

## **Déclaration relative à la protection des données concernant le traitement des données à caractère personnel dans le système de gestion des identités et des accès clients (CIAM) d'Okta**

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 en vertu des articles 16 et 17 RRPD. La présente déclaration relative à la protection des données porte sur le traitement des données à caractère personnel au sein d'Okta. L'OEB utilise la plate-forme logicielle en tant que service (SaaS, Software-as-a Service) d'Okta infonuagique pour la gestion des identités et des accès.

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

Le traitement implique l'authentification des utilisateurs via Okta. L'authentification est requise à chaque tentative de connexion à une zone sécurisée des services en ligne de l'OEB qui est accessible au moyen d'une carte à puce ou d'identifiants de compte obtenus pour utiliser ces services.

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

Vos données à caractère personnel ne seront pas transférées en dehors de l'OEB à des destinataires qui ne sont pas visés à l'article 8 (1), (2) et (5), à moins qu'un niveau de protection adéquat soit garanti. En l'absence d'un niveau de protection adéquat, un transfert ne peut avoir lieu que si des garanties appropriées ont été mises en place et à la condition que les personnes concernées disposent de droits opposables et de voies de recours effectives.

### **2. Quelles données à caractère personnel traitons-nous ?**

Les catégories suivantes de données à caractère personnel des personnes concernées sont traitées :

- nom et prénom ;
- numéro de carte à puce ;
- langue préférée ;
- adresse de messagerie électronique ;
- nom d'utilisateur ;
- mot de passe ;
- numéro de téléphone ;
- données de connexion/localisation

### **3. Qui est responsable du traitement des données ?**

Le traitement des données à caractère personnel est réalisé sous la responsabilité du Chief Information Officer de l'OEB, qui est membre de la structure Business Information Technology (BIT) et agit en qualité de responsable délégué du traitement des données à l'OEB.

#### **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 » du personnel de l'OEB (administrateurs du système) du département de Sécurité de l'information 4.6.2.3 et de certains agents de l'OEB de la DG 1 à des fins de soutien à la clientèle. Elles sont également communiquées en fonction du « besoin de savoir » du personnel d'Okta à des fins de maintenance et d'assistance. 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 sauvegardons-nous vos données à caractère personnel ?**

Nous adoptons des mesures techniques, de sécurité informatique 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.

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 :

- authentification de l'utilisateur et contrôle de l'accès (p.ex. contrôle d'accès à base de rôles aux systèmes et au réseau, principe du « besoin de savoir » et du moindre privilège) ;
- renforcement de la sécurité logicielle des systèmes, équipements et réseaux ;
- protection physique : contrôle des accès effectués à l'OEB, contrôles supplémentaires des accès aux centres de données, politique de verrouillage des bureaux ;
- contrôles des transmissions et entrées (p.ex. audit des connexions, surveillance des systèmes et réseaux) ;
- interventions en cas d'incident de sécurité : surveillance des incidents 24 heures sur 24 et 7 jours sur 7, experts en sécurité de garde.

Pour les données à caractère personnel traitées par des systèmes qui ne sont pas hébergés dans les locaux de l'OEB, Okta s'est engagée 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 risques de sécurité.

Okta ne transférera pas de données à caractère personnel vers des pays ne présentant pas un niveau adéquat de protection des données à caractère personnel.

Okta a mis en place des mesures administratives, physiques et techniques visant à protéger la sécurité, la confidentialité et l'intégrité tant des données de clients que des données à caractère personnel. Ces mesures de protection sont décrites dans les documents de gouvernance et de conformité.

Okta a obtenu la certification [PRP \(Privacy Recognition for Processors\) du forum de coopération économique pour l'Asie-Pacifique](#) (APEC) et traite les données à caractère personnel en conséquence.

#### **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 ou de vous opposer à celui-ci (article 18 à 24 RRPD).

Conformément au RRPD, les limitations des droits des personnes concernées se fondant sur l'article 25(1)c), g) et h) RRPD et la [circulaire n°420](#) mettant en œuvre l'article 25 RRPD, peuvent être appliquées en cas d'enquêtes ou d'audits menés par le responsable de la protection des données en vertu de l'article 43(1)d) et (2) RRPD.

Si vous souhaitez exercer l'un de ces droits, veuillez adresser une demande écrite en ce sens au [responsable délégué du traitement](#), BIT, à l'adresse suivante : [DPOexternalusers@epo.org](mailto: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](#) 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 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 ».

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

Les données à caractère personnel traitées par le responsable délégué du traitement des données ou les prestataires de services sont conservées uniquement pendant une durée n'excédant pas celle nécessaire au regard de la finalité de leur traitement.

Les données à caractère personnel seront conservées pour la durée du contrat en vigueur avec Okta.

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 de vos données à caractère personnel, veuillez les adresser au responsable délégué du traitement à l'adresse suivante : [DPOexternalusers@epo.org](mailto:DPOexternalusers@epo.org).

Vous pouvez également contacter notre responsable de la protection des données à l'adresse suivante : [DPOexternalusers@epo.org](mailto: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.