**PRIVACY NOTICE**
**INTERNAL AUDIT ACTIVITIES**

The privacy notice explains how the Internal Audit Division of the Directorate of Internal Oversight (DIO) processes personal data.

## 1. Who is responsible for data processing?

The Internal Audit Division or "we" is the data controller, which means it has the decision-making power concerning the data processing. The processing of personal data by the Internal Audit Division 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. For what purposes do we process personal data?

The Internal Audit Division 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.

## 3. What categories of personal data do we process?

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. What is the legal basis for our processing of personal 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.

In addition, the Internal Audit Division aims to adhere to the Global Internal Auditing Standards (GIAS) of the Institute of Internal Auditors' (IIA). The relevant sections are reproduced hereafter:

"Principle 5 - Maintain Confidentiality
Internal Auditors use and protect information appropriately.

Standard 5.1 - Use of Information
Requirements

Internal Auditors must follow the relevant polices, procedures, laws, and regulations using information. The information must not be used for personal gain or in a manner contrary or detrimental to the organization's legitimate and ethical objectives.

Standards 5.2 – Protection of Information
Requirements
Internal auditors must be aware of their responsibilities for protecting information and demonstrate respect for the confidentiality, privacy, and ownership of information acquired when performing internal audit services or as the result of professional relationships.

Internal auditors must understand and abide by the laws, regulations, policies, and procedures related to confidentiality, information privacy, and information security that apply to the organization and internal audit function.

Considerations specifically relevant to the internal audit function include:
- Custody, retention, and disposal of engagement records.
- Release of engagement records to internal and external parties.
- Handling of, access to, or copies of confidential information when it is no longer needed.

Internal auditors must not disclose confidential information to unauthorized parties unless there is a legal or professional responsibility to do so.

Internal auditors must manage the risk of exposing or disclosing information inadvertently.

The chief audit executive must ensure that the internal audit function and individuals assisting the internal audit function adhere to the same protection requirements."

## 5. Who has access to your data?

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.

The results of the audits will not include personal data but only anonymised data. Such results will be shared with the relevant stakeholders.

## 6. 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.

## 7. How long will your data be stored?

Your personal data may be retained by the Internal Audit Division 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 can be kept for a period of up to ten years.

## 8. What are your data protection rights?

Under Article 8 of the Council of Europe Regulations on the Protection of Personal Data, 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.

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.

## 9. 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 send an email to:

- dio.dataprotection@coe.int;
- 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.