INTERNAL VACANCY NOTICE – Information Technology Officer – DevSecOps Profile (AD5-AD7)
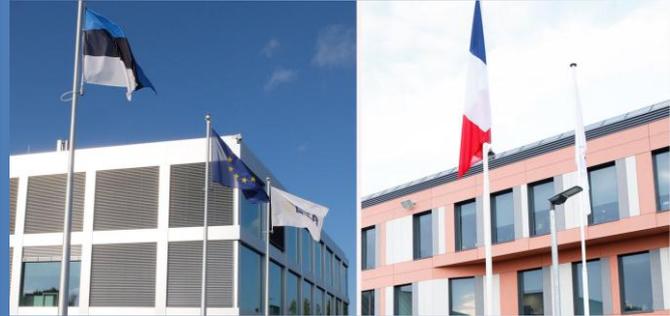Ref. eu-LISA/26/TA/AD5-AD7/7.2

Sector and Unit	Continuous Software Delivery Sector / Technology and Software Engineering Unit
Grade bracket	AD5-AD7 (Temporary Staff)
Place of Employment	Strasbourg (France)
Working model	Hybrid working arrangements – Permanent relocation required
Level of Security Clearance	SECRET UE/EU SECRET
Deadline for Application	28 April 2026[1] 12:59 pm Tallinn time/ 11:59 am Strasbourg time
Validity of the Reserve List	31 December 2029

About the unit

The Technology and Software Engineering Unit (TSU) is responsible for overseeing the successful technical implementation of all large-scale IT systems and solutions entrusted to eu-LISA. To support increasing eu-LISA's ownership of software development, TSU is responsible for implementing the Software Factory (SoFa) approach to ensure better consistency, scalability and quality in the development and evolution of software applications for the EU's Justice and Home Affairs domain.

In this role, TSU provides subject matter expertise and hands-on capabilities in the following engineering domains: Solutions and Architecture Design Sector (ARCS), the Software Development Sector (SODS), the Continuous Software Delivery Sector (CSDS) and the Solutions Quality Assurance Sector (SQAS).

TSU's Continuous Software Development Sector (CSDS) is responsible for the design, implementation, and the maintenance of eu-LISA's software delivery pipeline. This includes automating the build and deployment of software solutions, as well as selecting and integrating appropriate tools for continuous integration (CI) and continuous delivery (CD).

In this role, CSDS drives deployment readiness by ensuring that the software is always in a deployable state and that deployments are predictable and repeatable. To improve efficiency, speed and reliability, CSDS is committed to continuous optimisation of the delivery pipeline and drives the continuous improvement of software delivery practices across the Agency. Additionally, CSDS drives DevSecOps best practices to integrate security checks and practices throughout the software delivery pipeline.

---

[1] Date of publication: 27 March 2026

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice

Vesilennuki 5, 10415 Tallinn, Estonia
www.eulisa.europa.eu

1

CSDS works closely with teams under the Digital Solutions Operations Department, in particular Solutions Operations and Maintenance Sector (SOMS) under the Operations Unit (OPU) and partners with Platform and Infrastructure Unit (PIU) teams on issues related to infrastructure and platform management.

About the job

Working under the supervision of the Head of the Continuous Software Development Sector and reporting to the Head of Technology and Software Engineering Unit, you will support eu-LISA's mandate and ensure that the Agency achieves its objectives, enhances its reputation, and answers stakeholders' needs.

In this role, you will be responsible for designing, implementing and continuously improving the Agency's software delivery pipeline, ensuring that software systems are built, tested and deployed in a secure, reliable and scalable manner. You will contribute to the standardised Software Factory (SoFa) approach by enabling consistent, automated and high-quality software delivery practices across projects. You will act across two complementary dimensions: Project Management (Governance & Strategic Enablement) and Operational Engineering (Technical Delivery & Execution).

You will drive deployment readiness by ensuring that software is always in a deployable state, with predictable, repeatable and auditable release processes. Working in close collaboration with development and operations teams, you will promote DevSecOps principles and foster a culture of automation, quality and continuous improvement.

Your tasks will include a wide range of responsibilities that extend beyond the following list:

- Design, implement and maintain CI/CD pipelines to support agile and iterative software development, ensuring automated build, test, security scanning and deployment processes across multiple environments (development, testing, staging and production).

- Ensure that software releases are reliable, repeatable and traceable, establishing robust release management and versioning practices in on-premise and hybrid cloud environments.

- Integrate containerisation and orchestration security controls and automated security checks into the delivery pipeline in line with DevSecOps best practices.

- Collaborate closely with the Software Development Sector, the Architecture Design Sector and the Solutions Quality Assurance Sector to integrate code changes efficiently, optimise build performance and ensure alignment between development, delivery and testing.

- Contribute to implementing feedback loop with application design, platforms, operational and project management teams promoting clean, secure and maintainable code that aligns with pipeline and deployment requirements.

