form of fraud is easy to combat. Screen captures and an extra web-cam resolve this. A good lock-down browser is also often sufficient.

- *A second person monitoring or controlling the PC.*
  Just as an online proctor can monitor the PC, a student can give someone else remote access to their PC. This other person can then see their screen and even control the keyboard and mouse, which means they could complete the exam while the student is still sitting at their PC.
  - Countermeasure 1: if the proctor can see the student's keyboard and mouse then this would be detectable, the movements would not match what is happening on the screen. However, the likelihood that a proctor would notice this is quite small[38].
  - Countermeasure 2: if a student has to 'fake' that he/she is actually taking an exam for a whole hour, some deviating would soon be observed.
  - Countermeasure 3: only good logging software can combat this. This software can see in detail what software processes are running on a PC and what external connections are being made.

- *Software that provides answers*
  A student could install software that scans the questions on the screen and looks up the answers. The software could show the answers on the screen, or possibly even complete them directly.
  - Countermeasure 1: if the answer is clearly displayed on the screen, this would be easily detected using screen captures.
  - Countermeasure 2: it is more difficult to detect when the software is directly completing the answers. In that case, only good logging software would provide a suitable solution.

- *A virtual PC*
  A virtual PC is a simulation of an extra PC hosted within the usual computing environment. If the exam is taken within the virtual machine, the proctoring software will only see that PC's screen, and the software running on the host PC would be invisible. This opens up many of the previously mentioned and resolved fraud options again.
  - Countermeasure 1: if the use of a virtual PC during the exam is prohibited, it is possible to detect this using advanced software. However, this is not possible for all hardware and virtualisation software, and cannot be detected with proctoring software that is running in a browser.
  - Countermeasure 2: a second camera positioned behind the student would also help, because the screen would be in full view. This would prevent part of the fraud, such as having extra windows open. However, this would not detect any software running entirely in the background.

38 It is possible to disable the local keyboard so that the student can type without anything happening on the screen. If they type approximately in sync with the person completing the answers for them, then this would be difficult to detect.

Help in the environment

• *Another person in the room*

If there is another person in the room, the person sitting the exam could consult with them (either verbally or using gestures).

- ⊘ Countermeasure 1: a microphone would be partly able to detect this if the two people were speaking to each other. This would make it relatively complicated for the student and the other person to communicate. This is also standard practice for all proctoring software.
- ⊘ Countermeasure 2: the use of cameras would of course help. The student often has to show the entire room to the camera before the exam starts. But a second person could hide outside the field of view, especially when only one camera is used. They could give instructions by means of gestures or notes.[39]

• *Someone else using the PC*

Just as in a regular exam setting, attempts are sometimes made to have someone else sit the exam.

- ⊘ Countermeasure: ask someone to confirm their identity by showing their student card or identity document to the webcam. This is in fact standard practice and this risk can therefore be ignored.

• *Hidden crib sheets*

Crib sheets are regularly used in normal exam halls, and this is likely to increase when students take their exams at home.

- ⊘ Countermeasure 1: the use of crib sheets cannot be eliminated entirely. Camera images can help combat this, especially if a good and thorough check of the entire room is made before the exam. The room will never be fully visible during the exam, and hidden crib sheets remain a possibility.[40]
- ⊘ Countermeasure 2: ask the student to use a hand mirror to show the edges of the screen via the webcam (in order to be able to observe any sticky notes).

• *Remote monitoring by a third party*

We have already discussed the possibility of detecting someone using software to monitor the PC remotely. However there are other ways to monitor exams, such as placing a separate camera (in a phone or tablet) behind the student or using a so-called button camera on clothing. It is also possible to split or intercept the video output signal[41].

- ○ No countermeasure possible: when executed well, this method cannot be detected (a small camera is easy to hide between a row of books). The challenge for the student is then to ensure that someone else can send the answers. Here, the same applies as for crib sheets: this can always be hidden, as the entire space is never visible. This form of fraud is very simple, especially in case of multiple-choice exams, since very little information needs to be passed on (the number of the answer)[42]. However, this type of fraud can be complicated by randomising the answers.
- ○ However, the effect of this type of fraud can be counteracted by using open-ended questions with relatively long answers rather than multiple-choice questions. An additional combination with an open book exam format can be used. The longer and more extensive the expected answers are, the more difficult this type of fraud becomes.

