Déclaration relative à la protection des données concernant le traitement de données à caractère personnel dans le cadre d'activités d'enquête

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 de l'OEB (RRPD).

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 de données à caractère personnel suite à des allégations de faute à l'encontre des membres du personnel de l'OEB signalées à l'unité chargée des enquêtes de l'OEB, à l'exception des aspects concernant les processus du FRPSS, comme détaillé dans le code de conduite pour les FRPSS et les activités connexes, pour lesquels une déclaration relative à la protection des données distincte s'applique.

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

La présente déclaration relative à la protection des données explique la manière dont le traitement des données à caractère personnel, obtenues dans le cadre des procédures menées par l'unité chargée des enquêtes, est réalisé par les agents de la direction Éthique et conformité et par toute personne dûment habilitée.

Les données à caractère personnel sont traitées pour permettre aux membres de l'unité chargée des enquêtes de remplir leur fonction, qui consiste à détecter et prévenir les fautes commises par des agents de l'OEB, ainsi qu'à enquêter sur de telles allégations. Pour plus d'informations sur la finalité, veuillez consulter la Charte de l'Audit interne et des standards professionnels.

Dans le cadre des activités de l'unité chargée de l'enquête, ses membres prennent des mesures visant à recueillir des informations factuelles, y compris des entretiens et l'examen des documents, et rendent compte directement à l'autorité investie du pouvoir de nomination pour que celle-ci puisse déterminer si les agents se conforment à leurs obligations déontologiques, en vertu du statut des fonctionnaires et des autres agents de l'Office européen des brevets, et décider s'il y a lieu d'engager des procédures disciplinaires. Cela déclenche le traitement inévitable des données à caractère personnel des personnes qui soumettent une allégation de faute et de toute partie à la procédure d'enquête, notamment toutes les catégories d'agents, de plaignants (internes ou non) ou de prestataires de service externes en tant que personne mise en cause et observateur, ainsi que tout

témoin concerné. Les données à caractère personnel des agents de la direction Éthique et conformité et des enquêteurs extérieurs peuvent également faire l'objet d'un traitement, par exemple les données d'identification des enquêteurs assignés, ainsi que les données relatives à une déclaration de conflit d'intérêts.

Le traitement des données à caractère personnel est spécifiquement nécessaire pour :

- consigner et enregistrer les affaires, et tenir à jour les dossiers ;
- conduire des activités d'enquête, y compris des entretiens et toutes les étapes des procédures d'enquête ;
- enregistrer des activités et rapports d'enquête ;
- soumettre des rapports d'enquête à l'autorité investie du pouvoir de nomination ;
- transférer des affaires à d'autres unités ou aux instances nationales ;
- informer des parties à une procédure d'enquête du résultat de cette procédure ;
- satisfaire aux obligations légales qui s'imposent à l'OEB ;
- gérer et suivre des procédures d'enquête, y compris pour l'élaboration de statistiques ou de rapports anonymes (c'est-à-dire le Collège des commissaires aux comptes) ;
- élaborer des statistiques ou des rapports anonymes

Le traitement de vos données n'est pas censé servir à une prise de décision automatisée, notamment au profilage.

Certaines activités peuvent tirer profit de la puissance de l'intelligence artificielle (IA) dans leurs applications afin d'en améliorer l'efficacité. Plus précisément, nous sommes susceptibles d'utiliser Microsoft Teams pour enregistrer des entretiens en ligne et produire des transcriptions de ces entretiens. Le déploiement et l'utilisation de l'IA dans le cadre de ces activités de traitement respectent les exigences strictes du traitement de données à caractère personnel. Le traitement n'est pas censé servir à une prise de décision individuelle automatisée.

