Déclaration relative à la protection des données concernant la gestion du contrôle des accès et des cartes d'accès à l'OEB

L'Office européen des brevets (OEB) attache la plus haute importance à la protection de vos données. Nous nous engageons à respecter et à protéger les données à caractère personnel vous concernant, et à garantir le respect de vos droits en tant que personne concernée par le traitement de ces données. Toutes les données à caractère personnel vous identifiant, directement ou indirectement, seront traitées de manière licite, loyale et avec le plus grand soin.

Le traitement de ces données est régi par le règlement relatif à la protection des données (RRPD).

Les informations figurant dans la présente déclaration sont fournies conformément aux articles 16 et 17 du RRPD.

La présente déclaration porte sur le traitement de données à caractère personnel relatives à la gestion du contrôle des accès et des cartes d'accès à l'OEB. Elle expose la manière dont se déroulent les opérations de traitement.

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

Les données à caractère personnel sont traitées afin de gérer les accès aux différents bâtiments et parkings de l'OEB d'une manière efficiente et efficace.

Le système de gestion des cartes est utilisé pour :

1. gérer les badges permettant aux agents de l'OEB, aux membres de la famille, aux membres du Conseil d'administration, aux conseils en brevets, aux contractants, aux agents pensionnés de l'OEB, aux prestataires de services et aux visiteurs d'accéder aux bâtiments ;
2. vérifier que les visiteurs ne figurent pas dans la liste des personnes dont l'accès est interdit et ont le droit d'entrer dans les locaux de l'OEB avant qu'un badge de visiteur leur soit remis ;

vérifier l'identité des personnes qui reçoivent un badge d'accès à l'OEB au moyen de scanners d'identité automatisés, qui vérifient également en même temps l'authenticité du document d'identité scanné.

Dans le système de contrôle des accès, les données à caractère personnel sont traitées afin de gérer l'accès aux différents bâtiments et parkings de l'OEB d'une manière efficiente et efficace.

Le système de contrôle de l'accès est également utilisé pour s'assurer du respect des dispositions en vigueur (règlement des immeubles et circulaires relatives à la sécurité) ainsi qu'aux fins suivantes :

1.- fournir un accès aux bâtiments de l'OEB aux agents, aux visiteurs et aux contractants, y compris aux prestataires de services ;

2.- enregistrer le journal des accès aux sites pour lesquels une autorisation d'accès a été accordée à des utilisateurs ;

3.- enregistrer de manière automatisée (lors de l'arrivée du véhicule à l'entrée du parking) le numéro de la plaque d'immatriculation du véhicule des agents, des contractants et des visiteurs qui ont accès aux locaux de l'OEB pour :

a) assurer un suivi de l'utilisation du parking et limiter l'intervention des agents administratifs pour l'enregistrement des demandes de parking à long terme ;

b) automatiser la manière dont les agents sont informés lorsqu'ils enfreignent les règles relatives au parking en y laissant leur véhicule plus longtemps qu'il ne leur est permis (p. ex. envoyer des courriels automatiques à des agents qui ne respectent pas les règles concernées) ;

c) gérer d'une manière plus efficace les parkings (un véhicule par agent).

Pour réaliser le troisième objectif, les plaques d'immatriculation des véhicules qui s'approchent de l'entrée du parking sont enregistrées et associées à leur badge d'accès, afin d'identifier le propriétaire du véhicule et de pouvoir assurer le suivi de l'utilisation du parking (un véhicule par personne, une durée de stationnement d'une journée maximum).

4. - Déclencher des alarmes via le Security Management System, y compris les alarmes qui se déclenchent lorsque une porte est ouverte trop longtemps, lorsqu'une porte d'entrée ou une porte annexe est forcée et qu'un badge non-autorisé est utilisé à l'entrée.

2. Quelles données à caractère personnel traitons-nous ?

En ce qui concerne les agents de l'OEB, les employés des contractants, les agents pensionnés de l'OEB, les conseils en brevets et les membres du Conseil d'administration de l'OEB, les catégories suivantes de données à caractère personnel sont traitées : prénom, nom, numéro de badge, numéro du bâtiment, validité de la carte, début et fin du contrat, numéro de téléphone, code d'accès, service, adresse électronique, groupe et sous-groupe d'employés, genre, numéro de badge, langue de communication, site, tarifs pour l'obtention de rabais et informations techniques relatives aux systèmes standard de gestion des cartes.

