

PROTECTION OF YOUR PERSONAL DATA

This privacy statement provides information about the processing and the protection of your personal data

1. Introduction

The European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (hereafter, 'eu-LISA') is committed to protect your personal data and to respect your privacy. eu-LISA collects and further processes personal data pursuant to [Regulation \(EU\) 2018/1725](#) of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (repealing Regulation (EC) No 45/2001).

This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data

The information in relation to processing operation 'Online assessment - remote exam proctoring' undertaken by the Human Resources Unit (HRU) is presented below.

2. Why and how do we process your personal data?

eu-LISA collects and uses your personal information to support the selection and recruitment for different categories of statutory staff (temporary and contract staff) or non-statutory staff (seconded national experts/interns).

TestReach is a cloud-based online assessment solution used by organisations to create, manage and deliver computer-based tests. Tests can be delivered to candidates under human-led remote proctoring conditions. In this process, the candidate is monitored online by a remote proctor throughout the test via audio, video and screen-share, and the test may involve recording of a video of the candidate sitting the test with a computer webcam. Remote proctoring helps ensure that all tests are conducted fairly and with integrity, providing an equitable experience for all candidates. Recruitment staff use TestReach to create and deliver tests that may include written answers or auto-scored multiple-choice questions, depending on the requirements of the specific job role.

To maintain the highest level of personal data protection and to avoid additional processing of personal data by the vendor, candidates must follow the procedure for the installation and subsequent deletion of the application upon completion of tool usage.

At eu-LISA, recruitment personnel create the questions and tests within the TestReach system and enrol candidates using their name and email address. Before the scheduled test date, candidates receive an automated email from TestReach inviting them to take the test on behalf of eu-LISA. This email contains a link to download the TestReach application and provides the candidate with a unique Access Code for test entry. A different Access Code is issued for each test to ensure security and guarantee unique candidate access. Ahead of the test, the candidate will complete a straightforward system

check in the TestReach application, to ensure their device meets the requirements for sitting a remotely proctored test.

Your personal data will not be used for an automated decision-making including profiling.

Your personal data processed may be reused for the purpose of procedures before the EU Courts, national courts, or the European Court of Auditors.

3. On what legal ground(s) do we process your personal data

We process your personal data, because:

(a) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in eu-LISA;

- Article 5(1)(a) of Regulation (EU) 2018/1725.
- Staff Regulations of Officials (SR) and the Conditions of Employment of Other Servants of the European Communities (CEOS), in particular Art. 27-34 (SR) and Arts. 12-15 and 82-84 (CEOS).
- EC Decision (2017) 6760 on the general provisions for implementing Article 79(2) of CEOS governing the conditions of employment of contract agents employed by the Commission under the terms of Articles 3a and 3b.

(b) Necessary for the management and functioning of eu-LISA;

- Decision of Management Board of eu-LISA No 2015-166 laying down general implementing provisions on the procedure governing the engagement and use of temporary agents under Article 2(f) and 56 of the CEOS.
- Decision of Management Board of eu-LISA No 2019-271 for implementing Article 79(2) of CEOS governing the conditions of employment of contract agents employed by the Commission under terms of Article 3a.
- Decision of Management Board of eu-LISA No 2012-025 laying down rules on the secondment of National Experts (SNE) to the Agency.
- ED Decision 171 of 29 October 2018 on the eu-LISA Internship Policy.

4. Which personal data do we collect and further process?

In order to carry out this processing operation eu-LISA collects the following categories of personal data:

- Candidate's full name and personal Information (such as special adjustments for the exam, for example additional time allowed);
- Candidate's contact details (e-mail address, telephone number, mobile telephone number, etc.);
- Computer Information – May include IP address, browser header data (user agent), processes running, RAM & CPU usage statistics, installed drivers, Window ID, peripherals connected and also cookies.
- Candidate Exam Information: Candidate ID, Responses given, score, results data, access and activity data, video of candidate taking the exam (for remotely invigilated exams only).

The provision of personal data is mandatory to meet a statutory requirement of testing candidates. If a candidate does not provide their personal data, possible consequences are that the candidate might be excluded from further participation in the specific selection procedure.

We obtain candidates' personal data from the details they have declared and the answers they have provided themselves. IP address of the candidates is obtained from the testing tool

5. How long do we keep your personal data?

For candidates tested but not qualified, the paper dossiers (if any) are filed and stored in archive by eu-Lisa for 2 years. After this time, they are destroyed;

For applicants placed on a reserve list but not recruited: data are kept by eu-Lisa for the period of validity of the reserve list + 1 year. After this time, they are destroyed;

For recruited applicants, the data are kept by eu-LISA for a period of 10 years from the termination of employment or as of the last pension payment. After this time, they are destroyed.

TestReach retains customer data for as long as they have a contract in place with a customer, after which it is securely deleted (a certificate confirming destruction can be provided), 30 days after the contract termination date.

The exception to this is video recordings of remotely invigilated exams. Under normal operation, these are retained for a period of six weeks, unless they are specifically asked to retain an individual video for a longer timeframe, say in the event of an appeals process

6. Who has access to your personal data and to whom is it disclosed?

Access to your personal data is provided to eu-LISA staff responsible for carrying out this processing operation and to authorised staff of the external contractor according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law.

The external service provider authorised staff members could have access to your data according to the "need to know" principle. The TestReach application is fully hosted in the cloud by Amazon Web Services (AWS), which is a Tier 1 global leader in the provision of Infrastructure as a Service (IaaS). All TestReach servers are located in the EU - primary servers are in Dublin, with backup servers spread across different AWS data centre locations.

According to the providers' privacy statement (<https://www.testreach.com/testreach-privacy.html>), this personal data can be transferred to a destination outside the EEA ("EEA", being the EU plus Norway, Liechtenstein and Iceland) or the UK. To do so they need to make sure that they have a valid legal basis on which to transfer that data. Transfer can include using a cloud server that is located outside the EU/UK or allowing people who are located outside the EEA/UK access to personal data that is stored within the EEA.

The processor takes all steps reasonably necessary to ensure that personal data is treated securely. In particular, this means that:

The personal data will only be transferred to countries that have been deemed to provide an adequate level of protection of personal data by the European Commission. For further details, see European Commission: Adequacy of the protection of personal data in non-EU countries.

Where the processor uses certain service providers, they may use specific contracts approved by the European Commission which give personal data the same protection it

has in Europe. For further details, see European Commission: Model contracts for the transfer of personal data to third countries.

Where the processor uses providers based in the US, they may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the US. For further details, see European Commission: EU-US Privacy Shield.

7. What are your rights and how can you exercise them?

You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access, rectify or erase your personal data and the right to restrict the processing of your personal data. Where applicable, you also have the right to object to the processing or the right to data portability.

You have the right to object to the processing of your personal data, which is lawfully carried out pursuant to Article 5(1)(a).

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor.

8. Contact information

- The Data Controller

If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the Data Controller, *[indicate controller entity, and (ONLY) functional mailbox]*.

- The Data Protection Officer of eu-LISA

You may contact the Data Protection Officer (dpo@eulisa.europa.eu) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

- The European Data Protection Supervisor (EDPS)

You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.