A Lawful basis for online proctoring

Youssef Fouad[1], Arno Lodder[2], Jessica Hrudey[3], Silvester Draaijer[4]

[1]PwC, [2]Vrije Universiteit Amsterdam

OP4RE Online Proctoring for Remote Examination

What is Online Proctoring for Remote Examination?

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.

General Data Protection Regulation

Online Proctoring necessarily involves the processing of personal data, triggering the application of European Data Protection Law. At a glance, the *main rules* following from EU data protection law are:

- Lawfulness, fairness and transparency of the processing of personal data;
- Purpose limitation;
- Data minimization;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality.

(Special) categories of Personal Data

Online proctoring involves the processing of the following categories of personal data:

- video footage of the examinee;
- photo of the examinee;
- Government issued ID-card (containing a government issued unique identifier (eg. a social security number)).

These categories of personal data may be considered to be a *special category* of personal data because based on this date it is possible to determine:

- Race of the examinee;
- Religion of the examinee;
- Health-related information (handicap, glasses) concerning the examinee.

Video footage of the examinee can also be considered to be personal data where there is excess information captured from the surroundings/ background of the examinee (eg. captured footage of the home environment, revealing unique characteristics of the particular examinee). Additionally, in some EU-countries, the processing of government issued unique identifiers receive special treatment under the law and in some cases can only be processed if there is a legal reason to do s

As mentioned above, the GDPR contains a detailed regime for processing special categories of data (also called 'sensitive data' (see article 9 GDPR)). Exampled of sensitive personal data are data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union membership as well as for processing genetic and biometric data for the purposes of uniquely identifying a natural person (via technical means), and for data concerning health, a person's sex life or sexual orientation. The processing of sensitive personal data is prohibited in principle, unless exemptions apply or there is a legal obligation to process the data. A example of the latter is:

- Data subjects give their *Unambiguous consent freely*
- A national law provides an exemption, see for example article 25 of the Dutch Implementation Law of the GDPR (UAVG) in which it is stated that:
  - The processing of sensitive personal data (revealing racial or ethnic origin) is *not prohibited* when, for the purposes of identifying the data subject, the processing of personal data revealing racial or ethnic origin is *inevitable.*

Description of purpose(s) of the processing

In order to **detect** and **prevent** fraud during an exam, it is

1. **necessary** to remotely **identify** a test-taker and
2. **monitor** the exam process.

The processing of the data mentioned above *is strictly necessary and inevitable* for these purposes.
Data which is not relevant in order to achieve the aforementioned purposes are not be processed.

Possible Lawful basis

(green is well possible, orange is possible under conditions, red is not possible)

	Public Body (for example a Higher Education Institution	Private Company (for example a test publisher)
Consent		
Performance of a contract		
Legal obligation		
Protecting of vital interests		
Public interest and exercise of official authority		
Legitimate interest		

Definitions

- HEI: Higher Educational Institute
- Data Subject: the test-taker providing data
- Data Controller: the HEI processing the personal data
- Data Processor: a third party collecting and processing the data on behalf of the Data Controller - with online proctoring this is the online proctoring system provider.
- Data Protection Officer of the HEI: responsible for overseeing and ensuring compliance of the data protection issues of the HEI
- Data Protection Authority: the national authorities to which Responsible parties need to report to in case of, for example, data breaches or complaints by data subjects.

Categories of (Personal) Data involved

- Personal data: every type of information related to an identified or identifiable person;
- Special categories of personal data: personal data that fall under a stricter regime for processing (see above);
- As a note - Biometric data: Physical, physiological or behavioral characteristics of an individual, which are processed with technical means in order to identify that particular individual. Examples are: voice (recognition), typing behavior (recognition), iris (scanning and recognition), fingerprint (scanning and recognition). *In most proctoring situations, nog biometric data is involved as assessment of data is based solely on* ***human intervention***.