5.3 So what does this mean?

A little creativity can result in a considerable list of fraud opportunities in online proctoring.[43] Based on the examples in this section, a number of conclusions can be drawn:

39 This would be easiest to do if the second person could see the screen, but even if this were not possible, the student could speak out loud every now and again. It is difficult to ban talking altogether because some people like to think out loud.

40 It is easy to imagine plenty of ways to conceal a crib sheet during a room inspection, only to make it visible again during the exam. For instance, it could be covered up with something that can be removed using a thin piece of string. This is almost impossible to detect as long as the crib sheet's location remains out of shot during the exam.

41 This can be done using a small box positioned between the PC and the monitor that cannot be detected by the PC. The signal can then be sent to another person either via a cable or wirelessly.

42 For example, the student could be hiding four small lights in his or her room that are controlled by the person helping him or her. Each light would correspond to an answer, either A, B, C or D. There are dozens of surreptitious communication methods that are difficult or impossible to detect.

43 See for instance: http://madebyknight.com/knuckle-scanners-cheating-how-to-bypass-proctortrack/.

- Fraud involving manipulation of the hardware or software can usually be detected. Although this will soon have a greater impact on students' privacy, this may be necessary if no suitable alternative can be achieved (as may be the case during the coronavirus crisis).
- As long as the education institution has no control over the space where the exam is taking place and the student's computer, there will always be ways to commit fraud without detection being possible. In theory, all other exam hall factors can be simulated in exams on the institution's PCs, including online proctoring. Therefore, the maximum fraud resistance level of online proctoring is always lower than the maximum fraud resistance level of assessments in an exam hall.

Despite this, online proctoring is certainly useful as a resource that can be used to facilitate the organisation of digital exams in certain situations. However, it is important to make a well-founded decision that weighs up both the importance and the risk of the specific exam, as well as the benefits.

To help exam boards or assessment boards reach a decision for each situation, SURF has developed an assessment security selection model. This is described in the next section.

5.4 Assessment security selection model

To determine a suitable method for organising digital assessments – from 'bring your own device' (BYOD) to online proctoring or using your own computer rooms – the importance ('stakes') attached to a specific test is usually considered. Often only two levels are known: high stakes and low stakes exams. This results in a lot of nuance being missed:

1) All summative exams are regarded as high-stakes exams, including both interim tests and final exams.
2) No distinction is made based on the assessment format (multiple choice, oral exam or essay) despite the fact that this has a major impact on the suitability of different assessment methods.[44]

To enable a more nuanced consideration, SURF has developed a model in which both the risk of fraud and the importance of the exam result are taken into account. This model is not only suitable for online proctoring, but it can be widely used: it can help exam boards and test committees to determine whether the intended assessment situation is adequate, or to see which assessment methods would be suitable within the curriculum.

5.4.1 The importance of the exam

The selection model identifies four levels to indicate the importance of an exam:

- *Low*
  These are formative exams or online courses with no recognised social value. This might include MOOCs, such as courses by Coursera or programmes offered by the University of the Netherlands.
- *Medium*
  At this level, the exams do not directly contribute (significantly) to the grades list, but there are still consequences attached to them. Some examples are small weekly interim assessments that can yield one extra point together, or assessments that give students access to a module, exam or work placement.
- *High*
  These are exams that have a direct and significant impact on the student's study credits. This will apply to all exams for modules that attract study credits, but also to partial examinations that contribute towards the final assessment.
- *Very high*
  This category includes specific modules or tests which demand higher fraud prevention standards due to the nature of the courses or certain[45] (legal) consequences, such as assessments that would then allow you to work as a solicitor or in the judicial system (civil effect) or assessments for attaining BIG registration[46].

44 This is because the risk of fraud is much greater with multiple choice tests than in an oral exam.
45 These may be requirements imposed by the exam board, but may also ensue from the general wishes of society at large or from legislation and regulations. The ultimate assessment, however, will always be made by the exam board.
46 The register of professionals working in the healthcare sector. Only registered persons are authorised to practise their professions. See also: https://nl.wikipedia.org/wiki/BIG-register

It may also include exams that are very important for other social reasons, such as the CITO exam, final exams in secondary schools or language and maths tests for PABO (basic teacher training). Graduation assignments also come under this category, as they determine whether or not the student is awarded a diploma.

