PUBLIC

CALL FOR AN EXPRESSION OF INTEREST FOR A SECONDED NATIONAL EXPERT
Ref. eu-LISA/23/SNE/1.1

Post:	Security Expert – Protective Security
Sector/Unit/Department:	Protective Security and Continuity Sector / Security Unit
Status:	Seconded National Expert (SNE)
Location:	Strasbourg, FRANCE
Starting date:	01 October 2023
Level of Security Clearance:	SECRET UE/EU SECRET [1]
Closing date for applications	31 March 2023 at 23:59 EEST (Eastern European Summer Time) and 22:59 CEST (Central European Summer Time)[2]

1. INFORMATION ABOUT THE AGENCY

Applicants are invited to apply for the above-mentioned post 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 its revised Regulation[3] entered into force on 11 December 2018.

[1] Decision of the Agency Management Board, nr 2019-273, setting the Security Rules for Protecting EU Classified Information in eu-LISA
[2] Date of publication: 08/02/2023
[3] Regulation (EU) No 2018/1726 of the European Parliament and of the Council of 14 November 2018, OJ L 295, 21.11.2018, p. 99.

The seat of eu-LISA is Tallinn, Estonia. 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)[4], the Schengen Information System (SIS)[5] and the Visa Information System (VIS)[6].

These systems are essential for the normal functioning of the Schengen Area, for the efficient management of its external borders as well as for the implementation of common EU asylum and visa policies. 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)[7] is being developed by the Agency. As of 9 October 2018, the Agency is entrusted with the development and operational management of the European Travel Authorization and Information System (ETIAS). As of 11 June 2019, the Agency has also been 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), and the development of interoperability solutions between large-scale IT systems[8].

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 reporting on the usage and the performance of the IT systems the Agency operates, 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 the eu-LISA website: https://www.eulisa.europa.eu

---

[4] Regulation (EU) No 603/2013 of the European Parliament and Council of 26 June 2013.
[5] 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. 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. Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the 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.
[6] Regulation (EC) No 767/2008 of 9 July 2008 of the European Parliament and the Council 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.
[7] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017establishing an Entry/Exit System (EES), OJ L 327/20, 9.12.2017. Corrigendum to Regulation (EU) 2017/2225 of the European Parliament and of the Council of 30 November 2017 amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System (OJ L 327, 9.12.2017), OJ L 312, 7.12.2018.
[8] 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

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

The organisational structure of the Security Unit distributes the staff into four Sectors, namely Protective Security and Continuity, Cyber Security Operations, Security Policy and Coordination as well as Information Security and Assurance.

The Unit is located both in Tallinn, ESTONIA, and Strasbourg, FRANCE.

3. THE SECONDMENT

SNEs are seconded to eu-LISA according to the Decision No 2012-025 of the Management Board of eu-LISA as of 28 June 2012.

SNEs should enable eu-LISA to benefit from the high level of their professional knowledge and experience, in particular in areas where such expertise is not readily available.

The SNEs employer shall undertake to continue to pay his/her salary, to maintain his/her administrative status throughout the period of the secondment. The SNEs employer shall also continue to be responsible for all his/her social rights, particularly social security and pension.

SNEs shall assist eu-LISA's statutory staff members. They may not perform middle or senior management duties, even when deputising for their immediate superior. Under no circumstances may an SNE on his/her own represent the Agency with a view to entering into commitments, whether financial or otherwise, or negotiating on behalf of eu-LISA.

The SNE shall carry out the duties and conduct his/her tasks solely within the interests of eu-LISA. He/she shall neither seek nor take instruction from any government, authority, organisation nor person outside the Agency. He/she shall carry out the duties assigned objectively, impartially and in keeping with his/her duties of loyalty to the EU.

The initial period of the secondment may not be less than six months nor more than two years. It may be renewed once or more, up to a total period not exceeding four years, at the request of eu-LISA.

Exceptionally, where the interest of the service warrants it, the Executive Director of eu-LISA may ask to authorise one or more extensions of the secondment for a maximum of two more years at the end of the four-year period.

The secondment is authorised by the Executive Director and effected by an exchange of letters between the Executive Director and the Permanent Representation of the Member State concerned, the associated country's mission to the EU or the intergovernmental organisation (IGO).

The SNE is entitled, throughout the period of the secondment, to a daily subsistence allowance and a monthly subsistence allowance, applicable to the place of secondment.

