

OPEN CALL – AGENCY’S INTERNSHIP**Internship No: eu-LISA/21/INT/SEC/2.1**

Sector/Unit/Department:	Security Unit
Location:	Tallinn, ESTONIA
Starting date:	01 August 2021
Closing date for applications	30 April 2021¹, at 23:59 Eastern European Summer Time (EEST) / 22:59 Central European Summer Time (CEST)

1. THE AGENCY

Applicants are invited to apply for the above-mentioned internship position at the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (hereinafter referred to as “eu-LISA” or “Agency”). eu-LISA was established in 2011, and the new eu-LISA Regulation² entered into force on 11 December 2018.

The seat of eu-LISA is Tallinn, Estonia. The tasks related to development and operational management of the current and future systems are carried out in Strasbourg, France. eu-LISA also has a backup site in Sankt Johann im Pongau, Austria, and a Liaison Office in Brussels, Belgium.

eu-LISA is responsible for the long-term operational management of the European Asylum Dactyloscopy Database (Eurodac)³, the second generation Schengen Information System (SIS II)⁴ and the Visa Information System (VIS)⁵. These systems are essential for the normal functioning of the Schengen Area, for the efficient border management of its external borders as well as for the implementation of common EU asylum and visa policies.

¹ Date of publication: **29 March 2021**.

² Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018, OJ L 295, 21.11.2018, p. 99-137.

³ Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac', OJ L 108, 29.6.2013, p. 1-30.

⁴ Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third country nationals, OJ L 312, 7.12.2018, p. 1-13. Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2016, OJ L 312, 7.12.2018, p. 14-55. Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, OJ L 312, 7.12.2018, p. 56-106.

⁵ Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between member States on short-stay visas (VIS Regulation), OJ L 218, 13.08.2008, p. 60-81.

With a view to further improving the management of the external borders, and in particular, to verify compliance with the provisions on the authorised period of stay on the territory of the Member States, the European Entry/Exit System (EES)⁶ is being developed by the Agency. As of 09 October 2018, the Agency has been entrusted with the development and operational management of the European Travel Authorisation and Information System (ETIAS)⁷. As of 11 June 2019, the Agency was also be entrusted with the centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records System (ECRIS)⁸, and the development of interoperability solutions between large-scale IT systems⁹.

The core task of eu-LISA is to ensure the effective, secure and continuous operation of said IT-systems. The Agency is also responsible for taking the necessary measures to ensure the security of the systems and the security of the data therein.

Beyond these operational tasks, eu-LISA is responsible for information and communication management to ensure that the public and interested parties are rapidly given objective, reliable and easily understandable information with regards to its work; reporting, publishing, monitoring and organising specific training sessions on the technical use of the systems, implementing pilot schemes upon specific and precise requests of the European Commission and the monitoring of research relevant for the operational management of the systems.

Information about the Agency can be found on eu-LISA website:

<https://www.eulisa.europa.eu/>

2. THE SECURITY UNIT

The Security Unit is responsible for end-to end security tasks in the Agency. This includes the security of the systems which the Agency operates, the environment in which eu-LISA operates (hereunder the physical security of all Agency premises), the security of all Agency personnel and assets, as well as security related to outsourced activities.

The responsibilities of the Security Unit are organised in a Security and Continuity Management System (SCMS) split into five macro domains: Governance, Risk and

⁶ Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES), OJ L 327, 9.12.2017, p. 20-82.

⁷ Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, OJ L 236, 19.9.2018, p. 1-71. Regulation (EU) 2018/1241 of the European Parliament and of the Council of 12 September 2018 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS), OJ L 236, 19.9.2018, p. 72-73.

⁸ Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, OJ L 135, 22.5.2019, p. 1-26.

⁹ Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135, 22.5.2019, p. 27-84. Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019, on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135, 22.5.2019, p. 85-135.

Assurance; Business Continuity Management; Protective Security; Information Security; System Security Management & Operations.

The Unit is located both in Tallinn, Estonia and Strasbourg, France.

3. TASKS

The Internship aims at enhancing the educational and practical experience of the applicant through work assignments in their specific areas of competence. The Intern will be introduced to the EU professional world and to the opportunities therein.

