Bureau de la protection des données

# Présentation du référentiel d'adéquation de l'OEB

# Introduction

Conformément à l'article 9(2) du règlement relatif à la protection des données de l'OEB (RRPD de l'OEB), les transferts de données vers un pays ou une organisation internationale ne doivent avoir lieu que si un niveau de protection adéquat est assuré dans le pays du destinataire, dans un territoire ou un ou plusieurs secteurs déterminés de ce pays, ou au sein de l'organisation internationale en question.

La notion de "niveau de protection adéquat" se rapporte au niveau de protection des données à caractère personnel offert dans le pays tiers ou au sein de l'organisation internationale. Cette analyse porte sur le contenu des règles applicables[1] et sur les moyens pour assurer leur application effective.

La finalité des décisions d'adéquation du Président de l'Office européen des brevets (OEB) est de confirmer de manière officielle que le niveau de protection des données à caractère personnel offert par le pays d'un destinataire ou une organisation internationale peut être considéré comme étant substantiellement équivalent à celui offert à l'OEB.[2]

Le présent document définit dans les grandes lignes les éléments fondamentaux d'un cadre de protection des données et les mécanismes de procédure et de mise en œuvre qui doivent être évalués afin de déterminer si la protection offerte par le pays du destinataire[3] ou par une organisation internationale peut être considérée adéquate du point de vue de la protection des données.

# Référentiel d'adéquation

Le cadre de protection des données en place dans un pays ou au sein d'une organisation internationale doit inclure les principes fondamentaux de protection des données et les mécanismes de procédure et de mise en œuvre suivants.

## 1. Principes, droits et garanties

1.1. **Les notions et/ou principes clés de protection des données**. Bien qu'ils ne soient pas identiques, ces principes et notions doivent être conformes à ceux inscrits dans le cadre de protection des données de l'OEB.[4]

---

[1] Notamment l'évaluation du cadre légal permettant l'accès aux données à caractère personnel par les autorités publiques.

[2] La notion de "niveau de protection adéquat" a été introduite pour la première fois dans le droit européen par la Directive 95/46 puis a été développée par la CJUE, qui veut, notamment, que si le "niveau de protection" offert par un pays tiers ou une organisation internationale doit être "substantiellement équivalent" à celui garanti au sein de l'UE, "les moyens auxquels ce pays tiers a recours, à cet égard, pour assurer un tel niveau de protection peuvent être différents de ceux mis en œuvre au sein de [l'UE]" (voir affaire C-362/14, Maximillian Schrems c/ Data Protection Commissioner, 6 octobre 2015, paragraphes 73, 74). Bien que le droit de l'UE ne s'applique pas à l'OEB, les notions de "niveau de protection adéquat" et de "substantiellement équivalent" ont été adoptées dans le cadre de la protection des données au sein de l'OEB.

[3] Il faut entendre par "pays du destinataire" les pays tiers au sens de l'article 3u. et les pays de destinataires qui ne sont pas visés à l'article 8(1), (2) et (5) RRPD de l'OEB.

[4] À titre d'exemple, le RRPD de l'OEB contient les notions importantes suivantes : "données à caractère personnel", "traitement de données à caractère personnel", "responsable du traitement", "responsable du traitement des données", "destinataire" et "catégories particulières de données à caractère personnel".

1.2. **Motifs pour un traitement licite et équitable au regard de finalités légitimes.** Les données à caractère personnel doivent être traitées de manière licite, loyale et légitime, et les bases juridiques doivent être énoncées de manière suffisamment claire.

1.3. **Le principe de la limitation des finalités**. Les données à caractère personnel doivent être traitées à des fins spécifiques et n'être utilisées ultérieurement que dans la mesure où cela n'est pas incompatible avec la finalité du traitement.

1.4. **Les principes d'exactitude et de minimisation des données**. Les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour. Les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées.

1.5. **Principe de la limitation de la conservation**. En général, les données à caractère personnel doivent être conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles les données à caractère personnel sont traitées.

1.6. **Principes d'intégrité et de confidentialité**. Les données à caractère personnel doivent être traitées de façon à garantir leur sécurité. Cela comprend des mesures techniques et organisationnelles appropriées et la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle.

1.7. **Le principe de transparence**. Les personnes concernées doivent être informées de tous les éléments principaux du traitement de leurs données à caractère personnel sous une forme claire, aisément accessible, concise, transparente et compréhensible.

1.8. **Les droits d'accès, de rectification, à l'effacement et d'opposition.**

- Les personnes concernées doivent pouvoir obtenir la confirmation que le traitement de données les concernant a lieu ou non. Elles doivent aussi pouvoir accéder à leurs données, notamment obtenir une copie de toutes les données les concernant qui sont traitées.

- Les personnes concernées doivent pouvoir obtenir la rectification de leurs données le cas échéant, pour des motifs déterminés, par exemple, lorsqu'il apparaît que les données les concernant sont inexactes ou incomplètes. Les personnes concernées doivent aussi pouvoir obtenir l'effacement des données à caractère personnel les concernant, par exemple lorsque leur traitement est devenu inutile ou illicite.

- Les personnes concernées doivent également pouvoir s'opposer, à tout moment, au traitement de leurs données dans des conditions spécifiques définies dans le cadre juridique du pays ou de l'organisation internationale, pour des motifs tenant à leur situation particulière. Conformément au RRPD de l'OEB, par exemple, les personnes concernées ont le droit de s'opposer au traitement des données à caractère personnel les concernant en vertu de l'article 5a. 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".

