



LIGNES DIRECTRICES DU SECRÉTAIRE GÉNÉRAL INSTAURANT LE PROGRAMME DE GESTION DE LA VIE PRIVÉE DE L'OCDE

Date de prise d'effet : 28 octobre 2022

LIGNES DIRECTRICES DU SECRÉTAIRE GÉNÉRAL INSTAURANT LE PROGRAMME DE GESTION DE LA VIE PRIVÉE DE L'OCDE

Les présentes lignes directrices sont adoptées en application de l'article 10 b) de la *Décision du Secrétaire général relative à la protection des individus à l'égard du traitement de leurs données personnelles* (les « Règles de protection des données »), et il convient de les interpréter à la lumière desdites Règles. Quand il est fait usage, dans les présentes lignes directrices, de termes qui sont définis dans les Règles de protection des données, lesdits termes ont le même sens que dans les Règles.

Des adaptations des présentes lignes directrices pourront s'avérer nécessaires pour tenir compte des spécificités de la gouvernance et du fonctionnement d'entités et d'organes évoluant dans le cadre de l'OCDE tels que l'Agence internationale de l'énergie (AIE), l'Agence de l'OCDE pour l'énergie nucléaire (AEN) et le Forum international des transports (FIT). Ces adaptations seront définies par le Délégué à la protection des données, après consultation de l'entité ou de l'organe concernés.

Portée des présentes lignes directrices

1. Dans le prolongement des [Lignes directrices de l'OCDE sur la protection de la vie privée](#) (troisième partie), le présent document instaure un Programme de gestion de la vie privée (le « Programme ») qui a pour objet de contribuer à remplir les exigences formulées dans les Règles de protection des données en matière de responsabilité (article 6 des Règles de protection des données).

Rôles et responsabilités

2. Les Règles de protection des données énoncent clairement les rôles et les responsabilités du responsable de traitement et des sous-traitants¹ ainsi que du Délégué à la protection des données, du Commissaire à la protection des données et du Secrétaire général. L'association active d'un certain nombre d'autres acteurs issus de l'ensemble de l'Organisation est également nécessaire en appui à la fonction de protection des données. Cette association vient s'ajouter aux responsabilités que ces acteurs peuvent assumer en qualité de responsable de traitements ou de sous-traitants pour les activités placées sous leur responsabilité.

- Le **Cabinet du Secrétaire général** fixe le cap au sein de l'Organisation s'agissant de l'importance de la protection des données et du soutien à assurer aux activités du Délégué à la protection des données et du Commissaire à la protection des données, y compris par la fourniture des ressources et de l'appui administratif nécessaires.
- La **Direction exécutive (EXD)** favorise la prise en compte des considérations liées à la protection des données dans le processus d'élaboration des politiques informatiques et dans les opérations de communication menées dans l'ensemble de l'Organisation.
- Le **Bureau de la sécurité numérique (EXD/DKI/DSO)** prodigue des conseils sur les mesures de sécurité à mettre en place pour le traitement des données personnelles et définit une politique et des orientations pour la prise en charge des incidents, y compris des protocoles permettant d'aider le responsable de traitement à remplir ses obligations en matière de notification des violations de données (art. 6.4 des Règles de protection des données).

¹ Y compris quand l'Organisation elle-même intervient en qualité de sous-traitant.

- La **Direction des affaires juridiques (SGE/LEG)** prodigue des conseils à l'Organisation sur les aspects d'ordre juridique liés à l'interprétation des Règles de protection des données, en lien notamment avec les dispositifs et accords de partage des données mis en place avec des tiers.
- Le **Service du programme, du budget et de la gestion financière (EXD/PBF)** contribue à assurer la prise en compte des risques et des exigences liés à la protection des données dans le cadre du processus de passation de marchés et de conclusion de contrats, en concertation avec SGE/LEG.
- La **Direction des relations extérieures et de la communication (PAC)** contribue à sensibiliser aux questions liées à la protection des données dans le cadre de son travail de coordination des activités de communication et de dialogue avec les parties prenantes de l'OCDE.
- La **Direction des statistiques et des données (SDD)** contribue à sensibiliser aux questions liées à la protection des données dans le cadre de la coordination des travaux de la communauté des professionnels de la statistique et des données ainsi que dans le cadre des stratégies d'approvisionnement en données et de gestion des données.

