

Déclaration relative à la protection des données lors du traitement de données à caractère personnel dans le cadre de la gestion des prestataires (création, gestion de l'arrivée/du départ, suppression de prestataires externes de l'OEB)

Pour l'Office européen des brevets (OEB), la protection de votre vie privée est de la plus haute importance. 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 qui vous identifient directement ou indirectement seront traitées de manière licite, loyale et avec toutes les précautions nécessaires.

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

Les informations contenues dans la présente déclaration sont fournies conformément aux articles 16 et 17 RRPD.

Le cycle de vie des prestataires externes de l'OEB est géré via l'opération de traitement de gestion des prestataires. La gestion des prestataires s'applique à tous les prestataires travaillant dans une unité organisationnelle de l'OEB, quelle qu'elle soit.

L'opération de traitement se base sur l'intégration de la logique métier et des données en lien avec le contrat concerné, le fournisseur, les membres de l'équipe responsables du contrat, les administrateurs du contrat et les prestataires.

Grâce à une application frontale de ServiceNow, les gestionnaires des contrats de l'OEB peuvent directement créer, associer, libérer et supprimer des prestataires liés à un contrat, mais également les prolonger et leur offrir les équipements et les ressources nécessaires (par exemple des badges, licences logicielles, infrastructures de bureau virtuel, etc.). Les gestionnaires des contrats de l'OEB ne pourront prolonger des prestataires ou gérer leur arrivée/départ que pour les contrats dont ils ont la charge. Ils pourront également avoir recours à des délégations, soit en chargeant un autre membre du personnel de l'OEB d'agir en tant que gestionnaire des contrats de l'OEB à leur place, soit en demandant l'intervention d'un gestionnaire de contrats externe, ce qui nécessite l'approbation préalable du gestionnaire de contrats de l'OEB ou de ses délégués.

1. Quelles sont la nature et la finalité de l'opération de traitement ?

La présente déclaration de protection des données concerne le traitement de la gestion des prestataires qui comprend la création, la gestion de l'arrivée/du départ des prestataires externes de l'OEB et leur suppression des systèmes de l'OEB.

Les données à caractère personnel sont traitées en vue des finalités suivantes :

1. faciliter la création, la gestion de l'arrivée et du départ, la suppression des prestataires de l'OEB dans les principaux systèmes sources par le biais d'une application frontale intégrée à ServiceNow ;
2. gérer l'affectation de chaque prestataire au contrat correspondant et gérer les procédures connexes ;
3. rendre disponible une piste d'audit pour chaque opération effectuée.

Le traitement de vos données n'est pas censé servir à une prise de décision automatisée, notamment au profilage.

L'opération de traitement de la gestion des prestataires ne consiste pas à traiter des données à caractère personnel dans le sens de l'article 12 RRPD, c'est-à-dire que les condamnations pénales de la personne concernée, ses infractions, les suspicions concernant ces infractions et les mesures de sécurité prises à

l'encontre de la personne concernée dans le cadre d'une procédure pénale (ou administrative) ne font en aucun cas l'objet d'un traitement.

Dans le cas où un prestataire quitte prématurément un contrat, ce départ est saisi dans l'application de gestion des prestataires sans indication de motifs circonstanciels.

Vos données à caractère personnel ne seront pas transmises à des destinataires extérieurs à l'OEB s'ils ne sont pas visés à l'article 8(1), (2) et (5) RRPD, à moins qu'un niveau de protection adéquat ne soit assuré. En l'absence d'un niveau de protection adéquat, un transfert ne peut avoir lieu que s'il est prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de recours effectives, ou si les dérogations pour des situations particulières visées à l'article 10 RRPD s'appliquent.

2. Quelles données à caractère personnel traitons-nous ?

Les données à caractère personnel des personnes externes, des prestataires et des membres du personnel de l'OEB sont traitées.

Les données à caractère personnel des personnes externes sont traitées lors des premières étapes du provisionnement. Une fois le provisionnement et l'intégration réussis, les personnes externes deviennent des prestataires.

Les catégories suivantes de données à caractère personnel peuvent être traitées :

Pour les personnes externes :

- Informations de contact : adresse électronique professionnelle ;
- Données d'identification personnelle : prénom, nom, sexe, date de naissance, nationalité, signature ;
- Informations sur l'emploi : entité dans la société, type de contrat, nom/numéro du service, emplacement du bureau, rythme de travail, langue préférée pour la communication.

