EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY
**Competitions, Selections & Secondments**

Brussels
12/05/2026
HR.B.1.003

# VACANCY NOTICE FOR A POST OF SECONDED NATIONAL EXPERT ([1])

| | |
|---|---|
| **DG – Directorate – Unit**<br>DG - Direction – Unité<br>GD - Direktion - Referat | DIGIT.B.1 |
| **Post Number in Sysper**<br>Numéro de poste dans Sysper<br>Stellennummer in Sysper | 459545 |
| **Provisional Starting Date**<br>Date d'entrée en fonction prévisionnelle<br>Gewünschter Dienstantritt<br><br>**Initial Duration (months)**<br>Durée initiale (mois)<br>Dauer (Monate)<br><br>**Place of Secondment**<br>Lieu de détachement<br>Abordnungsort | Q1 2027<br><br>24<br><br>Brussels<br>Bruxelles<br>Brüssel |
| **Type of Secondment**<br>Type de détachement<br>Art der Entsendung | With allowances<br>Avec indemnités<br>Mit Vergütung |
| **This Vacancy Notice is open to**<br>Cet avis de vacance est ouvert aux<br>Die Stelle ist offen für | Member States<br>États membres<br>Mitgliedstaaten |
| **Deadline for Applications**<br>Date limite de candidature<br>Bewerbungsschluss | 27/07/2026 |
| **Eligibility Criteria**<br>Critères d'éligibilité<br>Zulassungsbedingungen | English Version, Version Française, Deutsche Version |

([1]) To ensure accessibility and inclusivity, this notice is provided in the three official languages of the European Union: English, French, and German. For the job descriptions please refer to your preferred language version.

Brussels
12/05/2026
HR.B.1.003

**Entity presentation:**

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:**

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:**

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, for the AI Governance, risk and compliance (supporting) services, 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, computer scientists and 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, implementation of generative AI based applications, including ethics and privacy, and cybersecurity aspects. 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 AI@EC Communication work program, supporting governance, risk and compliance activities referred to the AI Act and corporate AI governance, 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 governance enforcement.
• Engage with relevant stakeholders to address challenges, raise awareness and communication purposes as trainings or webinars.
• Follow the internal digital and AI 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.

Brussels
12/05/2026
HR.B.1.003

**Présentation de l'entité:**

Le secteur « DIGIT B1.001 – Politique en matière de données, d'IA et d'innovation » a pour mission de couvrir les besoins en matière de politique d'entreprise dans les domaines des données, de l'IA et de l'innovation au moyen de services numériques pertinents.

Les activités du secteur dans les domaines des données, de l'intelligence artificielle et de la politique de l'innovation contribuent à la mise en œuvre des priorités numériques de l'entreprise dans le cadre de la stratégie numérique de la Commission européenne (ECDS), à la réalisation des objectifs de l'entreprise dans les domaines des données, de l'intelligence artificielle et de l'innovation numérique, ainsi qu'à l'atteinte des objectifs spécifiques du plan stratégique de numérisation.

Le portefeuille de l'offre de services de DIGIT B1.001 comprend :

des services de soutien à la gouvernance, aux risques et à la conformité des données (Data GRC) ;
des services de soutien à la gouvernance, aux risques et à la conformité en matière d'IA (IA GRC) ;
des services de soutien à l'innovation numérique ;
des services de sandboxing réglementaire de l'IA.
La fonction « Gouvernance, risques et conformité de l'IA » fait partie du secteur « Politique en matière de données, d'IA et d'innovation ». Sa mission est de fournir des services d'appui à la gouvernance, à la gestion des risques, à la conformité, à la communication et à la sensibilisation dans le domaine de l'IA. Les aspects relatifs à la politique de cybersécurité de l'IA constituent un domaine important de la fonction.

**Présentation du poste:**

"L'agent « Politique de cybersécurité de l'IA » de la fonction « Gouvernance, risques et conformité de l'IA » couvre les aspects de cybersécurité de la politique institutionnelle en matière d'IA, en étroite collaboration avec la direction « Cybersécurité – DIGIT S ».