- Contribute to the design and configuration of distributed systems, event-driven architectures and messaging systems (e.g. Apache Kafka), service mesh technologies (e.g. Openshift Service Mesh/Istio) aligned with business objectives and technical.

- Monitor and optimise pipeline performance, identifying bottlenecks and implementing improvements to increase speed, stability and efficiency of software delivery.

- Ensure compliance with internal policies, security requirements and relevant regulatory obligations throughout the software delivery lifecycle.

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice

Vesilennuki 5, 10415 Tallinn, Estonia
www.eulisa.europa.eu

2

- Contribute to the definition and evolution of software engineering standards, including DevSecOps, CI/CD tooling, automation frameworks, guidelines and reusable assets within the Software Factory framework.

Eligibility criteria

To be eligible for recruitment and selection, you need to meet the following formal criteria, which need to be fulfilled by the deadline for applications:

General conditions

- You produce the appropriate character requirements for the duties involved;
- You are engaged within eu-LISA as Temporary Staff 2(f) in function group AD, grade 5-7, on the closing date for applications and on the day of filling the post.

Selection criteria

The suitability of candidates will be assessed against the following criteria during different stages of the selection procedure:

Professional experience and knowledge

1. Experience similar to the duties outlined in the section "About the Job" in the specified technical context.
2. Experience with implementing or maintaining DevSecOps pipelines using tools such as Git, Jenkins, Ansible, Artifactory and SonarQube.
3. Experience with deploying and managing containerised applications using Kubernetes or OpenShift and tools, such as Helm and ArgoCD and using automation approaches, such as GitOps or Infrastructure as Code (e.g. Ansible).

Education

4. University degree related to the duties mentioned under Section "About the Job".

Personal competencies

5. Ability to act upon eu-LISA's values and guiding principles (We get the job done - We take ownership - We are all role models - We act together as one).
6. Ability to work with cross-functional teams and collaborate effectively with various stakeholders in a fast-paced environment
7. Ability to analyse and resolve complex technical challenges, balancing short-term operational needs with long-term architectural objectives.
8. Strong problem-solving skills combined with a proactive and continuous improvement mindset.

Language

9. Strong drafting and communication skills in English, both orally and in writing, at least at the C1[2] level.

---

[2] Cf. Language levels of the Common European Framework of reference: http://europass.cedefop.europa.eu/en/resources/european-language-levels-cefr

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice

Vesilennuki 5, 10415 Tallinn, Estonia
www.eulisa.europa.eu

3

Advantageous

10. Experience with administering public cloud technologies.
11. Experience with developing Java distributed systems.

Application process and next steps

Ready to join us in building a safer Europe? Apply now!

Before submitting your application, you should carefully check whether you meet all eligibility requirements.

Please complete your application form via the e-recruitment platform here. Due to the fact that this is an internal selection, one must select 'Internal' next to the 'Selection procedure type' field and click 'Search' here.

eu-LISA does not accept applications submitted by any other means (e.g., e-mail or post), or any spontaneous applications. Your application should contain personal details, educational background, professional experience, language proficiency, motivation letter, and responses to pre-screening questions if applicable. Candidates are requested to support their application with adequate, concise examples of their work experience and qualifications, especially if not directly addressed in the duties listed in the application under professional experience.

Please note that if at any stage of the selection procedure it is established that any of the requested information provided by a candidate is false, they will be disqualified.

If a candidate reaches the final stage, they will be requested to supply documentary evidence in support of the statements that they made for this application.

If you encounter any difficulties during the application process or have any further questions, please do not hesitate to reach out to the Talent Acquisition Service via eulisa-RECRUITMENT@eulisa.europa.eu.

Join our diverse team, where you will have the opportunity to grow both professionally and personally while enjoying the journey.

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice

Vesilennuki 5, 10415 Tallinn, Estonia
www.eulisa.europa.eu

4

Selection procedure

The selection procedure includes the following steps:

- A Selection Committee, designated by the Appointing Authority, is established for the selection procedure;

- Each application is checked to verify whether the candidate meets the eligibility criteria;

- All eligible applications are evaluated by the Selection Committee based on a combination of certain selection criteria defined in the Vacancy Notice;

- The quality of the information provided by the candidate in their application is of utmost importance. Candidates are requested to support their application with adequate, concise examples of their work experience (including traineeships, voluntary work etc), and qualification, especially if not directly addressed in the duties listed in the application under professional experience. Certain selection criteria may be assessed jointly and some criteria may be assessed in two or more stages of the selection procedure;

- Once the list of the most qualified candidates is determined, a preliminary assessment may take place (e.g., a pre-recorded video interview and/or a remote written test)[3] prior to the shortlist phase;

- In the shortlist phase[4] consisting of a shortlist interview which may be complemented by a written test, the Selection Committee scores the candidates in accordance with the selection criteria. Candidates may also be required to prepare a presentation on a topic to be presented during the shortlist phase, which would be evaluated as part of the shortlist interview;

- In order to be considered for this selection, candidates must receive at least 60% of the maximum scores in the shortlist phase;

- Interviews and written tests are predominantly conducted in English[5];

- After the shortlist phase, the Selection Committee establishes a non-ranked list of the most qualified candidates and proposes it to the Appointing Authority for selection;

- The Appointing Authority may choose from the list a candidate for the post;

- All shortlisted candidates will be informed about the outcome of the selection process.

