Déclaration de protection des données relative au traitement des données à caractère personnel pour l'outil SEARCH basé sur ANSERA et utilisé par les offices nationaux de brevets

L'Office européen des brevets (OEB) attache la plus haute importance à la protection de votre vie privée. Nous nous engageons à protéger vos données à caractère personnel et à veiller au respect des droits des personnes concernées lors de l'exécution de nos tâches et lors de la fourniture de 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.

Cet enregistrement des activités de traitement concerne la gestion de l'outil SEARCH basé sur ANSERA accessible aux utilisateurs enregistrés (les examinateurs de brevets des offices nationaux de brevets). Les données couvertes par l'outil SEARCH basé sur ANSERA se limitent aux informations publiées sur les brevets. Avec la recherche basée sur Ansera, et en utilisant des expressions de recherche complexes, les utilisateurs enregistrés peuvent rechercher des informations sur les brevets relativement à l'état de la technique. Les informations liées à la recherche et les annotations saisies par un utilisateur ne sont visibles que par l'utilisateur lui-même. Elles ne sont pas visibles pour d'autres utilisateurs, à l'exception des utilisateurs administrateurs qui peuvent accéder aux annotations. Les utilisateurs des ONB habilités à utiliser l'outil SEARCH basé sur ANSERA seront préalablement intégrés au système de gestion des identités de l'OEB via le portail d'accès unique. Vous trouverez plus d'informations sur la recherche basée sur Ansera dans les documents techniques publiés sur le portail d'accès unique (epn.epo.org).

1. Quelle est la nature du traitement et quelle est sa finalité ?

La présente déclaration de protection des données concerne le traitement des données à caractère personnel dans le cadre de l'outil SEARCH basé sur ANSERA utilisé par les offices nationaux de brevets.

Les données à caractère personnel sont traitées aux fins suivantes :

- Fournir aux examinateurs de brevets des offices nationaux un outil de recherche.
- Exploiter et assurer la maintenance de l'outil SEARCH basé sur ANSERA.
- Surveiller la disponibilité et les performances de l'outil SEARCH basé sur ANSERA.
- Effectuer des dépannages techniques et gérer les incidents de sécurité.
- Assurer la planification des capacités et la gestion des licences.

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

En l'absence d'un niveau adéquat de protection, vos données à caractère personnel ne seront pas transmises à des destinataires extérieurs à l'OEB qui ne sont pas visés par l'article 8(1), (2) et (5) du RRPD. En l'absence d'un niveau adéquat de protection, un transfert peut uniquement avoir lieu si des garanties appropriées sont prévues et si 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 sont les données à caractère personnel traitées par l'OEB ?

Les catégories de données à caractère personnel des utilisateurs enregistrés de l'outil SEARCH basé sur ANSERA sont les suivantes :

- Informations Compte utilisateur : ID utilisateur, rôle utilisateur spécifique par rapport à la demande de brevet, autorisations en tant que membre.
- Informations de navigation : Adresse IP, URL, informations sur les cookies, agent utilisateur du navigateur, type de navigateur, date et heure de navigation.
- Données d'interaction Réseau/Application : contenu de la session, informations sur la session, métadonnées de la session, y compris informations sur la session dossier.
- Journaux système : journaux d'audit, données de fichiers, journaux de pare-feu/routeur/commutateur, ports, données de registre, fonctionnement.
- Processus, journaux de serveurs liés au système, à l'application et à la sécurité, informations sur les transactions, journaux de serveurs web.
- Identification personnelle : nom complet, e-mail professionnel, pays.
- Requête de recherche et annotations.
- Actifs physiques et/ou numériques identifiables utilisés.

3. Qui est responsable du traitement des données ?

Les données à caractère personnel sont traitées sous la responsabilité de la DP 4.5, dirigée par le Chief Technology Officer de l'OEB agissant en qualité de responsable délégué du traitement de l'OEB.

Les sous-traitants externes participant à la fourniture des services 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 communiquées sur la base du "besoin de savoir" au personnel de l'OEB travaillant à la direction BIT (Équipe d'automatisation des tests et des déploiements Kubernetes, Opérations, équipe du projet de coopération informatique 4.5.2, équipe d'assistance aux bureaux nationaux, équipe Ansera et développeurs de logiciels, équipe de l'outil SEARCH basé sur ANSERA et développeurs de logiciels).

Les données à caractère personnel peuvent être communiquées à des prestataires de services tiers lors de la fourniture du service, de la maintenance, de l'assistance et du développement, mais aussi lors de l'analyse des besoins utilisateurs aux fins de planification.

Les données à caractère personnel seront uniquement accessibles aux personnes habilitées, 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 à caractère personnel ?

