AVIS DE VACANCE

EXPERT NATIONAL DETACHE A LA COMMISSION EUROPEENNE

Intitulé du poste: (DG-DIR-UNITE)	**CNECT-H-2**
Chef d'unité : **Adresse e-mail :** **Téléphone :** **Nombre de postes disponibles:** **Prise de fonction souhaitée :** **Durée initiale souhaitée :** **Lieu d'affectation :**	**Jakub Boratyński** **CNECT-H2@ec.europa.eu** **+32 2 296 9452** **1** **3ème trimestre 2021**[1] **2 ans**[1] ☒ **Bruxelles** ☐ **Luxembourg** ☐ Autre: ……..
	☒ **Avec indemnités** ☐ **Sans frais**
Cet avis est également ouvert ☐ **aux pays AELE suivants :** ☐ **Islande** ☐ **Liechtenstein** ☐ **Norvège** ☐ **Suisse** ☐ **Accord AELE-EEE in-Kind (Islande, Liechtenstein, Norvège)** ☐ **aux pays tiers suivants:** ☐ **aux organisations intergouvernementales suivantes:**	

1. Nature des fonctions

L'unité Cyber sécurité et vie privée numérique (CNECT/H/2) élabore des politiques et prépare la législation dans les domaines de la cyber-sécurité et de la protection de la vie privée sur internet.

Dans le domaine de la cyber sécurité, l'unité est responsable, entre autres, de la mise en œuvre de la stratégie de cyber sécurité de l'UE, y compris la mise en œuvre de la première loi de l'Union sur la cyber-sécurité, connue sous le nom de directive sur la sécurité des réseaux et des systèmes d'information (directive NIS), y compris la proposition de révision de la directive NIS, le règlement relatif à l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et au cadre européen de certification («Cybersecurity Act»).

Dans le domaine de la vie privée numérique, l'Unité négocie la proposition de règlement concernant le respect la vie privée et la protection des données à caractère personnel dans les communications électroniques (règlement "vie privée et communications électroniques"). L'unité est également responsable du suivi de la mise en œuvre nationale de l'actuelle directive sur la vie privée et les communications électroniques.

L'unité collabore étroitement avec l'unité « Renforcement des capacités et technologies en matière de cyber sécurités » (CNECT.H.1) ainsi qu'avec d'autres unités de la DG et des services associés dans d'autres DGs.

La Direction a une approche axée sur le travail en équipe, encourage la collaboration "no-silo" alimentée par l'expertise de la DG CNECT dans le domaine des TIC et du marché unique numérique et rassemblant des équipes d'experts venants de l'ensemble de ses unités, mais aussi d'autres directions de la DG CNECT, en particulier des domaines de l'internet des objets et de l'intelligence artificielle.

L'unité est dynamique, engagée, a un bon esprit d'équipe et une atmosphère très conviviale.

[1] Les précisions liées à la date de prise de fonctions et à la durée du détachement sont données à titre indicatif uniquement (article 4 de la décision END).

Nous proposons un poste intéressant et stimulant en tant que responsable des politiques dans un domaine fascinant et émergent, recoupant plusieurs domaines politiques. Le candidat retenu travaillera au sein de l'équipe cyber sécurité, mais collaborera également avec les membres de l'équipe impliqués dans la protection de la vie privée.

Les tâches allouées au / à la candidate sélectionné(e) seront tirées de la liste indicative suivante:

- Contribuer à et faciliter la mise en œuvre de la Directive sur la sécurité des réseaux et des systèmes d'information (Directive SRI), notamment en ce qui concerne la coopération entre les États membres;
- Contribuer au travail de négociations sur la proposition de révision de la directive NIS (NIS2) ;
- Contribuer à la mise en œuvre des aspects de la législation portant sur la sécurité des réseaux et de la société de l'information (par exemple, la Directive Cadre et le futur code des communications);
- Suivi des actions liées à la stratégie de sécurité de l'Union et à la recommandation de la Commission d'une réponse coordonnée face aux incidents et crises de cyber-sécurité majeurs ;
- Suivi de la mise en œuvre de la stratégie de cyber-sécurité de l'UE pour la décennie numérique, en coopération avec d'autres services de la Commission et avec le SEAE;
- Traiter les questions parlementaires, les questions des citoyens et les briefings;

Le/la candidat/e retenu/e travaillera en étroite collaboration avec une équipe solide et dynamique possédant un très bon niveau d'expertise en matière de cyber sécurité.

La répartition finale des tâches dépendra de l'expertise spécifique et du profil du/de la candidat/e retenu/e.

2. Qualifications requises

a) Critères d'éligibilité

Les critères d'éligibilité doivent être obligatoirement remplis par l'END pour être détaché auprès de la Commission. Par conséquent, le candidat qui ne remplirait pas tous ces critères serait automatiquement éliminé de la procédure de sélection.

- 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 auprès de son employeur, c'est-à-dire être employé depuis au moins un an par un employeur éligible au sens de l'article 1 de la décision END, dans un cadre statutaire ou contractuel avant le détachement;

- 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. L'END d'un pays tiers doit justifier posséder une connaissance approfondie d'une langue de l'Union européenne nécessaire à l'accomplissement des tâches qui lui seront confiées.

b) Critères de sélection

Diplôme
- diplôme universitaire ou
- formation professionnelle ou expérience professionnelle de niveau équivalent

dans le(s) domaine(s) : sciences politiques, gestion et/ou sciences économiques avec une connaissance approfondie des nouvelles technologies et/ou des questions de la protection de la vie privée. Inversement, des études en sciences informatiques/technologies numériques avec connaissance poussée des politiques publiques seraient également considérées comme un atout.
Un bagage juridique serait considéré comme un atout supplémentaire.

