EUROPEAN COMMISSION

VACANCY NOTICE FOR A POST OF SECONDED NATIONAL EXPERT

DG – Directorate – Unit	DIGIT-B-1 – Data, Artificial Intelligence and Web
Post number in sysper:	288740
Contact person: Provisional starting date: Initial duration: Place of secondment:	DIEZ PEREZ Esther Q3 quarter 2024 2 years ☒ Brussels ☐ Luxemburg ☐ Other: Click or tap here to enter text.
Type of secondment	◉ With allowances ○ Cost-free
This vacancy notice is open to: ◉ EU Member States as well as ☐ The following EFTA countries: ☐ Iceland ☐ Liechtenstein ☐ Norway ☐ Switzerland ☐ The following third countries: …. ☐ The following intergovernmental organisations: … ○ EFTA-EEA In-Kind agreement (Iceland, Liechtenstein, Norway)	
Deadline for applications	○ 2 months ◉ 1 month Latest application date: 25-07-2024

Entity Presentation (We are)

The mission of 'Digit B1.001 – Data, AI and Innovation Policy' sector is to cover the corporate policy needs in the areas of data, AI and innovation through relevant digital services.

The activities of the sector in the areas of data, artificial intelligence and innovation policy contribute to the realisation of the corporate digital priorities of the European Commission

Digital Strategy (ECDS), to the realisation of the corporate objectives in the areas of data, artificial intelligence and digital innovation, and to the realisation of the specific objectives of the Strategic Plan of Digit.

The portfolio of Digit B1.001 service offering includes:

- Data governance, risk and compliance (Data GRC) supporting services;
- AI governance, risk and compliance (AI GRC) supporting services;
- Digital innovation supporting services; and
- AI regulatory sandboxing (supporting) services.

The 'AI Governance, Risk and Compliance' function is part of the 'Data, AI and Innovation Policy' sector. The mission of the function is to provide governance, risk, compliance, communication and awareness raising supporting services in the area of AI. The cybersecurity policy aspects of AI are an important area of the function.

Job Presentation (We propose)

The 'AI Cybersecurity Policy' officer of the 'AI Governance, Risk and Compliance' function covers the cybersecurity aspects of the corporate AI policy in close collaboration with the Directorate for 'Cybersecurity - DIGIT S'. Key objective of the job is to define the scope of the AI cybersecurity policy services, and to develop and deliver them at corporate level. The job holder formulates the technical vision, provides strong leadership, coordinates and contributes to the activities of the area; develops the business case and the delivery model for the services of the area, whenever necessary in cooperation with external contractors; evaluates, deploys and maintains tools and solutions needed to deliver the services; communicates with business owners and technical stakeholders; proposes improvements to the operational processes; defines the related performance indicators; and reports on the efficiency and on the maturity of the processes of the area.

Jobholder Profile (We look for)

AI Cybersecurity Policy Officer

Under the supervision of the Head of Sector on 'Data, AI and Innovation Policy', the seconded national expert will be responsible for carrying out tasks to support the unit implementing cybersecurity and technical aspects of the AI Act, especially in relation to general-purpose AI models and systems as detailed below. The profile on the 'AI cybersecurity policy' officer may relate to research scientists, cyber security and computer scientists, software engineers.

The successful candidate should have a technological background in AI, complemented by experience in cybersecurity and computer science. Proven technical experience is required in the field of AI technologies such as for example machine learning, deep learning, frameworks including ethics and privacy, and cybersecurity. In addition, experience in risk management, project management, drafting of IT security/AI guidance,

implementation of legislation/standards, contracts and communication would be a strong asset.

Tasks may include, but are not limited to:

- Contribute to the implementation of the AI Act, by establishing evidence-based approaches, guidelines and analytical frameworks for cybersecurity and related aspects.
- Contribute to the development of policies and procedures including the relevant internal digital workflows for internal AI Act enforcement.
- Engage with relevant stakeholders to address challenges and to communicate.
- Follow the internal digital services, market products and technology trends to support the AI policy services.
- Carrying out monitoring and control activities. Support the assessment of cybersecurity and other elements of Internal IT projects using AI elements.
- Drafting and reviewing technical annexes for procurement procedures.

Eligibility criteria

The secondment will be governed by the **Commission Decision C(2008) 6866** of 12/11/2008 laying down rules on the secondment to the Commission of national experts and national experts in professional training (SNE Decision).

Under the terms of the SNE Decision, you need to comply with the following eligibility criteria at **the starting date** of the secondment:

- Professional experience: at least three years of professional experience in administrative, legal, scientific, technical, advisory or supervisory functions which are equivalent to those of function group AD.

- Seniority: having worked for at least one full year (12 months) with your current employer on a permanent or contract basis.

- Employer: must be a national, regional or local administration or an intergovernmental public organisation (IGO); exceptionally and following a specific derogation, the Commission may accept applications where your employer is a public sector body (e.g., an agency or regulatory institute), university or independent research institute.

- Linguistic skills: thorough knowledge of one of the EU languages and a satisfactory knowledge of another EU language to the extent necessary for the performance of the duties. If you come from a third country, you must produce evidence of a thorough knowledge of the EU language necessary for the performance of his duties.

Conditions of secondment

During the full duration of your secondment, you must remain employed and remunerated by your employer and covered by your (national) social security system.

You shall exercise your duties within the Commission under the conditions as set out by aforementioned SNE Decision and be subject to the rules on confidentiality, loyalty and absence of conflict of interest as defined therein.

In case the position is published with allowances, these can only be granted when you fulfil the conditions provided for in Article 17 of the SNE decision.

Staff posted in a European Union Delegation are required to have a security clearance (up to SECRET UE/EU SECRET level according to Commission Decision (EU, Euratom) 2015/444 of 13 March 2015. It is up to you to launch the vetting procedure before getting the secondment confirmation.

Submission of applications and selection procedure

If you are interested, please follow the instructions given by your employer on how to apply.

The European Commission **only accepts applications which have been submitted through the Permanent Representation / Diplomatic Mission to the EU of your country, the EFTA Secretariat or through the channel(s) it has specifically agreed to**. Applications received directly from you or your employer will not be taken into consideration.

You should draft you CV in English, French or German using the **Europass CV format** (Create your Europass CV | Europass). It must mention your nationality.

Please do not add any other documents (such as copy of passport, copy of degrees or certificate of professional experience, etc.). If necessary, these will be requested at a later stage.

Processing of personal data

The Commission will ensure that candidates' personal data are processed as required by Regulation (EU) 2018/1725 of the European Parliament and of the Council ([1]). This applies in particular to the confidentiality and security of such data. Before applying, please read the attached privacy statement.

([1]) Regulation (EU) 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39