The Agency for the operational management of large-scale IT systems in the area of freedom, security and justice

CALL FOR EXPRESSION OF INTEREST FOR TEMPORARY AGENTS

HOME/TA/AD7/07/11

PROFILE:	**SECURITY**
GRADE:	**AD 7**

You are advised to read this call for expression of interest with the utmost care, as it contains all the information you need to apply and to assess your eligibility for the chosen profile.

1. GENERAL CONTEXT

The Regulation establishing the **Agency for the operational management of large-scale IT systems in the area of freedom, security and justice** (hereinafter called "the Agency"), a new European regulatory Agency which will progressively grow to 120 staff, has been adopted on 25 October 2011 and was published in the Official Journal of the European Union on 1 November 2011[1]. The Agency will become operational on 1 December 2012. Staff will be gradually recruited as of July 2012. The present selection procedure is organised by the European Commission (Directorate General - Home Affairs) acting in view of the establishment of the Agency. This procedure has been launched to provide a reserve list of approximately **9** successful candidates.

The Agency will be responsible for the long-term operational management of the second generation Schengen Information System (SIS II)[2], the Visa Information System (VIS)[3] and EURODAC[4]. In the future, the Agency 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.

The Agency's core task is to ensure the effective, secure and continuous operation of the IT-systems. The Agency will also be responsible for the adoption of the necessary measures to ensure the security of the systems and the security of data. Beyond these operational tasks, the Agency shall be responsible for the tasks related to reporting, publishing, monitoring, organising specific trainings on the technical use of the systems, implementing pilot schemes upon the specific and precise request of the Commission and monitoring of research relevant for the operational management of the systems.

[1] Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 286, 01.11.2011.

[2] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the 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.

[3] 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, 13.8.2008.

[4] Council Regulation (EC) No 2725/2000 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.

The seat of the Agency will be Tallinn, Estonia. The tasks related to development and operational management of the current and future systems will be carried out in Strasbourg, France. A backup site (BCU) will be installed in Sankt Johann im Pongau, Austria. It is estimated that approximately 45 staff members will be allocated to administrative tasks within the Agency and will be based at the Agency's headquarters in Tallinn, while approximately 75 staff members will be working on the operational management and development of large-scale IT-systems, and will therefore be based in Strasbourg. At this stage it is not foreseen to base staff permanently in Austria. The daily operation of the back-up site will be performed by staff travelling from Strasbourg.

2. ELIGIBILITY CRITERIA

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

2.1. GENERAL CONDITIONS

a) Be citizens of a Member State of the European Union, Norway, Iceland, Liechtenstein or Switzerland.[5]

b) Enjoy full rights as a citizen.[6]

c) Have fulfilled the obligations imposed on them by the laws of their home country concerning military service.

d) Meet the character requirements for the duties involved.

e) Have a thorough knowledge of one of the official languages of the European Union (language 1) and satisfactory knowledge of French, English or German (language 2).

f) Be physically fit to perform their duties.[7]

2.2 SPECIFIC CONDITIONS

A. EDUCATION

Have a level of education which corresponds to completed university studies attested by a diploma when the normal period is 4 years or more,

Or

[5] 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.
[6] Prior to any appointment, the successful candidate will be asked to provide a certificate issued by the competent authority attesting the absence of any criminal record.
[7] Before appointment, the successful candidate shall be medically examined in line with requirement of art. 12 (2)d of the Conditions of employment of other servants of the European Communities.

A level of education which corresponds to completed university studies attested by a diploma and appropriate professional experience of at least 1 year when the normal period of university education is a least 3 years.

NB: The minimum of one year's professional experience required is deemed to be an integral part of the diploma and cannot be counted towards the professional experience required below.

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

B. PROFESSIONAL EXPERIENCE REQUIRED

At least 6 years' graduate-level professional experience relevant to the duties involved acquired after the award of the university diploma described under point 2.2.A.

3. PROFILE / DUTIES

The principal role of administrators in the field of security is to support the management in fulfilling the mission of the Agency in areas such as physical security, IT security and risk management. The duties described below may imply travels to the backup site as well as shift-work or work on duty during nights and/or weekends.