L'OEB prend les mesures techniques et organisationnelles nécessaires pour préserver vos données à caractère personnel et les protéger de toute destruction, perte ou modification accidentelle ou illicite et de toute communication ou de tout accès non autorisé. Toutes les données à caractère personnel sont conservées dans des applications informatiques sécurisées conformément aux normes de sécurité de l'OEB. Des niveaux d'accès appropriés sont accordés à titre individuel aux seuls destinataires mentionnés ci-dessus.

En ce qui concerne les systèmes hébergés dans les locaux de l'OEB, les mesures sécuritaires de base suivantes s'appliquent généralement :

- 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, des équipements 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 de la transmission et des entrées (par exemple, journaux d'audit, surveillance des systèmes et du réseau)
- 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 une politique de gestion dématérialisée. Toutefois, 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 sécurisé et verrouillé, à accès restreint.

Pour les données à caractère personnel traitées sur des systèmes qui ne sont pas hébergés dans les locaux de l'OEB, les prestataires externes traitant ces données s'engagent, dans le cadre d'un accord contraignant, à se conformer aux obligations afférentes à la protection des données découlant des cadres juridiques applicables relatifs à la protection des données. L'OEB a également effectué une analyse relative à la confidentialité et au risque de sécurité. Ces systèmes doivent disposer de 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 réseau, des systèmes de détection des intrusions (IDS) sur le réseau, des systèmes de protection contre les intrusions (IPS) sur le réseau, des journaux d'audit) ; des mesures de contrôle du transport des données (p. ex. sécurisation des données en transit par chiffrement).

6. Comment 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 d'en limiter le 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 DPOexternalusers@epo.org. Afin de nous permettre de répondre plus rapidement et précisément, vous devez toujours assortir votre demande de certaines informations préliminaires. Nous vous conseillons donc de remplir ce formulaire et de l'envoyer avec votre demande.

Nous répondrons à votre demande dans les meilleurs délais et, dans tous les cas, 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 en fonction 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 sur la base de l'article 5a RRPD. (Ce traitement est nécessaire à l'accomplissement d'une tâche relevant des activités officielles de l'Organisation européenne des brevets ou de 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 ?

Les données à caractère personnel seront uniquement conservées pendant une durée n'excédant pas celle nécessaire à la finalité de leur traitement.

L'infrastructure IT fournit de nombreuses informations relatives aux ressources cloud du projet Search basé sur Ansera. Deux espaces de stockage par défaut sont créés automatiquement dans GCP : "_Default" et "_Required". Leur durée de conservation est définie comme suit : 30 jours pour "_Default" et 400 jours pour "_Required".

Avant que les requêtes des utilisateurs n'atteignent l'application de recherche, l'infrastructure IT vérifie qu'elles ne contiennent pas de contenu malveillant. Les journaux sont disponibles de façon native dans le système Search pendant 30 jours et transmis au système de stockage des journaux de l'équipe de sécurité de l'information de l'OEB.

Les journaux GCP sont transmis au dépôt central des journaux de l'équipe de sécurité de l'information de l'OEB. Leur période de conservation est de 12 mois.

Les journaux des applications opérationnelles de l'outil de recherche - y compris les demandes reçues - sont enregistrés aux fins de dépannage et de contrôle des performances et de la sécurité. L'accès aux journaux opérationnels - au sein du cluster de recherche basé sur Ansera - est restreint. Ces journaux ne sont pas transmis au dépôt central des journaux de l'équipe de sécurité de l'information de l'OEB. Les composants de l'application Search qui enregistrent les marqueurs de recherche sont configurés pour remplacer ces entrées par une marque de réservation. Les journaux des applications opérationnelles sont conservés pendant 12 mois.

Les données de recherche sont liées au cycle de vie des comptes utilisateurs. Les comptes utilisateurs sont gérés (création et suppression) par l'administrateur de l'ONB à l'aide d'une fonction d'administration des utilisateurs.

Les données de recherche (marqueurs, données bibliographiques, données sur l'état de la session utilisateur, concepts, annotations et aROSS) sont conservées avec le système de cryptage EKMS de l'OEB pour une durée indéterminée. Les annotations faites par les utilisateurs sur un dossier dans l'outil Search sont stockées jusqu'à ce que l'utilisateur supprime le dossier. Elles peuvent également être supprimées sur demande.

Les informations d'identification des utilisateurs de l'outil de recherche sont conservées dans le système principal de Search (Single Access Portal) jusqu'à leur marquage comme étant inactives. Une fois marquées comme inactives, le système de gestion des identités de l'OEB les conserve pendant 30 jours supplémentaires, puis les efface.

9. Personnes à contacter et coordonnées

En cas de questions sur le traitement des données à caractère personnel vous concernant, veuillez vous adresser au responsable délégué du traitement à l'adresse suivante : *DPOexternalusers@epo.org*.

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

Réexamen et exercice des voies de recours

Si vous estimez 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. Si vous n'êtes pas satisfait du résultat de ce réexamen, vous avez le droit d'exercer les voies de recours prévues à l'article 50 RRPD.