European Maritime Safety Agency

Data Protection Privacy Statement

on the processing of personal data in relation to online proctoring of written tests in the context of selection procedures

The protection of privacy is of high importance to the European Maritime Safety Agency (´EMSA´). EMSA is responsible for the personal data it processes. Therefore, we are committed to respecting and protecting the personal data of every individual and to ensuring efficient exercising of data subject's rights. All the data of personal nature, namely data that can identify an individual directly or indirectly, will be handled fairly and lawfully with the necessary due care.

This processing operation is subject to Regulation (EU) No. 2018/1725 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data. The information in this Privacy Statement is given pursuant to Articles 15 and 16 of the Regulation (EU) No. 2018/1725.

1. Nature and the purpose(s) of the processing operation[1]

The purpose(s) of the processing of personal data is to allow written tests to be conducted remotely. The written tests can be held in situ at the EMSA premises or remotely. Where written tests are held remotely, EMSA may avail of the services of an external contractor to assist in the running of the tests. The contractor, acting as a processor, conducts remote written test by having the candidates supervised by an external proctor (remote invigilator) during the examination. Remote invigilation of the written test in the selection process guarantees the security, fairness and integrity of the selection process.

In such a case, several steps will be taken by the contractor as follows;

Candidates are invited to register in the Test Reach Platform.

On the exam day, candidates are connected to a remote invigilator (RI) who will be able to see the candidate's screen along with a live video stream of them and their exam environment via webcam. They will communicate with the candidate via audio and via chat.

A validation procedure is then carried out to verify the candidate's identity and to ensure that the testing area is secure:

- ID check: Valid, in date and fits the organisation's requirements.
- Hold for screenshot: This is taken by the RI to validate candidate identity.
- 360º pan of test environment: The candidate will be asked to pan their monitor / camera around the room to get a 360° view. This is to ensure that: There is no second monitor / computer visible in the room; There are no notes / wall boards with information on them.
  The candidate will also be asked to scan their desk (including any shelves under the desk), this is to make sure that there are no phones, books, post-its etc. nearby. If the supervisor observes any unauthorised items, they will request that the candidate removes them from the testing area.

[1] Please, provide a brief description of the processing operation and clearly define the purpose(s).

recruitment@emsa.europa.eu
EMSA, Praça Europa 4, 1249-206 Lisbon, Portugal / emsa.europa.eu

- Device check: The candidate will be asked to use the selfie mode on their camera or a small mirror in order to show no sticky notes or pages have been stuck to the screen of their device.
- Phone check: The candidate will be asked to switch their phone off and put it out of reach.
- Wrist and ears check: This is carried out to ensure no smart watches/fitbits/Bluetooth headpieces are present.
- Empty Pockets: The candidate will be asked to empty any pockets on their person in order to ensure no unauthorised materials are present.
- Resources Check: The candidate will be asked to show the permitted items to the camera e.g. a blank page on both sides.

While candidates complete the test, the RI will monitor the candidate via webcam. The RI is also able to monitor audio feedback to ensure that there are no verbal answers or communication from any outside source. The invigilator will be able to: see the candidate via webcam and see the candidate's screen; use a chat box to communicate to the candidate; hear the candidate and all times and talk with them when required.
When monitoring the exam, the supervisor will watch the screen at all times to check visually for suspicious/fraudulent behaviour. They will check for: Eye movement/Head movement/Hand movement/Talking or mouthing or other indications of external communication. If the invigilator notices any of the above behaviours they will send the candidate an Instant message or talk to them asking them to refrain from the behaviour e.g. "please keep your eyes on the screen", "please keep within view of the webcam", "there is no talking allowed – thank you", etc. They may ask the candidate to repeat a validation step i.e. "Please show me behind your desk again". The platform records video, audio and actions undertaken on the computer and the invigilator. Possible infringements are:

- Minor Infringements: A Minor Infringement is one that is deemed a low-level exception. Minor Infringements may not compromise the test and can be rectified immediately however all minor infringements are logged: Leaning out of view of the camera, blocking the computer camera, commencing hand movements that could be interpreted as sign language, glancing at other areas of the room that the supervisor cannot see (in this instance prior to raising an infringement the supervisor will query the candidate and ask the candidate to pan the room and in particular that area to check, behaving in an unsuitable manner to the supervisor.
- Major Infringements: A Major Infringement is one that is deemed a medium level exception. One that does not compromise the test and one that is rectified quite quickly with the candidate during the test: Accessing (or trying to access) another site / document when online, referring to any material – if there are no resources allowed, not removing objects that are deemed interactive such as smart watches, not agreeing or responding to the validation questions asked by the invigilator.
- Blocker Infringements: A Blocker Infringement is one that is deemed a high level exception. One that compromises the test and may cause the test to be terminated. Supervisors will warn the candidates in advance: Leaving the test centre area for ANY reason, communication of any sort with a third party, mobile phones usage once the exam has commenced.

