PRIVACY NOTICE
INTERNAL AUDIT ACTIVITIES

The processing of personal data by the Directorate of Internal Oversight (DIO), including activities carried out by the Internal Audit Division, is done in accordance with the Council of Europe Regulations on the Protection of Personal Data. The DIO is the Data Controller in this respect.

1. PURPOSE OF THE DATA PROCESSING

The Internal Audit Division of the DIO processes personal data for the purpose of conducting internal audit activities. The aim of internal audit activities is to provide independent assurance, advice and insight in order to enhance and protect organisational value, contribute towards evidence-based decision making, and promote organisational learning, transparency, integrity and accountability. This is done by conducting different types of assignments: performance audits, compliance audits, Information Technology audits as well as advisory services at the request of management related to governance, risk management and/or internal control.

The audit process is broken down into three stages: preparatory work (including collection and analysis of data), field work (including audit tests on the basis of the data collected, interviews and/or surveys) and the communication of results (including the presentation of anonymised data). Throughout the audit process, personal data is collected and processed.

2. LEGAL BASIS FOR THE PROCESSING

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.

In addition, the Internal Audit Division aims to adhere to the mandatory elements of the Institute of Internal Auditors' (IIA) International Professional Practices Framework, including the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the International Standards for the Professional Practice of Internal Auditing and the Definition of Internal Auditing.

3. CATEGORIES OF PERSONAL DATA PROCESSED

In the framework of the aforementioned assignments, the Internal Audit Division may process any relevant data deemed necessary, for example data related to personal and family status or related to expenses incurred or refunded by the Organisation. This may include sensitive data as defined in Article 5 of the Council of Europe Regulations on the Protection of Personal Data.

4. WHO HAS ACCESS TO YOUR INFORMATION AND TO WHOM IS IT DISCLOSED?

Audit assignments are confidential. Information gathered in the course of any audit assignment 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, if an audit is performed with the help of an external party, your data may be transferred to designated persons internal or external to the Council of Europe involved in the process.

In that case, the safeguards outlined in Article 9 of the Council of Europe Regulations on the Protection of Personal Data will apply.

5. HOW DO WE PROTECT AND SAFEGUARD YOUR INFORMATION?

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.

6. HOW LONG DO WE KEEP YOUR DATA?

Your personal data may be retained by the DIO according to the Council of Europe's legal framework. The Council of Europe financial regulations foresee that the Organisation keep accounting records for a period of ten years. Audit records are kept for the same duration.

7. WHAT ARE YOUR RIGHTS AND HOW CAN YOU EXERCISE THEM?

As per the provision of Article 8 of the Council of Europe Regulations on the Protection of Personal Data, you have the right to request access, rectification, erasure, or restriction of processing of your personal data and you can object to their processing on grounds relating to your particular situation. Any request to exercise one of these rights should be directed to the Data Controller (at the following email address dio.dataprotection@coe.int).

Please note that, as per the provision of Article 7, Article 8, and Article 10 of the Council of Europe Regulations on the Protection of Personal Data, exceptions and restrictions may apply. Further guidelines in this respect might also be found in DIO's Data Protection Guidelines.

8. CONTACT DETAILS OF THE DATA PROTECTION OFFICER

You may contact the Data Protection Officer of the Council of Europe (dpo@coe.int) with any queries related to the processing of your personal data under the Council of Europe data protection legal framework applicable to the DIO.

9. RIGHT OF APPEAL

You also have the right to lodge an appeal with the Council of Europe Data Protection Commissioner (datacommissioner@coe.int), if you consider that your rights under the Council of Europe Regulations on the Protection of Personal Data have been infringed as a result of the processing of your personal data by the DIO.