2. Quelles données à caractère personnel traitons-nous ?

Les catégories suivantes de données à caractère personnel sont traitées :

- **données d'identification** (p. ex. nom) ;
- **coordonnées** (p. ex. adresse électronique, numéro de téléphone) ;
- **données relatives à l'emploi** (p. ex. parcours professionnel, congés, missions, informations relatives à la rémunération, performances, sanctions disciplinaires et informations relatives au règlement de litiges) ;
- **données relatives au rôle dans l'affaire** (p. ex. plaignant, témoin, personne mise en cause, observateur) ;
- **données techniques** (p. ex. utilisation de systèmes informatiques ou d'appareils de télécommunication de l'OEB) ;
- **données relevant du domaine privé** (p. ex. activités extérieures) ;
- **preuves produites** pour étayer une allégation ;
- **données contenues dans les documents** relatifs au problème faisant l'objet d'une enquête ;
- **enregistrements audio** d'entretiens (le cas échéant) ;
- **catégories particulières de données à caractère personnel**, notamment les données sensibles telles que définies à l'article 11(1) RRPD, ou les données à caractère personnel relatives à des condamnations pénales et à des infractions, en vertu de l'article 12 RRPD, lorsqu'elles présentent un intérêt ou constituent un élément important pour l'affaire ou la procédure d'enquête (p. ex. fraude en matière de soins de santé, discrimination ou infractions

pénales).

Les données à caractère personnel peuvent être collectées par tout moyen prévu dans le statut et les règlements d'application. Cela comprend l'accès aux documents et informations pertinents, sous forme physique ou numérique, détenus par l'OEB, ainsi qu'aux locaux de l'OEB, et les informations orales obtenues grâce à des entretiens enregistrés, ainsi que des informations et des communications de tiers, comme des communications entre des individus et Cigna, y compris des informations médicales, en cas de suspicion de fraude.

Des personnes externes, des agents ou anciens agents de l'OEB, des personnes et des entités qui travaillent pour l'OEB ou accomplissent un travail pour son compte, des sources anonymes ou confidentielles, ainsi que des informations accessibles au public peuvent constituer des sources d'information. Si, au cours d'une enquête, la direction Éthique et conformité entre en possession de données à caractère personnel qui ne sont pas pertinentes pour la procédure d'enquête, telles que des données divulguées dans des déclarations, ces données seront enregistrées pour préserver l'intégrité de la déclaration mais ne feront pas l'objet d'un traitement ultérieur. De même, les données à caractère personnel contenues dans des documents utilisés comme moyens de preuve non pertinents ou sans lien avec la procédure d'enquête ne feront pas l'objet d'un traitement ultérieur.

3. Qui est responsable du traitement des données ?

Les données à caractère personnel sont traitées sous la responsabilité de l'agent de la direction Éthique et conformité nommé chef des enquêtes par le directeur principal de la direction Audit interne et standards professionnels, DP 0.4, agissant en qualité de responsable délégué du traitement à l'OEB dans le cadre du mandat d'enquête de la direction Éthique et conformité.

Le traitement des données à caractère personnel est réalisé par les agents de la direction Éthique et conformité participant à la conduite et à la gestion des activités d'enquête, ainsi que par les membres du personnel dûment désignés.

Les membres du personnel assurant la maintenance des systèmes informatiques et fournissant un support technique peuvent également traiter des données à caractère personnel dans le cadre de l'exercice de leurs fonctions, avec un accès limité.

Les prestataires de service externes ou les personnes à qui des activités d'enquête sont confiées peuvent également traiter des données à caractère personnel ou y avoir accès. Les données à caractère personnel sont partagées avec ces prestataires de service externes ou d'autres personnes conformément aux accords sur le traitement des données ou aux dispositions de protection intégrées dans les contrats en vigueur entre eux et l'OEB. À titre d'exemple, les enregistrements audio des entretiens sont transcrits par un service externe des transcriptions. Les fichiers audio sont partagés par les agents de la direction Éthique et conformité, via une application dédiée et sécurisée, et leur sont retournés de la même manière. Aucune autre donnée n'est partagée avec eux. Une fois terminée, la transcription est incluse dans le dossier et le service des transcriptions est chargé d'effacer les données du système concerné, habituellement dans un délai d'un mois après réception.

Concernant les décisions de renvoi devant une instance nationale et les demandes correspondantes de ces autorités qui peuvent inclure des données à caractère personnel, le traitement de ces données est réalisé sous la responsabilité du Président de l'Office.

4. Qui a accès à vos données à caractère personnel et à qui sont-elles communiquées ?

Selon la Charte de l'Audit interne et des standards professionnels : "Les agents de la direction principale Audit interne et standards professionnels [...] ne divulguent ces informations qu'avec les autorisations requises, à moins qu'une obligation légale ou professionnelle ne les oblige à le faire." Par conséquent :

Les agents de la direction Éthique et conformité sont tenus par le principe de stricte confidentialité,

article 4(1) du règlement d'application.

