Guidelines on the application of the Council of Europe Data Protection Regulations in the context of the Directorate of Internal Oversight activities

GUIDELINES FOR DATA PROTECTION WITHIN THE DIO ACTIVITIES

General Provisions

Article 1

Object and purpose

1.1 The protection of personal data is a fundamental right governed by the European Convention on Human Rights and by the Data Protection Regulations of the Council of Europe (CoE) which refers to the principles of data protection contained in Convention 108 and its amending protocols. The aim of these Guidelines is to guide those conducting evaluations, assurance engagements (audits), consulting engagements, and investigative processes as well as to set out specific data protection safeguards relating to the processing of personal data in relation to these activities. Such processing is likely to interfere with the rights and fundamental freedoms of individuals implicated in the activities, in particular, their right to privacy.

1.2 These Guidelines aim to complement the Data Protection Regulations of the Council of Europe (the Regulations) and other provisions governing the activities of the Directorate of Internal Oversight (DIO) relating to processing of personal data and do not aim to replace them. Instead, they outline the specific needs of the DIO in the field of data protection when carrying out evaluations, assurance engagements (audits), consulting engagements, and investigative processes.

1.3 The purpose of these Guidelines is to:

- ensure that the data protection rules on the use of different means for collecting evidence are reflected in writing and that the least intrusive means are used for the collection of personal data;
- make those conducting activities involving personal data collection and elaboration fully aware of the rules which apply to the processing of sensitive information;
- help those conducting the activities outlined in these Guidelines to identify what personal data means in this context as well as the affected individuals, to determine their rights of information, access, and rectification. Consideration should be given to the fact that restrictions to these rights are allowed by the Regulations, as long as the necessity and proportionality of this decision is assessed, complied with, and documented;
- provide guidance on how to assess the appropriate competence of the data recipient (internal or external) and then limit the transfer of personal information to only what is strictly relevant and necessary;
- specify how to implement security measures based on a risk assessment analysis in order to guarantee a lawful and secure processing of personal data.

Article 2

Definitions

For the purposes of these Guidelines:

2.1 the definitions set forth in Article 2 of the Council of Europe Regulations on the Protection of Personal Data are to be considered applicable whenever a reference to such terms is made within these Guidelines;

2.2 the term “DIO” refers to the Directorate of Internal Oversight in its entirety, i.e. comprising of the evaluation, internal audit, and investigation functions, as well as its central office dealing with general administrative tasks;

2.3 the term "evaluation" means a systematic and impartial assessment of an activity, project, programme, strategy, policy, topic, theme, sector, operational area, or institutional performance, as defined in the Council of Europe Evaluation Policy;
2.4 the term "assurance engagements" means audits which consist of an objective examination of evidence for the purpose of providing independent assessment of performance, governance, risk management, and control processes of the Organisation, the nature and scope of which are determined by the Internal Audit function, as defined in the DIO Charter;

2.5 the term "consulting engagements" means advisory and related client service activities the nature and scope of which are agreed with management, intended to add value and improve the Organisation's governance, risk management, and control processes, without the Internal Audit function assuming management responsibilities, as defined in the DIO Charter;

2.6 the term "investigative process/proceeding" means a fact-finding process aimed at establishing whether fraud, corruption, or other wrongdoing. as defined in the Organisation's legal framework, has occurred;

2.7 the term "investigation subject" means any person who is a subject of an investigation for alleged wrongdoing, as defined in Organisation's legal framework.

Article 3

Scope

3.1 The present Guidelines shall apply to the processing of personal data by the DIO when performing any activity falling under the DIO's mandate. Such activities are evaluations, assurance engagements (audits), consulting engagements, investigative processes, and any administrative and support activities carried out by the DIO's central office. The DIO is committed to respecting the principles of protection of personal data enshrined in Article 4 of the Council of Europe Regulations on the Protection of Personal Data.

3.2 These Guidelines and examples provided herein are intended to be used as a practical guide for the DIO staff responsible for conducting activities falling within its remit; they should be thus viewed as advisory in nature. They do not create any substantive rights or confer, impose, or imply any new rights or obligations other than those contained in the CoE's legal framework that would be actionable in a court of law or in administrative proceedings by or against the CoE or the DIO staff responsible for conducting the respective activities.