Contact

Youssef Fouad
Arno Lodder
Jessica Hrudey
Silvester Draaijer

Vrije Universiteit Amsterdam
De Boelelaan 1105
1081 HV Amsterdam, The Netherlands
www.onlineproctoring.eu

Define Use Case Precisely

The following template can be used to define the use case at a given institution. Based on the use case, the appropriate lawful basis and measures to protect data can be better defined.

Template:

- The data controller (HEI) has status X (public vs. Private instituition) and is located in Country Y.
- The test-taker (data-subject) is located in Country Z.
- Personal data is (not) processed A) with/out *technical means (*implying the use of biometric data*) AND/OR* based on *human intervention*.

Example
- The data controller is a Public University (HEI) according to the Dutch 'Wet op het Hoger Onderwijs' and is located in the Netherlands.
- The test-taker can be located in any country of the EU/EEA and or countries with an adequate level of data protection as determined by the EU Commission.
- Personal data is (not) processed with *technical means,* but authentication and proctoring is fully based on *human intervention*.

Provide Arguments for the Lawful Basis

Example continued:

Consent deemed not appropriate

- Freely given consent, requires that consent can be freely revoked. However, if the test-taker withdraws his or her consent before the review of the examination by data controller has been concluded the examination process is hindered.
- Freely obtained consent may not be possible because the test-taker may feel that there is an imbalance of power between him/her and the data controller.

Contract deemed not appropriate

- The data processing that online proctoring entails is not strictly necessary for the performance of the contract between the test-taker and the data controller.

Legitimate interest deemed appropriate

- Article 6 (1) (f) of the GDPR may be deemed appropriate, as it provides that personal data may be lawfully processed if it is strictly necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (test-taker) which require protection.
- In the Netherlands in response to this prohibition to process special categories of data states in article 25 of the Dutch Implementation Law of the GDPR (UAVG) that:
- *The processing of sensitive personal data (revealing racial or ethnic origin) is not prohibited when for the purposes of identifying the data subject the processing of personal data revealing racial or ethnic origin is* ***inevitable****.*

Interests:

Controller (HEI)

- To make education more accessible for test-takers by offering them exams remotely via online proctoring.
- Prevent and detect fraud in remote exams via online proctoring (also see recital 47 of the GDPR, stating purposes of preventing fraud are deemed to be legitimate interests).

Data subject (test-taker)

- Special and sensitive personal data not being processed illegitimately (see below)
- The data-subject (test-taker) has the opportunity to opt-out of a remote exam; i.e. exams can be taken onsite at the HEI instead.
- For test-takers, taking an exam remotely decreases costs and offers exponentially more chances to seek admission and lowers the bar for access to education.

Third parties

Other test-takers

- by ensuring the legitimacy of exams, which in turn ensures the legitimacy of degrees obtained by third parties even when they are remotely obtained.

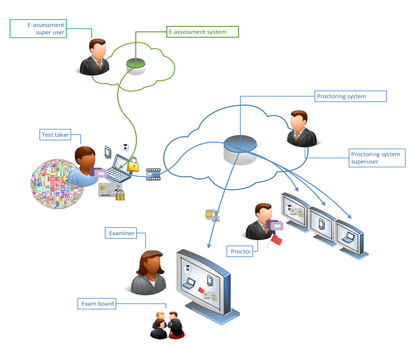
Describe System, Threats, Impacts and Mitigations (DPIA elements)

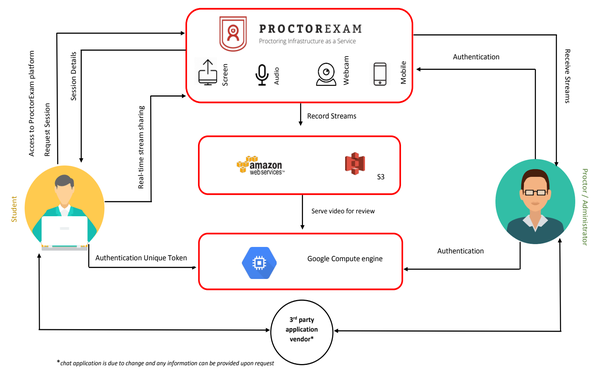
Example continued:

Data minimization:

- All recordings are destroyed after 7 weeks
- Only data that are required to prevent fraud are processed; no other data are processed

Category (sorteer hiernaar)	Phase	Type of Risk	Risk for	Risks/Threat description	Direct consequence	Impact	Controls/Measures mitigating the risks: What can the Candidate do?	Controls/Measures mitigating the risk: What can the Proctoring company and institution do?
A. Illegitimate access	Exam	Fraud Data Protection	Candidate	Theft or redirection of tests during session (Man-in-the-middle/browser attack): session is intercepted by other person changing the answers.	- Can be an incidental fraud occurence. - Can be a systematic fraud occurence if attack method is posted online and easy to execute by 'normal' Candidates.	idem - If this illegal behavior of Candidates gets out into the media, serious deterioration of brand image of the HEI.		- Proctor Provider follows the guidelines, (in particular top 10 guidelines) of OWASP. - Proctor Provider keeps track of complying with OWASP guidelines as can been found in this online document .... - Proctor Provider performs a regular penetration test.
A. Illegitimate access	Exam	Privacy	Candidate	Proctor can see what the Candidate does on the Candidates computer or mobile device after the exam, because screen sharing remains on or the ProctorExam App is not closed.	- Can be an incidental individual violation of rights and freedom if a proctor watches by coincidence. - Can be an incidental but systematic violation of rights and freedom if a proctor by uses video for others purposes than to prevent fraud. - HEI: Obligation to inform Candidates and the National DPA of the illegitimate access. Deterioration of the brand image.	idem - If this illegal behavior of proctors gets out into the media, serious deterioration of brand image of the HEI.	Read and follow-up detailed instructions to: - Double check to close the proctoring session by closing the Browser. - Disable/uninstall all proctor software after the exam.	Have the proctoring personnel read and follow-up detailed instructions to: - avoid reviewing video footage after having ended the exam. - destroying the video as soon as possible, as soon as the exam results are determined and fixed.
A. Illegitimate access	Exam	Privacy	Candidate	Unwillingly sharing of confidential details in de webcam video (e.g. objects in the home environment) or in the screen recording.	- Can be an incidental individual violation of rights and freedom if a proctor watches by coincidence. - Can be an incidental but systematic violation of rights and freedom if a proctor sees this on a structural basis. - HEI: Obligation to inform Candidates and the National DPA of the illegitimate access. Deterioration of the brand image.	idem - If this illegal behavior of proctors gets out into the media, serious deterioration of brand image of the HEI.	Read and follow-up detailed instructions to: - Hide any confidential information, e.g. objects in the room you take the test in or images and files on your computer desktop.	- Provide Candidate with detailed instructions to hide any confidential information from view. - Haver proctors and reviewers sign agreement to handle all information according to specific guidelines (e.g. not to view video's in public places) - Provide training for the proctors and reviewers. - Do irregular audits on behavior of proctors and reviewers.
Cont.	Cont.	Cont.						





Argue the Balancing Test

Example continued:

Considering:

- the minimal likelyhood of illigitemate processing; and
- the legitimate interest of the controller (HEI);

we consider that the legitimate interest of the controller (HEI) overrides the interests or fundamental rights of the data-subject (test-taker). Furthermore it is also in the interest of the data-subject to have remote access to exams and education.

List of Safeguards (for this example)

- The data-subject (test-taker) is offered the possibility to opt-out of a remote exam via online proctoring and is offered the opportunity to take an exam at the HEI institution.
- Data are destroyed after 7 weeks.
- If data are downloaded by the HEI, they are only stored on secure storage devices compliant with the HEI data storage regulations.
- Etc.

RESEARCH POSTER PRESENTATION DESIGN © 2015
www.PosterPresentations.com