The selected applicant will need to have, or be in a position to obtain, a valid Personnel Security Clearance Certificate (SECRET UE/EU SECRET level). A Personnel Security Clearance Certificate (PSCC) means a certificate issued by a competent authority establishing that an individual is security cleared and holds a valid national or EU PSC, which shows the level of EU Classified Information (EUCI) to which that individual may be granted access, the date of validity of the relevant PSC and the date of expiry of the certificate itself. For more information about EUCI please consult the Decision of the Agency Management Board, nr 2019-273, setting the Security Rules for Protecting EU Classified Information in eu-LISA[9].

Applicants, who currently hold a valid security clearance, shall provide a copy of the security clearance to eu-LISA and specify the issuing authority, level and date of expiry. In case the validity of the security clearance expires within six months, the renewal procedure to be initiated expeditiously. For applicants, who do not hold a security clearance, the procedure will be initiated expeditiously by eu-LISA. Failure to obtain the required security clearance certificate from the National Security Authority during the secondment, will give the right to eu-LISA to terminate the secondment.

4. TASKS AND RESPONSIBILITIES

As part of the Security Unit, the Security Expert will support the Agency in the management of the security and continuity management system (SCMS), with particular focus on protective security, under the coordination of the Head of the Sector and reporting to the Head of the Unit.

Main functions and duties of the Security Expert:

1. Protective security:

- Ensuring the physical security, health and safety of eu-LISA sites and buildings, in cooperation with other business areas like Operations and Corporate Services;

[9] https://www.eulisa.europa.eu/AboutUs/Documents/MB%20Decissions/2019-273_EUCI%20rules.pdf

- Ensuring the maintenance and working order of the physical security and safety systems to guarantee protection of eu-LISA personnel, information and premises;
- Liaising with contractors and suppliers of security products and services (including the development of technical specifications, managing procurement procedures and contracts);
- Developing and maintaining evacuation plans and procedures, including establishment and maintenance of fire warden systems;
- Coordinating and assuring the quality of fire drills, training on fire evacuation and safety procedures;
- Ensuring personnel assurance processes through clearance and vetting procedures;
- Ensuring that the personnel of eu-LISA, contractors/subcontractors fulfil the security requirements as per specific contract or SLAs in place;
- Performing specific security awareness sessions for eu-LISA personnel, contractors and visitors.

2. Business Continuity and disaster recovery:

- Supporting the continuous improvement programme of the eu-LISA Business Continuity Management System.

3. Other tasks and duties:

- Acting as first responder during a security incident or a crisis situation and as focal point for all security related matters;
- Investigating and recommending appropriate corrective actions for security incidents or identified risks;
- Monitoring the implementation of security policies and procedures and all matters pertaining to the protection of personnel, premises and assets;
- Preparing periodic reports to the Head of Unit and to the Head of Sector on all domains outlined above;
- Liaising with national Law Enforcement and Security Services Agencies when needed;
- Executing any other relevant tasks assigned by the Head of Unit;
- Being part of an on-call duty roaster to support in incident troubleshooting during out of business hours.

5. QUALIFICATIONS AND EXPERIENCE REQUIRED

5.1. Eligibility criteria

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

- to be a national of one of the Member States of the European Union, Norway, Iceland, Liechtenstein or Switzerland and enjoy the full rights as a citizen;

- to be employed by a national, regional or local public administration or an Inter-Governmental Organisation (`IGO`);
- to have worked for the employer on a permanent or contractual basis for at least 12 months before the secondment and shall remain in service of the employer throughout the period of secondment;
- to have a thorough knowledge of one of the European Union languages and a satisfactory knowledge of another European Union language to the extent necessary for the performance of the duties. SNE from non-member country must produce evidence of a thorough knowledge of one European Union language necessary for the performance of his/her duties.

Only duly documented professional activity is taken into account. In case of part-time work the professional experience will be calculated pro-rata in line with the workload stated by the applicant.

Compulsory military service or equivalent civilian service shall be taken into consideration as professional experience if the official documentation is provided.

5.2. Selection criteria

Suitability of applicants will be assessed against the following criteria in different steps of the selection procedure.

5.2.1. ***Professional experience and knowledge:***

The applicant will be required to demonstrate that he/she has:

- At least five (5) years of full-time work experience within tasks mentioned above;
- A level of education, which corresponds to completed university studies of at least three years attested by a diploma;
- Knowledge of and/or work experience with ISO 27000 (Information Security) family of standards and/or a formal security certification (e.g. ISO 27001 Lead Implementer/Lead Auditor, CISM, etc.);
- Work experience in the development, implementation or operational management of security and/or safety systems (access control system, CCTV system, intrusion detection system, fire detection system, building management system, etc.);
- Work experience in coordination and/or management of security guards or other security-related personnel;
- Work experience in protective (personal) security and/or emergency action fields;
- Work experience in applying Risk Management methodologies, tools and processes;
- Work experience in development of protective security policies and procedures;
- Experience in the reporting to the senior management.

