Déclaration relative à la protection des données lors du traitement de données à caractère personnel dans le cadre de la gestion des identités au moyen d'Active Directory et d'Azure Active Directory

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 (RRPD) de l'OEB.

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

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

La présente déclaration relative à la protection des données concerne la création de comptes utilisateurs ainsi que les règles d'accès des utilisateurs et les attributions correspondantes en utilisant Active Directory (AD) et Azure AD qui constituent le référentiel central des identités des utilisateurs.
L'OEB utilise AD et Azure AD aux fins de gestion des identités et des accès.

Deux cas de figure de création de comptes utilisateurs sont actuellement prévus :

1. Les utilisateurs internes (agents et fournisseurs) sont définis dans FIPS (système maître) qui est synchronisé avec On Premise AD. Ce dernier est ensuite synchronisé avec AD Azure.

2. Les utilisateurs des offices nationaux des brevets : la source maîtresse est le portail d'accès unique, dans lequel les utilisateurs sont créés, mis à jour et supprimés. Le portail d'accès unique est synchronisé avec On Premise AD. Ce dernier est ensuite synchronisé avec AD Azure.

Les comptes utilisateurs sont par la suite utilisés à des fins d'authentification et d'autorisation.

L'OEB ne traitera pas les données dans le but d'une prise de décision automatisée, notamment le profilage.

Nous ne transfèrerons pas vos données à caractère personnel à l'extérieur de l'OEB à des parties qui ne sont pas visées 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, nous ne transfèrerons vos données à caractère personnel 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 des dérogations pour les situations particulières visées à l'article 10 RRPD s'appliquent.

2. Quelles sont les données à caractère personnel traitées par l'OEB ?

Nous traitons les données à caractère personnel suivantes dans le cas où la personne concernée est un agent de l'OEB ou un fournisseur :

- informations d'identification : prénom, nom, genre, photographie, langue de communication préférée, signature numérique, certificat numérique

- informations de contact : adresse électronique professionnelle, numéros de téléphone, numéro de téléphone portable
- informations relatives au compte utilisateur : numéro personnel, identifiant de l'utilisateur, identifiant du compte, ancienneté du compte, mot de passe du compte, hash du mot de passe, heure de la dernière connexion, autorisations de qualité de membre et de détention
- informations de navigation : type de navigateur, agent utilisateur du navigateur, date et heure de navigation, durée de navigation
- données d'interaction réseau/application : métadonnées de la session, détails de la session, adresse IP
- journaux système : journaux des serveurs associés au système, à l'application et à la sécurité
- données de gestion des appareils : identifiant Windows pour les appareils Windows, identifiant du locataire, identifiant de l'appareil Azure Active Directory
- informations professionnelles : nom et/ou numéro du département, division de l'unité opérationnelle, numéro personnel, indicateur actif/inactif, responsable hiérarchique, numéro de salle, fonctions, adresse des bureaux, entité de la société (uniquement pour les fournisseurs)
- actifs physiques et/ou numériques : nom d'hôte du poste de travail (physique ou virtuel), salle de visioconférence/identifiant d'équipement (uniquement pour les agents), nom du dispositif mobile, version du système d'exploitation
- secteur du bâtiment et site

Nous traitons les données à caractère personnel suivantes dans le cas où la personne concernée est externe :

- informations d'identification : prénom, nom, pays
- informations de contact : adresse électronique professionnelle, numéros de téléphone
- informations relatives au compte utilisateur : numéro du compte, ancienneté du compte, mot de passe du compte, hash du mot de passe, autorisations de qualité de membre et de détention
- informations de navigation : type de navigateur, durée de navigation
- données d'interaction réseau/application : métadonnées de la session, détails de la session, adresse IP
- journaux système : journaux des serveurs associés au système, à l'application et à la sécurité
- informations professionnelles : entité de la société

Nous traitons les données à caractère personnel suivantes dans le cas où la personne concernée est un ancien agent :

- informations d'identification : prénom, nom
- informations relatives au compte utilisateur : identifiant de l'utilisateur, ancienneté du compte, hash du mot de passe, autorisation de qualité de membre.
- informations de navigation : type de navigateur, durée de navigation
- données d'interaction réseau/application : métadonnées de la session, détails de la session, adresse IP
- journaux système : journaux des serveurs associés au système, à l'application et à la sécurité

3. Qui est responsable du traitement des données ?

Le traitement des données à caractère personnel est réalisé sous la responsabilité du Chief Information Officer de l'OEB (DP 4.6 BIT),
agissant en qualité de responsable délégué du traitement des données à l'OEB.

Le traitement des données à caractère personnel est également réalisé par les agents de la DP 4.6 qui participent à la gestion des applications visées dans la présente déclaration.

Les prestataires externes participant aux tâches de gestion des identités et d'accès peuvent également traiter les données à caractère personnel, ce qui peut inclure l'accès à celles-ci.

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

Nous communiquons des données à caractère personnel en tant que de besoin aux personnes suivantes :

- le personnel permanent et contractuel de l'OEB (administrateurs système) du département de la sécurité de l'information 4.6.2.3
- l'ensemble du personnel de l'OEB : droit d'accès en lecture (directement par le navigateur), p. ex. via l'annuaire téléphonique ou indirectement via les API, à d'autres applications Microsoft (p. ex. Outlook, MS Teams, etc.), à des données à caractère personnel appartenant à d'autres membres du personnel
- les données à caractère personnel AD/Azure AD sont accessibles par des applications de l'OEB à des fins d'authentification/d'autorisation des utilisateurs

Il se peut également que nous communiquions des données à caractère personnel à des prestataires de services tiers à des fins de maintenance, de soutien et de sécurité.

