Déclaration relative à la protection des données concernant le traitement des données à caractère personnel dans le cadre des applications Microsoft 365

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 conformément aux articles 16 et 17 RRPD.

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

La présente déclaration relative à la protection des données se rapporte au traitement effectué par les applications Microsoft 365, ce qui comprend les applications sur le cloud suivantes : OneDrive, SharePoint Online, MS Teams, MS Forms, Word, Excel et PowerPoint. L'ensemble des applications comprises dans Microsoft 365 est mis à disposition des utilisateurs afin de renforcer la flexibilité et d'améliorer la communication et la collaboration, à la fois au sein de l'OEB et entre l'OEB et les parties prenantes externes.

Tel que précédemment indiqué, les applications Microsoft 365 comprennent MS Teams, dont les fonctionnalités principales comprennent la messagerie professionnelle, les appels, les réunions audio et vidéo ainsi que le partage de fichiers. MS Teams est une application sur le cloud permettant d'organiser des réunions et téléconférences virtuelles, à la fois au sein de l'OEB et entre l'OEB et les parties prenantes de l'OEB. Outre ces fonctionnalités principales, MS Teams permet également d'enregistrer les réunions virtuelles et d'utiliser des sous-titres en direct. L'utilisation de ces fonctionnalités n'est octroyée qu'à des parties prenantes spécifiques conformément aux politiques internes de l'OEB relatives à l'utilisation de MS Teams.

En outre, Microsoft 365 comprend également des « expériences connectées » non optionnelles qui visent à permettre de renforcer la création, la communication et la collaboration.

Les applications Microsoft 365 sont utilisées par les agents de l'OEB dans le cadre de l'accomplissement de leurs tâches quotidiennes.

En outre, les données à caractère personnel sont traitées en vue des finalités suivantes établies par le responsable délégué du traitement, à savoir le Chief Information Officer de l'OEB (Technologie des informations commerciales) – Direction principale 4.6) :

• Remettre les applications Microsoft 365 et les services aux agents de l'OEB et aux prestataires.
• Fournir aux utilisateurs finaux une assistance et un dépannage pour les applications et fonctionnalités Microsoft 365.
• Gérer le contenu téléchargé vers les applications Microsoft 365.
• Gérer les paramètres Microsoft 365.
• Effectuer l'assistance, l'exploitation et l'entretien des applications Microsoft 365.

Ce traitement ne fait l'objet d'aucune prise de décision automatisée, y compris le profilage.

Les applications Microsoft Office sont susceptibles d'être utilisées pour différentes finalités et dans le cadre de différents scénarios, que la présente déclaration relative à la protection des données ne décrit pas dans leur intégralité. Les scénarios spécifiques dans le cadre desquels les applications Microsoft 365 sont utilisées pour traiter des données à caractère personnel et les finalités spécifiques pour lesquelles elles peuvent l'être sont décrits dans des déclarations relatives à la protection des données émises à cet égard ainsi que des enregistrements des activités de traitement connexes.

Vos données à caractère personnel ne seront pas transférées vers des destinataires hors de l'OEB qui ne sont pas couverts par les articles 8(1), (2) et (5) RRPD, à moins qu'un niveau de protection adéquat ne soit garanti. En l'absence d'un niveau de protection adéquat, ce transfert ne peut se produire que si des garanties appropriées sont prévues et à la condition que les personnes concernées disposent de droits opposables et de voies de recours effectives ou si des dérogations – au titre de situations particulières – en vertu de l'article 10 RRPD, s'appliquent. Dans le cadre de l'utilisation des applications Microsoft précédemment énumérées, des transferts sont susceptibles de se produire en vue des finalités limitées suivantes : protection contre des logiciels malveillants, connexion à Azure Active Directory, équilibrage de la charge, données de diagnostic, expériences connectées et traitement des opérations commerciales de Microsoft.

2. Quelles données à caractère personnel traitons-nous ?

Dans les applications Microsoft 365, les catégories et types de données à caractère personnel suivants peuvent être traités :

Si la personne concernée est un agent de l'OEB :

