Déclaration relative à la protection des données concernant le traitement des données à caractère personnel dans le cadre de l'utilisation de la messagerie électronique à l'OEB

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 du règlement relatif à la protection des données (RRPD) de l'OEB.

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 à travers les applications de messagerie électronique et de gestionnaire des tâches de l'OEB qui sont mises à disposition des agents de l'OEB. Les opérations de traitement exploitent Microsoft Exchange Online et Microsoft Outlook ; Outlook comprend également des expériences connectées non optionnelles, conçues en vue de renforcer la création, la communication et la collaboration.

Des données à caractère personnel sont traitées pour les finalités suivantes :

- permettre la transmission de courriers électroniques, pièces jointes et actions liées au gestionnaire des tâches entre les agents de l'OEB et les utilisateurs externes via des clients utilisateurs et des Interfaces de programmes d'applications (API) ;
- mettre à disposition des utilisateurs du système de messagerie électronique de l'OEB un carnet d'adresses afin de récupérer les adresses des destinataires, des listes et groupes de diffusion de l'OEB ;
- disposer d'une chaîne de courriers électroniques à des fins de dépannage informatique et de cybersécurité ;
- disposer d'un mécanisme de sauvegarde permettant aux utilisateurs du système de messagerie électronique de l'OEB de récupérer des courriers électroniques supprimés récemment et accidentellement.

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

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 de Microsoft Outlook et Exchange Online, 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 le cadre de l'utilisation de la messagerie électronique, 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, signature numérique ;
- informations de contact : adresse de messagerie électronique professionnelle, numéros de téléphone, coordonnées ;
- informations professionnelles : société, nom du département et/ou numéro, fonctions correspondant au poste, numéro de salle, emplacement du bureau, supérieur hiérarchique (uniquement pour les agents internes) ;
- informations liées au compte utilisateur : Identifiant utilisateur, autorisation de détention, autorisation de qualité de membre
- actifs identifiables physiques et/ou numériques : nom d'hôte de la station de travail, version du système opérationnel, certificat numérique ; salle de visioconférence/identifiant de l'équipement (uniquement pour les agents spécifiques) ;
- données d'interaction avec le réseau/ les applications : métadonnées de session, contenu de session, détails de session ;
- informations de navigation : type de navigateur, agent utilisateur du navigateur, informations relatives aux cookies, URL, date et heure de navigation, adresse IP, historique d'interaction avec le réseau ;
- informations sensorielles et numériques : statut de présence ;
- journaux systèmes : données liées au fichier (nom, taille et/ou hachage), 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 l'envoi de courriers électroniques aux fins d'activités professionnelles (p. ex. messages, images, fichiers, courriers vocaux, réunions programmées, contacts, et analogues), ainsi que toute autre information supplémentaire que la personne concernée est susceptible de fournir en échangeant des communications sans l'intervention de l'expéditeur (p. ex. lorsqu'un expéditeur envoie un courrier électronique en utilisant un navigateur internet, le moteur d'expédition peut ajouter l'adresse IP du navigateur dans l'un des en-têtes SMTP du message).

Si la personne concernée est un utilisateur externe :

- identification personnelle : nom, prénom, signature numérique ;
- 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, date et heure de navigation, historique des interactions avec le réseau ;
- journaux systèmes : informations liées aux transactions, journaux systèmes, journaux applications et journaux liés à la sécurité du serveur, données liées aux fichiers (nom, taille et/ou hachage) ;
- informations personnelles communiquées volontairement par la personne concernée dans l'envoi de courriers électroniques aux fins d'activités professionnelles (p. ex. messages, images, fichiers, courriers vocaux, réunions programmées, contacts, et analogues), ainsi que toute autre information supplémentaire que la personne concernée est susceptible de fournir en échangeant des communications sans l'intervention de l'expéditeur (p. ex. lorsqu'une personne concernée envoie un message électronique en utilisant un navigateur internet, le moteur d'expédition peut ajouter l'adresse IP du navigateur dans l'un des en-têtes SMTP du message).

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 pour la mise à disposition, l'exploitation, l'assistance et l'entretien de Exchange Online et Outlook.

