

CALL FOR AN EXPRESSION OF INTEREST FOR A SECONDED NATIONAL EXPERT

Ref. No: eu-LISA/16/SNE/2.1

Post:	Information Security Expert
Unit/Department:	Security Sector
Status:	Seconded National Expert (SNE)
Place of secondment:	Strasbourg, FRANCE
Starting date:	as soon as possible
Duration of secondment:	2 years and it may be renewed if it is justified in the interests of eu-LISA
Level of Security Clearance:	SECRET EU/EU SECRET ¹
Closing date:	04 June 2016²

1. THE AGENCY

The European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (hereinafter referred to as *eu-LISA*) is established under the Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011³ (hereinafter referred to as '*the Regulation*').

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. A backup site is installed in Sankt Johann im Pongau, Austria.

eu-LISA is responsible for the long-term operational management of the second generation Schengen Information System (SIS II)⁴, the Visa Information System (VIS)⁵ and EURODAC⁶. In the future, it may also be made responsible for the preparation, development and operational management of other large-scale IT systems in the area of freedom, security and justice, if so entrusted by means of separate legal instruments.

Core task of eu-LISA is to ensure the effective, secure and continuous operation of the IT-systems. The Agency is also responsible for the adoption of the necessary measures to

¹ COMMISSION DECISION (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information

² Date of publication: **04 May 2016**.

³ Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011, OJ L 286, 01.11.2011.

⁴ Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381, 28.12.2006, and Council Decision 2007/533 JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205, 7.08.2007.

⁵ 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.

⁶ Council Regulation (EC) No 2724/2000 of 11 December 2000 concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316, 15.12.2000.

ensure the security of the systems and the security of data.

Beyond these operational tasks, eu-LISA is responsible for the tasks related to reporting, publishing, monitoring and organising specific trainings on the technical use of the systems, implementing pilot schemes upon the specific and precise request of the Commission and monitoring the research relevant to the operational management of the systems.

The working language of eu-LISA is English.

2. THE SECURITY SECTOR

The Security Sector is responsible for the governance of all aspects of security in eu-LISA. This includes the security of the systems which eu-LISA operates, the environment in which it operates (hereunder the physical security of all eu-LISA premises), the security of its personnel and relevant stakeholders, as well as the security in outsourced activities and all eu-LISA assets.

The responsibilities of the Security Sector are generally organised under five 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 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.

The SNE should have the security clearance at a level "SECRET UE/EU SECRET". In case the candidate is not cleared before joining eu-LISA, a security clearing process will be initiated with the competent NSA.

4. TASKS AND RESPONSIBILITIES

The principal role of the Information Security Expert is to support the eu-LISA Security Office in performing security management tasks concerning the large-scale IT system operated by eu-LISA. The Information Security Expert will be part of the Security Sector's Strasbourg 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 eu-LISA Security Officer and the team leader in Strasbourg, who leads the information security team within the Agency.

The Information Security Expert's main duties entail:

1. Security and Continuity Management System

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

2. Security Architecture

- a) Supporting the further development of the Agency's security architecture framework.
- b) 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

- a) Reviewing and updating security policies, standards, procedures and guidelines in accordance with ISO27001 and international good practice.

- b) 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.
- c) Supporting the development and maintenance of security plans and related documentation.

4. Security Operations

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

5. Security Assurance

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

5. QUALIFICATIONS AND EXPERIENCE REQUIRED

5.1. Selection 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:

- to be a national of one of the Member States of the European Union, Norway, Iceland, Liechtenstein or Switzerland⁷ and enjoy the full rights as a citizen⁸;
- to be employed by a national, regional or local public administration⁹ or an IGO.
- 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;
- to have worked for the employer on a permanent or contract basis for at least 12 months before the secondment and shall remain in service of the employer throughout the period of secondment;
- to have at least 3 years' experience of technical functions.

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.

⁷ Appointment of staff from countries associated with the implementation, application and development of the Schengen acquis and EURODAC-related measures is subject to the conclusion of the arrangements defined in article 37 of the founding Regulation of the Agency.