Working language of eu-LISA is English. Therefore, the ability to communicate in English is an essential requirement.

5.2.2. *Personal qualities*

- Excellent analytical and problem-solving skills, ability to think creatively and strong sense of initiative and responsibility;
- Engaging and motivating presentation skills, strong inter-personal and negotiation skills and strong service-orientation;
- High level of capability to organise and plan the work, pro-activeness and ability to handle multiple tasks, when required, as well as accuracy and attention to detail and ability to work under pressure.

6. 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.

7. SELECTION PROCEDURE

The selection procedure includes the following steps:

- Selection Committee designated by the Appointing Authority (eu-LISA`s Executive Director) is set up for the selection procedure;
- After registration, each application is checked to verify whether the applicant meets the eligibility criteria;
- All eligible applications are evaluated by the Selection Committee based on the selection criteria defined in the open call;
- The best-qualified applicants, who obtained the highest number of points, are short-listed for an interview, which may be complemented by a written competency test;
- The interview and written test are conducted in English. In case English is a mother tongue of an applicant, some interview or test questions may be held in language indicated by the applicant on the application form as the 2nd EU language;
- During the interview and the written test, the Selection Committee examines the profiles of applicants and scores the applicants in accordance with the selection criteria;
- After the interviews and tests, the Selection Committee draws up a non-ranked list of the most suitable candidates to be included on a reserve list for the post and proposes it to the Appointing Authority. The Selection Committee may also propose to the Executive Director the best suitable applicant to be offered secondment for the post;
- The Appointing Authority choses from the reserve list an applicant to whom to offer the secondment;
- Applicants put on the reserve list may also be used for secondment to a similar post depending on the needs of the eu-LISA and budgetary situation as long as the reserve list is valid;

- The reserve list established for this selection shall be valid **until 31 December 2025** (the validity period may be extended);
- Each applicant invited for an interview will be informed whether or not he/she has been placed on the reserve list. **Applicants should note that inclusion on a reserve list does not guarantee a secondment by eu-LISA.**

The Selection Committee's work and deliberations are strictly confidential and any contact with its members is strictly forbidden.

Because English is the working language of eu-LISA and because the successful applicant will be requested to immediately be operational, the selection procedure will be performed in English and all communication with applicants will be held in English.

8. PROTECTION OF PERSONAL DATA

eu-LISA ensures that applicants' 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.

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 (HRU), within the Corporate Services Department. The controller for personal data protection purposes is the Head of HRU.

The information provided by the applicants will be accessible to a strictly limited number of staff members of the HRU staff, to the Selection Committee, 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.

Processing begins on the date of receipt of the application. Our data storage policy is as follows:

- for applications received but not selected: the paper dossiers are filed and stored in archives for 2 years after which time they are destroyed;
- for applicants placed on a reserve list but not recruited: data is kept for the period of validity of the reserve list + 1 year after which time it is destroyed;
- for recruited applicants: data is kept for a period of 10 years as of the termination of employment or as of the last pension payment after which time it is destroyed.

All applicants may exercise their right of access to and right to rectify personal data. In the case of identification data, applicants 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' submission.

Any substantiated query concerning the processing of his/her personal data can be addressed to HRU at eulisa-SNEPOSTING@eulisa.europa.eu

Applicants 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).

9. APPLICATION PROCEDURE

In order for application to be valid and considered eligible, the applicant is required to submit:

- eu-LISA standard application form filled in in English and hand-signed (scanned into PDF format);
- proof of the National Administration Authorisation – Form 1A (Employer authorisation for SNE applicant), provided on eu-LISA website;
- a copy of security clearance (if available).

Applications must be sent by the Permanent Representation or a national contact point or by the associated countries competent authority or the administration of IGO to the following e-mail address before the deadline: eulisa-SNEPOSTING@eulisa.europa.eu. Please liaise with your Permanent Representation to ensure that your application meets deadline.

The standard application form can be downloaded from eu-LISA website:
http://www.eulisa.europa.eu/JobOpportunities/Pages/SecondedNationalExpert.aspx

The closing date for submission of applications is:

- **31 March 2023 at 23:59 EEST (Eastern European Summer Time) and 22:59 CEST (Central European Summer Time).**

The subject of the e-mail should include the **title of the Open Call and Reference No eu-LISA/23/SNE/1.1.**

Incomplete applications and applications received by eu-LISA after the deadline will be disqualified and treated as non-eligible.

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 registered, applicants will receive an 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.

In case of any queries about the selection process, please contact through the e-mail: eulisa-SNEPOSTING@eulisa.europa.eu.