AVIS DE CONFIDENTIALITÉ
ACTIVITÉS DE L'AUDIT INTERNE

Cet avis de confidentialité explique la manière dont la division de l'Audit interne de la Direction de l'Audit interne, de l'Évaluation et de l'Investigation (DIO) traite les données à caractère personnel.

1. Qui est responsable du traitement des données ?

La division de l'Audit interne, également désignée par "nous" dans le présent document, est responsable du traitement des données ce qui signifie qu'elle a le pouvoir de décision en matière de traitement de données. Le traitement des données par la division de l'Audit interne est régi par le Règlement du Conseil de l'Europe sur la protection des données à caractère personnel adopté par le Comité des Ministres le 15 juin 2022.

2. À quelles fins traitons-nous des données à caractère personnel ?

La division de l'Audit interne traite des données à caractère personnel dans le cadre de ses activités d'audit interne, qui consistent à donner une assurance, des conseils et un éclairage utile en toute indépendance afin d'améliorer et de protéger la valeur organisationnelle, de contribuer à la prise de décisions basées sur des éléments concrets et de promouvoir l'apprentissage, la transparence, l'intégrité et la responsabilisation au sein de l'Organisation. Différents types de missions sont réalisés à cet effet, tels que des audits de performance, des audits de conformité, des audits des technologies de l'information et des services de conseil effectués à la demande du management sur des questions de gouvernance, de gestion des risques et/ou de contrôle interne.

Le processus d'audit comporte trois étapes : le travail préparatoire (comprenant la collecte et l'analyse de données), le travail de terrain (comprenant les tests d'audit fondés sur les données collectées, les entretiens et/ou les enquêtes) et la communication des résultats (comprenant la présentation de données anonymisées). Des données à caractère personnel sont collectées et traitées tout au long du processus d'audit.

3. Quelles sont les catégories de données à caractère personnel que nous traitons ?

Dans le cadre des missions susmentionnées, la division de l'Audit interne peut traiter toute donnée pertinente jugée nécessaire, incluant par exemple des données relatives à la situation personnelle et familiale ou aux dépenses engagées ou remboursées par l'Organisation. Il peut s'agir de données sensibles telles que définies à l'article 5 du Règlement du Conseil de l'Europe sur la protection des données à caractère personnel.

4. Quel est le fondement juridique de notre traitement des données à caractère personnel ?

Ces opérations de traitement des données ont pour fondement juridique le Statut du personnel et les Arrêtés relatifs au personnel du Conseil de l'Europe, la Charte de la DIO et d'autres instruments juridiques applicables adoptés par le Conseil de l'Europe. Des orientations et des principes concernant les pratiques de la DIO en matière de protection des données figurent également dans les Lignes directrices de la DIO sur la protection des données.

De plus, la division de l'Audit interne vise à adhérer aux Normes internationales d'audit interne (GIAS) de l'Institut des auditeurs internes (IIA). Les sections pertinentes sont reprises ci-après :

« Principe 5 – Préserver la confidentialité
Les auditeurs internes utilisent et protègent l'information de façon adéquate.

Norme 5.1 - Utilisation de l'information
Exigences :
Lorsqu'ils utilisent des informations, les auditeurs internes doivent suivre les politiques et les procédures applicables, ainsi que la législation et la réglementation en vigueur. Ces informations ne doivent pas être utilisées pour en retirer un bénéfice personnel, ou d'une manière qui contreviendrait ou porterait préjudice aux objectifs éthiques et légitimes de l'organisation.

Norme 5.2 – Protection de l'information
Exigences :
Les auditeurs internes doivent être conscients de leurs responsabilités en matière de protection de l'information et démontrer qu'ils respectent la confidentialité, la vie privée et la propriété de l'information recueillie dans le cadre de la réalisation des services d'audit interne ou résultant de relations professionnelles.

Les auditeurs internes doivent comprendre et respecter la législation et la réglementation, ainsi que les politiques et les procédures relatives à la confidentialité, à la sécurité de l'information et à la protection de la vie privée, et applicables à l'organisation comme à la fonction d'audit interne.

La fonction d'audit interne doit notamment tenir compte des considérations suivantes :
- La garde, la conservation et la destruction des documents de la mission ;
- La mise à disposition des documents de la mission à des parties internes et externes ;
- Le traitement des accès aux informations confidentielles (originaux ou copies) lorsque celles-ci ne sont plus nécessaires.