5.4.2 The risk of fraud

The selection model identifies three levels to indicate the risk of fraud in relation to a particular exam:

- *Low*
  This is an exam where the student submits an entirely unique work, such as a thesis, essay or practical assignment. However, this also includes practical assignments. In these cases, fraud prevention focuses on detecting plagiarism and establishing that the student has done the work themselves.
- *Medium*
  An exam requiring unique answers, but which is not entirely the student's own work (as with a thesis or essay). This may be a written test with open-ended questions, where the answers are of sufficient length to be unique to each student. This might be a test requiring advanced mathematical calculations on paper, or where answers have to be substantiated with extensive text.
- *High*
  Exams in which only a single answer is possible, and in which students in most cases do not give unique answers. This includes all closed-ended questions, including multiple choice.

5.4.3 The selection model

The selection model is based on the allocation of risk and importance, as described above. The model below has been partially completed to illustrate how it can be used. Every exam board or assessment board can adapt it to their own context. When doing so, they should also take into account the context of the curriculum. For example, if certain knowledge is assessed multiple times during a study programme, the exam board may attach less importance to an earlier test than to a later test. After all, the knowledge would be retested and a student committing fraud would then find themselves caught out.

For each combination of importance and risk, the model indicates the corresponding security level. This may mean, for instance, that a selection is made between different forms of online proctoring, or that a decision is made between BYOD and a fixed configuration for digital assessment.

In the case of online proctoring, four levels have been identified:

- *Level 0:* Online conferencing software with up to 10 students;
- *Level 1:* Record & review, screen capture, one camera and logging websites;
- *Level 2:* Record & review, screen capture, one camera, computer lockdown capabilities and website & application logging;
- *Level 3:* Live proctoring with computer lock-down capabilities and full computer activity logging[47], or record & review that includes a second camera and the same features.

In some areas of education (associated with both high risks and a high or very high level of importance), the security of online proctoring also carries even greater risks where live proctoring is chosen. In such cases, a different assessment method could be chosen in order to reduce the risk of fraud. That might be a well-equipped computer lab, or possibly a secure form of BYOD exam within the institution's own exam hall.[48]

Institutions can also always fall back on the highest level of security: an exam hall with paper assessments. Please note that an exam hall is not 100% fraud-proof either, and not every exam hall is the same. A bad exam hall with too few invigilators may be less fraud-proof than good online proctoring. For the best comparison, we should also define different levels of exam halls.

47 Including computer logging of websites, applications and background processes.
48 The possibilities and security of BYOD solutions or existing computer labs were not examined for the purposes of this white paper. However, in these situations the institution does have control over the environment (the weak point in online proctoring), so they can probably be made more secure than would ever be possible with online proctoring.

However, that is not SURF's expertise. It is up to the education institutions to develop this. The selection model therefore does not state that every exam hall is more secure than online proctoring, but that the *maximum* level of security of online proctoring is inherently lower than the *maximum* security level of an exam hall.