Expérience professionnelle

Nous cherchons une personne dynamique, ayant une vaste expertise en politiques publiques du numérique, en particulier celles liées à la cyber-sécurité.

Une expérience de travail liée à la mise en œuvre et application de la législation nationale sur la sécurité des réseaux (Directive SRI) et la Directive «vie privée et communications électroniques», y compris une expérience au sein des enceintes compétentes de l'UE, telles que le groupe de travail SRI ou de l'ENISA dit «art. 13», ainsi qu'une expérience acquise dans le domaine de la gestion de crises et de réponse aux incidents, serait un atout majeur.

Une expérience de travail dans les relations interinstitutionnelles, notamment les négociations législatives et/ou la mise en œuvre du droit de l'Union, serait également un atout.

Le candidat doit faire preuve d'un grand intérêt pour la fine pointe des politiques du numérique. Le candidat doit démontrer sa proactivité et sa capacité à travailler de manière autonome.

Langue(s) nécessaire(s) pour l'accomplissement des tâches

Le poste nécessite une excellente connaissance de la langue anglaise, à la fois en compétences rédactionnelles et en communication verbale. Une bonne compréhension et un niveau opérationnel du français seraient bienvenus.

3. Soumission des candidatures et procédure de sélection

Les candidats doivent envoyer leur candidature sous format **CV Europass** (http://europass.cedefop.europa.eu/fr/documents/curriculum-vitae) en français, anglais ou allemand **uniquement à la représentation permanente / mission diplomatique de leur pays auprès de l'UE**, qui la transmettra aux services compétents de la Commission, dans les délais fixés par ces derniers. Le CV doit obligatoirement mentionner la date de naissance et la nationalité du candidat. **Le non-respect de cette procédure ou des délais invalidera automatiquement la candidature.** Les candidats sont priés de ne pas joindre à leur candidature d'autres documents (tels que copie de carte d'identité, copie des diplômes et attestations d'expérience professionnelle, …). Ces documents leur seront demandés, le cas échéant, à un stade ultérieur de la procédure de sélection.
Les candidats seront informés du suivi de leur candidature par l'unité concernée.

4. Conditions du détachement

Les détachements sont régis 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).

L'END restera employé et rémunéré par son employeur durant toute la durée du détachement. Il restera également couvert par la sécurité sociale nationale durant son détachement.
Sauf pour les END sans frais, des indemnités de séjour peuvent être versées à l'END qui remplit les conditions, conformément à l'article 17 de la décision END.
Durant le détachement, l'END sera soumis aux obligations de confidentialité, de loyauté et d'absence de conflit d'intérêt prévues par les articles 6 et 7 de la décision END.
Toute déclaration incomplète ou fausse pourra entraîner le refus de la candidature.

Toute personne postée dans une **délégation de l'Union européenne** doit avoir 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, OJ L 72 du 17.03.2015, p. 53). Le candidat choisi aura l'obligation de lancer cette procédure d'habilitation de sécurité avant d'obtenir la confirmation de son détachement.

5. Traitement des données à caractère personnel

Toute mise en œuvre de la procédure de sélection, de détachement et de fin de détachement des END aura pour effet le traitement, par les services compétents de la DG HR, du PMO, de la DG BUDG et de la DG concernée par le présent avis, de données à caractère personnel relatives à l'END, sous la responsabilité du chef de l'unité HR.DDG.B4. Ce traitement est basé sur la décision de la Commission relative aux END et est soumis au Règlement (UE) No 2018/1725.
Les données des END seront conservées pendant 10 ans à compter de la fin du détachement (2 ans pour les END dont la candidature n'a pas été retenue ou a été retirée).
En tant que personne concernée, vous avez des droits spécifiques en vertu du chapitre III (articles 14 à 25) du règlement (UE) 2018/1725, notamment le droit d'accès, de rectification ou d'effacement de vos données à caractère personnel et le droit de limiter le traitement de vos données personnelles. Le cas échéant, vous avez également le droit de vous opposer au traitement ou au droit à la portabilité des données.
Vous pouvez exercer vos droits en contactant le responsable du traitement ou, en cas de conflit, le responsable de la protection des données. Si nécessaire, vous pouvez également vous adresser au contrôleur européen de la protection des données. Leurs coordonnées sont indiquées ci-dessous.

Informations de contact

- **Le contrôleur de données**

Si vous souhaitez exercer vos droits en vertu du règlement (UE) 2018/1725, ou si vous avez des commentaires, des questions ou des préoccupations, ou si vous souhaitez déposer une plainte concernant la collecte et l'utilisation de vos données à caractère personnel, n'hésitez pas à contacter le contrôleur de données, HR.DDG.B.4, HR-MAIL-B4@ec.europa.eu.

- **Le délégué à la protection des données (DPD) de la Commission**

Vous pouvez contacter le délégué à la protection des données (DATA-PROTECTION-OFFICER@ec.europa.eu) pour toute question relative au traitement de vos données à caractère personnel en vertu du règlement (UE) 2018/1725.

- **Le contrôleur européen de la protection des données (CEPD)**

Vous avez le droit de saisir le contrôleur européen de la protection des données (edps@edps.europa.eu) (c'est-à-dire que vous pouvez porter plainte) si vous estimez que vos droits en vertu du règlement (UE) 2018/1725 ont été violés par le contrôleur des données.

À l'attention des candidats ressortissant de pays tiers: vos données personnelles peuvent être utilisées aux fins des vérifications nécessaires.