Article 4

Legitimacy of data processing

4.1 The activities carried out by the DIO aim to protect the CoE's interests, provide independent and objective assurance to its management and Member States, and help it accomplish its objectives. To fulfil its role as set out in the DIO's Charter, the Directorate might process and access personal data with the legitimate need to carry out the necessary activities for the fulfilment of its mandate in line with the Organisation's legal framework.

4.2 The DIO shall consider, nonetheless, whether the collection of the data is necessary and proportionate on a case-by-case basis, according to the specifics of each processing of personal data.

4.3 The DIO shall ensure that any data processing is compliant with the Organisation's data protection framework. The DIO may access, request, obtain, and otherwise process data, which is already held and processed by the Organisation, where there is a legitimate need for it and respecting the above-mentioned principles of necessity and proportionality of such processing. The Organisation's legal framework explicitly provides that the DIO can have access to any information which it considers necessary and proportionate to carry out its role.

4.4 the DIO is also committed to respecting general data processing principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, and security.

Article 5

Processing of special categories of data

5.1 In consideration of the nature of the activities and the mandate of the DIO, the processing of personal data, regardless of their sensitivity, shall be carried out using additional appropriate safeguards if processed in the context of an evaluation, assurance engagement, consulting engagement, or investigative process.

Article 6

Data security

6.1 The DIO is committed, *inter alia*, to the following security measures against risks such as accidental or unauthorised access, destruction, loss, use, modification, or unauthorised disclosure of personal data:

- Clean-desk policy, i.e. removal of any sensitive information from the working environment whenever leaving the work premises for a prolonged amount of time and in any case at the end of the working day. This includes paper documents containing personal data and unprotected devices such as notebooks and USB drives.
- Lock and key policy, i.e. usage of locked closets and drawers for the storage of documents and files when outside the premises, together with locking of the doors of offices when absent for a prolonged amount of time and in any case at the end of the working day.
- Exclusive use of safe-printing mode for all documents containing personal data.
- Refraining from printing documents containing personal data, unless necessary.
- Shredding of physical files before disposal or equivalent measures to ensure non-recoverability.
- Pseudonymisation and encryption of personal data, whenever possible and appropriate.
- Avoiding removal of documents from the premises, except when authorised and/or needed for specific work-related reasons.

6.2 In addition to these commitments, the DIO shall implement the applicable policies and strive to follow guidelines and best practices issued by the Directorate of Information Technology ("DIT"), in particular:

- Clear-screen policy, i.e. use of the lock screen when leaving the workstation unattended even for a short period of time.
- Teleworking operational security indications, e.g. avoiding working on sensitive documents in public spaces and though public networks, access to the Intranet only from trusted devices and private networks, commitment to avoid unnecessary download of files and in any case deletion of such files at the earliest possible moment.
- Usage of access groups in the Data Management System, managed internally by the DIO.

6.3 Considering the need of ensuring an appropriate level of security to certain types of documents and/or information, the Investigation function may resort to additional security measures for storage, such as safes located on the Organisation's premises.

6.4 In order to fulfil the duty of notification of data breaches to the Data Protection Officer, whenever a data breach is detected by the DIO, the Director of the Internal Oversight shall be informed in writing immediately.

6.5 In the absence of any specific guidance to the contrary, the DIO staff are obliged to report data breaches brought to their attention, using the template provided in Appendix 1 to the present Guidelines (access restricted to DIO staff members only) whenever feasible. The information shall contain as a minimum a brief description of the facts relating to the personal data breach and its likely effects.

6.6 The Director of Internal Oversight shall notify the Data Protection Officer as provided for by the Regulations. After the receipt of the report mentioned in the preceding paragraph, the Director of the Internal Oversight shall decide, on a case-by-case basis and having regard to the content and nature of the breach as well as the confidentiality needs of the DIO, what data shall be included in such notification. In the same notification, the Director of the Internal Oversight may also request that the Data Protection Officer temporarily postpones the notification which is to be provided under Art. 6(5) of the Regulations to the data subjects of the breach, if reasons for that exist (e.g. if the confidentiality of an investigative process needs to be preserved or other dully justified reasons exist). If needed, the DIO should provide on request any necessary information that would enable the Data Protection Officer to form their opinion on the matter.

