**Déclaration relative à la protection des données concernant le traitement des données à caractère personnel relatives à l'usage opérationnel de FIPS (SAP)/myFIPS au sein de la DP 4.1 et de la DP 4.7**

L'Office européen des brevets (OEB) attache la plus haute importance à la protection de vos données. Nous nous engageons à protéger vos données à caractère personnel et à veiller au respect des droits des personnes concernées lorsque nous accomplissons nos tâches et fournissons nos services. Toutes les données à caractère personnel vous identifiant, directement ou indirectement, seront traitées de manière licite, loyale et avec le plus grand soin.

Les opérations de traitement décrites ci-après sont régies par le règlement relatif à la protection des données (RRPD) de l'OEB.

Les informations contenues dans la présente déclaration sont fournies en vertu des articles 16 et 17 RRPD.

Conformément au règlement financier, la DP 4.1 et la DP 4.7 traitent les données disponibles dans FIPS afin de faciliter les procédures d'achat et les paiements.

**1. Quelles sont la nature et la finalité des opérations de traitement ?**

Le système FIPS (SAP) et myFIPS (interface en ligne de FIPS) sont utilisés en matière de financement et d'achats afin d'enregistrer et de stocker l'ensemble des documents opérationnels requis pour le bon fonctionnement des procédures d'achats et de financement. Étant donné que SAP est un système intégré qui couvre également la partie RH, cette évaluation couvrira uniquement les parties qui sont directement en lien avec les procédures d'achat.
FIPS est utilisé de manière holistique pour poster des documents et inclut de la documentation enregistrée à partir de différentes applications afin de garantir la pleine transparence des décisions pour tous les agents impliqués. Sont couvertes les principales procédures suivantes : la planification, la budgétisation, la réservation de fonds, le sourçage, la gestion des contrats, les achats/commandes, la réception des biens/services, la facturation, les paiements, la trésorerie, la PSCD, les ventes et les recettes, le controlling, les données permanentes, le reporting, la gestion des utilisateurs, etc. L'ensemble des procédures mentionnées ci-dessus impliquent la plupart des agents de l'OEB qui ont pour mission de valider différentes étapes de la procédure, du reporting, du controlling et des activités opérationnelles. Par conséquent, de multiples sources d'informations sont traitées et enregistrées dans cet outil afin de garantir sa vérifiabilité et d'assurer un bon contrôle des procédures. L'accès aux données est géré de manière centralisée sur la base du "besoin de savoir" par les collègues du BIT qui sont responsables du respect des règles du système et de la gouvernance. En ce qui concerne les tâches opérationnelles, les collègues fournissent eux-mêmes l'ensemble des informations et documents nécessaires pour valider et auditer en interne les publications d'appels d'offre.
Outre les agents internes, certaines informations spécifiques (fondées sur des requêtes approuvées) sont accessibles aux auditeurs, aux agents du soutien informatique (internes ou externes), aux consultants impliqués dans un projet, aux gestionnaires de contrats.

Le traitement ne doit faire l'objet d'aucune prise de décision automatisée, y compris un profilage.

Les données à caractère personnel vous concernant ne seront pas transférées à des destinataires en dehors de l'OEB qui ne sont pas visés à l'article 8(1), (2) et (5) RRPD, à moins qu'un niveau de protection adéquat puisse être garanti. En l'absence d'un niveau de protection adéquat, un transfert ne peut avoir lieu que si des garanties appropriées ont été mises en place et à la condition que les personnes concernées puissent faire valoir leurs droits et disposent de voies de recours effectives, ou si des dérogations pour des situations particulières telles que prévues à l'article 10 RRPD s'appliquent.