L'objectif principal du poste est de définir le champ d'application des services stratégiques en matière de cybersécurité de l'IA, ainsi que de les développer et de les fournir au niveau de l'entreprise. Le titulaire du poste définit la vision technique, assure un leadership fort, coordonne et contribue aux activités du domaine ; élabore l'analyse de rentabilisation et le modèle de prestation des services, le cas échéant, en coopération avec des prestataires externes ; évalue, déploie et maintient les outils et les solutions nécessaires à la fourniture des services ; communique avec les responsables métier et les parties prenantes techniques ; propose des améliorations aux processus opérationnels ;

définit les indicateurs de performance correspondants ; et rend compte de l'efficacité et de la maturité des processus du domaine.

**Profil du titulaire du poste:**

"Responsable des politiques en matière de cybersécurité dans le domaine de l'IA

Sous la supervision du chef de secteur « Politique en matière de données, d'IA et d'innovation », l'expert national détaché sera chargé d'exécuter des tâches d'appui à l'unité chargée de la mise en œuvre de la cybersécurité et des aspects techniques de la législation sur l'IA, dans le cadre des services de gouvernance, de gestion des risques et de conformité en matière d'IA, en particulier en ce qui concerne les modèles et systèmes d'IA à usage général, comme indiqué ci-dessous. Le profil du responsable de la politique de cybersécurité de l'IA peut correspondre à des chercheurs, des spécialistes de la cybersécurité, des informaticiens et des ingénieurs logiciels.

Le candidat retenu doit disposer d'une formation technologique en IA, complétée par une expérience en cybersécurité et en informatique. Une expérience technique avérée est requise dans le domaine des technologies de l'IA, telles que l'apprentissage automatique, l'apprentissage profond, les cadres (frameworks), la mise en œuvre d'applications génératives fondées sur l'IA, y compris les aspects d'éthique et de protection de la vie privée, ainsi que les aspects liés à la cybersécurité. En outre, une expérience en gestion des risques, en gestion de projets, en rédaction d'orientations en matière de sécurité informatique et d'IA, en mise en œuvre de la législation et/ou des normes, en gestion contractuelle et en communication constituerait un atout important.

Les tâches peuvent inclure, sans toutefois s'y limiter :

Contribuer à la mise en œuvre du programme de travail sur la communication AI@EC, en soutenant les activités de gouvernance, de gestion des risques et de conformité prévues par la législation sur l'IA et par la gouvernance d'entreprise en matière d'IA, en définissant des approches, des lignes directrices et des cadres d'analyse fondés sur des données probantes pour la cybersécurité et les aspects connexes.
Contribuer à l'élaboration de politiques et de procédures, y compris les flux de travail numériques internes pertinents pour l'application de la gouvernance interne de l'IA.
Dialoguer avec les parties prenantes concernées pour relever les défis, sensibiliser et communiquer, sous la forme de formations ou de webinaires.
Suivre les tendances internes en matière de services numériques et d'IA, ainsi que les produits et technologies du marché, afin de soutenir les services stratégiques en matière d'IA.
Effectuer des activités de surveillance et de contrôle. Soutenir l'évaluation de la cybersécurité et d'autres éléments des projets informatiques internes utilisant des composantes d'IA.
Rédiger et réviser les annexes techniques pour les procédures de passation de marchés.

Brussels
12/05/2026
HR.B.1.003

**Entitätsvorstellung:**

Die Aufgabe des Sektors DIGIT. B1.001 – Daten-, KI- und Innovationspolitik“ besteht darin, den unternehmenspolitischen Bedarf in den Bereichen Daten, KI und Innovation durch einschlägige digitale Dienste zu decken.
Die Tätigkeiten des Sektors in den Bereichen Daten, künstliche Intelligenz und Innovationspolitik tragen zur Verwirklichung der digitalen Prioritäten der Unternehmen der Digitalstrategie (ECDS) der Europäischen Kommission, zur Verwirklichung der Unternehmensziele in den Bereichen Daten, künstliche Intelligenz und digitale Innovation sowie zur Verwirklichung der spezifischen Ziele des Digitalen Strategieplans bei.
Das Leistungsportfolio von Digit B1.001 umfasst:
• Unterstützende Dienstleistungen für Data Governance, Risk and Compliance (Data GRC);
• Unterstützende Dienstleistungen für KI Governance, Risiko und Compliance (AI GRC);
• Unterstützende Dienstleistungen für digitale Innovation; und
• KI-Regulierungs-Sandboxing-Dienste (Unterstützungsdienste).
Die Funktion „KI-Governance, Risiko und Compliance“ ist Teil des Sektors „Daten-, KI- und Innovationspolitik“. Aufgabe der Funktion ist die Bereitstellung von unterstützenden Diensten in den Bereichen Governance, Risiko, Compliance, Kommunikation und Sensibilisierung im Bereich KI. Die Aspekte der Cybersicherheitspolitik der KI sind ein wichtiger Bereich der Funktion.