The main duties of administrators in the field of Security may include:

- Develop, implement and disseminate internal security-related standards, policies, procedures and guidelines for the Agency;
- Maintain the security of the IT systems entrusted to the Agency in optimal working condition;
- Facilitate and support security audits of the Agency by external organisations;
- Ensure the security of the Agency to prevent harm or damage to staff, premises and information of the Agency;
- Ensure the physical security and safety of the Agency sites, in coordination with local authorities when necessary;
- Act as first responder during a security incident or a crisis situation and as focal point for all security related matters;
- Identify and assess ICT security risks to new and existing infrastructure;
- Investigate and recommend appropriate corrective actions for security incidents or identified risks, including those related to ICT;
- Report regularly on security to the Agency management and/or to relevant stakeholders;
- Contribute to the development of the Business Continuity Plan, monitor its performance and test its effectiveness;
- Conduct frequent security inspections and audits to ensure full compliance with standards, policies, procedures and guidelines of the Agency;
- Manage security-related contracts;
- Coordinate with the service contractors of the Agency to ensure that their activities are carried out in accordance with standards, policies, procedures and guidelines of the Agency;
- Coordinate and implement the security policy of the IT-systems;

- Liaise with national security authorities of the host Member State on matters related to the security of the Agency, its operations and its staff;
- Liaise with other EU institutions security services.

4. SELECTION CRITERIA

Candidates need an excellent written and oral command of English, any additional language being an asset. They have excellent analytical and problem-solving skills and are able to think creatively. They have good organisational skills and an adequate command of office equipment and applications (word processing, spread sheets, presentations, electronic communication, Internet, etc.). They are able to maintain accuracy and speed under pressure and to work in multicultural teams. They are aware of the mission of the Agency. Holding a security clearance may be an asset.

In addition, candidates will be assessed on the basis of the following selection criteria:

- Knowledge of and/or work experience with ISO 27000 series and/or of BSI IT Grundschutz and /or Common Criteria (ISO 15408) and/or a Formal ICT security certification and/or a diploma in the security field;
- Work experience in the development or application of Information Systems Security Management frameworks;
- Work experience in the field of Risk Management methodologies, tools or processes;
- Work experience with frameworks for secure software development;
- Work experience with the setting up of secure IT- technical architectures;
- Work experience in the security incident management process;
- Work experience in the field of business continuity planning or disaster recovery planning;
- Work experience in the field of physical security;
- Work experience in the field of security documentation development (security gap analysis, security plans, security policies, security standards, business impact analysis, security tests specifications);
- Work experience in the coordination of security activities involving several organizations, contractors and external stakeholders;
- Work experience in the reporting of security activities to senior management;
- Previous work experience in similar functions within an international and multicultural environment, preferably in a European Institution, Agency or body.

5. CONDITIONS OF EMPLOYMENT

The successful candidates may be offered a temporary contract pursuant to Article 2 a) of the Conditions of Employment of other servants of the European Communities[8].

The initial duration of the contract is five years, with possibility of renewal for another period not exceeding five years. Renewals for a second prolongation will be indefinite.

The grade of recruitment for this call for expression of interest will be AD 7.

[8] URL <http://ec.europa.eu/reform/2002/index_en.htm>

The salaries of temporary agents are subject to a community tax deducted at source. They are exempt from national tax. The European institutions have their own social security and pension scheme. The basic monthly salaries, before any deductions or allowances, at 1 July 2010 for the corresponding grades at first step can be consulted here:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:338:0001:0006:EN:PDF

The basic salary will be weighted by the correction coefficient (currently 116,1% for France).

The successful applicants will be required to undergo a security vetting and clearance procedure. Non-obtainment of the security clearance may lead to termination of the contract.

The place of employment for this profile will be Strasbourg, France, where the technical site of the Agency will be based.

6. EQUAL OPPORTUNITIES

The Agency applies a policy of equal opportunities and accepts applications without distinction on the 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. THE SELECTION PROCESS

A Selection Committee will be set up for the selection process. As part of the online application, candidates are required to answer a series of questions with a view to facilitate the processing of their applications. The answers to these questions will reflect the candidates' qualifications and will be decisive for the next stages of the selection process.

Depending on the number of applications received, candidates may be asked to undergo a computer-based pre-selection test. This computer-based pre-selection test will be composed of a series of tests comprising multiple-choice questions to assess general aptitudes and competencies as regards verbal reasoning, numerical reasoning and abstract reasoning.

