EUROPEAN COMMISSION
INTERNAL AUDIT SERVICE

PROTECTION OF YOUR PERSONAL DATA

This privacy statement provides information about
the processing and the protection of your personal data.

Processing operation: The internal audit activities

Data Controller: The Internal Audit Service Directorates A, B and C of the European Commission

Record reference: DPR-EC-00539

Table of Contents

1. Introduction

The European Commission (hereafter 'the Commission') is committed to protect your personal data and to respect your privacy. The Commission collects and further processes personal data pursuant to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (repealing Regulation (EC) No 45/2001).

This privacy statement of the Internal Audit Service (IAS) of the European Commission explains the reason for the processing of your personal data, the way the IAS collects, handles and ensures protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.

The information in relation to processing operation *"The internal audit activities"* undertaken by the IAS Directorates A, B and C is presented below.

2. Why and how do we process your personal data?

Purpose of the processing operation: The IAS collects and uses your personal information to conduct internal audit activities in accordance with Articles 117 to 123 of Regulation (EU, Euratom) 2018/1046 ('Financial Regulation'), the IAS mission Charter[1] and the respective applicable legal framework (as specified under Heading 3 below). In this respect, the IAS enjoys complete independence, full and unlimited access to all information required in the conduct of its internal audit activities in relation to all the activities and departments of the Union institution concerned, if necessary also on-the-spot access, including in Members States and third countries (Art. 118.2 of the Financial Regulation).

We advise other Commission departments, executive agencies, as well as Union decentralised agencies and other autonomous bodies receiving contributions from the Union budget on how to deal with risks, by issuing independent opinions on the quality of management and control systems and by issuing recommendations for improving the conditions of implementation of operations and promoting sound financial management.

The internal audit activities performed in the Commission and its executive agencies, and in the Union decentralised agencies and other autonomous bodies vary in form and content, ranging from assurance (including risk assessments) and consulting engagements, to reviews with a limited scope and follow-up engagements. The internal audit activities carried out by the IAS involve assessing the suitability and effectiveness of internal management systems and the performance of departments in implementing policies, programmes and actions, the efficiency and effectiveness of the internal control and audit systems applicable to each budget implementation operation. We therefore interview staff responsible for these operations, and/or conduct online survey(s) analyse underlying documentation (internal guidance, checklists, payments made, etc.) and transactions in information systems and assess the operation of the internal controls put in place by management in respect of these operations. The IAS may apply digital auditing techniques with support of analytical tools during internal audit activities allowing to perform business process analyses, for example while auditing grant or procurement processes. Analyses can include identification of the most common process path, deviations, bottlenecks, undesired process patterns, compliance issues as well as

[1] C(2022) 8450 final

exploration of concerned data more deeply, for example data quality checks, statistical analysis, crosschecking of data accuracy from different data sources, identification of control gaps and creating various visualisations. Processing of personal data does not constitute the major aim of the engagement, as the internal audit activities do not aim at investigating/inquiring particular individuals and/or conduct. Consequently, the internal audit activities do not typically target natural persons as such. However, during analysis of underlying documentation, the IAS might process personal data of natural persons in Member States, third countries and international bodies and organisations. Therefore, during the course of our activities, personal data within the meaning of Article 3(1) of Regulation (EU) 2018/1725 are inevitably processed.

Your personal data *will not* be used for an automated decision-making including profiling.

3. On what legal ground(s) do we process your personal data

Although our engagements do not target individuals as such, we may come across your personal data during the course of our internal audit activities.

We process this personal data, because of the following sub-paragraph of Article 5(1) of Regulation (EU) 2018/1725:

a) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body:

- Commission and its executive agencies on the basis of Articles 118 and 119(2) of the Financial Regulation;
- Decentralised EU Agencies and other autonomous bodies, set up under EU law that receive contributions charged to the EU budget, on the basis of Articles 70(5) and 71 of the Financial Regulation;
- European Schools, under the Service Level Agreement signed between the Internal Audit Service and the European Schools, on the basis of Article 44 of the Financial Regulation applicable to the budget of the European Schools, approved by written procedure 2017/46 by the Board of Governors;
- European Data Protection Supervisor, under the Service Level Agreement signed between the Internal Audit Service and the European Data Protection Supervisor, in line with Article 117 of the Financial Regulation;
- European External Action Service, under Article 117 of the Financial Regulation.

4. Which personal data do we collect and further process?

In performing its internal audit activities, the IAS collects the following categories of personal data: identification data, contact data, professional data and data related to or brought in connection with the subject matter of the activity.

