≋ EUROPOL

The Hague, 16 March 2015

Reg. n°: Europol/2015/TA/AD6/188

VACANCY NOTICE

Name of the Post: **Specialist – ICT Infrastructure Engineering (AD6), within the ICT Business Area, ICT Operations Group, Infrastructure Engineering Team at Europol**

Reporting to: **Senior Specialist on the Infrastructure Engineering Team**

1.   About Europol

Applications are invited for this position at the European Police Office (Europol).[1]

Europol is located in The Hague, The Netherlands, and its main tasks are the following:

  a) to collect, store, process, analyse and exchange information and intelligence;

  b) to aid investigations in the Member States, in particular by forwarding all relevant information to the national units;

  c) to ask the competent authorities of the Member States concerned to initiate, conduct or coordinate investigations and to suggest the setting up of joint investigation teams in specific cases;

  d) to provide intelligence and analytical support to Member States in connection with major international events;

  e) to prepare threat assessments, strategic analyses and general situation reports relating to its objective, including organised crime threat assessments.

For more information please visit Europol's website www.europol.europa.eu.

Europol applies a policy of equal opportunity for men and women and accepts applications without distinction on ground of sex, race colour, ethnic or social origin, genetic characteristics, and language, religious, political or other convictions and opinions, financial situation, disability, age sexual orientation, marital status or family situation. Applications from female candidates are particularly encouraged. Employment at Europol is open to nationals of the EU Member States. There is no national quota system in operation but Europol is required to strive for a broad range of nationalities in order to keep a well balanced geographical distribution among its staff members.

---

[1] Europol has been established under the Council Decision (EC) No. 2009/371 of 6 April 2009.

EDOC#758769

2.   Background and main purpose of the post

The ICT Business Area has the responsibility for developing and operating high-quality ICT solutions and capabilities supporting the core mission and support processes of Europol. Some 110 internal staff members are responsible for developing, delivering and maintaining information management and communication technology capabilities that ensure enhanced criminal information exchange between Europol Member States.

The main role of the ICT Operations Group is implementation, installation and maintenance of all ICT Infrastructure components for Europol, the Member States and third parties as well as the support of all computerized systems at Europol.

The ICT Operations group also provides a contact point for services regarding technical enquiries of Member States and Europol staff.

The ICT Operations Group is comprised of several functional teams (e.g. Infrastructure Engineering, Infrastructure Operations, Application Operations, IT Operations Center, Service Management and Service Desk) together with an Embedded Security Team that spans across functional teams in a matrix fashion.

The successful candidate will be part of the ICT Operations Group, Infrastructure Engineering Team within the ICT Business Area working as a Specialist - ICT Infrastructure Engineering.

In his/her functional role, (s)he will be in charge of developing detailed design of ICT Infrastructure with particular focus on VMware and storage solutions. Implement the infrastructure solutions in line with design. Provide 3rd level support for the solutions in scope.

3.   Tasks and responsibilities

The successful applicant will have to carry out the following main duties:

Members of the Infrastructure Engineering team, in their own specific domain area of competence, are in charge of the following tasks:

- Specify technical standards, aligned with the overall Europol Architecture guidelines;

- Actively review Architecture guidelines to ensure manageability and full understanding of technical consequences;

- Specify technical requirements for ICT infrastructure solutions including relevant security controls;

- Create technical design of ICT infrastructure solutions in accordance with solution architecture guidelines and standards, translating high-level solution architectures into concrete designs, procedures and specifications of ICT infrastructure solutions;

- Facilitate installation and configuration activities by ICT operations teams in accordance with engineering designs and specifications, performing trial installation and configuration activities in testing and pre-production environments;

- Develop and maintain sufficient knowledge about the interdependencies of all infrastructure components deployed in the production environment in order to prevent incidents and problems;

- Participate in multi-disciplinary project teams and ICT development initiatives providing technical advice and support and specifying technical designs of ICT infrastructure solutions in alignment with software application designs, ensuring end-to-end operability and supportability by design, in accordance with ICT operational standards;

- Acting as a third level support, perform technical analysis, investigation, troubleshooting and resolution of incidents or problems affecting the Europol ICT infrastructure;

- Provide support to capacity management activities, recommending changes in ICT infrastructure in order to address capacity demands;

- Liaise with ICT engineering teams in partner organisations, including in particular Europol National Units in Member States, acting as primary point of contact for technical changes affecting the interfaces between external and Europol ICT infrastructure;

- Contribute to ICT-wide technical knowledge management, maintaining up-to-date technical documentation and contributing to the ICT knowledge base;

- Provide technical advice and engineering support to other teams in the ICT Business Area;

- Monitor technology developments maintaining up-to-date knowledge of state-of-the-art solutions;

- Perform any other tasks in the area of competence as assigned by the line management.

