

RECORDING OF PROCESSING ACTIVITY

NOTIFICATION TO THE DATA PROTECTION OFFICER (ARTICLE 31 REGULATION 1725/2018)

NAME OF PROCESSING ACTIVITY¹: Processing of personal data in relation to online proctoring of written tests in the context of selection procedures for 2(f) temporary agents, 3(a) contract agents positions at EMSA (internal, external and through the inter-Agency job market).

1) Controller(s) ² of data processing operation (Article 31.1(a))
<p>Controller: European Maritime Safety Agency (EMSA)</p> <p>Organisational unit responsible³ for the processing activity: Unit 4.1, Human Resources and Internal Support.</p> <p>Data Controller: Cristina Romay Lopez, Head of Unit A.1, Human Resources and Internal Support.</p> <p>Data Protection Officer (DPO): Radostina Nedeva-Maegerlein: dpo@emsa.europa.eu</p>
2) Who is actually conducting the processing? (Article 31.1(a)) ⁴
<p>The data is processed by EMSA itself. <input checked="" type="checkbox"/></p> <p>The organisational unit conducting the processing activity is: Unit 4.1, Human Resources and Internal Support.</p>
<p>The data is processed by a third party (contractor) <input checked="" type="checkbox"/> or the processing operation is conducted together with an external third party</p> <p>TestReach, Block 9-10 Nexus UCD, Belfield Office Park, Beech Hill Road, Dublin 4, D04V2N9, Ireland.</p> <p>Contact point at external third party: info@testreach.com</p> <p>TestReach, NexusUCD, Block 9-10 Belfield Office Park, Clonskeagh, Dublin 4 Ireland</p> <p>TestReach on +353 (0)1 536 3820</p>

¹ **Personal** data is any information relating to an identified or identifiable natural person, i.e. someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. This information may, for example, be the name, date of birth, a telephone number, biometric data, medical data, a picture, professional details, etc.

Processing means any operation or set of operations which is performed on personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

² In case of more than one controller (e.g. joint operations), all controllers need to be listed here

³ This is the unit that decides that the processing takes place and why.

⁴ Is EMSA itself conducting the processing? Or has a provider been contracted?

3) Purpose of the processing (Article 31.1(b))

Why are the personal data being processed? Specify the rationale and underlying reason for the processing and describe the individual steps used for the processing.

In order to fulfil its mandate, EMSA needs to employ high quality staff. For this purpose, EMSA recruits 2(f) temporary agents and 3(a) contract agents using selection procedures in line with the applicable rules on the engagement of each category of staff. As parts of the selection procedure, following the examination of the applications, candidates who are invited to interview at EMSA need to take both an oral and a written test.

The oral and 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.
 - 360° 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.

 - 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.

4) Lawfulness of the processing (Article 5 (a)–(d)): Processing necessary for:

Mention the legal basis which justifies the processing

- (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) ☒

Under 15.2(e) of the EMSA Founding Regulation, Regulation (EC) No 1406/2002, as amended, the Executive Director shall exercise (e) he/she shall exercise, in respect of the staff, the powers laid down in Article 6(2). Articles 14 and 84 of the Conditions of Employment of Other Servants.

Decision of the Administrative Board of 25 March 2015 laying down general implementing provisions on the procedure governing the engagement and use of temporary staff under Article 2(f) of the Conditions of Employment of Other Servants of the European Union.

Decision of the Administrative Board of 24 June 2019 on the general provisions for implementing Article 79(2) of the Conditions of Employment of Other Servants of the European Union, governing the conditions of employment of contract staff employed under the terms of Article 3a thereof.

Decision of the EMSA Administrative Board of 25 July 2018 laying down implementing rules on the middle management staff.

- (b) compliance with a legal obligation to which EMSA is subject ☐

- (c) necessary for the performance of a contract with the data subject or for the preparation of such a contract ☐

- (d) Data subject has given consent (*ex ante*, explicit, informed) ☐

5) Description of the categories of data subjects (Article 31.1(c))

Whose personal data are being processed?

EMSA staff ☒

In the event of internal calls for application, or EMSA staff applying through inter-Agency job market calls for applications and external calls for applications.

Non-EMSA staff ☒

Non-EMSA staff applying to inter-Agency job market call for applications and external calls for applications.

Visitors to EMSA building ☐

Relatives of the data subject ☐

Other (please specify):

6) Categories of personal data processed (Article 31.1(c))

Please tick all that apply and give details where appropriate

(a) **General personal data:**

The personal data contains:

Personal details ☒

First name, family name, title, email address and mobile number.

ID Card or Passport details.

Education & Training details ☐

Employment details ☐

Financial details ☐

Family, lifestyle and social circumstances ☐

Goods or services provided ☐

Other (please give details): ☒

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 Test 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.

(b) **Sensitive personal data** (Article 10)

Racial or ethnic origin ☒

Image

Political opinions ☐

Religious or philosophical beliefs ☐

Trade union membership ☐

Genetic, biometric or data concerning health ☐

Information regarding an individual's sex life or sexual orientation ☐

There is a risk that the candidate discloses sensitive personal data or data of personal nature during the invigilated written test thus a DPIA to identify the risks for the rights and freedoms of the candidates is to be performed.

7) Recipient(s) of the data (Article 31.1 (d))

Recipients are all parties who have access to the personal data

Data subjects themselves ☒

Upon request, candidates can ask for access to their written test but not the video recording.

Managers of data subjects ☐

Designated EMSA staff members ☒

Selection panel 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 the Contractor.

Other (please specify):

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

8) Transfers to third countries or recipients outside the EEA (Article 31.1 (e))

If the personal data are transferred outside the European Economic Area, this needs to be specifically mentioned, since it increases the risks of the processing operation.

Data are transferred to third country recipients:

Yes



No



If yes, specify to which country:

If yes, specify under which safeguards:

Adequacy Decision of the European Commission



Standard Contractual Clauses



Binding Corporate Rules



Memorandum of Understanding between public authorities



9) Technical and organisational security measures (Article 31.1(g))

Please specify where the data are stored during and after the processing

How is the data stored?

EMSA network shared drive

☐

Outlook Folder(s)

☒

There is a dedicated Outlook folder created for each recruitment procedure where e-mails with the contractor and candidates are stored.

Hardcopy file

☐

Cloud (give details, e.g. public cloud)

☐

Servers of external provider

☒

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. AWS adheres to the highest levels of service and maintains an array of certifications to validate compliance. All data is hosted and processed in EU only.

Other (please specify):

☒

The written test is stored in the selection procedure files in the H drive.

The full set of documentation for each recruitment is stored in ARES.

10) Retention time (Article 4(e))

How long will the data be retained and what is the justification for the retention period? Keep in mind that there are pre-determined retention periods for most types of files. Those are explained in the Records Management Policy and Procedure of the Agency. You can check EMSA Records Management Policy and Procedure [here](#).

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.