Déclaration relative à la protection des données lors du traitement de données à caractère personnel par le service Microsoft Defender pour point de terminaison 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 (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 porte sur le traitement de données sensibles par le service Microsoft Defender pour point de terminaison (Microsoft Defender for Endpoint, MDE) de l'OEB. Ces données sont collectées à partir de points de terminaisons embarqués (postes de travail Windows et serveurs Windows) et transmises à un locataire cloud séparé dédié au service MDE de l'OEB, pour être traitées et faire l'objet d'alertes de manière automatisée. La Direction principale (DP) 4.6 Business Information Technology (BIT) collecte les données relatives aux alertes de sécurité MDE à partir du locataire cloud MDE et les stocke sur site dans Splunk de manière automatisée.

L'OEB traite les données à caractère personnel aux fins suivantes :

- prévenir les incidents de sécurité affectant le réseau et les données de l'OEB, tels que les infections par des logiciels malveillants ;
- détecter et signaler les activités compromettantes ou malveillantes sur les points de terminaison au sein de l'infrastructure de l'OEB ;
- enquêter sur les incidents de sécurité au sein de l'infrastructure de l'OEB et y remédier.

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

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

Les catégories suivantes de données à caractère personnel sont traitées.

Si la personne concernée est un agent de l'OEB ou un prestataire de l'OEB (employé d'un prestataire de services externe) :

- informations d'identification : prénom, nom ;

- informations de contact : numéros de téléphone, adresse électronique professionnelle ;
- informations relatives au compte utilisateur : numéro de compte, identifiant utilisateur ;
- informations relatives à l'emploi : titre du poste, nom et/ou numéro de département ;
- données d'interaction réseau/application : détails de la session, métadonnées de la session ;
- informations de navigation : temps passé à naviguer, date et heure de la navigation, type de navigateur, adresse IP, catégorie, URL, historique des sites internet, historique des interactions avec le réseau ;
- données de gestion des appareils : dispositif d'identification Azure Active Directory ;
- actifs identifiables physiques et/ou numériques : adresse MAC de l'adaptateur réseau du poste de travail, numéro de série du poste de travail, version du système d'exploitation, nom d'hôte du poste de travail (physique ou virtuel), modèle fournisseur du poste de travail, version BIOS, type de processeur, extensions de navigateur installées avec indications de leur état (actif / inactif), certificats installés avec indications de leurs propriétés, applications logicielles installées ;
- journaux du système : journaux d'audit (ou pistes d'audit), journaux du serveur liés au système/aux applications/à la sécurité, données du registre, processus en cours d'exécution, ports, données relatives au fichier (nom, taille et/ou hachage).

Si la personne concernée est un utilisateur externe :

- informations de navigation : temps passé à naviguer, adresse IP, données d'interaction réseau/application, métadonnées de la session.

3. Qui est responsable du traitement des données ?

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

Les données à caractère personnel sont traitées par les agents du département 4.6.2.3 BIT Information Security impliqués dans la gestion du service visé par la présente déclaration.

Les prestataires externes impliqués dans l'assistance et la maintenance de l'application Microsoft – y compris Microsoft elle-même – peuvent également accéder aux données à caractère personnel et les traiter.

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

Les données à caractère personnel sont communiquées par l'intermédiaire de la console du locataire cloud MDE aux destinataires suivants en tant que de besoin :

- les agents de l'OEB travaillant au sein du département 4.6.2.3 BIT Information Security (uniquement les personnes désignées) ;
- les personnes nommément désignées au sein de la DP 4.6 ayant le rôle d'administrateur général Microsoft O365 ou de lecteur Microsoft O365.

Les données à caractère personnel peuvent être communiquées à des prestataires de services tiers agissant pour le compte de la BIT à des fins de maintenance et d'assistance. En principe, la majorité des opérations de service pour les produits Microsoft sont automatisées afin de réduire la nécessité d'un accès humain. Tout accès requis est limité dans le temps et soumis à des limitations des droits d'accès.

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 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.

Pour les données à caractère personnel traitées par des systèmes qui ne sont pas hébergés dans les locaux de l'OEB, l'OEB a effectué une analyse en matière de confidentialité et de risque de sécurité. 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.

Toutes les données à caractère personnel transmises sur des réseaux publics entre l'OEB et Microsoft, ou entre les centres de données de Microsoft, sont cryptées par défaut. Les données personnelles qui sont fournies à Microsoft par l'OEB ou en son nom par l'utilisation du service Microsoft Defender pour point de terminaison sont cryptées au repos. En ce qui concerne la mise en œuvre du cryptage, Microsoft utilise des technologies de cryptage de pointe. En outre, Microsoft utilise des mécanismes d'accès selon le principe de moindre privilège pour contrôler l'accès aux données à caractère personnel qui lui sont fournies par l'OEB, ainsi que des contrôles d'accès basés sur les rôles pour garantir que l'accès à ces données à caractère personnel n'est possible que pour des opérations de service légitimes soumises à l'approbation de la direction. En ce qui concerne les services Microsoft, tout accès requis par Microsoft est limité dans le temps.