Coordination interne

3. L'intégration des opérations de protection des données au sein de l'ensemble des activités de l'Organisation est d'une importance cruciale pour optimiser l'impact et tirer le meilleur parti des ressources.
 - a) Il convient que, de manière régulière, le Délégué à la protection des données dialogue avec les groupes de coordination pertinents de l'ensemble de l'Organisation, tels que les groupes chargés de la coordination informatique, des stratégies numériques, de la sécurité numérique, de la sécurité de l'information, des statistiques et de la gouvernance des données, et qu'il participe à leurs travaux.
 - b) Le Délégué à la protection des données pourra occasionnellement avoir des échanges avec le Groupe des directeurs ainsi qu'avec les communautés et réseaux de conseillers en gestion des ressources ou autres conseillers et de spécialistes de la communication et de l'informatique.

Intégration et cohérence

4. Les Règles de protection des données s'inscrivent dans le cadre général du Statut et du Règlement applicables aux agents de l'Organisation, et il convient de les appliquer au regard de ce cadre. Il convient en particulier que leur application respecte les articles suivants du Statut du personnel :
 - a) Les agents ne sont soumis à aucune discrimination pour des raisons d'origine raciale ou ethnique, de nationalité, d'opinions ou de croyance, de sexe, d'orientation sexuelle, d'état de santé ou de handicap [article 5 a) du Statut] ;
 - b) Les agents ont droit au respect de leur vie privée [article 5 c) du Statut].

Évaluation des risques pour la protection des données

5. En matière de protection des données, il convient que l'Organisation mette en œuvre une démarche fondée sur les risques, conformément aux Règles de protection des données.

- a) Il convient que le Délégué à la protection des données mette en place une méthodologie pour aider le responsable de traitement à procéder à l'évaluation des risques pour la protection des données et à définir des garanties appropriées pour atténuer les risques (art. 6.2 des Règles de protection des données).
- b) Une évaluation unique peut être effectuée pour des activités multiples ou répétées posant des risques similaires, telles que l'organisation de manifestations et de réunions.

Registre des données personnelles

6. Des pratiques rigoureuses de conservation d'archives sont essentielles au respect des règles applicables à la protection des données, et elles aident l'Organisation à hiérarchiser et à gérer les risques, à répondre aux demandes des personnes concernées et à favoriser la transparence.

- a) Il convient que le Délégué à la protection des données s'appuie sur les obligations pesant sur le responsable de traitement et sur les sous-traitants en matière de conservation d'archives [art. 6.1 b) des Règles de protection des données] et sur les consultations relatives à l'évaluation des risques pour la protection des données [art. 6.2 des Règles de protection des données] pour créer et tenir un registre des activités de traitement de données personnelles.
- b) Il convient de coordonner la création et la tenue de ce registre des données personnelles avec les autres initiatives de conservation d'archives liées aux données sensibles, aux statistiques et aux infrastructures et systèmes informatiques.

Achats et contrats

7. Pour veiller à ce que les sous-traitants de l'Organisation s'acquittent de leurs responsabilités aux termes des Règles de protection des données (art. 6 des Règles de protection des données) et conformément au principe consistant à intégrer la protection des données dès l'étape de la conception (art. 6.3 des Règles de protection des données), il convient que l'Organisation mette en œuvre des mesures de protection des données dans le cadre de son processus d'achat.

- a) Quand l'Organisation fait l'acquisition de services impliquant le traitement de données personnelles, il convient que la consultation de marché ou l'appel d'offres informent les candidats qu'il leur faut démontrer leur aptitude et leur détermination à fournir des garanties contractuelles conformes aux exigences applicables aux sous-traitants aux termes des Règles de protection des données ainsi qu'à respecter toute réglementation applicable en matière de protection des données.
- b) De manière générale, il convient de considérer les aptitudes en matière de protection des données comme des exigences *a minima* dans le cadre du processus œuvre.
- c) Il convient que l'Organisation rédige des clauses types de protection des données à intégrer dans les contrats impliquant le traitement de données personnelles, y compris les contrats pour lesquels aucune procédure de mise en concurrence n'est nécessaire. Il convient que ces clauses prévoient une série de protections de base par défaut, et que des mesures plus robustes puissent être intégrées au besoin, en fonction du contexte et des risques.