Les données à caractère personnel obtenues et traitées dans le cadre d'une procédure d'enquête ne peuvent être consultées que selon le principe du "besoin de savoir" par les agents participant aux activités d'enquête, par toute personne dûment désignée par le responsable délégué du traitement dans le cadre de la procédure d'enquête et, uniquement dans la mesure nécessaire à la fourniture d'un soutien technique en rapport avec l'exploitation ou la maintenance des outils informatiques utilisés pour la gestion des dossiers d'enquête pour lesquelles ils sont engagés, par du personnel et des contractants externes fournissant un soutien technique à l'OEB.

Les données ne seront divulguées qu'en cas d'obligation juridique ou professionnelle. Lorsqu'elle sera obligatoire, la divulgation se fera selon les principes de nécessité et de minimisation des données : les données ne seront divulguées que selon le principe du besoin de savoir aux destinataires habilités, et le niveau de détail se limitera aux données nécessaires au destinataire pour exécuter ses tâches. Dans la mesure du possible, les données sont partagées de manière anonyme ou minimisées afin d'éviter ou de limiter l'identification des personnes concernées. Dans les circonstances décrites, le risque d'identification d'une personne persiste tout de même.

Plus précisément, la divulgation des données à caractère personnel est accordée aux catégories de personnes suivantes :

- **Les membres du personnel de la direction Éthique et conformité** participant aux activités d'enquête, dans le but de conduire, de gérer et de documenter les enquêtes conformément à leur mandat.
- **Des personnes dûment désignées par le responsable délégué du traitement**, dans le cadre de la procédure d'enquête au titre d'une délégation officielle, pour l'exécution de fonctions de support clairement définies.
- **L'autorité investie du pouvoir de nomination**, dans le but de recevoir des constatations, des recommandations et des conclusions résultant de procédures d'enquête afin de prendre les décisions administratives appropriées.
- Les agents de l'OEB ou les personnes qui sont **parties à l'enquête** (p. ex. témoins, personnes mises en cause, observateurs) conformément aux principes d'équité et de transparence et pour permettre la participation à la procédure d'enquête.
- Les agents de l'OEB ou **les personnes dont le concours est demandé dans le cadre des activités d'enquête** (p. ex. personnel de surveillance physique, services techniques, sécurité de l'information, ressources humaines), lorsque leur participation est nécessaire pour permettre le bon déroulement de l'enquête.
- **Les prestataires de service externes ou les experts auxquels sont officiellement confiées des activités d'enquête** (p. ex. administrateur en soins de santé, fournisseur de transcriptions, enquêteur extérieur), uniquement pour l'exécution de tâches dans le cadre défini de leur mission.
- **Les agents de l'OEB fournissant des conseils juridiques ou des avis sur un sujet donné** (p. ex. conseillers juridiques concernant le droit applicable aux agents et à la protection des données), afin de s'assurer que les enquêtes sont menées conformément aux cadres juridiques applicables.
- **Les agents de l'OEB chargés d'assurer la liaison avec les instances nationales,** lorsque la communication avec ces instances est requise dans le cadre de l'enquête.
- **Les agents ou les services de l'OEB qui reçoivent des affaires transférées par la direction Éthique et conformité en vue d'actions de suivi** (p. ex. ressources humaines) dans le but de mettre en œuvre des mesures administratives, des mesures correctives ou de soutien résultant de l'enquête.

- **Les organes de l'OEB ou les personnes participant à des procédures disciplinaires ou judiciaires connexes** (p. ex. membres de la commission de discipline, de la commission de recours ou du Tribunal administratif de l'OIT), dans la mesure nécessaire pour permettre de telles procédures.
- **Les instances nationales compétentes non membres de l'OEB** (p. ex. les forces de l'ordre), si l'affaire implique une potentielle infraction pénale ou nécessite l'assistance des instances nationales eu égard à la nature des allégations et aux intérêts des parties ou de l'Office. Dans de tels cas, et sur décision du Président de l'Office, la direction Éthique et conformité peut transmettre ses conclusions, des pièces justificatives et d'autres informations pertinentes, en se limitant strictement à ce qui est nécessaire pour permettre à l'instance nationale d'exercer ses prérogatives.
- **D'autres organisations internationales non membres de l'OEB**, en particulier dans le contexte des enquêtes portant sur la fraude ou le détournement de prestations, telles que la vérification des indemnités accordées aux conjoints et conjointes dans les cas impliquant un emploi dans plus d'une institution internationale.