Les prestataires externes impliqués dans l'assistance, l'exploitation ou l'entretien de Outlook et Exchange Online – y compris, sans pour autant s'y limiter, Microsoft lui-même – sont également susceptibles d'accéder à des données à caractère personnel et de 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 en fonction du « besoin de savoir » aux :

- destinataires d'un seul courrier électronique et/ou d'un seul évènement programmé : potentiellement quiconque ;
- destinataires dans BIT PACE 4615 aux fins d'administration, d'exploitation et d'entretien du système de messagerie électronique ; destinataires dans BIT Security 4623 aux fins de cybersécurité de la messagerie électronique ;
- employés de Microsoft et agents de l'OEB au sein de la Direction principale 4.6 en charge de la mise à disposition, de l'administration, de l'exploitation et de l'entretien du service de messagerie électronique ;
- tout utilisateur de la messagerie électronique de l'OEB (agent ou prestataires), disposant d'un droit d'accès en lecture aux informations du carnet d'adresses d'Outlook de l'OEB.

Au sein de Microsoft 365 (ensemble d'applications comprenant Exchange Online et Outlook), la majorité des opérations de services sont, en principe, automatisées pour 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.

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 l'état de la technique. 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 faisant partie de toute donnée fournie 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 évènements), 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 disposition 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 Exchange Online et Outlook :

- la vérification des habilitations de l'OEB par le biais d'une authentification moderne est exigée afin d'accéder à la boîte de messagerie électronique ;

- l’accès à partir de dispositifs qui ne sont pas associés à un domaine est soumis à une authentification multifacteur (MFA) ;
- authentification et autorisation fondées sur le rôle ; la MFA s’applique pour activer tout rôle ;
- évaluation des accès sur les rôles existants ; historique d’audit.

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 (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 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 externes à l’OEB) ou ce formulaire (pour les personnes concernées 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. Quelle est la base juridique du traitement de vos données à caractère personnel ?

Les données à caractère personnel sont traitées conformément à l’article 5a) RRPD, c. à. d., lorsque « 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 ».

Afin de respecter les exigences relatives à la cybersécurité, les données à caractère personnel sont traitées en vertu de l’instrument juridique suivant : la circulaire nº 382 "Directives relatives à la sécurité de l’information à l'OEB" (article 7 : « Surveillance, contrôles, audits et suite de la procédure »).

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 :

• Les informations relatives aux courriers électroniques et à tout carnet d’adresses personnel établis par l’utilisateur du système de messagerie électronique de l’OEB sont stockées aussi longtemps que l’utilisateur souhaite conserver le message et pendant toute la durée des obligations contractuelles pesant sur l’utilisateur vis-à-vis de l’OEB.
• Les courriers électroniques supprimés volontairement par l’utilisateur sont conservés pendant 90 jours, puis effacés.
• Les informations personnelles comprises dans le carnet d’adresses global et la boîte de messagerie électronique d’un utilisateur sont stockées pendant toute la durée des obligations contractuelles pesant sur

l'utilisateur (p. ex. un agent, un prestataire) vis-à-vis de l'OEB. Une fois que le contrat de l'utilisateur prend fin, les informations sont conservées pendant une durée maximale d'un an et demi (18 mois), aux fins de leur collecte par l'OEB ou de l'éventuel renouvellement du contrat. Suite à l'expiration de cette période, ces informations sont effacées.
• En cas de procédure judiciaire ou d'enquête administrative, nonobstant le fait qu'elles se rapportent à une sanction disciplinaire ou à une condamnation pénale, des données à caractère personnel sont susceptibles d'être conservées au-delà des délais de conservation indiqués ci-dessus. Dans de tels cas, qui font partie des fonctions des personnes agissant en tant que responsables délégués du BIT de la Direction principale 4.6, la conservation des données à caractère personnel fait l'objet d'une décision au cas par cas par le responsable délégué compétent.

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 Outlook et Exchange Online, les extraire et les effacer. Microsoft conservera les données de l'OEB qui demeurent stockées dans les Services en ligne 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 le client 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 stockées dans les Services en ligne 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 versées au dossier 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 du traitement en vertu de l'article 49 RRPD et, si vous n'êtes pas d'accord avec le résultat du réexamen, le droit d'exercer des voies de recours en vertu de l'article 50 RRPD.