

Privacy in Online Proctoring

What is Online Proctoring

Online proctoring offers an examinee the possibility to take an exam remotely. Online proctoring solutions have to ensure the integrity of the examination which eventually serves to certify an examinee's competence. Through online proctoring, for example, entry tests to educational institutions can be offered to potential students regardless where they are based. For candidates, taking an exam remotely decreases costs and offers exponentially more chances to seek admission. Ultimately, online proctoring is about access to education.

Online proctoring has to be conducted in a fraud-proof but privacy respecting manner. Let me start explaining the methods used to ensure the integrity of online proctoring. In order to detect and prevent fraud during an exam, it is necessary to remotely identify a candidate and monitor the exam process. Imagine, that a live proctor monitors the actual exam at a distance through two simultaneous video streams. The candidate simply sets up the webcam of the laptop, the mobile phone camera that monitors the surrounding and the laptop shares the screen during the exam with the live proctor.

Bearing all this in mind, the candidate and the educational institutions can reasonably expect that online proctoring conforms with the law and best practices of data privacy protection and security. It is possible to guarantee the candidate's interests in a fair and privacy respecting exam without compromising the adoption of online proctoring solutions. Note however, that every instance of online proctoring needs to be assessed on its own merits and in light of applicable law.

Online proctoring and data privacy protection step by step

The process of online proctoring necessarily involves the collection of a candidate's personal data, which triggers the application of European Union (EU) data protection laws. Moreover, it is important to recognize that in EU law the protection of privacy and personal data are protected as fundamental rights. This, from the outset, puts a high bar for online proctoring's legal compliance. Let me walk you through how online proctoring can be designed to comply with EU data protection law, which is certainly one of the strictest regulations by comparison worldwide.

EU data protection law is based on a number of principles and, this may sound strange for non-EU providers but, every instance of processing of personal data requires a legal basis. The online proctoring provider performs its role as an agent for the educational institution. In other words, the legal bases can be derived from the relationship between the candidate and the educational institutions. The provider of online proctoring facilitates the exam in line with the instructions of the educational institution.

All activities and responsibilities are formalized in a contract between the educational institution and the online proctoring provider. Legal obligations with the exam candidate mostly arise with the educational institution, unless the online proctoring provider deviates from the contract. In that event, the online proctoring provider would become directly liable under the data protection law itself.

Another principle of the law is to minimize the collection of personal data to what is essentially necessary to perform the task at hand. For online proctoring, it implies to reduce as much as possible the data trail after an exam has been validated. For this reason, educational institutions in Europe are not interested in a record of the online exam, but the verification of the integrity of the exam situation. Only in the rare event that there is a suspicion of an exam fraud, a video record would need to be preserved.

What can make online proctoring particularly challenging is that video may reveal individual aspects, such as race and gender, but also religion or health of the candidate. Such individual aspects are especially protected under the law and require additional safeguards. Educational institutions are in charge of obtaining the requisite consent of the candidates, which can be embedded in the process of online proctoring. Note however that there must be an alternative for candidates to take the exam nevertheless.

The responsibility of the provider of online proctoring requires that there are organisational and technical safeguards to ensure an adequate level of data security. This means in particular that the architecture and back-end of online proctoring conforms with best practises in data security. In its most basic form, it involves encryption, regular security updates and access controls.

Exam candidates have several rights that they can invoke against the educational institution, such as:

- the right to access their personal data;
- the right to demand rectification and erasure of their personal data;
- the right to restrict the processing of their personal data.

Think of a candidate who asks the educational institution for his data, note that he or she doesn't need to give a particular reason for this. The provider of online proctoring has to assist the educational institution to turn over the personal data that have been processed for online proctoring.

What will change with the upcoming GDPR?

In order to catch up with technological developments and the prevalence a data driven business models, a new General Data Protection Regulation (GDPR) will enter into force in May next year. In many ways the new law will continue the approach of its predecessor, but a few important changes should be highlighted. At the outset the new regulation has much more teeth with sanctions that can amount up to four percent the annual turnover of the organisation handling the personal data.

Now, compliance has to be more thoroughly demonstrated through documenting all steps that would lead to a lawful processing . This means educational institutions should be able to show how a certain processing activity is aligned with the GDPR. A privacy impact assessment may be required for new online proctoring technologies. The results of the assessment should be taken into account from the start of development, ensuring that the processing of data is kept to a minimum of what is necessary (privacy by design).

Under the new law algorithmic decision-making and profiling is much more regulated. In relying on a live proctor, the monitoring of the exam process is presently not delegated to algorithms. Were this to change, a more careful approach should be taken when developing algorithmically controlled online proctoring.

All in all, online proctoring offers educational institutions more options in conducting exams and candidates the flexibility to sit exams when and wherever they are ready. Take as an example the global audience of Massive Open Online Courses (MOOC), which candidates can now conclude with an accepted examination. Or, the situation of a professional taking distant learning courses who is now able to sit an exam on the weekend. European universities are conservative institutions, but willing to rely on online proctoring solutions if they can not only deliver exam integrity and full EU data protection compliance. This is possible.

If you have any (legal) questions about online proctoring you can e-mail directly to y.fouad@posteo.nl .

Youssef Faoud

BIO: Youssef Fouad is an expert in telecoms and privacy law. Based in Amsterdam, he advises ProctorExam about personal data protection. He is legal counsel at COIN, the Dutch association of telecoms providers. He studied information law at the University of Amsterdam.

Picture