Under the supervision of the Tutor and with the overall reporting capacity to the Head of Security Unit, the Intern is expected to carry out mainly security- and business continuity-related tasks, to provide daily support to the entire Security team (to colleagues in Tallinn and Strasbourg) as identified in terms of fulfilling business activities, tasks and responsibilities. The Intern also participates in meetings concerning security aspects, with the possibility to learn about processes and daily challenges of the work in the security and business continuity field.

The tasks may also include:

- supporting the implementation of security and business continuity awareness and outreach activities, including review and update of communications, visual material and other related content;
- assisting the security team in carrying out procurement-related tasks concerning security-related assets and services, e.g. market research;
- supporting with the development of risk assessments and other analyses related to security legal requirements and good practices;
- working closely with other colleagues on different projects and cross-cutting themes;
- assisting in the collection of business requirements and providing daily and weekly updates during the Unit's meetings;
- assisting in the organisation of security and business continuity related meetings and events with internal and external counterparts (e.g. drafting meeting agenda, preparing briefing notes and presentations on security and business continuity matters, registering updates and assisting in the follow-up communication exchanges);
- supporting with the drafting and review of security, business continuity and health and safety related material, e.g. procedures, guidelines, policies;
- assisting the Security Unit in raising its visibility, by bringing security awareness into internal and public knowledge.

The tasks may be adjusted by the Tutor, the Head of Security Policy and Coordination Sector and/or the Head of Security Unit according to the demonstrated competence of the intern and the current business needs.

4. QUALIFICATIONS AND EXPERIENCE REQUIRED

4.1. Eligibility criteria

Applicants will be considered eligible for the selection on the basis of the following formal criteria to be fulfilled by the deadline for applications:

- 4.1.1. to be a national of the Member States of the European Union or Schengen Associated Countries;
- 4.1.2. to have completed at least three years (six semesters) of higher education course (university education or studies equivalent to university) or obtained the relevant degree (minimum a Bachelor or its equivalent) by the closing date for applications. Applicants must provide copies of certificates or declaration from the relevant University;
- 4.1.3. to have knowledge of the working language of eu-LISA (English) at least at level C1¹⁰.

Only qualifications that have been awarded in EU Member States or that are subject to the equivalence certificates issued by the authorities in the said EU Member States shall be taken into consideration.

4.2. Selection criteria

4.2.1. Professional experience and knowledge

- knowledge of the security, risk management or business continuity international policies/standards or the EU rules and regulations in this field of activity¹¹;
- excellent written and verbal command of English proved by experience in drafting documents, minutes and notes in English;
- a sound knowledge of Microsoft Office applications, in particular Outlook, Excel, PowerPoint and Word.

4.2.2. The following attributes would be advantageous:

- general understanding of the EU system and EU institutions and bodies;
- understanding of IT systems and issues pertaining their security;
- general understanding of cyber security;
- knowledge of producing awareness material (e.g. presentations, leaflets, posters, newsletters)

4.2.3. Personal qualities

- good general communication and interpersonal skills, including flexibility, ability to multitask and service-oriented attitude;
- ability to work as part of a team and in a multicultural environment;
- interest to learn and gain knowledge on the various security domains;
- ability to take initiative and work with limited supervision;
- a strong sense of integrity and discretion.

¹⁰ Cf. Language levels of the Common European Framework of reference: <http://europass.cedefop.europa.eu/en/resources/european-language-levels-cefr>

¹¹ For example the 2015/444/EC, Regulation 2018/1725, the EC 1049/2001, ISO 27000 family standards.

5. EQUAL OPPORTUNITIES

eu-LISA applies an equal opportunities policy and accepts applications without distinction on grounds of sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

6. CONFIDENTIALITY

Intern must exercise the greatest discretion regarding facts and information that come to his/her knowledge during the course of internship. He/she must not, in any matter at any time, disclose to any unauthorised person any document or information not already made public. To ensure this discretion, the Intern will be requested to implement and sign the eu-LISA Declaration of Confidentiality before starting the internship.

7. SELECTION PROCEDURE, ENGAGEMENT AND CONDITIONS OF INTERNSHIP

The selection procedure includes the following steps:

- Each application is checked to verify whether the applicant meets the eligibility criteria.
- All the eligible applications are evaluated by Selection Panel based on defined selection criteria.
- Applicants may be contacted by e-mail, telephone and/or Skype by the representative of the Security Unit and/or a representative of Human Resources Unit (HRU) to arrange an interview or to discuss mutual expectations prior to the final selection decision.