Pour les prestataires :

- Informations de contact : adresse électronique professionnelle ;
- Données d'identification personnelle : prénom, nom, sexe, date de naissance, nationalité, signature ;
- Informations sur l'emploi : entité dans la société, type de contrat, numéro personnel, supérieur hiérarchique, date de début et date de fin de contrat, nom/numéro du service, emplacement du bureau, rythme de travail, langue préférée pour la communication ;
- Lieu d'affectation ;
- Informations relatives au compte utilisateur : rôle d'utilisateur spécifique à l'application, identifiant utilisateur tiers ;
- Données de gestion des appareils, par exemple identifiant de compte, identifiant pour l'inscription des appareils dans Azure Active Directory, identifiant de l'appareil EAS, clé de chiffrement, identifiant de l'appareil Intune, identifiant pour la gestion des appareils Intune, dernière date et heure de connexion, adresse MAC, plaque d'identification de l'appareil dans l'application gérée, identifiant de l'application gérée, emplacement d'installation de l'application gérée, nom de l'application gérée, taille de l'application gérée, version de l'application gérée, identifiants spécifiques à la plateforme, identifiant Tenant, identifiant Windows pour les appareils Windows, identifiant Apple pour les appareils iOS/iPadOS ;
- Éléments physiques et/ou numériques identifiables comme le numéro IMEI (identité internationale d'équipement mobile), le nom et le numéro de fabrication de l'appareil mobile, le modèle fournisseur de la station de travail, le numéro de fabrication et le nom d'hôte (physique ou virtuel) de la station de travail.

Pour le personnel de l'OEB :

- Informations de contact : adresse électronique professionnelle ;
- Informations d'identification : prénom, nom ;
- Informations relatives au compte utilisateur : identifiant, rôle d'utilisateur spécifique à l'application.

3. Qui est responsable du traitement des données ?

Les données à caractère personnel sont traitées sous la responsabilité de la ou du Chief Information Officer/de la DP 4.6 agissant en qualité de responsable délégué du traitement pour l'OEB.

L'équipe centrale des administrateurs qui enregistre les prestataires se trouve dans l'équipe UserReg au sein du BIT 4634 Informatique utilisateur, ou dans l'équipe registration.externals@epo.org.

Les sous-traitants internes peuvent appartenir à n'importe quelle unité organisationnelle de l'OEB. Ils peuvent se voir attribuer l'un des quatre rôles définis dans l'application de gestion des contrats : 1) administrateur des contrats de l'OEB ; 2) administrateur des fournisseurs ; 3) administrateurs complémentaires des contrats de l'OEB ; 4) administrateur complémentaire des fournisseurs.

Les prestataires externes participant à la fourniture et au maintien des plateformes et services sous-jacents peuvent également traiter des données à caractère personnel ou y avoir accès.

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

Les données à caractère personnel sont divulguées en fonction du "besoin de savoir" aux personnes suivantes :

- les membres du personnel de l'OEB qui travaillent en tant qu'administrateur des contrats de l'OEB, administrateur des fournisseurs, administrateur complémentaire des contrats de l'OEB ou administrateur complémentaire des fournisseurs.
- Les membres de l'équipe centrale des administrateurs qui reçoivent et approuvent l'intégration des prestataires dans ServiceNow avec toutes les informations requises, et qui créent un nouvel utilisateur dans SAP.
- SAP. En plus que de gérer l'arrivée des prestataires, les administrateurs des contrats peuvent effectuer d'autres actions depuis l'application de gestion des prestataires, par exemple les prolonger, les embaucher de nouveau, mettre fin (prématurément) à leur contrat, etc. Contrairement aux demandes d'intégration, aucun des changements qui résultent de ces actions ne nécessite l'intervention de l'équipe centrale des administrateurs.

Des données à caractère personnel peuvent être communiquées à des prestataires de services tiers à des fins de maintenance et d'assistance.

Les données à caractère personnel seront partagées uniquement avec les personnes responsables des opérations de traitement nécessaires. Elles ne seront pas utilisées à d'autres fins ni divulguées à d'autres destinataires.