- identification personnelle : nom, prénom, photo, signature numérique ;
- informations de contact : adresse de messagerie électronique professionnelle, numéros de téléphone ;
- informations professionnelles : société, nom du département et/ou numéro, fonctions correspondant au poste, numéro de salle, emplacement du bureau, langue préférée (aux fins de communication) ;
- informations liées au compte utilisateur : Identifiant utilisateur, numéro de compte, ancienneté du compte, autorisation de détention, autorisation de qualité de membre ;
- actifs identifiables physiques et/ou numériques : nom du dispositif mobile, nom d'hôte de la station de travail, version du système opérationnel ;
- données liées à la gestion du dispositif : dernière heure de connexion, identifiant de compte ;
- données d'interaction avec le réseau/ les applications : métadonnées de session, contenu de session, détails de session ;
- informations de géolocalisation ;
- informations de navigation : type de navigateur, agent utilisateur du navigateur, historique des sites internet, informations relatives aux cookies, URL, date et heure de navigation, adresse IP, historique d'interaction avec le réseau, heure de navigation ;
- informations sensorielles et numériques : statut de présence, informations audios et visuelles ;
- données d'interaction téléphonique : métadonnées de session téléphonique, contenu de session téléphonique, détails de session téléphonique ;
- informations relatives aux appels téléphoniques : numéro de téléphone appelé, numéro de téléphone de l'appelant, date et heure de l'appel téléphonique, historique des appels, historique des interactions téléphoniques, durée des appels ;
- journaux systèmes : données liées au fichier (nom, taille et/ou hachage), données de registre, processus actifs, numéros de port, journaux des serveurs internet, journaux systèmes, journaux applications et journaux liés à la sécurité du serveur, journaux d'audit, détails des transactions ;
- informations personnelles fournies volontairement par la personne concernée dans le cadre de partages de fichiers aux fins d'activités professionnelles (p. ex. messages, images, fichiers, courriers vocaux, réunions programmées, contacts, etc.) ainsi que toute autre information supplémentaire que la personne concernée est susceptible de fournir en échangeant des communications ;

Si la personne concernée est externe à l'OEB :

- informations de contact : adresse de messagerie électronique personnelle et/ou professionnelle ;
- données d'interaction avec le réseau/ les applications : métadonnées de session, contenu de session, détails de session ;
- informations de navigation : adresse IP, historique des sites internet, date et heure de navigation, historique des interactions avec le réseau, informations relatives aux cookies, URL, agent utilisateur du navigateur, type de navigateur ;
- informations sensorielles et numériques : statut de présence, informations audios et visuelles ;
- données d'interaction téléphonique : métadonnées de session téléphonique, contenu de session téléphonique, détails de session téléphonique ;
- informations relatives aux appels téléphoniques : numéro de téléphone appelé, numéro de téléphone de l'appelant, date et heure de l'appel téléphonique, durée de l'appel téléphonique, historique des appels, historique des interactions téléphoniques ;
- journaux systèmes : journaux des serveurs internet, journaux systèmes, journaux applications et journaux liés à la sécurité du serveur ;
- informations personnelles communiquées volontairement par la personne concernée dans le cadre de partages de fichiers aux fins d'activités professionnelles (p. ex. messages, images, fichiers, courriers vocaux, réunions programmées, contacts, etc.) ainsi que toute autre information supplémentaire que la personne concernée est susceptible de fournir en échangeant des communications.

3. Qui est responsable du traitement des données ?

Les données à caractère personnel sont traitées sous la responsabilité du Chief Information Officer de l'OEB (Technologie des informations commerciales – Direction principale 4.6), agissant en tant que responsable délégué du traitement.

Les données à caractère personnel sont traitées par les agents de la Direction principale 4.6 impliqués dans la gestion des applications visées par la présente déclaration.

Les prestataires externes impliqués dans l'assistance, l'exploitation ou l'entretien des applications Microsoft 365 – y compris, sans pour autant s'y limiter, Microsoft lui-même – sont également susceptibles de traiter les données à caractère personnel, ce qui peut impliquer d'y accéder.

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 » aux destinataires suivants :

• Agents de l'OEB et utilisateurs externes compris dans les applications Microsoft 365 utilisées pour l'échange d'informations (par exemple, les participants à une réunion MS Teams).
• La Direction principale 4.6 de l'OEB et le personnel des prestataires externes de la Direction principale 4.6 impliqués dans le traitement des données nécessaires aux fins de prestation des services.

Au sein de Microsoft 365, en principe, la majorité des opérations de services sont automatisées afin de réduire la nécessité d'un accès par des humains. Tout accès requis à partir de Microsoft l'est pour un temps limité et les droits d'accès sont également limités.

Lorsqu'une réunion virtuelle est enregistrée dans MS Teams, l'enregistrement peut éventuellement être divulgué à l'OEB dans son ensemble ou en dehors de l'OEB, en fonction de la réunion en question. Dans tous les cas, la personne concernée sera dûment informée par l'organisateur de la réunion des détails de l'opération de traitement (p. ex. par le biais d'une déclaration relative à la protection des données spécifiques).

Pour les sondages, formulaires ou questionnaires organisés par un propriétaire via MS Forms, les questions et les réponses sont conservées dans Microsoft cloud. Seuls les propriétaires d'un sondage peuvent accéder aux réponses soumises au sondage. En cas de sondage anonyme, aucune information de contact des participants n'est incluse dans la réponse. En cas de sondage confidentiel (= non anonyme), le propriétaire a accès aux nom, adresse de messagerie électronique, date et heure d'ouverture du sondage, date et heure de soumission des réponses des participants.

