COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

# AVIS DE CONFIDENTIALITÉ
# ÉVALUATION DES RISQUES DE FRAUDE

***Ce document explique comment la Direction de l'Audit Interne, de l'Évaluation et de l'Investigation (DIO) traite les données à caractère personnel dans le cadre des évaluations des risques de fraude de deux entités administratives majeures (MAE) du Conseil de l'Europe : la Cour européenne des droits de l'homme (Cour) et la Direction européenne de la qualité du médicament & soins de santé (EDQM). Nous avons décrit ici comment vos données personnelles seront traitées, c'est-à-dire manipulées, stockées, protégées et utilisées. Nous nous engageons à garantir la confidentialité et la sécurité de vos données et à utiliser les informations uniquement aux fins des évaluations des risques de fraude.***

---

## 1. Qui est responsable du traitement des données ?

La Division de l'Investigation de la **DIO** est « responsable du traitement » des données à caractère personnel dans le cadre des évaluations des risques de fraude de la Cour et de l'EDQM (les « évaluations des risques de fraude »), ce qui signifie qu'elle a le pouvoir de décision concernant le traitement des données. Le traitement de vos données personnelles 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 2002.

## 2. Quelles données traitons-nous et dans quel but ?

Nous traitons toutes les catégories de données personnelles que nous collectons et recevons dans le cadre des évaluations des risques de fraude, y compris les données sensibles telles que définies à l'article 5 du Règlement du Conseil de l'Europe sur la protection des données à caractère personnel.

Les données sont collectées dans le cadre des évaluations des risques de fraude à partir des sources suivantes et aux fins suivantes :

- Intranet du Conseil de l'Europe pour mener des recherches et un examen des documents sur les MAE afin (a) d'établir la structure et les procédures des MAE pertinentes pour les évaluations des risques de fraude, et (b) de détecter les procédures mal conçues qui perpétuent les fraudes ou permettent des fraudes potentielles ou compromettent les buts et objectifs du projet/programme.
- Entretiens et investigations auprès du personnel pour recueillir la perception des seniors managers sur les principaux risques de fraude dans leurs MAE.
- Données de FIMS pour vérifier la possibilité de : (a) manipulation des estimations, consolidation des comptes subsidiaires, examens analytiques des budgets et des chiffres réels, ratios, préoccupations des organes de gouvernance, (b) altération des factures, demandes de remboursement en double, paiements en double, falsifications des remboursements de frais, fausses demandes d'urgence, fournisseurs fictifs, surfacturation, utilisation abusive des avances, (c) écrémer, systèmes de facturation, remboursements de frais (frais mal caractérisés, fictifs, surévalués), (d) pots-de-vin, collusion, fausse facturation, manipulation des spécifications, truquage d'offres et compromis sur la qualité des produits, ainsi que (e) recouper les données du personnel et des fournisseurs.
- Données d'inventaire pour vérifier la possibilité de vol de fournitures, d'inventaire ou d'expédition sortante, d'espèces, d'actifs attrayants et d'actifs incorporels.
- Données de PeopleSoft pour vérifier la possibilité de : (a) gestion du personnel et recrutement tels que les fraudes à la paie (employés fantômes, salaires gonflés, modifications non autorisées des dossiers de paie), népotisme dans les décisions d'embauche, utilisation abusive des fonds de formation, absence de vérification des antécédents et faux certificats, et (b) recouper les données relatives au personnel et aux fournisseurs.

## 3. Quelle est la base juridique du traitement de vos données ?

La base juridique de ce traitement est le Statut et le Règlement du personnel du Conseil de l'Europe, la Charte de la DIO et les autres instruments juridiques applicables adoptés par le Conseil de l'Europe. Les lignes directrices et les principes de la DIO en matière de protection des données figurent également dans les directives de la DIO en matière de protection des données.

Plus précisément, les éléments pertinents se trouvent au paragraphe 32 de la Charte de la DIO (les évaluations des risques de fraude sont considérées comme des activités de prévention de la fraude), lue conjointement avec le paragraphe 12 (accès aux documents pour toutes les activités menées par la DIO) et le paragraphe 40 (rapports d'évaluation des risques de fraude).

