Déclaration relative à la protection des données lors de l'archivage de documents du secrétariat du Conseil comprenant des données à caractère personnel

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 du Conseil d'administration (RRPD du CA).

Les informations contenues dans la présente déclaration sont fournies en vertu de l'article 6 RRPD du CA, en liaison avec les articles 16 et 17 du règlement relatif à la protection des données de l'Office européen des brevets (RRPD).

La présente déclaration relative à la protection des données explique comment le secrétariat du Conseil traite les données à caractère personnel en vue de l'archivage d'enregistrements de nature et de portée diverses à des fins administratives, institutionnelles, juridiques et historiques, le cas échéant.

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

Depuis 2010, le secrétariat du Conseil (SC) a – à des fins historiques – exécuté les actions suivantes en vue de l'archivage d'enregistrements de nature et de portée diverses à des fins administratives, institutionnelles, juridiques et historiques. Les données à caractère personnel peuvent être traitées par le secrétariat du Conseil lors de l'archivage de documents du secrétariat du Conseil, pour les motifs suivants :

- indexer, cataloguer, numériser et téléverser tous les documents CA et CA/C dans les bases de données MICADO Documents et MICADO-C dédiées. Il s'agit de dépôts de documents du Conseil gérés par le Secrétariat, tandis que MICADO-C ne contient que les documents confidentiels du Conseil.
- indexer, cataloguer et stocker la correspondance papier des Présidents et délégations.
- indexer, cataloguer et stocker des enregistrements de contentieux confidentiels concernant les décisions prises par le CA en tant qu'autorité investie du pouvoir de nomination. Il s'agit d'enregistrements papier confidentiels portant sur les recours internes et les dossiers disciplinaires.
- indexer, cataloguer et stocker des enregistrements (papier) portant sur l'élaboration, l'approbation et la publication de documents CA.
- stocker des documents administratifs, notamment des fiches de déplacements et des remboursements à l'intention de délégués et d'experts.

Plus important encore, compte tenu du rôle évident du secrétariat du Conseil dans la préservation de la mémoire institutionnelle de l'OEB, le secrétariat du Conseil a conservé toutes les archives papier des documents CA et d'autres fichiers papier ou électroniques pertinents pour l'entreprise depuis la fin des années 1970.

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 transférées vers des destinataires extérieurs à l'OEB s'ils ne sont pas visés à l'article 7 RRPD du CA, 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 données à caractère personnel traitons-nous ?

Les données à caractère personnel suivantes des membres des délégations aux organes du Conseil et des personnes nommées par le Conseil, des personnes internes de l'OEB et, le cas échéant, des personnes extérieures sont traitées :

- pays
- prénom et nom
- adresse professionnelle
- titre
- service et nom de l'Office national des brevets (ONB) de l'agent, le cas échéant
- numéro de téléphone ;
- numéro de téléphone portable (facultatif)
- adresse électronique ou adresse postale
- le cas échéant, le rôle exercé au sein d'un organe du Conseil (par exemple, représentant, suppléant, expert externe participant aux sessions du Conseil) ainsi que les dates de début et de fin de ce rôle
- photo
- nationalité
- préférences linguistiques
- durée d'affectation

3. Qui est responsable du traitement des données ?

Les données à caractère personnel sont traitées sous la responsabilité du chef du secrétariat du Conseil, agissant en qualité de responsable délégué du traitement des données du CA.

Le traitement des données à caractère personnel est réalisé par les membres du personnel du secrétariat du Conseil impliqués dans la gestion de l'initiative, du projet ou de l'activité visés dans la présente déclaration.

Les prestataires externes fournissant la plateforme d'archivage numérique et les services d'archivage externes peuvent également traiter des 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 ?

Des données à caractère personnel sont communiquées selon les besoins au personnel de l'OEB travaillant au sein du secrétariat du Conseil. En outre, les destinataires provenant des différentes unités opérationnelles de l'OEB peuvent accéder aux données à caractère personnel sur demande et sur évaluation de leur 'cas d'affaire.

Plus spécifiquement, tous les agents de l'Office ont accès aux bases de données MICADO Documents et MICADO-U, ainsi qu'aux documents CA et CA/C disponibles.

La direction générale DG5 Services juridiques et le Cabinet du Président peuvent, sur demande et avec l'approbation du chef du secrétariat du Conseil, avoir accès à certaines parties des informations contenues dans d'autres enregistrements qui ne sont pas stockés dans les dépôts MICADO Documents, selon les besoins (par exemple, des informations sur des dossiers de contentieux pour la préparation de la défense juridique).

Les documents administratifs (fiches de déplacement et remboursement aux délégués et experts) sont conservés temporairement à des fins de comptabilité et d'audit et les copies numérisées sont envoyées aux Pensions et services spécifiques à des fins de traitement.