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

Nous adoptons des mesures techniques et organisationnelles appropriées afin de sauvegarder et protéger vos données à caractère personnel, contre toute destruction, perte, altération, divulgation non autorisée ou l'accès non autorisé à de telles données. Pour les données à caractère personnel traitées dans 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 à caractère personnel en vertu des cadres juridiques de protection des données applicables. L'OEB a également effectué une évaluation des risques en matière de confidentialité et de sécurité.

Toute donnée à caractère personnel en transit via des réseaux publics entre l'OEB et Microsoft ou entre les centres de données de Microsoft est chiffrée par défaut. Les données à caractère personnel faisant partie de toute donnée communiquée à Microsoft par l'OEB ou pour son compte à travers l'utilisation des services Microsoft 365 sont chiffrées au repos. Concernant la mise en œuvre du chiffrement, Microsoft utilise des technologies de chiffrement de pointe. En outre, Microsoft utilise des mécanismes d'accès du moindre privilège afin de contrôler l'accès aux données à caractère personnel qui font partie des données fournies à Microsoft par l'OEB et des contrôles d'accès fondés sur les rôles sont utilisés afin de s'assurer que l'accès à ces données à caractère personnel requis pour les opérations de services se fasse pour une finalité adéquate et soit approuvé par la supervision de la gestion. Pour les applications Microsoft 365, tout accès requis par Microsoft est limité dans le temps.

Les applications Microsoft 365 mettent en œuvre et maintiennent de multiples mesures de sécurité pour la protection des données à caractère personnel fournies à Microsoft par l'OEB via l'utilisation des services Microsoft 365. Elles comprennent les éléments suivants : organisation de la sécurité de l'information (p. ex. prise en charge de la sécurité, rôles et responsabilité en la matière, programme de gestion des risques), gestion des actifs (p. ex. inventaire des actifs et gestion des actifs), sécurité des ressources humaines (p.ex. formation sur le thème de la sécurité), sécurité physique et de l'environnement (p. ex. accès physique aux locaux, accès physique aux composants, protection contre les interruptions, élimination des composants), contrôles de la gestion des opérations et communications (p. ex. politique opérationnelle, procédure de récupération des données, contrôles anti-logiciels malveillants, journalisation des événements), mesures de contrôle d'accès (p. ex. politique d'accès, autorisation d'accès, moindre privilège, intégrité et confidentialité, authentification, conception de réseau), gestion des incidents en matière de sécurité de l'information (p.ex. processus d'intervention en cas d'incident, service de surveillance) et gestion de la continuité des activités. En outre, Microsoft met en œuvre et maintient des mesures techniques et organisationnelles appropriées pour la protection de toute autre donnée à caractère personnel distincte de celles sus-décrites, qui sont décrites dans la Politique de sécurité de Microsoft.

Les applications Microsoft 365 ont été configurées afin de préserver la confidentialité des informations en mettant en œuvre les mesures indiquées précédemment. En outre, un accès anonymisé est interdit. Toute information que vous rajoutez dans Microsoft 365, que ce soit dans le cadre d'un chat, d'une visioconférence ou du partage de fichiers, sera uniquement disponible pour les utilisateurs et groupes spécifiques mentionnés dans la section 4 précédente.

Les applications Microsoft 365 sont certifiées conformes à différentes normes de sécurité et notamment : ISO27001, SOC1 Type II, SOC2 Type II, ainsi que ISO27018 « code de pratique pour la protection des informations personnellement identifiables dans les nuages », et satisfont aux exigences énoncées dans la norme ISO27002.

Microsoft réalise des audits annuels sur la sécurité des ordinateurs, de l'environnement informatique ou des centres des données physiques que Microsoft utilise dans le cadre du traitement des données à caractère personnel. Les audits sont effectués par des auditeurs tiers indépendants conformément aux exigences et règles des organismes de réglementation et d'accréditation pour chaque norme ou cadre de contrôle applicable.

Les données à caractère personnel sont conservées en Europe conformément à la configuration d'application mise en œuvre par l'OEB. Elles peuvent, néanmoins, être mises à dispositions de sous-traitants ultérieurs dans d'autres pays, en fonction des exigences d'entretien, d'assistance ou d'exploitation des services sur le cloud et de la disponibilité de cette expertise. L'accès est, le cas échéant, toujours accordé de façon temporaire et uniquement concernant les données requises pour la procédure d'entretien, d'assistance ou d'exploitation spécifique réalisée. Les garanties suivantes sont mises en œuvre :
• Pour tous les transferts vers des sous-traitants ultérieurs se trouvant dans des pays tiers, Microsoft utilise des clauses types européennes.
• Microsoft exige des sous-traitants ultérieurs qu'ils adhèrent à son Programme d'assurance de sécurité et de confidentialité des fournisseurs. Ce programme vise à normaliser et renforcer les pratiques de manipulation, afin de s'assurer que les processus commerciaux et systèmes des fournisseurs soient en ligne avec ceux de Microsoft.