Microsoft met en œuvre et maintient de nombreuses mesures de sécurité pour la protection des données à caractère personnel qui lui sont fournies par l'OEB par l'utilisation du service Microsoft Defender pour point de terminaison. Ces mesures de sécurité englobent l'organisation de la sécurité de l'information (par exemple, la propriété de la sécurité, les rôles et responsabilités en matière de sécurité, le programme de gestion des risques), la gestion des actifs (par exemple, l'inventaire des actifs et leur manipulation), la sécurité des ressources humaines (par exemple, formation à la sécurité), sécurité physique et environnementale (par exemple, accès physique aux installations, accès physique aux composants, protection contre les perturbations, élimination des composants), contrôles de gestion des communications et des opérations (par exemple, politique opérationnelle, procédures de récupération des données, contrôles anti-programmes malveillants, journaux des événements), mesures de contrôle d'accès (par exemple, politique d'accès, autorisation d'accès, moindre privilège, intégrité et confidentialité, authentification, conception du réseau), gestion des incidents de sécurité de l'information (par exemple, processus de réponse aux incidents, surveillance des services) et gestion de la continuité des activités. Microsoft met également en œuvre et maintient des mesures techniques et organisationnelles appropriées pour la protection de toute autre donnée à caractère personnel distincte de celles décrites ci-dessus. Ces mesures sont décrites dans la Politique de sécurité de Microsoft.

Microsoft Defender pour point de terminaison a été configuré pour préserver la confidentialité des informations en employant les mesures énumérées ci-dessus. En outre, l'accès anonyme n'est pas autorisé. Toute information recueillie par le biais de Microsoft Defender pour point de terminaison ne peut être consultée que par les utilisateurs et groupes spécifiquement mentionnés dans la section 4 ci-dessus.

Microsoft Defender pour point de terminaison est certifié conformément à plusieurs normes de sécurité, notamment ISO27001, SOC1 Type II, SOC2 Type II et ISO27018 (Code de pratique pour la protection des données personnelles dans le cloud), et respecte les exigences énoncées dans la norme ISO 27002.

Microsoft effectue des audits annuels de la sécurité des ordinateurs, de l'environnement informatique et des centres de données physiques qu'elle utilise pour traiter les données à caractère personnel. Les audits sont réalisés par des auditeurs tiers indépendants, conformément aux normes et règles de l'organisme de réglementation ou d'accréditation pour chaque norme de contrôle ou cadre applicable.

Les données à caractère personnel sont conservées au sein de l'UE selon la configuration d'application mise en œuvre par l'OEB. Elles peuvent toutefois être mises à la disposition de sous-traitants pour être traitées dans d'autres pays, en fonction des exigences de maintenance, d'assistance ou d'exploitation des services hébergés dans le cloud, et des compétences techniques disponibles. Si l'accès est accordé, celui-ci est toujours temporaire et ne concerne que les données nécessaires à la procédure spécifique de maintenance, d'assistance ou d'exploitation en cours. Les mesures de protection suivantes sont mises en œuvre.

• Pour tous les transferts vers des pays tiers, Microsoft impose des clauses contractuelles types de l'UE pour le transfert des données à ses sous-traitants réalisant le traitement.

• Microsoft exige des sous-traitants réalisant le traitement qu'ils adhèrent au programme Microsoft Supplier Security and Privacy Assurance. Ce programme est conçu pour normaliser et renforcer les pratiques de traitement des données et pour garantir que les processus et systèmes commerciaux des fournisseurs sont compatibles avec ceux de Microsoft.

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 (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 : 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 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".

Les données à caractère personnel sont traitées sur la base de l'instrument juridique suivant : Article 7 "Surveillance, contrôles, audits et suite de la procédure" de la circulaire nº 382 (29 mars 2017) Directives relatives à la sécurité de l'information à l'OEB.

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

Les données à caractère personnel sont conservées uniquement pendant une durée n'excédant pas celle nécessaire au regard de la finalité de leur traitement. Plus précisément, les données à caractère personnel sont stockées conformément aux règles de conservation suivantes :

- les données sont conservées dans un espace de cache temporaire dans le point de terminaison lui-même pour une durée maximale de trois jours.

- les données sont conservées dans l'environnement cloud MDE pendant une période de 180 jours à l'issue de laquelle elles sont supprimées du locataire cloud MDE.

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

Si vous avez des questions sur le traitement des données à caractère personnel vous concernant, veuillez les adresser au responsable du traitement à l'adresse DP_BIT@epo.org (pour les agents de l'OEB) ou DPOexternalusers@epo.org (pour les personnes concernées externes).

Les personnes internes peuvent également contacter notre responsable de la protection des données à l'adresse électronique suivante : dpo@epo.org, et les personnes externes à l'adresse électronique suivante : 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.