The provision of such data is mandatory to meet a statutory requirement to which we are subject (Articles 117 to 123 of the Financial Regulation). If you do not provide this data, you may be in breach of Article 118(2) of the Financial Regulation, which allows the IAS full and unlimited access to all information required to perform its duties.

Your personal data may be obtained during our audit activities from documents we analyse and interviews we organise in the course of our engagements (minutes of meetings, transactions in

information systems, operational instructions given by or on behalf of the auditee or other types of data specific to the engagement, etc.).

In the course of its audit activities, the IAS may process special categories of personal data, pursuant to Article 10 of Regulation (EU) 2018/1725, or personal data related to criminal convictions and offences, pursuant to Article 11 of Regulation (EU) 2018/1725, only if necessary for a task carried out in the public interest and to comply with the legal obligations to which the IAS is subject under the Financial Regulation. As such, the IAS may process, for example, data required prior to recruitment such as data concerning health or criminal record in the context of an audit on recruitment by the Commission or the respective EU agency or body.

The processing of such data will not constitute the major aim of the engagement, as the internal audit activities do not aim at investigating/inquiring particular individuals and/or conduct. In addition, the processing of the data falls within the reasonable expectations of data subjects, based on their relationship with the IAS (a candidate participating in a recruitment procedure in an EU Institution or body can expect that an IAS audit on the recruitment process may involve the processing of his or her personal data). Furthermore, the risks to the fundamental rights and freedoms of data subjects, related to the processing of special categories personal data do not relate to the internal audit process, but to the activities for which they were initially collected (personal data available in recruitment files may be accessed by the IAS, but the IAS has no influence over the purpose and means of the initial processing). In addition, the IAS has put in place appropriate safeguards to protect the fundamental rights and freedoms of data subjects (confidentiality of communications, restriction of access, encryption, storage on a secure drive).

5. How long do we keep your personal data?

The IAS only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing. The IAS adheres to the Commission's e-Domec policy for electronic archiving and document management and uses the corporate IT tools to implement these rules. It also uses an audit software to document its internal audit activities. The common retention list for the European Commission files specifies the retention periods applicable to documents governed by the e-Domec policy. The administrative retention period for internal audit reports is 10 years. Audit documents and records (e.g. audit working papers) not governed by the e-Domec policy are kept for 6 years.

At the end of the administrative retention period, the files related to the internal audit activity (including personal data) are transferred to the historical archives of the Commission (in the case of audit reports) or destroyed (in the case of supporting documents, e.g. audit working papers).

6. How do we protect and safeguard your personal data?

All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored on the servers of the European Commission or of its contractors. All processing operations are carried out pursuant to the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

The Commission's contractors providing the cloud based analytical tool is bound by a specific contractual clause for any processing operations of personal data on behalf of the Commission, and by the confidentiality obligations deriving from the transposition of the General Data Protection Regulation in the EU Member States ('GDPR' Regulation (EU) 2016/679) and/or Regulation (EU) 2018/1725.

In order to protect your personal data, the Commission has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

In addition, all IAS audit staff have received the appropriate briefing on the legal provisions of Regulation (EU) 2018/1725 and are expected to respect the code of ethics of the Institute of Internal Auditors, which requires internal auditors to, inter alia, be prudent in the use and protection of information acquired in the course of their duties. Documentation stored in the audit management system is encrypted. The audit management system, the analytical tools, shared drives, collaborative platform and tools are all hosted on-premises in the EC data center.

In case of processed special categories of personal data pursuant to Article 10 of Regulation (EU) 2018/1725, or personal data related to criminal convictions and offences, pursuant to Article 11 of Regulation (EU) 2018/1725, the IAS has put additional appropriate safeguards to protect the fundamental rights and freedoms of data subjects (confidentiality of communications, restriction of access, encryption, storage on a secure drive).

7. Who has access to your personal data and to whom is it disclosed?

Access to your personal data is provided to the Commission staff responsible for carrying out this processing operation and to authorised staff according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

The Commission's contractor providing the cloud based analytical tool is bound by a specific contractual clause for any processing operations of personal data on behalf of the Commission, and by the confidentiality obligations. The core data hosting remains in the EU. Some exceptions at administrative and technical assistance level (e.g. customer support online) might occur were limited personal data might be transferred to countries outside the EU or EEA, then Standard Contractual Clauses are used by the processors and sub-processors as a basis for international data transfers as adopted in the Commission Implementing Decision (EU) 2021/3972. Special categories of personal data pursuant to Article 10 of Regulation (EU) 2018/1725, or personal data related to criminal convictions and offences, pursuant to Article 11 of Regulation (EU) 2018/1725 as well as personal data leading to directly identifiable natural person ('data subject') such as user ID's, person's name, surname, job position, job title or contact information in the context of their professional work are not processed in the cloud based analytical tool.