Mesures spécifiques relatives à l'enregistrement des réunions MS Teams :

Lorsqu'une réunion virtuelle est enregistrée, les participants peuvent limiter le traitement de leurs données à caractère personnel en activant/désactivant leur microphone et caméra. En outre, s'ils se fondent sur des motifs légitimes, les participants peuvent également demander via la fonctionnalité chat la suspension temporaire de l'enregistrement afin qu'ils puissent y participer sans être enregistrés.

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, de les effacer, ainsi que de limiter leur traitement et/ou de vous opposer à celui-ci (articles 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 des données à l'adresse DP_BIT@epo.org. Les utilisateurs externes doivent contacter le responsable du traitement des données et/ou le responsable délégué du traitement des données à l'adresse suivante : 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 encourageons par conséquent, à remplir le présent formulaire (pour les personnes concernées internes à l'OEB) ou ce formulaire (pour les personnes concernées externes) 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. Quelle est la base juridique du traitement de vos données à caractère personnel ?

Les données à caractère personnel seront traitées conformément à 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 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 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 conservées de la manière suivante :

- Le contenu de Teams Chats, Teams Channel Messages, One Drive et SharePoint Online est conservé jusqu'à la résiliation par l'OEB du contrat avec Microsoft.
- One Drive : les données à caractère personnel sont automatiquement effacées de OneDrive un an après la suppression du compte de l'utilisateur.
- MS Teams : si un chat ou un message dans Teams est supprimé par un utilisateur ou si tout contenu dans OneDrive et SharePoint Online est supprimé par un utilisateur, il est conservé avant la suppression finale, pour une période d'un an suite à la dernière date de modification dans un lieu uniquement accessible par un administrateur.

  Pour Teams, l'historique des appels téléphoniques est conservé pendant 90 jours et peut être visualisé par les administrateurs. Un utilisateur final ne peut visualiser une liste de ses propres appels téléphoniques que pour une durée de 30 jours.

  Les enregistrements des réunions Teams réalisés en utilisant la fonctionnalité d'enregistrement sont conservés pendant une période de 3 mois avant suppression, à moins que cela ne soit défini autrement par l'enregistreur. Les enregistrements des événements Live Teams sont conservés pendant 180 jours. Ces enregistrements peuvent être conservés pour plus d'un an en fonction de la nature de la réunion, moyennant quoi la période de conservation est définie conformément à la finalité de l'enregistrement.
  Si un enregistrement devient désuet ou obsolète avant la fin de la période de conservation, il sera effacé. La période de conservation spécifique sera indiquée dans une déclaration relative à la protection des données spécifique et/ou un avis envoyé conjointement à l'invitation à la réunion.
- MS Forms : pour les sondages réalisés via MS Forms, le propriétaire du sondage est tenu de définir, communiquer et exécuter manuellement la conservation qu'il a décidée.

  En outre, à tout moment au cours de la durée d'exécution du contrat de l'OEB avec Microsoft, l'OEB peut accéder aux données stockées dans les applications, les extraire et les effacer. Microsoft conservera les données de l'OEB qui demeurent stockées dans les applications dans un compte de fonctions limitées pour une période de 90 jours suite à l'expiration ou résiliation du contrat par l'OEB afin que l'OEB puisse extraire les données. Suite 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 dans un délai supplémentaire de 90 jours, à moins que Microsoft ne soit autorisé à les conserver en vertu du contrat conclu avec l'OEB. Pour les données à caractère personnel se rapportant aux applications, Microsoft effacera toutes les copies suite à la réalisation des finalités commerciales pour lesquelles les données ont été collectées ou transférées, ou plus tôt, si l'OEB en fait la demande, à moins que Microsoft ne soit autorisé à les conserver en vertu du contrat conclu avec l'OEB.

En cas de recours formel/contentieux, toutes les données détenues lorsque 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 de vos données à caractère personnel, veuillez adresser une demande écrite au responsable délégué du traitement à l'adresse DP_BIT@epo.org pour les membres du personnel, ou à DPOexternalusers@epo.org pour les personnes concernées externes.

Les personnes concernées internes peuvent également contacter notre responsable de la protection des données à l'adresse suivante : dpo@epo.org, alors que les personnes concernées externes peuvent contacter notre responsable de la protection des données à l'adresse 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 délégué du traitement en vertu de l'article 49 RRPD et le droit d'exercer des voies de recours en vertu de l'article 50 RRPD.