Please note that the Selection Committee's work and deliberations are strictly confidential. Any contact with its members linked to this selection is strictly prohibited.

---

[3] The Selection Committee has the discretion to choose between remote and on-site interviews/tests as deemed appropriate. For remote interviews, the Selection Committee reserves the right to conduct the interview using an online video interviewing tool for synchronous and/or asynchronous (e.g., recorded) interviews.

[4] The provisions of the preceding footnote apply.

[5] As English is eu-LISA's working language, the selection procedure will be predominantly conducted in English, except when English is the mother tongue of a candidate or when the mother tongue of the candidate is not an official language of the European Union. In these cases, some of the interview and/or written test questions may be asked in the language indicated as their 2nd EU language.

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice

Vesilennuki 5, 10415 Tallinn, Estonia
www.eulisa.europa.eu

5

eu-LISA's working language is English. Any communication related to the selection procedure will be conducted in English.

Assignment and conditions of employment

The selected candidate will be assigned by the Authority Authorised to Conclude Contracts of employment from the final list of suitable candidates. Once the candidate receives an assignment offer, they may be required to accept the offer within a short timeframe and be available to start the contract as agreed with their line manager.

The successful candidate will be assigned to the new post according to the assignment decision without an impact on their current contract (with an amendment to the employment contract).

All selected candidates may be required to have, or be in a position to obtain, a valid Personnel Security Clearance Certificate (SECRET UE/EU SECRET) depending on the specific job profile and the need-to-know requirements. Failure to obtain the required security clearance certificate from the candidate's National Security Authority, either during or after the expiration of the probationary period, will give eu-LISA the right to terminate any applicable employment contract where the security clearance is a requirement.

Protection of personal data

eu-LISA ensures that candidates' personal data is processed in accordance with Regulation (EU) No 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[6].

The legal basis for the selection procedure of Temporary Staff (TA 2(f)) are defined in the Conditions of Employment of Other Servants of the European Communities[7].

The purpose of processing personal data is to enable selection procedures.

The selection procedure is conducted under the responsibility of eu-LISA's Human Resources Unit ('HRU'). The controller, in practice, for personal data protection purposes is the Head of the Human Resources Unit.

The information provided by the candidates will be accessible for a limited number of authorised HRU personnel, to the Selection Committee, and, if necessary, to the Executive Director, Security and/or the Legal personnel of eu-LISA.

Almost all fields in the Application Form are mandatory; the answers provided by the candidates in the fields marked as optional will not be taken into account to assess their merits.

Processing begins on the date of receipt of the application. eu-LISA's data storage policy is as follows:

---

[6] Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October 2018, OJ L 295, 21.11.2018, p. 39.
[7] CEOS, in particular the provisions governing conditions of engagement in Title II.

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice

Vesilennuki 5, 10415 Tallinn, Estonia
www.eulisa.europa.eu

6

— for applications received but not selected: the paper dossiers are filed and stored in archives for two (2) years after which time they are destroyed;

— for candidates included in a reserve list but not recruited: data is kept for the period of validity of the reserve list + one (1) year after which time it is destroyed;

— for recruited candidates: data is kept for a period of ten (10) years as of the termination of employment or as of the last pension payment after which time it is destroyed.

All candidates may exercise their right of access to and rectification or erasure of their personal data or restriction of processing.

In the case of identification data, candidates can rectify the data at any time during the procedure. In the case of data related to the admissibility criteria, the right of rectification cannot be exercised after the closing date of applications.

Any substantiated query concerning the processing of the candidate's personal data should be addressed to the eu-LISA's HRU (eulisa-RECRUITMENT@eulisa.europa.eu).

Candidates may have recourse at any time to eu-LISA's Data Protection Officer (dpo@eulisa.europa.eu) and/or the European Data Protection Supervisor (edps@edps.europa.eu).

Appeal procedure

If a candidate considers that they have been adversely affected by a particular decision, they can lodge a complaint under Article 90(2) of the Staff Regulations of Officials of the European Union and Conditions of employment of other servants of the European Union, to the following address:

eu-LISA

(European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice)

Vesilennuki 5

10415 Tallinn, Estonia

The complaint must be lodged within three (3) months. The time limit for initiating this type of procedure starts from the time the candidate is notified of the act adversely affecting them.

THE DIGITAL OF SCHENGEN

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice

Vesilennuki 5, 10415 Tallinn, Estonia
www.eulisa.europa.eu

7