The output of the internal audit work is an engagement report which is delivered to the head of the organisational entity audited (i.e. a Commission Directorate-General, office or an executive agency).

Copies are made available to:

- the contact person(s), Resource Director(s)/Internal Control Coordinator(s) and other services responsible for the implementation of the recommendations;
- Head of the Cabinet(s) responsible for the IAS and the DG(s) concerned, including that of the Vice-President in charge of coordination of the relevant audited process/subject matter;
- the Audit Progress Committee;
- the European Court of Auditors;
- the Secretary-General of the Commission, the Central Financial Service, the Director-

General of DG BUDG, the Accounting Officer of the Commission and other Central Services concerned;
- OLAF, in exceptional cases where there is a suspicion of fraud or indications or findings related to systemic weaknesses or individual situations that show a potential vulnerability of EU legislation, contracts, agreements, administrative guides or practices as regards fraud, corruption or other illegal activities, in line with the administrative arrangements between the IAS and OLAF;
- DG HR/DS where there are critical and/or very important findings and recommendations on IT security, in compliance with Commission Decision (EU, Euratom) 2017/46 of January 2017 on the security of communication and information systems in the European Commission;
- the Director(s)-General of the parent DG(s) of the Executive Agency concerned;
- Further transmission of the report by the auditee within his own department is decided by the head of the organisational entity.

Dissemination of a report and additional copies are provided to whoever is entitled in accordance with the legal framework in place (i.e. to the public under Regulation 1049/2001, to the entities listed above under Articles 118(3) and 118(9) of the Financial Regulation. The working papers containing audit evidence are not transmitted.

Engagements in autonomous entities receiving contributions from the EU budget.

The output of the internal audit work is a final engagement report which is delivered to the head of the entity audited (Executive Director) and, the Chairperson of the Board (who is expected to distribute the final audit report to the members of the Board and the members of the Audit Committee, in case it exists), the contact person for the IAS appointed by the auditee, the European Court of Auditors, the Commission representative in the Board and the Accounting Officer of the Commission, if he/she is also the Accounting Officer of the Body. Transmission of this report by the auditee within his own entity is decided by its head. In exceptional cases where there is a suspicion of fraud or indications or findings related to systemic weaknesses or individual situations that show a potential vulnerability of EU legislation, contracts, agreements, administrative guides or practices as regards fraud, corruption or other illegal activities, in line with the administrative arrangements in place, the report may be made available to the European Anti-Fraud Office (OLAF). The working papers containing audit evidence are not transmitted.

The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law.

8. What are your rights and how can you exercise them?

You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access, rectify or erase your personal data and the right to restrict the processing of your personal data. Where applicable, you also have the right to object to the processing or the right to data portability.

You have the right to object to the processing of your personal data, which is lawfully carried out pursuant to Article 5(1)(a).

In order to protect our own internal audit activities, audits of public authorities of Members States, its audit tools and methods, as well of the rights of other persons related to its internal audit activities, we may, in exceptional cases and for a limited period of time, restrict data subjects' rights. Such restriction would concern the provision of information, the application of the rights to access, erasure, restriction of processing, and the communication of a data breach,

in line with Article 25(1)(c), (g) and (h) of Regulation (EU) 2018/1725. We will document each case, including an assessment of its necessity and proportionality, and we will not keep any restriction for longer than the reasons justifying it remain applicable, in accordance with Commission Decision (EU) 2018/1961 of 11 December 2018. As a general rule, you will be informed on the principal reasons for a restriction unless this information would cancel the effect of the restriction as such.

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given under Heading 9 below.

Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description (i.e. their Record reference(s) as specified under Heading 10 below) in your request.

9. Contact information

- The Data Controller

If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the Data Controller of the Internal Audit Service at: IAS-Data-Protection-Coordinator@ec.europa.eu

- The Data Protection Officer (DPO) of the Commission

You may contact the Data Protection Officer (DATA-PROTECTION-OFFICER@ec.europa.eu) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

- The European Data Protection Supervisor (EDPS)

You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.

10. Where to find more detailed information?

The Commission Data Protection Officer (DPO) publishes the register of all processing operations on personal data by the Commission, which have been documented and notified to him. You may access the register via the following link: http://ec.europa.eu/dpo-register.

This specific processing operation has been included in the DPO's public register with the following Record reference: DPR-EC-00539.