Privacy & Online proctoring

Important aspects to keep in mind

citrus andriessen

GDPR

- Online proctoring involves collecting personal data, thus the GDPR applies.
- Processing personal data requires a legal basis: consent from the examinee and legitimate foundation from the (exam)institution.
- Video recording contains special personal data (gender, race, religion). Collecting these data requires additional reasons of using and additional safeguards. This should specifically be mentioned in the consent form and be well implemented in the procedures of the (exam)institution and proctoring service provider.

Consent must be

- Given in freedom: refusing consent must be without significant consequences. A student must still be able to take the exam. Also create an exam that does not rely on recording and storing personal data.
- Formulated specifically: what's the purpose, what data will be collected, how long will it be stored, how can consent be withdrawn and what are the consequences of withdrawal?
- Given before starting the examination.
- Able to be withdrawn at any time to prevent further processing of the data.

Collection of personal data

- Collection of personal data should be minimized to what is necessary to perform the task i.e. the verification of the exam situation.
- Only when fraud is suspected, a video record will be preserved. After an exam has been validated all proctoring related data must be removed.
- Perform a Data Protection Impact Assessment (DPIA/PIA) before starting with online proctoring to mitigate privacy and security risks.

Online proctoring provider

- Must destroy the collected data as soon as the exam results have been finalized with a maximum retention period of 30 days after recording.
- Must have organizational and technical safeguards to ensure an adequate level of data security.

Candidate has the right to

- Access their personal data without specific reason.
- Demand rectification and erasure of personal data.
- Restrict the processing of their personal data.

The (exam) institution must

- Make data processing agreements with the processor. The processor is responsible for processing data according to regulations, can't use data for their own purposes and must provide detailed information about the tool and the security measures taken to ensure safe data processing.
- Create a policy to prevent data leaks and security breaches.
- Supervise the data and ensure that only authorized people have access to the data.
- Inform and instruct all users about the policies and procedures.

Inform candidates well

- That they will be recorded as well as their screen.
- To cover Social Security and other privacy related data on their ID.
- That they need to hide or remove private objects before taking the exam.