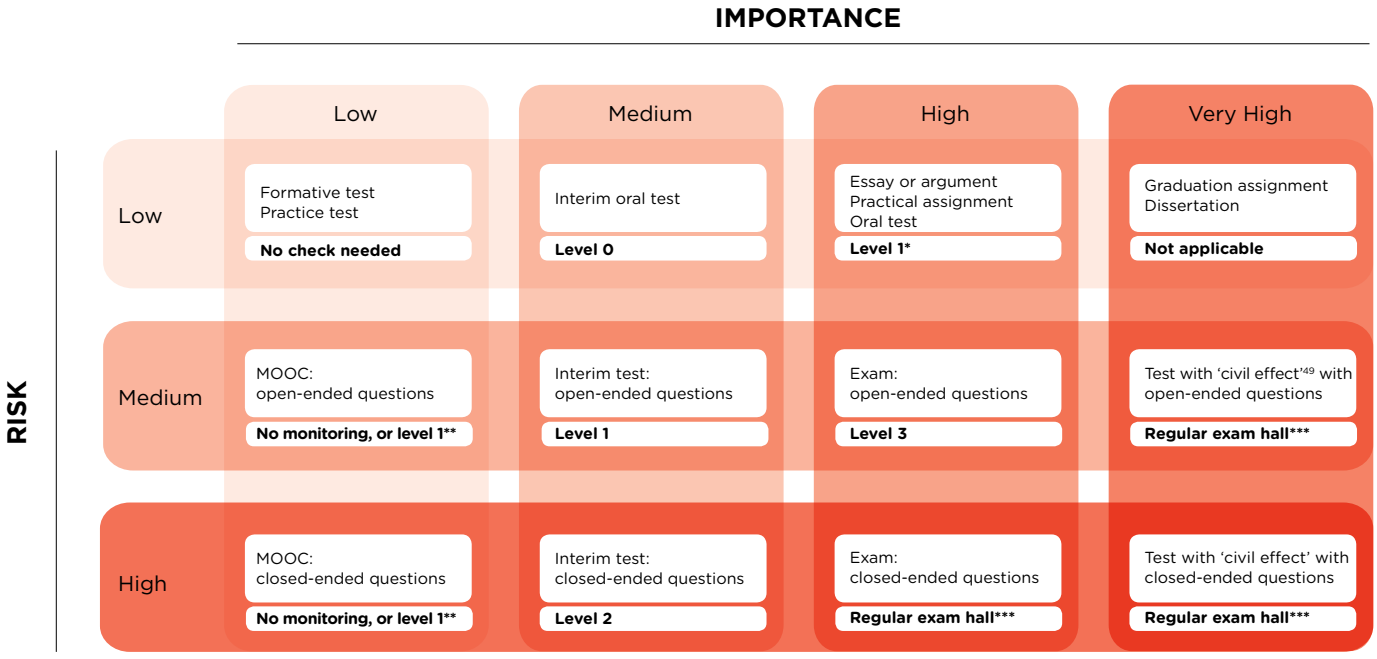
The coronavirus crisis may make the use of exam halls impossible. In that case, the exam committee will have to estimate which form of assessment is appropriate in their opinion. This could be live proctoring – the most fraud-resistant form of online proctoring – or an adjustment of the assessment format, for example open-ended questions instead of multiple choice questions. The same applies to the choice of security level for the proctoring.
The desired form of online proctoring may not be available based on feasibility, technical possibilities and other practical factors. The education institution may then choose to use a lighter form of proctoring to ensure that the exam can go ahead. This could be live proctoring – the most fraud-resistant form of online proctoring – or an adjustment of the assessment format, for example open-ended questions instead of multiple choice questions.

The same type of consideration applies to the level of proctoring. The desired form of online proctoring may not be available based on feasibility, technical possibilities and other practical factors. The education institution may then choose to use a lighter form to ensure that the exam can go ahead. In that case, education institutions will have to be aware of the increased risk. This risk increases as online proctoring is applied over time and on a large scale, as the likelihood of software being developed and distributed to circumvent online proctoring increases.

However, alternative forms of exposure with a low impact on privacy and a lower risk of fraud will also have to be considered. The technical capabilities of the student and of the providers of the assessment application and proctoring software will also need to be taken into account.

However, if it is not possible to replace an closed-ended questions exam with an open book exam for example, the highest possible level of security will have to be applied.

Model of choice for safe assessments



* Naturally, online proctoring is unsuitable for essays and work performed over long periods of time. It is particularly suitable for verbal exams with a limited duration (for example up to 3 hours).
** For MOOCs, this depends on the value placed on the MOOC.
*** During the coronavirus crisis, level 3 may be a solution if exam halls are not available. It is then up to the exam committee to consider the risk of fraud.

49 For instance, authorisation to enter professional practice as a lawyer or in the judicial system.

CREDITS

Author
Lex Sietses (SURF)

Contributions by
Cora Arts (Privacy Company)
Willem Brouwer (Amsterdam University of Applied Sciences)
Natasa Brouwer-Zupancic (University of 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 (University of Amsterdam)
Anne Martine Koetsier (Privacy Company)
Roos van Leeuwen (LSVb National Student Union)
Rolf Marteijn (Wageningen University and Research)
Alf Moens (SURF)
Annette Peet (SURF)
Wilfred Rubens (SURF)
Guusje Smit (University of Amsterdam)
Sebas Veeke (SURF)
Marja Verstelle (Leiden University)
Jenny de Werk (SURF)
Ulrike Wild (Wageningen University and Research)

Editing
Erik van der Spek

Design
De Hondsdagen, Bunnik

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

SURF
www.surf.nl/onderwijs
onderwijsinnovatie@surf.nl

Disclaimer
This publication has been compiled with the greatest of care. Despite this, no rights can be derived from the contents of this publication.

April 2020

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