**Quelles données à caractère personnel traitons-nous ?**

**Les catégories de personnes concernées comprennent les agents de l'OEB et les employés des fournisseurs externes.**

**Les catégories de données à caractère personnel peuvent être les suivantes :**

- Enregistrements SAP
- Informations de contact : coordonnées, pays, numéro de téléphone mobile, numéros de téléphone, adresse électronique professionnelle ;
- Correspondance : toute information susceptible d'être fournie dans le cadre d'échanges, le contenu de chats, les informations personnelles fournies volontairement.
- Formation et compétences : p. ex. le parcours académique et les formations, les diplômes, les langues, l'expérience en gestion de projets.
- Informations relatives à l'emploi : division de l'unité commerciale, filiale de l'entreprise, nom et/ou numéro du service, numéro du badge pour accéder à l'OEB, date d'expiration, intitulé du poste, fonction, numéro du bureau.
- **Informations financières**
- **Données d'identification personnelle**
- **Journal système :** données relatives au fichier (nom, taille et/ou hash, données du registre, journal SAP
- **Informations sur la billetterie**
- **Informations de contact :** coordonnées, numéro de téléphone, adresse électronique professionnelle
- **Actifs identifiables physiques et/ou électroniques,** comme le certificat numérique

Outre les données ci-dessus, les informations relatives aux fournisseurs et aux soumissionnaires qui ont participé aux procédures d'achat accompagnées de l'information indiquant si un contrat a été conclu ou non avec eux.

**3. Qui est responsable du traitement des données ?**

Les données à caractère personnel sont traitées sous la responsabilité du directeur principal Achats et gestion des fournisseurs, DP 4.7, agissant en qualité de responsable délégué du traitement à l'OEB.

Les données à caractère personnel sont traitées par les agents de l'OEB participant à la gestion des initiatives, projets ou activités de la DP 4.1 auxquels il est fait référence dans la présente déclaration.

**4. Qui a accès à vos données à caractère personnel et à qui sont-elles communiquées ?**

Les données à caractère personnel sont communiquées en fonction du besoin de savoir à l'ensemble des agents/consultants/auditeurs sur la base des rôles attribués par l'équipe BIT. D'autres acteurs auront accès aux données opérationnelles agrégées via le reporting.

Les données à caractère personnel seront partagées uniquement avec des personnes habilitées qui sont responsables des opérations de traitement nécessaires. Elles ne seront pas utilisées à d’autres fins ou communiquées à d’autres destinataires.

**5. Comment protégeons-nous et sauvegardons-nous vos données à caractère personnel ?**

La DP 4.7 prend les mesures techniques et organisationnelles appropriées afin de sauvegarder et protéger vos données à caractère personnel de toute destruction, perte, altération accidentelle ou illégale, ainsi que de la divulgation non autorisée de ces données ou de l'accès non autorisé à ces dernières.

L'ensemble des données à caractère personnel est conservé dans des applications informatiques sécurisées conformément aux normes de sécurité de l'OEB. Des niveaux d'accès appropriés sont accordés à titre individuel uniquement aux destinataires mentionnés ci-dessus.

L'ensemble des données à caractère personnel contenues dans FIPS/myFIPS est enregistré dans des applications informatiques sécurisées et sont conformes aux normes de sécurité BIT de l'OEB, qui incluent les mesures suivantes :

- authentification de l'utilisateur : tous les postes de travail et serveurs requièrent une ouverture de session, les dispositifs mobiles de l'OEB requièrent une ouverture de session au site de l'OEB, les comptes privilégiés requièrent une authentification supplémentaire et plus stricte ;
- contrôle de l'accès (p.ex. contrôle de l'accès aux systèmes et au réseau en fonction du rôle, principes du « besoin de savoir » et du « moindre privilège ») ; séparation des rôles d'administrateur et d'utilisateur, les utilisateurs ayant un minimum de privilèges et les rôles d'administrateur étant maintenus au minimum ;
- renforcement de la sécurité logicielle des systèmes, équipements et réseaux : 802.1x pour l'accès au réseau, le chiffrement des dispositifs de point d'extrémité, l'installation d'antivirus sur tous les dispositifs ;
- protection physique : contrôle des accès à l'OEB, contrôles d'accès supplémentaires au centre de données, politiques relatives à la fermeture des bureaux ;
- intervention en cas d'incident de sécurité : surveillance des incidents 24 heures sur 24 et 7 jours sur 7, expert en sécurité de garde.