4. Requirements

4.1 Eligibility criteria:

a. Candidates must:

- Be a national of one of the Member States of the European Union and enjoy full rights as a citizen;

- Have fulfilled any obligations imposed by the applicable laws on military service;

- Produce appropriate character references as to his or her suitability for the performance of the duties;

- Be physically fit to perform the duties pertaining to the position;[2]

- Produce evidence of a thorough knowledge of one of the languages of the Union and a satisfactory knowledge of another language of the Union to the extent necessary for the performance of the duties.

---

[2] Prior to appointment the successful candidate will be medically examined by one of the institution's medical officers in order that the institution may be satisfied that the candidate fulfils the requirements of Article 12(2)(d) CEOS

b. Candidates must have:

- Possess a level of education which corresponds to completed university studies, preferably in the area of Computer Science or Information Technology, attested by a diploma when the normal period of university education is at least 3 years;

  OR

  One of the following professional certifications of an equivalent level in a relevant area: MCSE (Desktop and/or Server Infrastructure), VMware Certified (Advanced) Professional, Symantec Certified Specialist Altiris Client Management Suite, CISSP (Certified Information Systems Security Professional), Citrix Certified Professional (Expert).

- **In addition** to the above at least **3** years of work experience gained following the award of the diploma or first relevant certificate.

4.2 Selection criteria:

a. Professional experience:

Essential:

- Experience of working in an large and complex IT environment;
- Experience with Enterprise-level managed deployments of Microsoft technologies (client and server);
- Experience with diverse endpoint technologies including mobile devices, their integrations and related security aspects;
- Experience with automated deployment technologies (e.g. Altiris);
- Experience with virtualisation technologies (e.g. VMWare);
- Experience with Server-based computing technologies (e.g. Citrix XenApp).

Desirable:

- Experience with managed deployments of Linux technologies (client and server).

b. Professional knowledge:

Essential:

- Sound knowledge of recent Microsoft Operating systems and their security aspects;
- Sound knowledge of wide range of end-user applications with aspects of deploying and supporting them;
- Sound knowledge of Networking, Communication Protocols, Security and System Policies;
- Sound knowledge of client endpoint hardware configuration and related maintenance and troubleshooting (e.g. workstations, mobile devices, print and scanning devices);

- Sound knowledge of client endpoint design and configuration of remote deployment of system images and application packages.

Desirable:

- Sound knowledge of Linux endpoints and servers and their security aspects;
- Knowledge of sandbox concepts and IT forensic evidence processing;
- Project management methodologies.

c. Technical skills and competencies:

Essential:

- Excellent communication skills in English, both orally and in writing;
- Ability to write structured documentation, translating high level architecture concepts into an implementable design, test approach and handover to Operations;
- Ability to recognise market trend and blend them into an ICT Infrastructure roadmap in the area of expertise, in line with Architecture concepts;
- Ability to analyse technical problems and provide practical solutions taking security considerations into account;
- In addition to managing own work, ability to clearly define statements of work and perform contractors' work supervision including monitoring production of quality deliverables;
- Ability to act independently on timely execution of work-plans, resolving arising issues with limited involvement of supervisors and other teams, while maintaining required project timelines and communication standards;

d. Social skills and competencies:

Essential:

- Excellent interpersonal skills;
- Stress resilience and demonstrated ability to work well under pressure, both independently and in a team;
- High level of customer-orientation;
- Ability to establish and maintain effective working relations with co-workers in an international and multi-disciplinary work environment;
- High degree of commitment and flexibility.

5. Selection procedure[3]

The Contracting Authority sets up a Selection Committee which consists of at least three members, one from the Business Area Administration/Recruitment and Selection Team of Europol, one from the concerned Business Area or Department and one designated by the Staff Committee.

For **non-restricted** posts the Contracting Authority may designate up to two additional members to the Selection Committee on a proposal from the Management Board, either from another service of Europol, from outside Europol or from outside the community institutions including Member States.

The Selection Committee determines candidates' suitability for the position by assessing their skills, experience and qualifications against the established job profile and makes an initial selection from the applications received.

The Selection Committee will invite the 5 highest scoring candidates (short-listed). All candidates having a score equal to the 5th highest scoring candidate will be included to the list of invited candidates.

Shortlisted applicants are invited to participate in a post-related selection procedure, generally consisting of written and/or practical tests and competency-based interviews.

