PUBLIC

CALL FOR AN EXPRESSION OF INTEREST FOR A SECONDED NATIONAL EXPERT
Ref. eu-LISA/21/SNE/3.1

Post:	Information Security Expert
Sector/Unit/Department:	Information Security and Assurance Sector / Security Unit
Status:	Seconded National Expert (SNE)
Location:	Tallinn, ESTONIA Strasbourg, FRANCE
Starting date:	as soon as possible
Level of Security Clearance:	SECRET UE/EU SECRET [1]
Closing date for applications	**Extended until 31 January 2022** ~~30 November 2021~~ at 23:59 EET (Eastern European Time) and 22:59 CET (Central European 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

[1] EC Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information
[2] Date of publication: 07/10/2021

(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.

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

[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.
[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

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

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 organized 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.

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, at the request of the Head of Sector concerned and where the interest of the service warrants it, the Executive Director of eu-LISA may 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.

4. TASKS AND RESPONSIBILITIES

The principal role of the Information Security Expert is to support the eu-LISA Security Unit in performing security management tasks mainly concerning the large-scale IT system operated by eu-LISA and its Corporate IT Systems. The Information Security Expert will be part of the Security Unit's Tallinn based staff.

Information Security Expert may be required to travel from time to time to the other Agency locations, to the locations of other EU Institutions and bodies or to the location of other stakeholders of eu-LISA. He/she will work under the direct supervision of the Head of Security Unit and the Head of Information Security and Assurance Sector.

The Information Security Expert's main duties entail:

1. Security and Continuity Management System

- Supporting the development, implementation, monitoring and maintenance of the overall eu-LISA's Security and Continuity Management System (SCMS) according to ISO27001 and ISO22301.
- Updating and maintaining SCMS related processes, documentation, templates and records.
- Performing security risks assessments for new information system(s) and reviewing/updating the risk assessments for existing information systems.

2. Security Architecture

- Supporting the further development of the Agency's security architecture framework.
- Reviewing the security architecture of the systems and the security requirements for the system in accordance with the Agency's security principles and security architecture framework.

3. Information security policy framework

- Reviewing and updating security and business continuity policies, standards, procedures and guidelines in accordance with ISO27001 and international good practice.
- Supporting the drafting the technical security requirements for the procurement processes of the project for the initial deployment of the new system(s) and for the further developments.
- Supporting the development and maintenance of security and business continuity/disaster recovery plans and related documentation.

4. Security Operations

- Monitoring the security logs and configuration of the system in order to identify any possible incident or event security related.
- Acting as a first responder during security incidents or crisis/emergency situations, if necessary.

5. Security Assurance

- Perform any internal security audit and testing of the systems as required.
- Supporting the implementation of security and business continuity exercises regarding the large-scale IT systems.
- Performing SCMS level audits and gap assessments.

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 3 years' professional experience relevant to the duties above, acquired after the award of the university diploma;
- work record with ISO 27000 standards family and/or a formal security and/or business continuity certification (e.g. ISO 22301 Lead Implementer/Lead Auditor, ISO 27001 Lead Implementer/Lead Auditor, CISM, CISA, CISSP, etc.) and/or an MD level diploma in the information management, business continuity, legal or security fields or any other related domain;
- experience in Information Security Management System;
- work experience in planning and conduction information security testing, exercising and training;
- work experience in applying Security Risk Management methodologies, tools and processes;
- work experience in information security planning;
- work experience in development security strategies, policies and procedures (gap analysis, plans, policies, standards, business impact analysis, etc.);
- experience in the reporting to senior management;
- excellent written and oral command of English, corresponding to at least C1[9] level .

5.2.2. Besides the following attributes would be advantageous

- at least B2[10] level of French;
- previous work experience in European Institutions, Bodies or Agencies or Agencies.

5.2.3. Personal qualities

- excellent analytical and problem-solving skills;
- engaging and motivating presentation skills;
- strong inter-personal and negotiation skills;
- ability to think creatively;
- high level of capability to organise and plan the work;
- pro-activeness and ability to handle multiple tasks when required;

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

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

- accuracy, attention to details and ability to work under pressure;
- strong sense of initiative and responsibility;
- strong service-orientation.

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 2024** (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)..Failure to obtain the required security clearance certificate from the successful applicant's National Security Authority, either during or after the expiration of the probationary period, will give the right to eu-LISA to terminate any applicable employment contract.

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:

- **Extended until 31 January 2022 ~~30 November 2021~~ at 23:59 EET (Eastern European Time) and 22:59 CET (Central European Time).**

The subject of the e-mail should include the **Title of the Open Call and Reference No eu-LISA/21/SNE/3.1.**

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.