**Stellenbeschreibung:**

Der Beauftragte für die KI-Cybersicherheitspolitik der Funktion „KI-Governance, Risiko und Compliance“ befasst sich in enger Zusammenarbeit mit der Direktion „Cybersicherheit – DIGIT S“ mit den Cybersicherheitsaspekten der KI-Politik der Unternehmen. Hauptziel der Stelle ist es, den Umfang der politischen Dienste für die KI-Cybersicherheit zu definieren und sie auf Unternehmensebene zu entwickeln und bereitzustellen. Der Stelleninhaber formuliert die technische Vision, bietet eine starke Führung, koordiniert und trägt zu den Aktivitäten des Bereichs bei; entwickelt den Business Case und das Liefermodell für die Dienstleistungen des Bereichs, wann immer dies in Zusammenarbeit mit externen Auftragnehmern erforderlich ist; evaluiert, implementiert und wartet Instrumente und Lösungen, die für die Erbringung der Dienstleistungen erforderlich sind; kommuniziert mit Unternehmern und technischen Interessenträgern; schlägt Verbesserungen der operativen Prozesse vor; legt die entsprechenden Leistungsindikatoren fest; und berichtet über die Effizienz und die Reife der Prozesse des Bereichs.

**Anforderungsprofil:**

KI-Cybersicherheitsbeauftragter
Unter der Aufsicht des Sektorleiters „Daten-, KI- und Innovationspolitik“ wird der abgeordnete nationale Sachverständige für die Wahrnehmung der Aufgaben zur Unterstützung des Referats, das Cybersicherheit und technische Aspekte des KI-Gesetzes umsetzt, für die KI-Governance-, Risiko- und Compliance- (Unterstützungs-)Dienste zuständig sein, insbesondere in Bezug auf KI-Modelle und -Systeme mit allgemeinem Verwendungszweck (siehe unten). Das Profil des Beauftragten für die KI-Cybersicherheitspolitik kann sich auf Forschungswissenschaftler, Cybersicherheitswissenschaftler, Informatiker und Softwareingenieure beziehen.
Der erfolgreiche Bewerber sollte über einen technologischen Hintergrund im Bereich KI verfügen, der durch Erfahrung in den Bereichen Cybersicherheit und Informatik ergänzt wird. Bewährte technische Erfahrung ist im Bereich der KI-Technologien erforderlich, wie z. B. maschinelles Lernen, Deep Learning, Frameworks, Implementierung generativer KI-basierter Anwendungen, einschließlich Ethik und Datenschutz, und Cybersicherheitsaspekte. Darüber hinaus wären Erfahrungen in den Bereichen Risikomanagement, Projektmanagement, Erstellung von IT-Sicherheits-/KI-Leitlinien, Umsetzung von Rechtsvorschriften/Standards, Verträge und Kommunikation von großem Vorteil.
Zu den Aufgaben können gehören, sind aber nicht beschränkt auf:
• Beitrag zur Umsetzung des Arbeitsprogramms „AI@EC Communication“ zur Unterstützung von Governance-, Risiko- und Compliance-Aktivitäten im Sinne des KI-Gesetzes und der KI-Governance von Unternehmen, indem evidenzbasierte Ansätze, Leitlinien und analytische Rahmen für Cybersicherheit und damit zusammenhängende Aspekte festgelegt werden.
• Mitwirkung an der Entwicklung von Strategien und Verfahren, einschließlich der einschlägigen internen digitalen Arbeitsabläufe für die Durchsetzung der internen KI-Governance.
• Zusammenarbeit mit einschlägigen Interessenträgern, um Herausforderungen anzugehen, das Bewusstsein zu schärfen und Kommunikationszwecke wie Schulungen oder Webinare zu fördern.
• Befolgen Sie die internen digitalen und KI-Dienste, Marktprodukte und Technologietrends, um die KI-Politikdienste zu unterstützen.
• Durchführung von Überwachungs- und Kontrolltätigkeiten. Unterstützung der Bewertung der Cybersicherheit und anderer Elemente interner IT-Projekte unter Verwendung von KI-Elementen.
• Ausarbeitung und Überprüfung technischer Anhänge für Vergabeverfahren.

