PROTECTION DES DONNÉES PERSONNELLES DANS LE CADRE DE L'ÉVALUATION

Les informations relatives à la protection des données et au traitement des données personnelles se trouvent dans notre politique de confidentialité disponible ici.

La section ci-dessous apporte quelques précisions sur :

1) L'accord de protection des données (APD) que les expertes et experts ou membres des commissions scientifiques et jurys du F.R.S.-FNRS et ses Fonds associés spécialisés sont tenus de signer avant l'examen de toute proposition ;
2) La liste des mesures techniques et organisationnelles proposées pour assurer la protection des données personnelles dans le cadre de la mission d'évaluation.

Comme indiqué dans notre politique de confidentialité, toute question concernant ces sujets peut être envoyée à privacy@frs-fnrs.be et nous ferons en sorte d'y répondre dans les meilleurs délais.

1. ACCORD DE PROTECTION DES DONNÉES

L'Accord de protection des données a pour objet d'assurer le respect des exigences du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (le "**RGPD**").

Les expertes et experts ou membres des commissions et jurys scientifiques du FNRS (l'"**Expert**") remplissent des missions de recherche scientifique (la "**Mission**") auprès du Fonds pour la recherche scientifique en Communauté française de Belgique, le Fonds de la Recherche Scientifique - F.R.S.-FNRS (le "**FNRS**") et ses Fonds associés spécialisés, impliquant le traitement et la consultation de données à caractère personnel.

Conformément au RGPD, le traitement des données à caractère personnel par l'Expert pour le compte du FNRS est régi par un contrat qui lie l'Expert à l'égard du FNRS. Le Contrat de protection des données énonce les engagements du FNRS et de l'Expert afin que les deux parties comprennent également leurs responsabilités et obligations, et contient les dispositions de l'article 28 du RGPD telles qu'interprétées par le Comité européen de la protection des données dans son avis 14/2019 (c'est-à-dire l'objet du traitement dans le Guide de l'évaluateur, les instructions du FNRS, les mesures de sécurité, les transferts de données à caractère personnel, etc.), afin de garantir la sécurité des données à caractère personnel traitées par l'Expert lors de l'exécution de la Mission (par exemple, lors de la consultation des données à caractère personnel mises à la disposition des experts par le FNRS).

Le FNRS et l'Expert peuvent signer l'Accord de protection des données par voie électronique sur la Plateforme E-Space[1].

[1] Si vous concluez l'Accord de protection des données au nom de l'Expert, vous garantissez que (a) vous disposez de l'autorité légale complète pour engager l'Expert à l'Accord de protection des

En cas de questions sur l'Accord de protection des données ou sur le traitement des données personnelles pour le compte du FNRS dans le cadre de la Mission, l'Expert peut contacter le FNRS à tout moment par courriel à l'adresse suivante : privacy@fnrs.be.

2. MESURES DE SÉCURITÉ TECHNIQUES ET ORGANISATIONNELLES

Le traitement et la consultation des données personnelles par l'Expert doivent être effectués uniquement sur la plateforme sécurisée E-Space du FNRS, en utilisant le login et le mot de passe personnels de l'Expert.

Le traitement et la consultation des données personnelles en dehors de la plateforme E-Space (par exemple, en cas de téléchargement des données depuis la plateforme) relèvent de la responsabilité de l'Expert exclusivement. L'Expert s'engage à ce titre à prendre toutes les mesures raisonnables pour assurer la sécurité et la protection des données personnelles. Une liste illustrative de ces mesures est présentée ci-dessous :

Mesures techniques et organisationnelles suggérées dans le cadre des missions d'expertise pour le F.R.S.-FNRS :

1. Mesures techniques

☐ Antivirus sur l'ensemble des PC/serveurs et mises à jour régulières
☐ Mesures contre la perte de données personnelles et back-ups réguliers
☐ Mise à jour systématique et automatique des logiciels
☐ Site Internet avec connexion https sécurisée
☐ Firewalls et système d'authentification
☐ Sécurité physique des serveurs (réception, local fermé à clé, autorisation du personnel habilité)
☐ Système d'accès avec un identifiant unique (login) pour chaque utilisateur et mécanisme d'authentification à mettre en place
☐ Configuration du matériel nouveau et existant afin de réduire les vulnérabilités
☐ Limitation des accès aux données personnelles détenues dans les systèmes d'information
☐ Mots de passe appropriées (sécurité et changement régulier) et processus de détection de tout accès non autorisé ou utilisation anormale
☐ Chiffrement (cryptage) sur le réseau et les appareils mobiles (ex : pour les données sensibles)
☐ Défenses antimalware
☐ Système de détection ou de prévention d'intrusion sur le réseau
☐ Wi-Fi protégé par un cryptage WPA2
☐ Processus de journalisation et de surveillance de l'activité des utilisateurs et du système pour identifier et aider à prévenir les violations de données
☐ Contrôle et gestion des supports amovibles pour empêcher toute divulgation non autorisée, codification, suppression ou destruction de données personnelles
☐ Dispositifs de stockage sécurisés pour protéger les dossiers, l'équipement et prévenir les pertes, les dommages, vols ou mises en péril de données personnelles
☐ Autres

données, et (b) vous acceptez, au nom de l'Expert, l'Accord de protection des données. Si vous n'avez pas le pouvoir légal de lier l'Expert, veuillez ne pas signer l'Accord de protection des données et le transmettre au représentant compétent.

2. Mesures organisationnelles

☐ Politique de sécurité interne (data breach scenario, procédure à l'arrivée et au départ du personnel, best practices ICT, etc.)
☐ Sensibilisation du personnel et management impliqué dans les traitements de données personnelles
☐ Formation du personnel et management impliqué dans les traitements de données personnelles
☐ Nomination d'un DPO ou Data Manager (Team)
☐ Désignation d'un responsable en sécurité de l'information
☐ Organigramme interne et répartition claire des tâches
☐ Anonymisation/Pseudonymisation des données (par exemple données sensibles)
☐ Restriction et contrôle d'accès aux locaux, à l'équipement et aux données en fonction des autorisations/fonctions (« need-to-know »)
☐ Prévention, détection et traitement des dangers physiques (incendie, dégâts des eaux, etc.)
☐ Processus de suppression sécurisée des données (ex : déchiqueteuse, etc.)
☐ Plan de recouvrement, catastrophe ou de secours (plan de continuité)
☐ Formation régulière de sensibilisation à la sécurité de l'information pour tout le personnel (et sous-traitants)
☐ Autres