Les auditeurs internes ne doivent pas divulguer d'informations confidentielles à des parties non habilitées, à moins qu'une responsabilité légale ou professionnelle ne les y oblige.

Les auditeurs internes doivent gérer le risque qu'une information soit divulguée, ou sa confidentialité compromise, par inadvertance.

Le responsable de l'audit interne doit s'assurer que la fonction d'audit interne et les personnes collaborant avec la fonction d'audit interne adhèrent aux mêmes exigences de protection. »

5. Qui a accès à vos données ?

Les missions d'audit sont soumises au principe de confidentialité. Les informations recueillies au cours des missions d'audit sont traitées de manière confidentielle par toutes les personnes impliquées et ne sont communiquées qu'en cas de nécessité, conformément aux dispositions règlementaires et politiques applicables.

Seul le personnel autorisé de la DIO a accès aux données traitées dans ce cadre. Par ailleurs, si un audit est effectué avec l'aide d'une tierce partie, les données peuvent être transférées à des personnes désignées, internes ou externes au Conseil de l'Europe, impliquées dans le processus.

Dans ce cas, les garanties prévues à l'article 9 du Règlement du Conseil de l'Europe sur la protection des données à caractère personnel s'appliquent.

Les résultats des audits ne comprendront pas de données à caractère personnel, se limitant uniquement à des données anonymisées. Ces résultats seront communiqués aux parties prenantes concernées.

6. Comment conservons-nous vos données à caractère personnel ?

Pour protéger vos données à caractère personnel, diverses mesures techniques et organisationnelles ont été mises en place. Les mesures techniques consistent en diverses actions visant à assurer la sécurité et la sûreté des données (par exemple, la pseudonymisation ou l'anonymisation, l'utilisation de plateformes cryptées, les politiques d'écran vide, de bureau propre et de verrouillage, la destruction de dossiers, etc.) et à prévenir l'altération des données ou l'accès non autorisé en fonction du niveau de risque que présente le traitement et de la nature des données traitées. Les mesures organisationnelles incluent la restriction de l'accès aux personnes autorisées ayant un besoin légitime de prendre connaissance des données aux fins du traitement. Les données à caractère personnel sont stockées sur des serveurs utilisés par le Conseil de l'Europe et situés à l'intérieur de l'Espace économique européen.

7. Combien de temps vos données seront-elles conservées ?

Vos données à caractère personnel peuvent être conservées par la division de l'Audit interne conformément au cadre juridique du Conseil de l'Europe. Selon le Règlement financier du Conseil de l'Europe, l'Organisation conserve les pièces comptables pour une période de dix ans. Les pièces d'audit peuvent être conservées pour une période pouvant aller jusqu'à dix ans.

8. Quels sont vos droits en matière de protection des données ?

Conformément aux dispositions de l'article 8 du Règlement du Conseil de l'Europe sur la protection des données à caractère personnel, vous êtes en droit de :

- demander l'accès aux données à caractère personnel que nous détenons à votre sujet ;
- demander la correction de données à caractère personnel incomplètes ou inexactes que nous détenons à votre sujet ;
- demander la suppression ou le retrait de vos données à caractère personnel lorsque nous n'avons plus aucune raison valable de les conserver ;
- vous opposer au traitement de vos données à caractère personnel pour des raisons tenant à votre situation.

Veuillez noter que des exceptions et des restrictions peuvent s'appliquer, conformément aux dispositions des articles 7, 8 et 10 du Règlement du Conseil de l'Europe sur la protection des données à caractère personnel. D'autres orientations à cet égard figurent également dans les Lignes directrices de la DIO sur la protection des données.

9. Contacts

Si vous souhaitez exercer les droits susmentionnés ou pour toute question, préoccupation ou encore demande sur la manière dont vos données sont collectées et utilisées, veuillez envoyer un courriel à l'adresse suivante :

- dio.dataprotection@coe.int ,
- au ou à la Délégué·e à la protection des données du Conseil de l'Europe à l'adresse suivante : dpo@coe.int.

Si vous estimez que nous n'avons pas répondu de manière satisfaisante à votre demande et que vous considérez que vos droits en matière de protection des données ont été violés à la suite du traitement de vos données à caractère personnel, vous êtes en droit de déposer une réclamation auprès du Commissaire à la protection des données du Conseil de l'Europe en envoyant un courriel à l'adresse suivante : datacommissioner@coe.int.