## 4. Qui a accès à vos données ?

Seul le personnel autorisé de la DIO a accès aux données traitées à cet égard.

En outre, une copie téléchargeable des informations requises pour les évaluations des risques de fraude sera placée sur une machine virtuelle sur le serveur du Conseil de l'Europe. Ces données seront manipulées à distance par Red Flag Oversight Consultancy Services. Red Flag Oversight Consultancy Services agit en tant que consultant externe conformément à l'article 33 de la Charte de la DIO. Les garanties énoncées à l'article 9 du Règlement du Conseil de l'Europe sur la protection des données à caractère personnel s'appliqueront.

Les résultats des évaluations des risques de fraude ne comprendront pas de données à caractère personnel. Ces résultats seront partagés avec les parties prenantes concernées.

## 5. Comment stockons-nous vos données personnelles ?

Pour protéger vos données personnelles, diverses mesures techniques et organisationnelles ont été mises en place. Les mesures techniques comprennent diverses actions visant à assurer la sécurité et la sûreté des données (par exemple, pseudonymisation ou anonymisation, utilisation de plateformes cryptées, politique d'effacement des écrans, politique de bureau propre, politique de verrouillage et de clé, destruction des fichiers, etc.), ainsi que la prévention de l'altération des données ou de l'accès non autorisé en fonction du niveau de risque présenté par le traitement et de la nature des données traitées. Les mesures organisationnelles comprennent également la restriction de l'accès aux données aux personnes autorisées ayant un besoin légitime de les connaître aux fins de cette opération de traitement. Les données à caractère personnel sont stockées sur des serveurs utilisés par le Conseil de l'Europe et situés dans l'Espace économique européen.

Nos consultants externes, Red Flag Oversight Consultancy Services, ont également mis en place des mesures pour protéger la sécurité des données, y compris des mesures appropriées pour empêcher que vos informations ne soient accidentellement perdues, utilisées ou consultées de manière non autorisée, modifiées ou divulguées.

Les données seront stockées sur une machine virtuelle sur le serveur du Conseil de l'Europe et manipulées à distance par Red Flag Oversight Consultancy Services.

Soyez assurés que l'accès à ces informations sera strictement limité aux personnes travaillant sur les évaluations des risques de fraude.

## 6. Combien de temps vos données seront-elles conservées ?

Les données collectées seront supprimées par le consultant externe un mois après la publication des rapports finaux d'évaluation des risques de fraude concernant les MAE.

La DIO conservera les données conformément au cadre juridique du Conseil de l'Europe. Les rapports d'investigation ainsi que tous les documents de travail et enregistrements d'entretiens connexes seront conservés pendant une période maximale de 10 ans. Ces documents sont anonymisés dès qu'un format permettant l'identification personnelle n'est plus nécessaire.

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

Vous avez le droit de :

- demander l'accès aux informations personnelles vous concernant que nous détenons ;
- demander que nous corrigions les informations personnelles incomplètes ou inexactes que nous détenons à votre sujet ;
- demander que nous supprimions ou retirions vos informations personnelles lorsqu'il n'y a pas de raison valable pour que nous les conservions ;
- vous opposer au traitement de vos informations personnelles pour des raisons spécifiques liées à votre situation.

## 8. Contacts

Si vous souhaitez exercer les droits susmentionnés, ou pour toute question, préoccupation ou demande que vous pourriez avoir concernant la manière dont vos données sont collectées et utilisées, veuillez contacter le Conseil de l'Europe :

- en envoyant un e-mail à la DIO à l'adresse dio.dataprotection@coe.int.
- en envoyant un e-mail au délégué à la protection des données du Conseil de l'Europe à l'adresse dpo@coe.int.

Si vous estimez que nous n'avons pas répondu de manière adéquate à votre demande et que vos droits en matière de protection des données ont été violés à la suite du traitement de vos données à caractère personnel, vous avez le droit de déposer une plainte auprès du Commissaire à la protection des données du Conseil de l'Europe en envoyant un e-mail à datacommissioner@coe.int.

***Fin du document*