

**Seconded National Expert (SNE)
at the General Secretariat of the Council of the European Union**

Directorate 2 Justice of DG Justice and Home Affairs

Ref.: SNE/04/2026 (JAI.2) - 1 post (312925)

Job description

A. Main tasks and responsibilities

As a member of the cyber team in DG JAI, the selected seconded national expert will in particular be expected to:

- Advise the Presidency on the handling of cyber policy files at all levels of the decision-making process (working party, Coreper, Council, trilogues, etc.); this includes advice on procedural aspects as well as on strategy for finding solutions and compromises in the different files.;
- Prepare draft documents, including discussion papers and compromise texts, to advance the work in the HWPCI and at other levels.
- Ensure the proper preparation of meetings of the HWPCI, including preparation of the agendas and working with the assistants of the cyber team to ensure the production and dissemination of documents.
- Write or contribute to briefs for the chairs (Coreper, Council, trilogues, European Council) on cyber-related issues.
- Attend meetings on cyber issues in different institutions, bodies and agencies.

The HWPCI covers a wide range of cyber policy issues. Because of the horizontal dimension of its mandate, it places an equally strong focus on both the internal and external dimension (including cyber diplomacy) of cyber policy. The files covered by the seconded national expert will depend on the profile of the selected candidate and on the issues dealt with in the Council during the secondment.

The seconded national expert will need to maintain a good contact network, including among delegations of Member States, the Commission, the European External Action Service, the European Parliament, the European Agency for cybersecurity (ENISA), CERT-EU, Europol and the European Cybersecurity Competence Centre (ECCC).

DG JAI.2 attaches great importance to internal coordination: the cyber team cooperates closely with staff responsible for related policy issues such as digital policy, combating cybercrime, external relations, restrictive measures or crisis management. It also cooperates closely with colleagues responsible for, among other things, the cybersecurity of the organisation.

The secondment may entail some missions abroad, for example to attend conferences or meetings organised by national authorities or EU agencies.

B. General conditions

According to the Decision¹ applicants must:

- have worked for their employer on a permanent or contract basis for at least 12 months before their secondment;
- remain in the service of their employer throughout the period of secondment;
- have at least three years' full-time experience of administrative, scientific, technical, advisory or supervisory functions relevant to the performance of the duties assigned to them;
- be nationals of one of the Member States of the European Union;
- have a thorough knowledge of one official language of the EU² and a satisfactory knowledge of a second language for the performance of their duties.

C. Qualifications and experience

- A level of education in a relevant field, which corresponds to completed university studies of at least three years attested to by a diploma, or equivalent vocational training attested to by a diploma, or a certificate issued by an institute for advanced studies or by an institute or an academy such as a national school of magistracy or police;
- Professional experience of at least three years in the field of cybersecurity policy or cyber diplomacy;
- Knowledge of the EU institutional and decision-making framework;
- A thorough oral and written command of English, and a good knowledge of French as an asset.

D. Required skills

- Pro-activity and ability to work independently, with a strong sense of responsibility;
- Capacity to plan and organise and to deliver quality results within deadlines;
- Political sensitivity in understanding complex files;
- Strong analytical skills, as well as judgement and problem-solving skills;
- Ability to adapt to and to work in a multicultural environment;
- Ability to coordinate between multiple stakeholders;
- Capacity to establish and maintain constructive relations with a wide variety of stakeholders;
- Strong interpersonal communication skills.

E. Security clearance

National security clearance at EU SECRET level is required. Such clearance needs to be obtained by the candidate from their competent authorities before secondment to the General Secretariat of the Council. The validity of the clearance should cover the entire period of the secondment. In the absence of security clearance, the General Secretariat reserves the right to refuse the candidate's secondment.

¹ Council Decision of 23 June 2015 concerning the rules applicable to experts on secondment to the General Secretariat of the Council.

² The languages of the EU are: Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, Irish, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish.

The GSC is committed to diversity and inclusion. We actively seek diversity and promote inclusion among staff. We embrace all differences based on geographical and demographic characteristics and identities and strongly believe that diversity enriches our perspectives, improves our performance, and increases our well-being. We therefore encourage applications from qualified candidates from diverse backgrounds and on the broadest possible geographical basis amongst the EU Member States.

Please find here a [link](#) to the privacy statement about the treatment of your personal data.

Further information on the nature of the post can be obtained from Mr Serge de Biolley, Director of JAI.2 in DG JAI (tel.: 02 281 90 11; email: serge.debiolley@consilium.europa.eu).