5. Comment protégeons-nous et préservons-nous vos données ?

Nous prenons les mesures techniques et organisationnelles nécessaires pour préserver vos données à caractère personnel et les protéger contre la destruction, la perte ou la modification accidentelles ou illicites, et contre la communication ou l'accès non autorisés.

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.

En ce qui concerne les systèmes hébergés dans les locaux de l'OEB, les mesures de sécurité élémentaires suivantes s'appliquent de façon générale :

Authentification de l'utilisateur et contrôle d'accès (par exemple, contrôle d'accès aux systèmes et au réseau en fonction des rôles,

et des principes de Besoin de savoir et de Moindre privilège) ;

- Renforcement de la sécurité logique des systèmes, de l'équipement et du réseau ;
- Protection physique : contrôles des accès à l'OEB, contrôles supplémentaires des accès au centre de données, politiques de verrouillage des bureaux ;
- Contrôles des transmissions et entrées (par ex. journaux d'audit, surveillance des systèmes et réseaux) ;
- Intervention en cas d'incident de sécurité : surveillance des incidents 24 heures sur 24 et 7 jours sur 7, expert en sécurité de garde.

Pour les données à caractère personnel traitées par des systèmes qui ne sont pas hébergés dans les locaux de l'OEB, les prestataires qui les traitent se sont engagés, dans un accord contraignant, à respecter leurs obligations en matière de protection des données découlant des cadres juridiques de protection des données applicables. L'OEB a également effectué une analyse relative à la confidentialité et au risque de sécurité. Il est exigé que ces systèmes aient mis en place des mesures techniques et organisationnelles appropriées comme les suivantes : mesures physiques de sécurité, mesures de contrôle des accès et du stockage, sécurisation des données inactives (par exemple 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, en limiter le traitement ou vous opposer à celui-ci ? 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, de les effacer et de limiter leur traitement ou de vous opposer à celui-ci (articles 18 à 24 RRPD).

Si vous souhaitez exercer l'un de ces droits, veuillez envoyer une demande écrite en ce sens au responsable délégué du traitement à l'adresse : DP_BIT@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 externes) ou ce [formulaire](#) (pour les personnes internes) 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 prolongation de délai vous sera notifiée.

7. Sur quelle base juridique se fonde le traitement de vos données ?

Les données à caractère personnel sont traitées en vertu de

- l'article 5a) RRPD ("*le traitement est nécessaire à l'accomplissement d'une tâche relevant des activités officielles de l'Organisation européenne des brevets ou l'exercice légitime de l'autorité publique dont est investi le responsable du traitement, ce qui comprend le traitement nécessaire à la gestion et au fonctionnement de l'Office*").

8. Combien de temps conservons-nous vos données ?

L'opération de traitement de la gestion des prestataires de l'OEB est effective depuis janvier 2024. Cette opération traite les données à caractère personnel des prestataires de l'OEB dont l'intégration est postérieure à cette date.

Les données à caractère personnel des prestataires et les informations liées au contrat et au fournisseur liés sont stockées dans l'application de gestion des prestataires (basée sur ServiceNow) pour les fins énoncées, dans le respect du règlement relatif à la protection des données de l'OEB, de la politique de conservation à l'OEB et du calendrier de conservation de l'OEB.

Les tâches effectuées dans le cadre de l'opération de traitement "Gestion des prestataires" de l'OEB sont actuellement soumises à la même durée de conservation par défaut (5 ans) que les tâches de l'opération de traitement "Gestion des flux de travail, données et connaissances basée sur les capacités de ServiceNow de l'OEB".

Les données des prestataires supprimés d'un contrat ne sont pas supprimées de l'application de gestion des prestataires, mais mises à jour avec l'ajout de la date de leur départ. Cela est plus efficace et permet de faciliter l'embauche ultérieure des mêmes prestataires et leur prolongation.

En cas de recours/contentieux formel, toutes les données détenues au moment où le recours/contentieux formel est engagé seront conservées jusqu'à la clôture de la procédure.

9. Personnes à contacter et coordonnées

Si vous avez des questions concernant le traitement de vos données à caractère personnel, veuillez contacter le responsable délégué du traitement à l'adresse DP_BIT@epo.org ou le bureau de la protection des données à l'adresse DPOexternalusers@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 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 les voies de recours prévues à l'article 50 RRPD.