6.7 After the duty of notification of data breaches has been fulfilled, where feasible, the function under which the data breach occurred must provide the Director of Internal Oversight with an analysis on the causes of the data breach and suggest appropriate mitigating measures. The Director of Internal Oversight may review working methods and recommend measures to be implemented in order to prevent further data breaches. The Data Protection Officer shall be informed of mitigative measures addressing the breach in case there is a risk of repetitive occurrence.

6.8 The DIO shall maintain a Register of Data Breaches. The layout of the Register is contained in Appendix 2 to these Guidelines (access restricted to DIO staff members only).

Article 7

Transparency of data processing

7.1 The DIO shall provide the data subject, where the latter does not already have the information, with the information set out in Article 7 of the Data Protection Regulation, except where the personal data are not collected from the data subjects themselves, it proves to be impossible, involves disproportionate efforts, or is likely to render impossible or seriously impair the achievement of the objectives of the processing. Considering the nature of the activities and the mandate of the DIO, in the context of an evaluation, assurance engagement (audit), consulting engagement, and investigative processes, the DIO may need to resort to restrictions contained in Article 10 and 7(2) of the Regulations, including on the data subjects' right to information.

7.2 Such restrictions may be, for example, a delay in transmitting information to a specific data subject (in the context of an investigative process) or the fulfilment of the duty to inform only through means such as appropriate links in the email signature and mention of the data processing in the mission letters.

7.3 When feasible, the DIO will coordinate with the Data Protection Officer to ensure that the form and modalities of such restrictions are in line with the objectives and requirements of the Regulations.

Article 8

Rights of the data subject and restrictions

8.1 Every data subject whose personal data is processed by the DIO shall have the rights enshrined in Articles 7 and 8 of the Data Protection Regulations of the Council of Europe. Considering the nature of its activities, however, in the context of an evaluation, assurance engagement (audit), consulting engagement, and investigative processes, the DIO may resort to restrictions contained in Article 10 of the Data Protection Regulation.

8.2 Such restrictions may be, for example, a delay/temporary deferral in the confirmation of the data processing after a request from the specific data subject (in the context of an investigative process).

8.3 The DIO shall process any request concerning personal data on a case-by-case basis. If the request comes from an external auditor, the Data Protection Officer shall be consulted on the reply and any modalities for the provision of requested information; there might be no need for consultation if it is agreed between the Data Protection Officer and the DIO how to proceed with recurring/standard requests for information made by the CoE's External Auditors. If the request comes from a data subject, the Data Protection Officer and the Directorate of Legal Advice and Public International Law ("DLAPIL") shall be consulted before responding to the request.

8.4 The co-ordination procedure may be omitted if a standard reply procedure is agreed upon by all the relevant stakeholders for frequent and standardised requests.

8.5 The DIO shall maintain a Register of Data Access requests and follow-ups. The layout of the Register is contained in Appendix 3 to these Guidelines (access restricted to DIO staff members only).

Article 9

Additional obligations

9.1 The carrying out of data processing by a third party/processor on behalf of the DIO shall be assigned under the condition of providing adequate warranties of compliance with the level of protection set forth in the Organisation's legal framework. In this case, the legal act shall set out the main aspects relating to the processing, including the nature and purpose of the processing; its duration; type of personal data; categories of data subjects; and obligations as well as rights of the Organisation and the processor.

9.2 Every processor on behalf of the DIO shall be provided with the present Guidelines and instructed to abide by the provisions contained herein when relevant and *mutatis mutandis*. As Controller, the DIO shall maintain the sole right to impose restrictions on the data subjects' rights in the context of its activities; i.e the processor shall be informed that restrictions can only be imposed after an approval by the DIO and in accordance with the CoE's Regulations and these guidelines.

9.3 Considering the specificity of the needs and the mandate of the DIO, the structure, content and methods of accessing the records kept by the controllers under Article 9(8) of the Regulations shall be detailed and agreed upon with the Data Protection Officer.

Article 10

Restrictions

10.1 As set forth in these Guidelines, the DIO may resort to the application of restrictions to Article 7 and 8 of the Regulations provided for under Article 10.

10.2 In specific cases, resorting to restrictions might be necessary and proportional to fulfil the DIO's role, which includes the protection of important financial interests of the Organisation, as well as its accountability, transparency, and the prevention or investigation of breaches of the internal legal framework and/or applicable laws as well as the conduct of disciplinary proceedings.