⁸ Prior to any appointment, the successful applicant will be asked to provide a certificate issued by the competent authority attesting the absence of any criminal record.

⁹ The Public administration means all State administrative services at central, federal and regional level, comprising ministries, government and parliament services, the courts, central banks, and the administrative services of local authorities, as well as the decentralised administrative services of the State and of such authorities.

5.2. Selection criteria

5.2.1. Professional competencies

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.).
- Proven work experience in Information Security Management System.
- Proven work experience in planning and conduction information security testing, exercising and training.
- Proven work experience in applying Security Risk Management methodologies, tools and processes.
- Proven work experience in information security planning, business continuity planning and disaster recovery planning.
- Proven work experience in development security strategies, policies and procedures (gap analysis, plans, policies, standards, business impact analysis, etc.).
- Proven work experience in the reporting to senior management.
- Excellent written and oral command of English, corresponding to at least C1 level¹⁰.

5.2.2. Besides the following attribute would be advantageous:

- at least B2¹¹ level of French.

5.2.3. Personal qualities

Attributes especially important to this post include:

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

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

¹¹ Cf. Language levels of the Common European Framework of reference: <http://europass.cedefop.europa.eu/en/resources/european-language-levels-cef>

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:

- the Selection Committee designated by the eu-LISA 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 the eligible applications are evaluated by the Selection Committee based on the selection criteria defined in the vacancy notice;
- the best-qualified applicants, who obtained the highest number of points are short-listed for an interview;
- the interview is held in English;
- during the interview, the Selection Committee examines the profiles of applicants and assesses their relevancy for the post in question;
- shortlisted applicants may be required to undergo written competency test and complete part of the process in their second EU language;
- applicants invited to an interview will be requested to present, on the day of the interview, originals of their evidence of their professional experience, clearly indicating the starting and finishing dates, and the workload;
- as a result of the interviews, the Selection Committee recommends the most suitable applicants for the post in question. Suitable applicants are put on the reserve list, which may also be used for recruitment to a similar post depending on the needs of the eu-LISA and budgetary situation, and shall be valid until **04 June 2018** (the validity period may be extended). Each applicant 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 acceptance of an SNE by eu-LISA.**

Please note that the Selection Committees work and deliberations 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 are processed in accordance with Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (12.1.2001, OJ, L 8). Please note that eu-LISA will not return applications to applicants. This applies in particular to the confidentiality and security of such data.

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

The selection procedure is conducted under the responsibility of eu-LISA's Human Resources and Training Unit, under the Resources and Administration Department. The controller in practice for personal data protection purposes is the Head of the HR and Training Unit.

The information provided by the applicants will be accessible to a strictly limited number of staff members of the HR staff, to the Selection Committee, and, if necessary, to 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. 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 they are 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 they are 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 the HR and Training Unit at eulisa-SNEPOSTING@eulisa.europa.eu

In the case of data related to the admissibility criteria, the right of rectification cannot be exercised after the closing date of candidatures' submission. Substantiated requests should be e-mailed to the Human Resources and Training Unit at eulisa-SNEPOSTING@eulisa.europa.eu. Applicants may have recourse at any time to eu-LISA's Data Protection Officer dpo@eulisa.europa.eu or directly to the European Data Protection Supervisor edps@edps.europa.eu.

9. APPLICATION PROCEDURE

Applications must be sent by the Permanent Representation 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 closing date for submission of applications is: **04 June 2016 at 23:59 Eastern European time (EET)**.

For applications to be valid, applicants shall include the following documents:

- an application form duly signed and completed - provided on eu-LISA website;
- proof of the national administration authorisation – Form 1A (Employer

- authorisation for SNE applicant) – provided on eu-LISA website;
• copy or certificate of security clearance, if available.

The subject of the e-mail should include the reference of the Call of an Expression.

Applications delivered in hand will not be accepted.

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.

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

Only applicants selected for the interview will be contacted.

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