En outre, l'exercice de ces droits ne doit pas être excessivement laborieux pour les personnes concernées et des limitations peuvent éventuellement être appliquées à ces droits.

1.9. **Catégories spéciales de données à caractère personnel**. Des garanties supplémentaires devraient être mises en place lorsque des types spécifiques de traitement sont effectués. Par exemple, lorsque des "catégories particulières de données à caractère personnel" sont concernées, des exigences plus strictes devraient être définies, telles que le consentement explicite de la personne concernée au traitement des données, ou la mise en place de garanties appropriées pour protéger les droits et libertés des personnes concernées.

1.10. **Prise de décision automatisée et profilage.** Les décisions fondées uniquement sur un traitement automatisé (prise de décision individuelle automatisée), y compris le profilage, qui produisent des effets juridiques à l'égard d'une personne concernée ou qui l'affectent de manière significative, ne peuvent intervenir que sous certaines conditions fixées par le cadre juridique du pays du destinataire ou de l'organisation internationale. Conformément au RRPD de l'OEB, ces conditions recouvrent, par exemple, la nécessité d'obtenir le consentement explicite de la personne concernée ou le caractère indispensable d'une telle décision à la conclusion ou à l'exécution d'un contrat entre la personne concernée et le responsable du traitement. Si la décision n'est pas conforme aux conditions énoncées par le cadre juridique du pays ou de l'organisation internationale, la personne concernée doit avoir le droit de ne pas en faire l'objet. Le cadre juridique du pays ou de l'organisation internationale devrait dans tous les cas fournir les garanties nécessaires, y compris le droit d'être informé des raisons spécifiques ayant fondé la décision et la logique sous-jacente, celui de corriger une information inexacte ou incomplète en obtenant une intervention humaine, et d'exprimer son point de vue et de contester la décision lorsqu'elle a été prise sur un fondement factuel erroné.

1.11. **Règles relatives aux transferts ultérieurs**. Le niveau de protection des données à caractère personnel des personnes concernées ne doit pas être compromis par des transferts ultérieurs. D'autres transferts de données à caractère personnel par le destinataire initial ne devraient être autorisés que si le destinataire ultérieur (soit le destinataire du transfert ultérieur) est également soumis à des règles (y compris à des obligations contractuelles) qui offrent un niveau de protection adéquat, conformément aux instructions correspondantes en cas de traitement des données pour le compte du responsable du traitement, pour des finalités limitées et spécifiques et pour autant qu'il existe un fondement juridique à ce traitement.

## 2. Mécanismes de procédure et de mise en œuvre

Bien que les mécanismes de voies de recours juridique et de contrôle dont disposent les personnes concernées dans le pays ou au sein de l'organisation internationale puissent être différents de ceux en place au sein de l'OEB, aux fins d'évaluer si le niveau de protection offert par le pays ou

l'organisation internationale est adéquat, les éléments suivants doivent être compris dans le cadre de protection des données pertinent.

2.1. Un mécanisme de contrôle compétent : un ou plusieurs mécanismes de contrôle indépendants ou des autorités hiérarchiques chargées de surveiller, d'assurer et de faire respecter les dispositions relatives à la protection des données et à la vie privée dans le pays ou au sein de l'organisation internationale. Le mécanisme de contrôle doit agir de manière indépendante et impartiale dans l'exercice de ses fonctions et de ses compétences et, ce faisant, ne doit solliciter ni accepter d'instructions. À cet égard, le mécanisme de contrôle doit disposer des pouvoirs et mandat nécessaires pour garantir le respect des droits de protection des données et promouvoir la sensibilisation.

2.2. Un niveau satisfaisant de conformité : le système de protection des données doit assurer (de manière cumulative) :
(i) un degré élevé d'obligation de rendre des comptes
(ii) la sensibilisation des responsables du traitement et des personnes qui procèdent au traitement de données à caractère personnel pour leur compte, à leurs obligations, tâches et responsabilités
(iii) les personnes concernées sont informées de leurs droits et des moyens pour les exercer.

2.3. Obligation de rendre des comptes : le cadre de protection des données d'un pays ou d'une organisation internationale devrait obliger les responsables du traitement et les personnes qui procèdent au traitement des données à caractère personnel pour leur compte à s'y conformer et à être en mesure de démontrer cette conformité, notamment à l'autorité hiérarchique compétente.[5]

2.4. Soutien et aide à chaque personne concernée dans l'exercice de ses droits et mécanismes de voies de recours appropriés : les personnes devraient pouvoir exercer des voies de recours pour faire valoir leurs droits rapidement, de manière effective et sans coûts prohibitifs ; cela permet également d'en garantir le respect. Il convient ainsi de mettre en place des mécanismes de contrôle qui permettent d'examiner les réclamations de manière indépendante, et d'identifier et de sanctionner en pratique toute violation du droit à la protection des données et à la vie privée. Lorsque des règles ne sont pas respectées, les personnes concernées devraient également disposer de voies de recours administratif et judiciaire effectives, notamment pour obtenir réparation de préjudices subis en raison du traitement illicite de leurs données à caractère personnel. Il s'agit d'un élément essentiel qui doit inclure un système d'adjudication ou d'arbitrage indépendant permettant le paiement d'une somme à titre compensatoire et le prononcé de sanctions si nécessaire.

[5] À titre d'exemple, les obligations de conserver la documentation relative à la protection des données.