The Contracting Authority makes a decision of appointment on the basis of advice from the Selection Committee. He will inform the Committee of his decision. All candidates who attend the selection procedure will be informed of the outcome.

Candidates who attended a selection procedure may request feedback on their performance of the written test and interview within three months after the selection procedure. Europol will not be in a position to respond to feedback inquiries received outside this time frame.

The Selection Committee's work and deliberations are confidential. It is forbidden for candidates to make direct or indirect contact with the members of the Selection Committee or for anyone to do so on their behalf. All enquiries or requests for information or documentation in relation to the competition should be addressed to the Europol Recruitment Team.

6. Salary

Scale: AD6

The basic monthly salary is EUR **4960, 64** (step 1) or EUR **5169, 10** (step 2).

The step in grade is determined on the basis of professional experience gained after the education required for the position and in line with applicable implementing rules.

In addition, if applicable, allowances such as expatriation allowance, household allowance, dependent child allowance and education may be granted.

Europol offers a comprehensive welfare package comprising additional benefits such as medical insurance, unemployment and invalidity allowance as well as a pension scheme.

Salaries are subject to a community tax but exempt from national taxation.

---

[3] Detailed information on the selection procedure, including the appeal procedure is available in the Europol Recruitment Guidelines, on Europol's website.

7.	Terms and conditions

7.1   Probation period

Engagement for this position is subject to the successful completion of a probationary period of **9** months. Within this period the successful candidate will have to undergo a post-related security screening.

Europol reserves the right to terminate the contract of employment during or at the end of the probation period in accordance with Article 14 of CEOS.

7.2   Security screening and certificate of good conduct

All candidates who have successfully passed a selection procedure are required to apply for a national "certificate of good conduct" at the time an offer of employment is made. The "certificate of good conduct" must be provided to Europol prior the signature of the employment contract. In case of unfavourable entries in the "Certificate of good conduct" Europol reserves the right not to award an employment contract.

However, the national certificate of good conduct does not substitute a valid full Personal Security Clearance Certificate (PSCC) that must be obtained for all Europol staff at the level indicated in the Job Description. A PSCC is a certificate issued by a competent authority establishing that an individual is security cleared. It contains: the level of clearance; the date of issuance and the date of expiry. Failure to obtain the requisite security clearance before the expiration of the probationary period may be cause for termination of employment contract.

The requested level of Security Clearance for this post is CONFIDENTIEL UE/EU CONFIDENTIAL.

7.3   Contract of employment

The successful candidate will be recruited as **Temporary Agent AD 6** pursuant to Article 2 (f) of CEOS, for a period of 5 years[4] (full-time – 40 hours a week).

The contract may be renewed once for a period of 4 years. Only in highly exceptional cases, Europol grants third contracts of an indefinite nature.

The place of employment will be The Hague, The Netherlands.

For further information on terms and conditions please consult the EC Staff Regulations which are available on Europol's website www.europol.europa.eu.

8.	Data Protection

The data submitted is processed in order to assess the suitability of candidates for a position at Europol. All personal data collected for the purpose of the selection procedure will only be used within this specific context and will not be disclosed to any third party, except for restricted posts in which the application may be transmitted to the National Unit and the respective Liaison Bureau.

---

[4] For the internal candidates the duration of the current contract will be taken into account in the total duration of the contract.

Any data provided will be treated in strict confidence and in full compliance with all applicable data protection rules. The legal bases for the processing of personal data are the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities (Title III Chapter 1) and their implementing rules.

All documents provided to Europol will be kept in Europol's files and will not be returned to the candidate. Applications of non-recruited candidates will be kept for a maximum of two years. Data of non-recruited applicants on the reserve list for appointment will be kept for a maximum of two years after the expiry of the reserve list. Data of recruited candidates will be transferred to their personal file.

The Head of Administration is responsible for the data processing operation. Candidates have the right to access, rectify, block and erase their personal data in accordance with the applicable data protection rules.

Candidates have the right of recourse to the Europol Data Protection Office (Data Protection Office - PO Box 90850, 2509 LW The Hague, The Netherlands) and the Joint Supervisory Body (www.europoljsb.consilium.europa.eu). Applications sent to the DPO or JSB will not be processed and will be deleted.

9. Additional Information

9.1 Main dates:

Deadline for application:	30 April 2015
Recruitment procedure:	to be determined
Starting date of employment:	as soon as possible

9.2 Selection procedure

Please refer to the EUROPOL RECRUITMENT GUIDELINES available on Europol's website www.europol.europa.eu for further details on the application process and the selection procedure.

9.3 Contact Details

For further details on the application process please call +31 (0) 70 353 1583 or +31 (0) 70 353 1628.