

**PRIVACY STATEMENT**  
**(Attached to the letter initiating the External Audit.**  
**The controlled entity has to internally inform all staff concerned))**

## **1. Context and Controller**

As the Commission service collects and further processes personal data in the context of financial audits, it is subject to Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

Audits and Controls cover:

1. Checks performed by Commission services on the implementation of the programme and the provisions of the grant agreements or service contracts.
2. Performance of desk controls and financial audits according to the provisions of the contracts or grant agreements with the EC.  
External audits aim at verifying whether the costs declared in the financial statements have been properly incurred and are eligible costs, as defined under the grant agreement or contract between the EC and the beneficiaries or contractors. These external audits are either directly carried out by staff of the EC ("own-resource-audits") or outsourced to external audit firms. During these audits and controls, documents that may contain personal information (such as salary slips, time-recording systems, presence sheets, credit assessment reports, etc) may be collected by the controllers as evidence of the eligibility of claims from the Community budget (such as: claims for co-financing of staff costs, travel expenses etc.). If collected, such information will be processed by the European Commission in the exercise of its duties to ensure the regular use of the Community budget in accordance with the Financial Regulation (Council Regulation (EC, Euratom) N° 1605/2002 of 25 June 2002, as amended) and Implementing Rules (Commission Regulation (EC, Euratom) N° 2342/2002 of 23 December 2002, as amended) applicable to the general budget of the European Communities.

In order to carry out efficient audits and desk controls and to detect anomalies, relevant Commission staff makes use of information available on the Internet (open source data mining). In accordance with international professional audit standards the Directorate-General has developed a multi-approach audit policy which includes a risk-analysis component in view of fraud prevention and stronger detection capabilities.

Processing operations are under the responsibility of the Head of Unit of the External Audit Unit, acting as Controller, of the Directorate General Information Society & Media.

## **2. What personal information do we collect, for what purpose, under which legal bases and through which technical means?**

## **Types of personal data**

Personal data collected and further processed are all relevant data that may be requested by the Commission with a view to verifying that the grant agreement or contract is properly managed and performed in accordance with its provisions. The indicative list of data requested is given in the annex to the letter initiating the audit, without prejudice for the EC services to ask any other relevant information as foreseen under the relevant Art. of the grant agreements or contracts.

## **Purpose**

Controls and audits of grant agreements or service contracts aim at verifying beneficiary's or contractor's or subcontractors' or third parties' compliance with the all contractual provisions (including financial provisions), in view of checking that the action and the provisions of the grant agreement or contract are being properly implemented and in view of assessing the legality and regularity of the transaction underlying the implementation of the Community budget.

## **Legal basis**

The possibility for the European Commission to carry out controls and audits is foreseen in the model grant agreement or model contract, to be signed between the EC and the beneficiary or contractor, as required by the Financial Regulation applicable to the General Budget of the European Communities (art. 170, 60.4), and its Implementing Rules (art. 47.4).

## **Technical means**

For the preparation of audit file and audit selection: use of data already existing in secured applications accessible only to relevant staff.

During the audit procedure, personal data are collected when relevant either by e-mail or on paper or as electronic files and stored in computer systems accessible only to relevant staff. Data are stored until 10 years after the final payment on condition that no contentious occurred; in this case, data will be kept until the end of the last possible legal procedure.

Data collected from open sources including information available from internet sources is kept under the same conditions as described at previous paragraph.

All data are kept under the responsibility of the Controller mentioned in point 1.

## **3. Who has access to your personal data and to whom is it disclosed?**

For the purpose detailed above, access to your personal data is given to the Commission services in charge of ex post controls and audits, without prejudice to a possible transmission to the bodies in charge of a monitoring or inspection task in

accordance with Community law (OLAF, Court of Auditor, Ombudsman, EDPS, IDOC, Internal Audit Service of the Commission).

#### **4. How do we protect and safeguard your information?**

The collected personal data and all related information are stored after closure of the desk control or audit on the premises of the Commission and on servers of a computer centre of DG Information Society & Media. The Commission premises and operations of all computer centres abide by the Commission's security decisions and provisions established by the Directorate of Security of DG HR.

#### **5. How can you verify, modify or delete your information?**

In case you wish to verify which personal data is stored on your behalf by the responsible Controller, have it modified, corrected, or deleted, please make use of the contact information mentioned below, by explicitly describing your request.

#### **6. How long do we keep your personal data?**

Data are stored until 10 years after the final payment on condition that no contentious occurred; in this case, data will be kept until the end of the last possible legal procedure.

#### **7. Contact information**

For any questions related to your rights, feel free to contact the Controller, by using the following contact information, and by explicitly specifying your request:

*Mailbox to be created*

#### **8. Recourse**

In case of conflict, complaints can be addressed to the [European Data Protection Supervisor](#) (EDPS).