Formation et sensibilisation

8. Pour une bonne mise en œuvre des mesures de protection des données, il est nécessaire que tous les membres du personnel intervenant dans le traitement de données personnelles disposent de connaissances de

base sur les cas où les Règles de protection des données s'appliquent, sur les opérations requises à des fins de conformité et sur les cas de figure où il convient de demander conseil au Délégué à la protection des données.

- a) Il convient que le Délégué à la protection des données élabore des supports de formation et d'information tels que des cours en ligne et des « guides pratiques » pour aider les membres du personnel à comprendre leurs responsabilités en matière de protection des données. Il convient de publier ces supports sur l'intranet de l'OCDE et de les faire connaître grâce aux canaux habituels de communication de l'Organisation. Il convient aussi de fournir les indications pertinentes aux nouveaux agents dans le cadre de leur processus d'intégration à l'OCDE.
- b) Il convient que l'OCDE mette en place un réseau de référents désignés par chaque direction ou service pour collaborer avec le Délégué à la protection des données et le Bureau de la sécurité numérique afin de faciliter la communication, de repérer les questions de sécurité et de respect de la vie privée soulevées par les activités courantes et d'intégrer de bonnes pratiques à la culture de travail de l'Organisation.
- c) Il convient que l'Organisation organise occasionnellement des activités de sensibilisation telles qu'une opération annuelle de communication à l'occasion de la Journée mondiale de la protection des données.

Transparence et visibilité externe

9. Il convient que l'OCDE, en sa qualité d'Organisation comptable de ses actes, fasse preuve de transparence sur son engagement en faveur de la protection des données, sur les règles qu'elle suit et sur les pratiques mises en place, et qu'elle fournisse des indications spécifiques sur les activités impliquant le traitement de données personnelles.

- a) Il convient que l'OCDE rende publique sa démarche de protection des données, en fournissant des liens permettant d'accéder aux Règles de protection des données, au présent Programme de gestion de la vie privée et aux rapports annuels d'activité du Commissaire à la protection des données.
- b) Il convient que l'OCDE suive une démarche de transparence à plusieurs niveaux concernant les données personnelles qu'elle traite, en particulier pour les personnes concernées qui n'appartiennent pas à son personnel. Il convient que le site internet de l'OCDE fournisse une description générale de la démarche de l'Organisation en matière de protection des données ainsi que de ses différentes activités de traitement de données, avec des liens permettant d'accéder à des avertissements d'ordre général pour les activités ordinaires de traitement de données (p. ex. recrutement, visites sur le site internet, présence dans les locaux). Pour les projets qui impliquent un traitement à plus grande échelle des données, il convient de faire apparaître sur les sites internet correspondants un avertissement relatif à la protection des données. De plus, il convient de mettre directement à la disposition des personnes concernées des avertissements spécifiques, si nécessaire.

Droits des personnes concernées

10. Il convient de répondre aux demandes des personnes concernées (art. 5 des Règles de protection des données) dans les meilleurs délais et, de façon générale, dans un délai d'un mois.

- a) Il convient, dans toute la mesure du possible, de limiter le recueil de données supplémentaires pour vérifier l'identité de l'auteur de la demande, sous réserve de la nécessité de contrôler l'authenticité de la demande et de prendre en compte les conséquences d'une éventuelle erreur.

- b) Il convient que le responsable de traitement veille à ce que les réponses à une demande fassent l'objet d'un contrôle visant à prévenir toute conséquence négative pour d'autres personnes concernées, et à ce que toute donnée personnelle transmise en réponse à une demande soit protégée au moyen de mesures de sécurité appropriées.

Suivi et réexamen

11. Tout en veillant à ce qu'il continue d'être conforme aux Règles de protection des données, il conviendra de réexaminer et d'adapter le présent Programme afin de refléter l'évolution des pratiques de l'OCDE en matière de traitement des données personnelles ainsi que la maturité acquise par l'Organisation en matière de protection des données et de gouvernance de l'information.

- a) Il conviendra de procéder à un réexamen du Programme tous les deux ans. Ce réexamen sera piloté par le Délégué à la protection des données, en concertation avec le Commissaire à la protection des données ainsi qu'avec le Cabinet du Secrétaire général et le Bureau du Directeur exécutif. Les autres acteurs mentionnés à l'article 2 ci-dessus pourront eux aussi être consultés.
- b) En plus des actualisations ou des modifications qu'il pourra être nécessaire d'apporter aux articles existants, on examinera la possibilité d'ajouter des éléments au Programme, par exemple pour améliorer le suivi et les éléments de mesure.