The Head of Security Unit makes the final decision with regards to the selection of the Applicant for the Internship position.

The decision on Intern's selection shall be based on the evaluation report carried out by the selection panel.

A reserve list of applicants may be established and used for the selection for similar internship positions depending on the needs of eu-LISA.

The Internship is expected to start on **01 August 2021** and the initial Internship period is offered for 6 (six) months, with a possibility of extension up to total 12 (twelve) months.

At any time prior to the start of the Internship applicants may withdraw their applications by informing eu-LISA HRU via e-mail: eulisa-INTERNS@eulisa.europa.eu

The internship will be awarded a monthly maintenance grant, which is 1/3 of the basic gross remuneration received by an official at the grade AD5/1 and already weighted by the correction coefficient (for Tallinn, Estonia 82.3%)¹².

Interns are solely responsible for the payment of any taxes due on grant received from eu-LISA by virtue of the laws in force in the country of origin. Grant awarded to Intern is not subject to the tax regulations applying to officials and other servants of the European Union.

¹² The correction coefficient is subject to a regular update.

Intern whose place of residence is different from place of the internship is entitled to get reimbursed of the travel expenses incurred at the beginning and at the end of the internship, subject to budget availability.

eu-LISA Intern is entitled to annual leave of two working days per each complete calendar month of service.

Please note that deliberations of the Selection Panel are strictly confidential and that any contact with its members is strictly forbidden.

8. PROTECTION OF PERSONAL DATA

eu-LISA ensures that applicants' personal data is processed in accordance with Regulation (EC) 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC. The new Regulation¹³ entered into force on 11 December 2018.

Please note that eu-LISA will not return applications to the applicants.

The legal basis for the selection procedures of Interns are defined in the eu-LISA Internship Policy, available on the website of eu-LISA:

<http://www.eulisa.europa.eu/JobOpportunities/Pages/Internships.aspx>

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

The selection procedure is conducted under the responsibility of the eu-LISA's Human Resources Unit, within the Corporate Services Department. The controller for personal data protection purposes is the Head of the Human Resources Unit.

The information provided by the applicants will be accessible to a strictly limited number of HR staff of eu-LISA, to the Selection Panel, and, if necessary, to the Executive Director, Security and/or the Legal Officer of eu-LISA.

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

eu-LISA will keep applicants' files for no longer than 2 (two) years. Beyond this period, aggregate and anonymous (scrambled) data on internship applications will be kept only for statistical purposes.

All applicants may exercise their right of access to, rectification or erasure or restriction of processing of their personal data. Personal data such as contact details can be rectified by the applicants 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' submission.

Any substantiated query concerning the processing of his/her personal data can be addressed to the Human Resources Unit at eulisa-INTERNS@eulisa.europa.eu.

Applicants may have recourse at any time to the European Data Protection Supervisor (edps@edps.europa.eu).

¹³ 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.

9. APPLICATION PROCEDURE

In order for application to be valid and considered eligible, the applicant is required to create an account in eu-LISA e-Recruitment tool, fill in the personal and CV information.

If you wish to apply for an Internship position at eu-LISA, you must apply to Open Call via the e-Recruitment tool (<https://erecruitment.eulisa.europa.eu/?page=advertisement>). eu-LISA does not accept applications submitted by any other means (e.g. email or post), or any speculative applications.

The closing date for submission of applications is: **30 April 2021 at 23:59 EEST (22:59 CEST)**.

Applicants are strongly advised **not to wait until the last day** to submit their applications, since heavy internet traffic or a fault with the internet connection could lead to difficulties in submission. eu-LISA cannot be held responsible for any delay due to such difficulties.

Once the applications have been received by eu-LISA e-Recruitment tool, applicants will receive an automatic acknowledgement message by e-mail confirming the receipt of the application.

Please note that if at any stage of the selection procedure it is established that any of the requested information provided by an applicant is false, the applicant in question will be disqualified.

Due to the large volume of applications, eu-LISA regrets to inform that only applicants selected for further steps of the selection procedure will be contacted.

You will be requested to supply documentary evidence in support of the statements that you make for this application if you are selected for further steps of the selection procedure.

In case of any queries about the selection process, please contact us via e-mail:

eulisa-INTERNS@eulisa.europa.eu.