10.3 In order to guarantee respect for the rights and fundamental freedoms of the data subjects, the adoption of any such measure shall require a written explanation of the reasons justifying the necessity of the measure. Nonetheless, as according to the Organisation's legal framework, investigative processes are confidential and an investigation subject shall be informed without undue delay, taking due care that the securing of evidence is not jeopardised, the notification of data subjects who might be considered as investigation subjects might, as a general principle, be postponed until found appropriate.

10.4 Restrictions cannot amount to an outright denial of the rights granted by the Regulations and the need for them shall be regularly re-assessed. In addition, as already provided in the Guidelines and pursuant to the Regulations, to the extent feasible, any restriction shall be:

- a temporary measure;
- decided on a case-by-case basis;
- applicable to one or more rights, depending on the circumstances of the case;
- imposed only after a necessity and proportionality test has been carried out by the controller;
- documented in an internal and confidential written record; and
- applied only when safeguards to prevent abuse, unlawful access, or transmission or transfer of the personal data have been implemented.

10.5 Without prejudice to the rights granted to data subjects by Article 18 of the Regulations, data subjects notified of one or more restrictions of their rights in the context of DIO activities can submit a motivated request for review. The request shall be addressed to the Director of Internal Oversight and shall be made within 30 working days from the notification. All requests shall include or make precise reference to the notification of the restriction and should include any other material (documents, statements, etc.) that may help the DIO in reconsidering and re-assessing the restriction.

Article 11

Obligations of staff members and other members of the Secretariat

11.1 In addition to the duties imposed by Article 11 of the Regulations, Secretariat members shall provide the DIO with direct and prompt access to personal data concerning Secretariat members and other persons involved in Council of Europe activities in any capacity, when necessary, proportionate, and requested to do so.

11.2 The DIO shall have the right of a timely and unrestricted access to other relevant documents as they consider necessary for the accomplishment of their tasks, pursuant to Article 12 of the DIO Charter. A refusal to comply with such a request should be duly motivated by the respective party. DIO staff shall invite the respective party to provide detailed argumentation why the processing of the information requested by the DIO would not comply with the principles of legality, necessity, proportionality and appropriateness. If necessary, the Data Protection Officer shall be requested to provide their opinion in the case of a refusal.

Article 12

Transfer of personal data to third parties

12.1 The transfer of personal data outside the Organisation to a recipient within a state's jurisdiction, to another international organisation, the EU institutions, bodies, offices, and agencies (IBOA) is subject to the requirements and safeguards set forth by article 12 (1) of the Data Protection Regulation. The notion of recipient within a state's jurisdiction includes, but it is not limited to, consultants and private donors to CoE activities.

12.2 The level of protection required by the Regulations for the transfer shall be assessed based on a list of states and international organisations, provided to the DIO by the Data Protection Officer and regularly updated. Legal provisions that might be of relevance shall also be considered, including multilateral or bilateral agreements, contracts, and memoranda. In case of a negative assessment or situation falling within the scope of Article 12(2)(2) of the Regulations, the Data Protection Officer will be consulted.

12.3 Specific consultations with the Data Protection Officer will be carried out to assess the level of protection required by the Regulations in the context of joint-evaluations and joint audits.

12.4 The referral to national authorities in the context of a preliminary assessment or an investigation may be carried out outside the safeguards, based on Article 12(3)(4) of the Data Protection Regulation and in compliance with the Organisation's legal framework. In any event, the DIO shall use the utmost care in ensuring an adequate level of protection for the rights of the data subject(s) involved.

12.5 The DIO may share certain information concerning the transfer of data which falls under Article 12(4) of the present Guidelines with the Data Protection Officer. The decision on whether to share information and the scope of the information provided shall be defined by the Director of Internal Oversight on a case-by-case basis, considering the confidential nature of some of its activities.

Article 13

Data Protection Officer

13.1 In addition to instances where an agreement with the Data Protection Officer is already mentioned in these Guidelines, the DIO shall co-ordinate and clarify with the Data Protection Officer, whenever necessary, issues related to the protection of the rights of data subjects and the treatment of personal data.