## 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 or have any questions, please follow the instructions and communication channels set up by your national administration.

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 ([2]). This applies in particular to the confidentiality and security of such data. Before applying, please read the attached privacy statement.

([2]) 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

## Critères d'éligibilité

Le détachement sera régi par la **décision de la Commission C(2008) 6866** du 12/11/2008 relative au régime applicable aux experts nationaux détachés et aux experts nationaux en formation professionnelle auprès des services de la Commission (décision END).

Aux termes de la décision END, vous devrez obligatoirement remplir les critères d'éligibilité suivants **à la date de début du détachement** :

- Expérience professionnelle : posséder une expérience professionnelle d'au moins trois ans dans des fonctions administratives, judiciaires, scientifiques, techniques, de conseil ou de supervision, à un grade équivalant au groupe de fonctions administrateur AD;
- Ancienneté de service : avoir une ancienneté d'au moins un an (12 mois) auprès de votre employeur actuel, dans un cadre statutaire ou contractuel;
- Employeur : être employé par une administration publique nationale, régionale ou locale, ou par une organisation intergouvernementale (OIG); exceptionnellement et après dérogation, la Commission peut accepter des candidatures lorsque votre employeur est un organisme du secteur public (e.g. agence ou institut de régularisation), une université ou un organisme de recherche indépendant.
- Compétences linguistiques : avoir une connaissance approfondie d'une des langues de l'Union européenne et une connaissance satisfaisante d'une autre langue de l'Union européenne dans la mesure nécessaire aux fonctions qu'il est appelé à exercer. Si vous venez d'un pays tiers, vous devrez justifier posséder une connaissance approfondie de la langue de l'Union européenne nécessaire à l'accomplissement des tâches qui vous seront confiées.

## Conditions du détachement

Durant toute la durée de votre détachement, vous devrez rester employé et rémunéré par votre employeur et devrez également rester couvert par votre sécurité sociale (nationale).

Vous exercerez vos fonctions au sein de la Commission dans les conditions fixées par la décision END précitée et serez soumis(e) aux règles de confidentialité, de loyauté et d'absence de conflit d'intérêts qui y sont définies.

Dans le cas où le poste est publié avec indemnités de séjour, celles-ci ne vous seront octroyées que si vous remplissez les conditions prévues à l'article 17 de la décision END.

Le personnel en poste dans une délégation de l'Union européenne doit obligatoirement disposer d'une habilitation de sécurité (jusqu'au niveau SECRET UE/EU SECRET conformément à la décision de la Commission (EU – Euratom) 2015/444 du 13 mars 2015. Il vous appartient de lancer cette procédure d'habilitation de sécurité avant d'obtenir la confirmation de votre détachement.

## Soumission des candidatures et procédure de sélection

Si vous êtes intéressé ou si vous avez des questions, veuillez suivre les instructions et les canaux de communication établis par votre administration nationale.

La Commission Européenne **acceptera seulement les candidatures qui auront été soumises par l'intermédiaire de la Représentation Permanente / Mission Diplomatique de votre pays auprès de UE, le secrétariat de l'AELE (EFTA) ou par le(s) canal (canaux) qui aura (auront) été spécifiquement convenu(s)**. Les candidatures reçues directement de votre part ou de votre employeur ne seront pas prises en considération.

Vous devez envoyer votre candidature sous format **CV Europass** (Créez votre CV Europass | Europass) en français, anglais ou allemand. Votre CV doit obligatoirement mentionner votre nationalité.

Veuillez ne pas ajouter d'autres documents (tels que copie de carte d'identité, copie des diplômes ou attestation d'expérience professionnelle, etc.). Le cas échéant, ces documents vous seront demandés ultérieurement.

## Traitement des données à caractère personnel

La Commission européenne veillera à ce que les données à caractère personnel des candidats soient traitées dans le plein respect du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([3]). Ces dispositions s'appliquent en particulier à la confidentialité et à la sécurité de ces données. Avant de postuler, veuillez lire la déclaration de confidentialité.

([3]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

## Zulassungsbedingungen

Abordnungen fallen unter den **Beschluss C(2008) 6866 der Kommission vom 12.11.2008** über die Regelung für zur Kommission abgeordnete oder sich zu Zwecken der beruflichen Weiterbildung bei der Kommission aufhaltende nationale Sachverständige (ANS-Beschluss).