Les bureaux nationaux des États membres peuvent, sur demande et après évaluation et approbation par le chef du secrétariat du Conseil, avoir accès à certaines parties des informations selon les besoins (par exemple, à des fins historiques concernant des documents qui n'étaient pas disponibles sous forme électronique sur MICADO avant 1996).

Les données à caractère personnel peuvent être communiquées à des prestataires de services tiers à des fins de maintenance, d'assistance et d'archivage.

Enfin, le public peut lui aussi demander des documents stockés et y avoir accès, après évaluation du cas d'affaire et en consultation avec Services juridiques et le secrétariat du Conseil. Les données à caractère personnel seront rendues anonymes chaque fois que cela s'avère possible.

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 protégeons-nous et préservons-nous vos données à caractère personnel ?

Nous prenons les mesures techniques et organisationnelles nécessaires pour préserver vos données à caractère personnel et les protéger contre la destruction, la perte ou l'altération accidentelles ou illicites, ainsi que contre toute divulgation non autorisée ou tout accès non autorisé.

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 uniquement aux 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 de l'accès (p. ex., contrôle d'accès à base de rôle aux systèmes et au réseau, principes du "besoin de savoir" et du moindre privilège) ;
- renforcement de la sécurité logique des systèmes, équipements et réseaux
- protection physique : contrôles des accès à l'OEB, contrôles supplémentaires des accès au centre de données, politique de verrouillage des bureaux
- contrôles de la transmission et de la saisie (par ex. journaux d'audit, surveillance des systèmes et du réseau)
- intervention en cas d'incident de sécurité : surveillance 24 heures sur 24 et 7 jours sur 7 en cas d'incident, expert en sécurité de garde.

L'OEB a adopté un système d'administration dématérialisé ; cependant, 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 sûr et verrouillé à accès restreint.

Pour les données à caractère personnel traitées par des systèmes qui ne sont pas hébergés dans les locaux de l'OEB, les prestataires qui traitent ces données se sont engagés dans le cadre d'un accord contraignant à se conformer aux obligations afférentes à la 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. Ces systèmes doivent avoir mis en place des 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 de réseau, des systèmes de détection des intrusions sur le réseau (IDS), des systèmes de protection contre les intrusions sur le réseau (IPS), un audit des connexions) ; des mesures de contrôle de l'acheminement des données (p. ex. sécurisation des données en transit par un chiffrement).

6. Comment pouvez-vous accéder à vos données, les rectifier et les recevoir, en demander l'effacement, limiter leur traitement ou vous opposer à celui-ci ? Vos droits peuvent-ils être restreints ?

Les utilisateurs ont le droit d'accéder à leurs 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 d'en limiter le traitement ou de s'opposer à celui-ci (article 6 RRPD du CA).

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 suivante : DPCouncil@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) ou ce formulaire (pour les pensionnés) 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 de vos données ?

Les données à caractère personnel sont traitées sur le fondement de l'article 4(a) RRPD du CA, qui stipule que le traitement des données à caractère personnel n'est légal que si et dans la mesure où il est nécessaire à l'accomplissement d'une tâche relevant des fonctions officielles du Conseil d'administration ou de toute autre activité confiée en vertu de la Convention sur le brevet européen.

8. Combien de temps conservons-nous vos données ?

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 spécifiquement, les enregistrements sont conservés indéfiniment, si cela est justifié, entre autres :

- à des fins historiques et dans l'intérêt du public (voir l'article 12/2) du règlement intérieur du CA)
- à des fins institutionnelles
- pour des motifs de sécurité juridique

Lorsque ces raisons ne s'appliquent pas ou cessent de s'appliquer, les documents ne sont plus conservés et la durée de conservation est limitée à 15 ans, contre 3 mois pour les documents administratifs et 3 ans pour les documents confidentiels relatifs à des litiges.

En cas de recours/contentieux en cours, toutes les données détenues au moment où le recours formel/contentieux est engagé seront conservées jusqu'à la clôture de la procédure près le Tribunal administratif de l'OIT.

9. Personnes à contacter et coordonnées

Si vous avez des questions concernant le traitement de vos données à caractère personnel, veuillez contacter le responsable délégué du traitement à DPcouncil@epo.org. Vous pouvez également contacter notre responsable de la protection des données à dpo@epo.org.

Les utilisateurs externes sont invités à nous contacter ou à contacter notre responsable de la protection des données 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 11(1) RRPD du CA et, si vous n'êtes pas d'accord avec l'issue de ce réexamen, d'exercer les voies de recours prévues à l'article 12(1) RRPD du CA.