If an invigilator is required to log an infringement, the invigilator will click on the Log Infringement button. The invigilator will click on the appropriate infringement described and then on the 'Take Action' button. By clicking the 'Take Action' button this will record the exceptional activity onto the 'Actions Log' and will automatically send a message to the candidate saying an exception has occurred. The candidate MUST click OK to this in order to resume their exam. This can be seen by the supervisor on the screen share.

Major and Blocker infringements will be reported to EMSA immediately and it will be at EMSA's discretion to decide on what action to take next either during the exam or post exam. Depending on the assessment of the infringement, candidates may be disqualified from the selection procedure.

Once the tests are finished, the contractor will pseudonymise the candidates' written test and send them to EMSA team in charge of recruitment, together with a decoding file for candidate identification and a report on execution if there were connectivity problems.

2. Categories/types of personal data processed

The categories/types of personal data processed are the following:

- Personal details: First name, family name, title, email address, mobile number. ID Card or Passport details.
- Other:
  Image of candidate's ID document captured during the validation before the exam starts.
  Video/ screen /audio recording of candidate while they are completing the test.
  Log of infringements, if applicable to a candidate, indicating suspicious/fraudulent behaviour
  Candidate Exam Information may include: Responses given, score, results data, access and activity data, video of candidate taking the exam.
  Computer Information may include: IP address, browser header data (user agent), processes running, RAM & CPU usage statistics, installed drivers, peripherals connected and also cookies are used.
  In some cases, it may be recorded on the system that reasonable adjustments are to be allowed for specific exam candidates, for example the addition of extra time during their exam. This is purely for the candidate's own benefit, and the specific reason for the adjustment, which may be medical, is not recorded.
    - Sensitive Personal Data: image of the candidate reveals racial and ethnic origin.

3. Processing the personal data

Data is processed on EMSA's behalf by the contractor TestReach, which stores data on servers located in the EU.

4. Access to and disclosure of personal data

The personal data is disclosed to the following recipients:

- Data subject themselves, upon request.
- Designated EMSA staff members: Head of Corporate Services and Head of Unit Human Resources and Internal Support. Relevant staff within Human Resources and Internal Support involved in the specific selection procedure.
- Designated Contractors' staff members: Relevant staff handling the written test and follow-up from the side of TestReach.
- Access will be given to EU staff with the statutory right to access the data required by their function, i.e. the European Ombudsman, the Civil Service Tribunal, the Internal Audit Service, the European Court of Auditors, OLAF and the European Data Protection Supervisor.

The information in question will not be communicated to any other third parties, except those outlined above.

Personal data are not intended to be transferred to third countries.

5. Protecting and safeguarding personal information

EMSA implements appropriate technical and organisational measures in order to safeguard and protect data subjects' personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to them.

All personal data related to the personal data concerned are stored in a secure IT application according to the security standards of the Agency accessible only to the authorised recipients. Appropriate levels of *access are granted* individually only to the above recipients.

All staff within the Human Resources and Internal Support Unit dealing with personal data sign a confidentiality declaration that is kept in his/her personal file.

6. Access, rectification, erasure or restriction of processing of personal data

Data subjects have the right to access, rectify, erase, and receive their personal data, as well as to restrict and object to the processing of the data, in the cases foreseen by Articles 17 to 24 of the Regulation (EU) No. 2018/1725.

If data subjects would like to exercise any of these rights, they should send a written request explicitly specifying their query to the delegated data controller, the Head of the Unit 4.1 Human Resources and Internal Support.

The right of rectification can only apply to inaccurate or incomplete factual data processed within the current procedure.

The above requests will be answered without undue delay, and in any event within one month of receipt of the request. However, according to article 14 (3) of the Regulation (EU) No. 2018/1725, that period may be extended by two further months where necessary, taking into account the complexity and number of the requests. EMSA shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

7. Legal basis for Data processing

Processing is based on Article 5 (a) of the Regulation (EU) No. 2018/1725 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data., providing that:

(a) a task carried out in the public interest or in the exercise of official authority vested in EMSA (including management and functioning of the institution).

8. Storing Personal data

EMSA does not keep personal data longer than necessary for the purpose(s) for which that personal data is collected.

.As standard, the contractor (TestReach) retains data for as long as they have a contract in place with EMSA, 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.

The written test of the candidates is part of the selection files of EMSA. The data retention of these files is 10 years after the expiry of the reserve list.

9. Data protection points of contact

Data subjects have the right to access and receive a copy of their data. Only if they withdraw from the selection procedure may they request for their data to be erased earlier than the regular retention period specified above. Such requests or any queries/questions that data subjects may have concerning the processing of their personal data, should be addressed to the data controller, the Head of Unit 4.1. Human Resources and Internal Support under the following mailbox: recruitment@emsa.europa.eu

Any data subject may also consult EMSA Data Protection Officer at: DPO@emsa.europa.eu.

Recourse:

Complaints, in cases where the conflict is not resolved by the Data Controller and/or the Data Protection Officer, can be addressed at any time to the European Data Protection Supervisor: edps@edps.europa.eu.