Nous partagerons les données à caractère personnel uniquement avec des personnes habilitées responsables des opérations de traitement nécessaires et nous ne les utiliserons pas à d'autres fins ni ne les communiquerons à d'autres destinataires.

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

L'OEB prend les mesures techniques et organisationnelles nécessaires pour préserver les données à caractère personnel vous concernant et les protéger contre la destruction, la perte ou la modification accidentelles ou illicites ainsi que contre la communication non autorisée desdites données ou l'accès non autorisé à celles-ci.

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 et uniquement aux destinataires mentionnés ci-dessus.

En ce qui concerne les systèmes de gestion des identités hébergés dans les locaux de l'OEB, les mesures de sécurité suivantes ont été mises en place :
L'ensemble des données à caractère personnel relatives à la gestion des identités est conservé dans des applications sécurisées IAM conformément aux normes de sécurité de l'OEB. Celles-ci comprennent :

- 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 en fonction du rôle aux systèmes et réseaux, principes du « besoin de savoir » et du « moindre privilège ») : séparation des rôles d'administrateur et d'utilisateur, les utilisateurs ayant un minimum de privilège et les rôles d'administrateur étant maintenus au minimum.
- installation d'antivirus sur tous les dispositifs
- protection physique : contrôles des accès effectués par l'OEB, contrôles supplémentaires des accès aux centres de données
- contrôle des transmissions et entrées : audit des connexions, surveillance des systèmes et réseaux, surveillance de la sécurité
- intervention en cas d'incident de sécurité : surveillance des incidents 24 heures sur 24 et 7 jours sur 7, experts en sécurité de garde.

En ce qui concerne 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 de protection des données découlant du cadre juridique de protection des données applicable. L'OEB a également effectué une analyse en matière de confidentialité et de risque de sécurité. Il est exigé que ces prestataires aient mis en place des mesures techniques et organisationnelles 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), journaux d'audit) ; des mesures de contrôle de l'acheminement des données (p. ex. sécurisation des données en transit par chiffrement).

Azure AD est certifié conformément à plusieurs normes de sécurité (p. ex. SOC 1 Type II, SOC 2 Type II).

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 ?

En tant que personne concernée, 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, ainsi que de limiter leur traitement ou de vous opposer à celui-ci (articles 18 à 24 RRPD).

Les utilisateurs externes qui souhaitent exercer l'un de ces droits, sont invités à adresser une demande écrite en ce sens au responsable délégué du traitement (DPOexternalusers@epo.org) tandis que les utilisateurs internes sont invités à envoyer une demande écrite à l'adresse suivante : 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), ce formulaire (pour les personnes internes) et/ou ce formulaire (pour les retraités), 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 des données vous concernant ?

Les données à caractère personnel sont traitées sur le fondement de l'article 5(a) RRPD, c'est à dire lorsque "ce traitement est nécessaire pour 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 à caractère personnel ?

Nous conserverons les données à caractère personnel uniquement pendant une durée n'excédant pas celle nécessaire au regard de la finalité de leur traitement.

Nous conserverons les données des utilisateurs jusqu'à ce que le système (source) maître (c'est-à-dire le portail d'accès unique) indiquent qu'elles sont inactives, puis nous les conserverons à la fois dans On Premise AD et dans Azure AD pendant 30 jours supplémentaires.

À tout moment au cours de son abonnement, l'OEB a la possibilité d'accéder aux données conservées dans les applications dans le cadre de la présente déclaration, de les extraire ainsi que de les effacer. Microsoft conservera les données de l'OEB qui restent stockées dans les applications dans un compte de fonction limité pendant 90 jours suivants l'expiration ou la résiliation de l'abonnement de l'OEB de sorte que l'OEB peut extraire les données.

À l'expiration de la période de conservation de 90 jours, Microsoft désactivera le compte de l'OEB et effacera les données de l'OEB ainsi que les données à caractère personnel pendant une durée supplémentaire de 90 jours, à moins que Microsoft ne soit autorisée en vertu de l'accord conclu avec l'OEB à conserver lesdites données.

En ce qui concerne les données à caractère personnel relatives aux applications dans le cadre de la présente déclaration, Microsoft effacera toute copie après que les objectifs professionnels pour lesquels les données ont été collectées ou transférées ont été remplis ou avant, à la demande de l'OEB, à moins que Microsoft ne soit autorisé en vertu de l'accord conclu avec l'OEB à conserver lesdites données. En cas de recours formel/contentieux, toutes les données détenues au moment où le recours formel/contentieux est engagé seront conservées jusqu'à la clôture de la procédure.

9. Personnes à contacter et coordonnées

Les personnes concernées externes ayant des questions concernant le traitement de leurs données à caractère personnel doivent contacter le responsable de la protection des données et/ou le responsable délégué du traitement à l'adresse suivante : DPOexternalusers@epo.org.

Les agents de l'OEB doivent contacter le responsable délégué du traitement à l'adresse suivante : DP_BIT@epo.org ou le responsable de la protection des données à l'adresse suivante : 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 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