En ce qui concerne les visiteurs, les données à caractère personnel suivantes sont traitées : prénom, nom, date de naissance et/ou numéro du document d'identité et personne de contact à l'OEB ainsi que la date et l'heure de leur accès aux bâtiments.

En ce qui concerne les membres de la famille des agents de l'OEB (les partenaires et les enfants à charge des agents de l'OEB âgés de plus de 16 ans enregistrés dans FIPS), les données à caractère personnel sont traitées afin de leur fournir un badge familial d'accès aux installations sportives de l'OEB et aux espaces semi-publics si la demande en a été faite via l'interface MyFIPS par l'agent qui les parraine. Figureront sur le badge la photo, le nom complet et la référence à l'agent de l'OEB en lien avec le membre de la famille.

L'ensemble des catégories de données contenues dans un document de voyage (passeport ou carte nationale d'identité) sont traitées mais ne sont pas enregistrées. Elles seront traitées uniquement pendant la vérification de l'identité effectuée au moyen de scanners de documents d'identité et supprimées une fois que le résultat est présenté.

La plaque d'immatriculation des véhicules des agents et des contractants qui ont accès aux parkings de l'OEB ainsi que la date et l'heure de leur accès à ces parkings. Toutes les catégories de données contenues dans le registre des opérations de traitement du système de gestion des cartes (y compris les photos des agents et des contractants afin de contrôler les accès).

Groupes ou personnes concernés :

- ✓ personnel de l'OEB
- ✓ membres de la famille du personnel de l'OEB (âgés de plus de 16 ans)
- ✓ agents pensionnés de l'OEB
- ✓ visiteurs (p. ex. utilisateurs de la cantine, personnes extérieures)
- ✓ employés des contractants
- ✓ personnel de l'agence de Berlin de l'Office allemand des brevets et des marques
- ✓ conseils en brevets

- ✓ membres du Conseil d'administration

3. Qui est responsable du traitement des données ?

Le traitement des données à caractère personnel est réalisé sous la responsabilité de la DG4 - DP 44 - Administration générale (représentée par le chef du service Facility Management sur chaque site de l'OEB) agissant en qualité de responsable délégué du traitement des données à l'OEB.

Les données à caractère personnel sont traitées par les agents de l'OEB participant à la gestion des initiatives, projets et activités au sein des services de sécurité du Facility Management.

Les contractants externes des services de sécurité du Facility Management impliqués dans cette activité peuvent également traiter les données à caractère personnel et accéder à ces dernières.

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 » au personnel de l'OEB travaillant au sein de la DG4 - DP 44 Administration générale et si nécessaire aux gestionnaires de contrats responsables de la gestion des contractants.

Les données à caractère personnel peuvent être communiquées à des prestataires de service tiers à des fins de maintenance ou de soutien.

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.

Si d'autres destinataires (p. ex. la Direction 0.4.4 Éthique et conformité, la police, un expert en sécurité) demandent ces informations, la requête sera présentée individuellement auprès du responsable délégué au traitement qui consultera le responsable de la protection des données.

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

Nous prenons les mesures techniques et organisationnelles appropriées afin de sauvegarder et protéger vos données à caractère personnel de toute destruction, perte, altération accidentelle ou illégale, ainsi que de la divulgation non autorisée ou de l'accès non autorisé à ces dernières.

L'ensemble des données à caractère personnel est enregistré 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 général, les mesures de sécurité de base suivantes s'appliquent au minimum :

- authentification de l'utilisateur et contrôle de l'accès (par ex. contrôle de l'accès aux systèmes et au réseau en fonction du rôle, principes du besoin de savoir et du moindre privilège) ;
- renforcement logique de la sécurité des systèmes, équipements et réseaux ;
- protection physique : contrôle des accès à l'OEB, contrôles d'accès supplémentaires au centre de données, politiques relatives à la fermeture 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 des incidents 24 heures sur 24 et 7 jours sur 7, expert en sécurité de garde.

L'accès aux données enregistrées dans les journaux de contrôle des accès est limité aux administrateurs de l'application. Les données ne seront accessibles que sur requête et avec l'autorisation du responsable du

traitement après avis favorable du responsable de la protection des données, sauf dans une situation d'urgence auquel cas le responsable de la protection des données en sera informé. Les autres utilisateurs qui peuvent consulter ces données comme le prestataire externe de sécurité auront uniquement accès aux données stockées afin d'enregistrer l'accès aux locaux de l'OEB.