Gemäß dem ANS-Beschluss müssen Sie **zu Beginn der Abordnung** die folgenden Zulassungskriterien erfüllen:

- Berufserfahrung: eine mindestens dreijährige Berufserfahrung mit Aufgaben im administrativen, justiziellen, wissenschaftlichen oder technischen Bereich in beratender oder leitender Funktion, die mit den Tätigkeiten der Funktionsgruppe Administration (AD) vergleichbar ist.
- Dienstalter: ein Dienstalter von mindestens einem Jahr (12 Monate) bei Ihrem derzeitigen Arbeitgeber in einem dienst- oder vertragsrechtlichen Verhältnis.
- Arbeitgeber: es muss sich um eine nationale, regionale oder lokale Verwaltung oder eine zwischenstaatliche öffentliche Organisation handeln; ausnahmsweise kann die Kommission nach einer besonderen Ausnahmeregelung Anträge annehmen, wenn es sich bei Ihrem Arbeitgeber um eine öffentliche Stelle (z. B. eine Agentur oder ein Regulierungsinstitut), eine Universität oder ein unabhängiges Forschungsinstitut handelt.
- Sprachkenntnisse: gründliche Kenntnisse einer Sprache der Europäischen Union und ausreichende Kenntnisse einer weiteren Sprache der Europäischen Union in dem für die Wahrnehmung der Funktion erforderlichen Maße. Sollten Sie aus einem Drittland kommen, müssen Sie nachweisen, dass Sie über gründliche Kenntnisse in der zur Ausübung Ihrer Tätigkeit erforderlichen Sprache der Europäischen Union verfügen.

## Bedingungen für die Abordnung nationaler Sachverständiger

Während der gesamten Dauer der Abordnung müssen Sie bei Ihrem Arbeitgeber angestellt bleiben, von diesem Ihre Bezüge erhalten und auch weiterhin Ihrem (nationalen) Sozialversicherungssystem angeschlossen bleiben.

Sie werden Ihre Aufgaben innerhalb der Kommission nach Maßgabe des genannten ANS-Beschlusses ausüben und den darin festgelegten Bestimmungen über Vertraulichkeit, Loyalität und Nichtvorliegen von Interessenkonflikten unterliegen.

Falls diese Stelle mit Vergütungen ausgeschrieben wird, können diese nur gewährt werden, wenn Sie die Bedingungen gemäß Artikel 17 des ANS-Beschlusses erfüllen.

Mitarbeiter/Mitarbeiterinnen, die in eine Delegation der Europäischen Union entsandt werden, benötigen eine Sicherheitsüberprüfung (nach SECRET UE/EU SECRET Niveau

gemäß der Entscheidung der Kommission (EU-Euratom) 2015/444, O.J. L 72, 17.03.2015, p.53). Es obliegt Ihnen, das Überprüfungsverfahren vor der Abordnung einzuleiten.

**Bewerbung und Auswahlverfahren**

Sollten Sie Interesse haben oder Fragen bestehen, folgen Sie bitte den von Ihrer nationalen Verwaltung eingerichteten Anweisungen und Kommunikationswegen.

Die Europäische Kommission akzeptiert nur Bewerbungen, die über die Ständige Vertretung/Diplomatische Vertretung bei der EU Ihres Landes, das EFTA-Sekretariat oder über die Kanäle, denen sie ausdrücklich zugestimmt hat, eingereicht wurden. Bewerbungen, die direkt von Ihnen oder Ihrem Arbeitgeber eingehen, werden nicht berücksichtigt.

Sie sollten Ihren Lebenslauf auf Englisch, Französisch oder Deutsch im Europass CV Format verfassen (Erstellen Sie Ihren Europass-Lebenslauf | Europass). Ihre Nationalität muss darin angegeben sein.

Bitte fügen Sie Ihrer Bewerbung keine anderen Dokumente (wie Kopien des Personalausweises, Kopien von Abschlusszeugnissen, Nachweise der Berufserfahrung usw.) bei. Diese Dokumente sind gegebenenfalls in einem späteren Stadium des Auswahlverfahrens vorzulegen.

**Verarbeitung personenbezogener Daten**

Die Kommission trägt dafür Sorge, dass die personenbezogenen Daten der Bewerber/innen gemäß den Anforderungen der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates verarbeitet werden ([4]). Dies gilt insbesondere für die Vertraulichkeit und Sicherheit dieser Daten. Bevor Sie sich bewerben, lesen Sie bitte die beigefügte Datenschutzerklärung.

([4]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).“