VACANCY NOTICE

SECONDED NATIONAL EXPERT TO THE EUROPEAN COMMISSION

Post identification: (DG-DIR-UNIT)	**CNECT-H-2**
Head of Unit: **Email address:** **Telephone:** **Number of available posts:** **Suggested taking up duty:** **Suggested initial duration:** **Place of secondment:**	**Jakub Boratyński** **CNECT-H2@ec.europa.eu** **+32 2 296 9452** 1 **3rd quarter 2021** [1] **2 years**[1] ☒ **Brussels** ☐ **Luxemburg** ☐ **Other: ……..**
	☒ **With allowances** ☐ **Cost-free**

This vacancy notice is also open to

☐ **the following EFTA countries :**
☐ **Iceland** ☐ **Liechtenstein** ☐ **Norway** ☐ **Switzerland**
☐ **EFTA-EEA In-Kind agreement (Iceland, Liechtenstein, Norway)**
☐ **the following third countries:**
☐ **the following intergovernmental organisations:**

1. Nature of the tasks

The Cybersecurity and Digital Privacy Policy Unit (CNECT/H/2) is responsible for policy and law in the areas of cybersecurity and the protection of individuals' privacy on the Internet.

In the area of cybersecurity, the Unit is responsible for the implementation of the EU cybersecurity strategy, including the implementation of the first Union cybersecurity law known as the Directive on Security of Network and Information Systems (NIS Directive), including the proposal for a revised NIS Directive, and of the Regulation on the European Network Information Security Agency (ENISA) and of the EU certification framework ("Cybersecurity Act").

In the area of digital privacy, the Unit negotiates the proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications (ePrivacy Regulation). The unit is also responsible for the monitoring of the national implementation of the current ePrivacy Directive.

The unit collaborates closely with the Cybersecurity Technology & Capacity Building Unit (CNECT.H.1) and with other units in the DG and associated services in other DGs.

The Directorate General applies a team oriented approach, applying collaboration benefiting from DG CONNECT's expertise in ICT and the digital single market and bringing together teams with expertise across the Directorate and DG CONNECT, for example in the areas of the Internet of Things and Artificial Intelligence.

The Unit is dynamic, committed, has a good team spirit and a very friendly atmosphere.

[1] These mentions are given on an indicative basis only (Art.4 of the SNE Decision).

We propose an interesting and challenging job as Policy Officer in a fascinating, emerging area, cutting across multiple policy domains. The successful candidate will work as part of the cybersecurity policy team, but will also collaborate with members of the Unit involved in privacy.

The tasks attributed to the successful candidate would be drawn from the following indicative list:

- Contribute to the work on and facilitate the implementation of the Directive on security of network and information systems (NIS Directive), in particular related to the cooperation between Member States;
- Contribute to the work on the negotiations of the legislative proposal for a revised NIS Directive (NIS2);
- Contribute to the work on the implementation of the legislation related to the security of public electronic communications networks or publically available electronic communications services (eg. Framework directive and forthcoming electronic communications code);
- Follow up on actions in relation to the EU Security Union Strategy and the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises and the blueprint;
- Follow up on the implementation of the EU Cybersecurity Strategy for the digital decade in cooperation with other Commission departments and EEAS ;
- Handle parliamentary questions, citizen questions and briefings.

The successful candidate will work closely with a solid team with a very good level of expertise in cybersecurity.

The final allocation of tasks would depend on the specific expertise and profile of the selected candidate.

2. Main qualifications

a) Eligibility criteria

The following eligibility criteria must be fulfilled by the candidate in order to be seconded to the Commission. Consequently, the candidate who does not fulfil all of these criteria will be automatically eliminated from the selection process.

- 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: candidates must have at least one year seniority with their employer, that means having worked for an eligible employer as described in Art. 1 of the SNE decision on a permanent or contract basis for at least one year before the secondment;

- 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. SNE from a third country must produce evidence of a thorough knowledge of one EU language necessary for the performance of his duties.

b) Selection criteria

Diploma
- university degree or
- professional training or professional experience of an equivalent level

in the field(s) : political science, business and/or economics with a profound understanding of ICT technologies and/or privacy issues or alternatively background in computer sciences/digital technologies with a profound understanding of policy issues would be considered an advantage.
A legal background would be considered an additional asset.

Professional experience

We look for a dynamic person with an extensive ICT policy expertise in particular on cybersecurity, with excellent analytical and drafting skills.

Work experience in the areas related to the implementation and enforcement of national law transposing the Directive on Network and Information Security (NIS Directive) and ePrivacy Directive, including some experience in EU fora, such as the NIS Cooperation Group or the so-called "Art 13 a ENISA group", would be an important advantage, as well as work experience in the area of cybersecurity incident response and crisis management.

Work experience in inter-institutional relations, notably legislative negotiations and/or implementation of Union law would also be an asset.

The candidate should have a strong interest in working on cutting edge legal and policy issues related to digital technologies.

The candidate should demonstrate a proactive approach and be able to work autonomously, while having a strong sense of team spirit.

S/he should be capable of coping with tight deadlines and periods of high workload.

Language(s) necessary for the performance of duties

The job requires excellent knowledge of English, both drafting skills and verbal communication. A solid understanding and operational working level of French would be an asset.

3. Submission of applications and selection procedure

Candidates should send their application according to the **Europass CV format** (http://europass.cedefop.europa.eu/en/documents/curriculum-vitae) in English, French or German **only to the Permanent Representation / Diplomatic Mission to the EU of their country**, which will forward it to the competent services of the Commission within the deadline fixed by the latter. The CV must mention the date of birth and the nationality of the candidate. **Not respecting this procedure or deadlines will automatically invalidate the application.**

Candidates are asked not to 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.
Candidates will be informed of the follow-up of their application by the unit concerned.

4. Conditions of the secondment

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).
The SNE will remain employed and remunerated by his/her employer during the secondment. He/she will equally remain covered by the national social security system.
Unless for cost-free SNE, allowances may be granted by the Commission to SNE fulfilling the conditions provided for in Art. 17 of the SNE decision.

During the secondment, SNE are subject to confidentiality, loyalty and absence of conflict of interest obligations, as provided for in Art. 6 and 7 of the SNE Decision.
If any document is inexact, incomplete or missing, the application may be cancelled.

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, OJ L 72, 17.03.2015, p. 53).

The selected candidate has the obligation to launch the vetting procedure before getting the secondment confirmation.

5. Processing of personal data

The selection, secondment and termination of the secondment of a national expert requires the Commission (the competent services of DG HR, DG BUDG, PMO and the DG concerned) to process personal data concerning the person to be seconded, under the responsibility of the Head of Unit of DG HR.DDG.B4. The data processing is subject to the SNE Decision as well as the Regulation (EU) 2018/1725.
Data is kept by the competent services for 10 years after the secondment (2 years for not selected or not seconded experts).
You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access, rectify or erase your personal data and the right to restrict the processing of your personal data. Where applicable, you also have the right to object to the processing or the right to data portability.
You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given below.

Contact information

- **The Data Controller**
  If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the Data Controller, HR.DDG.B.4, HR-MAIL-B4@ec.europa.eu.

- **The Data Protection Officer (DPO) of the Commission**
  You may contact the Data Protection Officer (DATA-PROTECTION-OFFICER@ec.europa.eu) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

- **The European Data Protection Supervisor (EDPS)**
  You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.
  To the attention of candidates from third countries: your personal data can be used for necessary checks.