En principe, l'OEB a adopté un système d'administration dématérialisé ; cependant, si des dossiers papier contenant des données à caractère personnel doivent être stockés dans les locaux de l'OEB, ces dossiers sont conservés dans un lieu sûr et verrouillé à accès restreint.
Si des données sont externalisées (p. ex. stockées, consultées et traitées), une analyse des risques en matière de confidentialité et de sécurité est effectuée et la déclaration générale suivante peut être incluse dans ce domaine :

Pour les données à caractère personnel traitées par des systèmes qui ne sont pas hébergés dans les locaux de l'OEB, les prestataires traitant les données à caractère personnel se sont engagés dans le cadre d'un accord contraignant à respecter leurs obligations en matière de protection des données découlant du cadre juridique de la protection des données applicable. L'OEB a également effectué une analyse des risques en matière de confidentialité et de sécurité. Il est exigé que ces systèmes aient mis en place des mesures techniques et organisationnelles appropriées telles que des mesures physiques de sécurité, des mesures de contrôle des accès et du stockage, la sécurisation des données inactives (p.ex. par chiffrement) ; des mesures de contrôle des utilisateurs, de la transmission et des entrées (avec p.ex. des pare-feu de réseau, des systèmes de détection des intrusions sur le réseau (IDS), des systèmes de protection contre les intrusions sur le réseau (IPS), un audit des connexions) ; des mesures de contrôle de l'acheminement des données (p.ex. sécurisation des données en transit par un chiffrement).

**6. Comment pouvez-vous accéder à vos données, les rectifier et les recevoir, en demander l'effacement, limiter leur traitement ou vous y opposer ? Vos droits peuvent-ils être restreints ?**

Vous avez le droit d'accéder à vos données à caractère personnel, de les rectifier et de les recevoir, de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, d'en demander l'effacement ainsi que de limiter leur traitement ou de vous y opposer (article 18 à 24 RRPD).

Si vous souhaitez exercer l'un de ces droits, veuillez adresser une demande écrite en ce sens au responsable délégué du traitement à l'adresse suivante : PDCProcuremet-dpl@epo.org. Afin de nous permettre de répondre plus rapidement et précisément, vous devez toujours assortir votre demande de certaines informations préliminaires. Nous vous encourageons par conséquent à remplir ce formulaire (pour les personnes de l'extérieur) ou ce formulaire (pour les personnes en interne) et à le transmettre avec votre demande.

Nous répondrons à votre demande dans les meilleurs délais et, en tout état de cause, dans un délai d'un mois à compter de la réception de votre demande. Toutefois, conformément à l'article 15(2) RRPD, ce délai peut être prolongé de deux mois supplémentaires si nécessaire, compte tenu de la complexité et du nombre de demandes reçues. Toute prorogation de délai vous sera notifiée.

**7. Quelle est la base juridique du traitement de vos données à caractère personnel ?**

Les données à caractère personnel sont traitées conformément à l'article 5 a) RRPD, le traitement est nécessaire à la gestion et au fonctionnement de l'OEB, toutes les opérations de traitement requises pour le fonctionnement de l'OEB ne sont pas explicitement prévues par la CBE.
En outre, les données à caractère personnel sont recueillies et traitées conformément au règlement financier (Directive relative à l'exécution du budget, Directives relatives à la passation des marchés, Instructions relatives aux contrats, Directive complétant certaines dispositions du règlement financier).

**8. Combien de temps conservons-nous vos données à caractère personnel ?**

Il existe des conditions légales prédéfinies concernant l'enregistrement des contrats et des factures et une politique relative à la conservation des données est en cours d'élaboration.

**9. Personnes à contacter et coordonnées**

Si vous avez des questions sur le traitement des données à caractère personnel vous concernant, veuillez les adresser au responsable délégué du traitement à l'adresse suivante : PDCProcurement-DPL@epo.org.

Vous pouvez également contacter notre responsable de la protection des données à l'adresse dpo@epo.org.

**Réexamen et exercice des voies de recours**
Si vous considérez que le traitement porte atteinte à vos droits en tant que personne concernée, vous avez le droit de demander un réexamen par le responsable délégué du traitement en vertu de l'article 49 RRPD et, si vous n'êtes pas d'accord avec l'issue de ce réexamen, d'exercer des voies de recours en vertu de l'article 50 RRPD.