The Selection Committee will evaluate applications (and the results of pre-selection tests if applicable), and select those candidates meeting the eligibility criteria and matching best the selection criteria as outlined above. The selected candidates will be invited to a written test in the form of a case study based on a EU-related scenario, presenting various problems which candidates will be asked to solve, or react to, solely on the basis of the material available. Candidates will be able to take the case study in English, German or French. However, candidates must choose a language for the case study that is not his/her mother tongue.

In addition to the case study, candidates will undergo an interview. During the interview candidates will be evaluated by the Selection Committee, mainly on their specialist knowledge in the field of the selection.

Candidates invited to an interview will be required to bring with them originals and copies or officially certified copies of the documents listed below:

- A document proving their citizenship (e.g. passport);
- Certificates attesting their educational and professional qualifications, in particular those giving access to the profile in question, including an extract from their police file;
- Documentary evidence of their professional experience after the date on which the candidate obtained the qualification giving access to the profile in question, clearly indicating the starting and finishing dates, whether full or part time, and the nature of the duties carried out.

After the interviews the Selection Committee will propose a shortlist of successful candidates to the Appointing Authority of the Agency (the Executive Director, or the interim Executive Director), which may draw up a reserve list of successful candidates valid for three years. The validity of the list may be extended.

As soon as this decision is taken, successful candidates will receive an information letter. However, candidates should note that inclusion in the reserve list does not guarantee recruitment.

Please note that the work of the Selection Committee and its deliberations are secret. Therefore, candidates shall not make direct or indirect contact with the Selection Committee or have anybody do so on their behalf. The Appointing Authority reserves the right to disqualify any candidate who disregards this instruction.

If at any stage in the procedure it is established that any of the information a candidate provided is incorrect, this candidate will be disqualified.

Please note that a binding commitment can only be made after verification of all conditions and it will take the form of a contract signed by the Executive Director (or the interim Executive Director) of the Agency.

8. APPLICATIONS

This selection procedure is published in parallel with the temporary agent selections for the following profiles: Management; IT Specialists; IT Support and Assistance. Candidates may apply for **only one** profile. However, within the Security profile candidates may apply for the two selections proposed: AD 5 (HOME/TA/AD5/06/11) and AD 7 (HOME/TA/AD7/07/11).

Applications must be submitted via the candidate's EPSO account by means of the on-line application form, following the instructions on the EPSO website relating to the various stages of the procedure.

Candidates who do not have an EPSO account[9] should create one by following the instructions for creating an account on the EPSO website http://www.eu-careers.eu/.

Candidates must have a valid e-mail address and are responsible for keeping it, as well as their personal details, up to date in the EPSO account.

It is the candidates' responsibility to complete the on-line application by the deadline. Once the deadline has passed, candidates will no longer be able to submit an on-line application[10]. The

[9] An EPSO account serves as an electronic interface between EPSO and anyone interested in a career in the European institutions. It is used for communicating with candidates, storing and updating their personal data, and keeping track of their applications in compliance with rules applying to the processing of personal data.

application procedure itself can take quite some time because of the amount of information to be provided.

In the course of their application, candidates will be assigned a number the first time they save any data. This will be the reference number should any technical problems arise during the application process. Once the application form has been completed, candidates must submit it by entering their password. They will be informed on-screen if this operation has been successful. The reference number will become the definitive application number, which will have to be quoted in all subsequent correspondence. If the on-screen confirmation does not appear because of some technical problem, candidates can reconnect to the EPSO account at any time, where they will be informed whether the application has been properly registered.

The closing date for the submission of applications is 21.12.2011 at 12 (midday), Brussels time.

Click here to apply: https://europa.eu/epso/application/passport/?comp_id=5335&lang=en

CONTACTS AND INFORMATION

EPSO must be notified of any technical problem concerning the application procedure as soon as possible, using the contact form available on the EPSO website[11].

For any request for information or question on the content of this notice of selection candidates should send an e-mail to the functional mailbox at the following address HOME-SELECTIONS-IT-AGENCY@ec.europa.eu

[10] You are strongly advised not to wait until the last few days before applying, since heavy Internet traffic or a problem with the Internet connection could lead to an on-line session being interrupted before the completion of an application, thereby obliging you to repeat the whole process.
[11] More information is available at: http://europa.eu/epso/apply/contact/details/index_en.htm.