PRIVACY NOTICE
FRAUD RISK ASSESSMENT

This document explains how the Directorate of Internal Oversight (the DIO) processes personal data in relation to the Fraud Risk Assessments of two Major Administrative Entities (MAEs) of the Council of Europe: the European Court of Humans Rights (the Court) and the European Directorate for the Quality of Medicines and HealthCare (the EDQM). Here we have outlined how your personal data will be processed, i.e. handled, stored, protected, and used. We are committed to ensuring the confidentiality and security of your data and using the information solely for the purpose of the Fraud Risk Assessments.

---

1. Who is responsible for data processing?

The Investigation Division of the **DIO** is the "data controller" with respect to the processing of personal data in relation to the **Fraud Risk Assessments of the Court and the EDQM** (the Fraud Risk Assessments), which means it has the decision-making power concerning the data processing. Processing of your personal data is governed by the Council of Europe Regulations on the Protection of Personal Data adopted by the Committee of Ministers on 15 June 2022.

2. What data do we process and for what purpose?

We process any categories of personal data that we collect and receive in the framework of the Fraud Risk Assessments, including sensitive data as defined in Article 5 of the Council of Europe Regulations on the Protection of Personal Data.

Data is collected as part of the Fraud Risk Assessments from the following sources and for the following purposes:

- Council of Europe Intranet to conduct research and a document review on the MAEs to (a) establish the structure and procedures of the MAEs relevant to the Fraud Risk Assessments, and (b) detect poorly designed procedures that perpetuate frauds or enable potential frauds or undermine the goals and objectives of the project/programme.
- Staff interviews and surveys to gather the perception of senior staff of the key fraud risks in their MAEs.
- FIMS data to check the possibility of: (a) manipulation of estimates, consolidation of subsidiary accounts, analytical reviews of budgets and actuals, ratios, concerns of governance bodies, (b) alteration of invoices, duplicate claims, duplicate payments, expense reimbursement falsifications, false emergency claims, fictitious vendors, overbilling, misuse of advances, (c) skimming, billing schemes, expense reimbursements (mischaracterised, fictitious, overstated expenses), (d) kickback, collusion, false invoicing, specs manipulation, bid rigging and compromise with quality of products, as well as (e) to cross check staff and supplier data.
- Inventory data to check the possibility of theft from supplies, inventory or outgoing shipment, cash, attractive assets, and intangible assets.
- PeopleSoft data to check the possibility of: (a) personnel management and recruitment such as payroll frauds (ghost employees, inflated salaries, unauthorized changes to pay records, inflated salaries), nepotism in hiring decisions, misuse of training funds, lack of background checks and false certificates, and (b) to cross check staff and supplier data.

3. What is the legal basis for our processing of your data?

The legal basis for this processing operation is the Council of Europe's Staff Regulations and Staff Rules, the DIO Charter, other applicable legal instruments adopted by the Council of Europe. Guidance and principles on the data protection practices of the DIO can also be found in the DIO's Data Protection Guidelines.

More specifically, the relevant elements are found in paragraph 32 of the DIO Charter (FRAs are regarded as fraud-prevention activities), read in conjunction with paragraph 12 (access to documents for any activities carried out by the DIO) and paragraph 40 (Fraud Risk Assessment reports).

4. Who has access to your data?

Fraud Risk Assessments are confidential. Information gathered in the course of any Fraud Risk Assessment is treated as confidential by all those involved and is shared only on a need-to-know basis in conformity with applicable rules, regulations and policies.

Only authorised DIO staff has access to data processed in this respect.

In addition, a downloadable copy of required information for the Fraud Risk Assessments will be put on a virtual machine on the server of the Council of Europe. This data will be manipulated by Red Flag Oversight Consultancy Services, remotely. Red Flag Oversight Consultancy Services act as external consultants pursuant to Article 33 of the DIO Charter. The safeguards outlined in Article 9 of the Council of Europe Regulations on the Protection of Personal Data will apply.

The results of the Fraud Risk Assessments will not include personal data. Such results will be shared with the relevant stakeholders.

5. How do we store your personal data?

To protect your personal data, various technical and organisational measures have been put in place. Technical measures include various actions to address security and safety of data (e.g. pseudonymisation or anonymisation, usage of encrypted platforms, clear-screen policy, clean-desk policy, lock-and-key policy, shredding of files, etc.), as well as prevention of alteration of data or unauthorised access depending on the risk level presented by the processing and the nature of the data being processed. Organisational measures also include restricting data access to authorised persons with a legitimate need to know for the purposes of this processing operation. Personal data are stored on servers used by the Council of Europe which are located within the European Economic Area.

Our external consultants, Red Flag Oversight Consultancy Services, also have put in place measures to protect the security of data, including appropriate measures to prevent your information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

The data will be stored on a virtual machine on the Council of Europe server and manipulated remotely by Red Flag Oversight Consultancy Services.

Be assured that access to this information will be strictly limited to those people working on the Fraud Risk Assessments.

6. How long will your data be stored?

Data gathered shall be deleted by the external consultant **1 month** after the publication of the final Fraud Risk Assessment reports in respect of the MAEs.

The DIO will retain the data according to the Council of Europe's legal framework. Investigation reports as well as all related working papers and interview records will be kept for a maximum period of 10 years. These documents are anonymised as soon as a personally identifiable format is no longer necessary.

7. What are your data protection rights?

You have the right to:

- request access to your personal information held by us;
- request that we correct incomplete or inaccurate personal information that we hold about you;
- request that we delete or remove your personal information when there is no valid reason for us to keep it;
- object to the processing of your personal information on specific grounds relating to your situation.

8. Contacts

If you wish to exercise the above rights, or for any queries, concerns, or requests you may have in connection with the way your data is collected and used, please contact the Council of Europe by:

- sending an email to the DIO at dio.dataprotection@coe.int.
- sending an email to the Council of Europe's Data Protection Officer at dpo@coe.int.

If you feel that we have not adequately responded to your request and consider that your data protection rights have been violated as a result of our processing of your personal data, you have the right to lodge a complaint with the Council of Europe Data Protection Commissioner by sending an e-mail to datacommissioner@coe.int.

***End of Document*