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 tout destinataire non autorisé.

5. Comment protégeons-nous et préservons-nous vos données ?

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.

Les données à caractère personnel sont conservées 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 rôles aux systèmes et au réseau, principe du "besoin de savoir" et du moindre privilège) ;
- renforcement de la sécurité logique des systèmes, de l'équipement et du réseau ;
- 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, gestion des droits relatifs à l'information) ;
- intervention en cas d'incident de sécurité : surveillance des incidents 24 heures sur 24 et 7 jours sur 7, experts en sécurité de garde ;

En principe l'OEB a adopté une **politique de gestion des affaires dématérialisée.** Cependant, si des dossiers papier contenant des données à caractère personnel doivent être stockés dans les locaux de l'OEB, ces dossiers sont conservés en toute sécurité **dans des pièces verrouillées et des armoires à serrure à combinaison** dans les locaux de l'OEB **à La Haye.** L'accès à ce type de stockage est strictement limité.

Concernant 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).

Des garanties supplémentaires ont été mises en place pour protéger davantage les données à caractère personnel au cours des entretiens d'enquête menés à distance :

- **Les outils de visioconférence** tels que Zoom ou Microsoft Teams peuvent être utilisés pour enregistrer des entretiens étant entendu que de strictes directives concernant l'usage interne sont appliquées pour limiter la durée au cours de laquelle les enregistrements et les transcriptions ne sont pas protégés dans l'espace SharePoint de la direction Éthique et conformité.
- **TechSmith Camtasia** est utilisé pour réaliser **des enregistrements uniquement audio** qui sont enregistrés directement
  sur le bureau local de l'enquêteur.
- **Les fonctionnalités de partage basées sur Internet sur Camtasia sont désactivées** pendant le processus d'enregistrement.
- Une fois le fichier audio ajouté au dossier, il est **supprimé de l'application d'enregistrement** pour empêcher la duplication ou la conservation non autorisée.

En outre, lorsque des données à caractère personnel doivent être partagées avec des destinataires externes (par ex., instances nationales), **des mesures de contrôle de la transmission** sont appliquées pour assurer la sécurité des données en transit. Il peut s'agir :

- **du chiffrement** des fichiers numériques ;
- **de services de messagerie sécurisés** ou de **l'envoi recommandé** ;
- **de la remise en main propre** des supports physiques, si nécessaire ;
- **de l'utilisation de transmissions numériques sécurisées (transmission par EPOSafe par exemple).**

Toutes les procédures de sécurité et de transmission sont conçues pour respecter le principe de minimisation des données et sont régulièrement révisées pour les adapter aux nouvelles menaces de sécurité et exigences réglementaires.

Les données à caractère personnel ne seront pas transférées en dehors de l'OEB à des destinataires qui ne sont pas visés par l'article 8(1), (2) et (5) RRPD, 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.

La direction Éthique et conformité applique la gestion des droits relatifs à l'information à toutes les données qu'elle détient et qui sont inactives, en particulier concernant les enquêtes et les incidents

clos.

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

Conformément aux articles 18 à 24 RRPD, 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 d'en limiter le traitement ou de vous opposer à celui-ci.

Veuillez noter que le RRPD limite toutefois ces droits :

Le droit de rectification (article 19 RRPD) ne s'applique qu'aux données factuelles traitées dans le cadre de la procédure d'enquête. Il ne s'applique qu'aux données objectives et factuelles inexactes ou incomplètes, telles que le nom, la date de naissance et l'adresse. Il ne s'applique pas aux déclarations subjectives, notamment aux opinions ou évaluations de tiers. Cela ne vous empêche pas, toutefois, de compléter votre déclaration en y ajoutant des clarifications ou des observations. Les personnes interrogées dans le cadre d'entretiens peuvent également demander, à tout moment de la procédure d'enquête, l'accès à l'enregistrement audio de leur entretien.

De plus, les droits des personnes concernées à demander la limitation du traitement des données ou à s'y opposer (au titre, respectivement, des articles 21 et 23 RRPD) ne sont pas équivalents au droit de garder le silence afin de ne pas s'incriminer ou incriminer un proche (article 21a [6] du statut des fonctionnaires).