13.2 All exchanges shall be recorded in writing and registered for future reference. The layout of the Register is contained in Appendix 4 to these Guidelines (access restricted to DIO staff members only). Exchanges containing personal data shall be appropriately redacted before being recorded in case they contain data which is prohibited from being shared with people not involved in specific activities (e.g. preliminary assessments and investigations).

13.3 The DIO, in the context of its activities, may have the need to resort to interim measures regarding data protection, i.e. provisional solutions in the absence of a specific agreement or opinion provided by the Data Protection Officer. Interim solutions shall in any case consider the rights granted to the data subjects by the Regulations and the principles contained in the previous guidance received. They can be adopted when prior contact with the Data Protection Officer is not feasible or an opinion has been expected but not yet provided; they do not exempt the DIO from the obligation under Article 13 (1) of the present Guidelines.

13.4 Interim solutions in use at the moment of entry into force of the Guidelines are contained in Appendix 5 to the present Guidelines (access restricted to DIO staff members only). Other interim solutions and any update to the ones mentioned in the appendices to these Guidelines will be registered and made accessible in accordance with the modalities mentioned in Article 13 (2) of the present Guidelines.

Article 14

Entry into force

14.1 These Guidelines on the application of the Council of Europe Data Protection Regulations in the context of the Directorate of Internal Oversight activities shall be applied as of 1 January 2023.

Article 15

Transitional measures

15.1 The Director of Internal Oversight shall ensure that processing of personal data already under way on the date these Guidelines enter into force are brought into conformity with these Guidelines within a reasonable timeframe.

Appendix 1 – Note to File for the report of data breaches

DMS link to the document

DIRECTORATE OF INTERNAL OVERSIGHT

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Note
For the attention of Mr/ Mrs…….—Director of the Directorate of Internal Oversight (DIO)
Subject: Report of personal data breach

Name and surname	Description of the breach*
Job title	
Date of the discovery	
Date of reporting of the incident (DIO)	
Date of reporting to the DPO	
Data subjects involved (number/categories)	
Number of data files/records involved	
Possible reasons for the breach	
Actions taken	
Further actions (proposed/recommended/needed)	
Estimated impact of the breach	
Comments	

Documents (if applicable)

Appendix 2 – Template of the Register of data breaches

DMS link to the document

Numbe	Year	Function	Date of discovery	Director informed?	Date of reporting	DMS link to the note	DPO contacted?	Date of DPO contact	DMS link to communication with the DPO	Actions taken	Actions to be taken	Notes
1	2023	AUD	01/01/2023	Yes	01/01/2023		Yes	01/01/2023				
		EVAL		No			No					
		INV										
		Multiple										

Appendix 3 – Template of the Register of data access requests

DMS link to the document

Ref. Nb	Year	Function concerned	Date of request	Date received	Person/entity who submitted the request	DMS link to the request	Director informed	DPO contacted	Date of DPO contact	DMS links to the exchanges with the DPO	DPO's opinion (main point/s)	Actions taken	Date of reply/closure	Comments
1	2023	AUD	01/01/2023				Yes	Yes	01/01/2023					
		EVAL					No	No						
		INV												
		Multiple												

Appendix 4 – Template of the Register of exchanges with the Data Protection Officer

DMS link to the document

Summary of the question from DIO	Date of submission of the question	Summary of the answer from DPO	Date of receipt of the answer	DMS link to the exchange documents
Text	01/01/2023	Text	01/01/2023	Link
Text	01/01/2023	Text	01/01/2023	Link
Text	01/01/2023	Text	01/01/2023	Link
Text	01/01/2023	Text	01/01/2023	Link

Appendix 5 – List of current interim solutions used by DIO on 1 January 2023

DMS link to the document

Description	Solution
INV: signature used in first email contacts	Please note that information about the protection of individuals with regard to automatic processing of personal data by the Council of Europe can be found here: https://www.coe.int/en/web/data-protection/data-protection-commissioner This message and any attachments are confidential and intended for the named addressee(s) only. If you have received it in an error, please notify immediately the sender and delete the message. Any unauthorized modification, edition, or dissemination is prohibited.
EVAL: text included in the invitation to take a survey in the context of an evaluation	For any queries you may have in connection with the way your data is collected and used, please contact the Council of Europe by sending an email either to [EVAL Staff member name] at [EVAL Staff member email] or to the Council of Europe's Data Protection Officer at dpo@coe.int.