L'accès à l'application et aux données enregistrées dans celle-ci est limité selon le principe du "besoin de savoir". Les administrateurs de la sécurité à l'OEB ont accès aux historiques enregistrés afin de s'assurer du respect des règles et le prestataire externe de sécurité a un accès limité pour gérer l'application.

L'accès à l'application nécessite une authentification via les outils BIT (mot de passe/active directory) ainsi qu'un mot de passe supplémentaire pour l'application. Pour les données à caractère personnel traitées par des prestataires externes, ces sociétés se sont engagées dans le cadre d'un accord contraignant à respecter leurs obligations en matière de protection des données découlant du cadre juridique de la protection des données applicable.

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 vertu des articles 18 à 24 du règlement relatif à la protection des données de l'OEB, vous avez le droit d'accéder aux données à caractère personnel vous concernant, de les rectifier, d'en demander l'effacement et de les recevoir, ainsi que de limiter leur traitement ou de vous y opposer.

Si vous souhaitez exercer l'un de ces droits, veuillez adresser une demande écrite en ce sens à DPOexternalusers@epo.org si vous êtes une personne de l'extérieur, ou au responsable délégué du traitement, à l'adresse suivante : DPL.PD44@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 de l'extérieur) ou ce formulaire (pour les personnes en interne) 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 prorogé de deux mois si nécessaire, compte tenu de la complexité des demandes reçues et de leur nombre. Toute prorogation 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 qui dispose que *« 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 ».* (Garantir que les bâtiments sont sûrs)

Les données à caractère personnel sont recueillies et traitées conformément à l'instrument juridique suivant :

Les tâches attribuées à l'OEB (Circulaire n°380, art. 2. e) : Le personnel de sécurité veille à ce que le présent règlement des immeubles soit respecté, à ce que l'exercice des activités de l'OEB ne soit pas entravé et à ce que les dispositions et règlements en vigueur soient appliqués. Le personnel de sécurité est autorisé à donner des ordres et à prendre toutes les mesures nécessaires à cet effet. Il peut notamment effectuer des contrôles d'identité et de sécurité.

Les motifs exposés ci-dessus sont considérés comme étant un moyen ciblé et proportionné de garantir la sécurité des personnes qui se rendent au travail, lorsque les agents de sécurité doivent fournir une réponse adaptée dans les situations d'urgence et maintenir le niveau approprié de sécurité des informations et des

biens à l'OEB, en utilisant à cette fin les systèmes de sûreté et de sécurité de sorte que les réponses en cas d'urgence soient efficaces.

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 à la finalité de leur traitement.

En ce qui concerne le système de contrôle des accès (ACS), les journaux d'accès de plus de 12 mois seront écrasés par un programme automatisé intégré dans le logiciel.

Les données relatives aux visiteurs seront conservées pendant 28 jours comme les enregistrements de vidéosurveillance et à des fins de sécurité. Cela permettra aux agents de sécurité d'effectuer des enquêtes de soutien sur l'accès des visiteurs si une infraction pénale a été rapportée.

Concernant le système de gestion des cartes (CMS), les données provenant de FIPS seront stockées et supprimées en fonction des délais de conservation fixés par FIPS (les données d'utilisateur relatives à un agent ou à un contractant seront supprimées après leur suppression dans FIPS).

Pour les groupes comme le Conseil d'administration ou les conseils en brevets ajoutés manuellement par le gestionnaire des données, ce dernier effectuera, au moins une fois par an ou dès qu'il sera informé d'un changement, un contrôle de conformité. À cette occasion, le gestionnaire des données vérifiera que les données sont toujours valides et exactes, effectuera les modifications et/ou les suppressions nécessaires pour garder les données à jour.

Dans le cas d'un recours formel/de litige, l'ensemble des données détenues à la date du recours formel/du litige doit être conservé jusqu'à ce que la procédure soit achevée.

9. Personnes à contacter et coordonnées

Les utilisateurs externes ayant des questions sur le traitement des données les concernant, peuvent s'adresser au responsable de la protection des données et/ou au responsable délégué du traitement à l'adresse : DPOexternalusers@epo.org. Les agents de l'OEB peuvent contacter le responsable délégué du traitement à l'adresse DPL.PD44@epo.org.

Vous pouvez également contacter notre responsable de la protection des données à l'adresse 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 du réexamen, le droit d'exercer les voies de recours prévues à l'article 50 RRPD.