Les droits de la personne concernée conférés par les RRPD ne s'étendent pas aux personnes qui sont simplement mentionnées dans le cadre de la collecte de preuves (réclamations, témoignages, entretiens ou documents), mais ne sont pas concernées par la procédure d'enquête.

Il est également important de souligner que les droits en matière de protection des données ne sont pas absolus et doivent être mis en balance avec d'autres droits et libertés fondamentaux. Cela signifie que, dans certaines circonstances, un ou plusieurs droits peuvent être refusés. En outre, en vertu de l'article 25 RRPD et de la circulaire n° 420, des droits peuvent être temporairement restreints pour des motifs légitimes, par exemple lorsque la transparence compromettrait le but de la procédure d'enquête, affecterait les droits et libertés d'autrui ou saperait l'environnement de travail. La circulaire prévoit que toute restriction de ce type sera limitée dans le temps et proportionnée, qu'elle respectera l'essence des droits de la personne concernée et sera dûment enregistrée par la direction Éthique et conformité. Nous vous informerons individuellement dès que possible, à moins que cela ne compromette la finalité de la restriction. Vous trouverez de plus amples informations à ce sujet ici.

Si vous souhaitez exercer l'un de ces droits, veuillez contacter le responsable délégué du traitement à l'adresse
DDEC-DPL@epo.org et lui envoyer une demande détaillée. Afin de faciliter le traitement de votre demande, nous vous encourageons à remplir le formulaire approprié (pour les personnes externes), ce formulaire (pour les personnes internes) ou ce formulaire (pour les pensionnés) et à le transmettre avec votre demande.
Nous vous répondrons 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 5(a) RRPD, selon lequel "ce 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."

Si des catégories spéciales de données à caractère personnel sont traitées, les fondements juridiques applicables sont l'article 5(a) RRPD, en liaison avec les articles 11(2) et 12 RRPD.

Les données à caractère personnel sont collectées et traitées conformément aux dispositions juridiques suivantes afin d'assurer la conformité avec les obligations de conduite et l'obligation de rendre des comptes et afin de prévenir, de détecter et de traiter les fautes : les articles 21 et 21bis(1) du statut, le règlement d'application y afférent, la circulaire n° 341 et l'article 20 du Protocole sur les privilèges et immunités.

L'article 5b) RRPD permet au personnel participant à la procédure d'enquête de se réserver le droit de partager toute information indiquant une activité illégale ou un risque de dommages graves avec les autorités appropriées.

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 et en fonction de l'issue de la procédure d'enquête.

Les données contenues dans les documents concernant le problème présenté seront conservées pendant toute la durée de l'affaire par l'unité chargée des enquêtes et traitées uniquement dans la mesure nécessaire au regard de la finalité de l'opération de traitement comme indiqué ci-dessus. Si les documents comprennent des données inutiles pour résoudre le problème, le traitement de ces données cessera.

Pour des durées de conservation spécifiques, veuillez consulter l'article 21 du règlement d'application ci-dessous :
"

(1) L'unité chargée des enquêtes conserve les dossiers complets afférents :
   i) aux examens initiaux et évaluations préliminaires, pendant trois ans à compter de la conclusion de l'étape respective de la procédure d'enquête lorsque ces examens initiaux et évaluations préliminaires ne débouchent pas sur une enquête ;
   ii) aux enquêtes, pendant sept ans à compter de la conclusion de l'enquête.

(2) L'Office conserve les rapports concluant qu'une faute a été commise, pendant dix ans à compter de leur soumission.

(3) L'Office conserve cette documentation au-delà des périodes spécifiées aux paragraphes 1 et 2 si :

i) l'affaire fait l'objet d'un litige ; ou
ii) on peut raisonnablement supposer que l'affaire fera l'objet d'un litige."

Après l'expiration de la durée de conservation applicable, toutes les données seront supprimées de manière irréversible.

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 l'adresse DDEC-DPL@epo.org

Vous pouvez également contacter notre responsable de la protection des données à l'adresse dpo@epo.org ou, si vous êtes une personne externe, à l'adresse 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 l'issue de ce réexamen, d'exercer les voies de recours prévues à l'article 50 RRPD.