ERCEA SERVICE SPECIFIC PRIVACY STATEMENT

EXTERNAL AUDIT AND EX POST CONTROLS

1. Context and Controller

As the European Research Council Executive Agency (ERCEA) services collects and further processes personal data in the context of financial audits and ex post controls, it is subject to Regulation (EU) 2018/1725. [1] Audits and ex post Controls cover:

1. Checks performed by ERCEA on the implementation of the FP7 programme and the provisions of the grant agreements or service contracts.

2. Performance of financial audits and desk controls according to the provisions of the contracts or grant agreements with the ERCEA. 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 and the beneficiaries or contractors. These external audits are either directly carried out by ERCEA staff ("own-resource-audits") or outsourced to external audit firms, acting as Processors. Very exceptionally, some external audits can be carried out jointly between the ERCEA staff and the external audit firms.

3. 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 ERCEA in the exercise of its duties to ensure the regular use of the Community budget in accordance with the Financial Regulation ("FR") (Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union Article 127, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012.

In order to carry out efficient financial audits and desk controls and to detect anomalies, relevant ERCEA staff and/or contracted external audit firms' staff make use of information available on the Internet (open source data search). In accordance with international professional audit standards the Agency has developed a multi-annual Audit Strategy which includes a risk analysis component in view of fraud prevention and detection.
Processing operations are under the responsibility of the Director of the ERCEA, represented by the Head of Unit "Audit and Ex-post controls", acting as Controller.

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

2.1 Types of personal data

[1] *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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC*

Personal data collected and further processed are all relevant data that may be requested by the Commission / ERCEA and/or contracted external audit firms 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 ERCEA services and/or contracted external audit firms to ask any other relevant information as foreseen under the relevant Article of the grant agreements or contracts.

2.2 Purpose

Financial audits and controls of grant agreements or service contracts aim at verifying beneficiary's or contractor's or subcontractors' or third parties' compliance with all the 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.

2.3 Legal basis

The possibility for the ERCEA to carry out financial audits and controls is foreseen in the FP7 model grant agreement or model contract, to be signed between the Agency and the beneficiary or contractor, as required by the Financial Regulation applicable to the General Budget of the Union (art. 132), and its Rules of Application (Art.201.2.g, art. 129).

2.4 Technical means

For the preparation of audit files and audit selection: use of data already existing in ERCEA 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 the last possible legal procedure.
Data collected from open sources including information available from internet sources is kept under the same time conditions as mentioned above.

3. Storage and retention

All data are kept under the responsibility of the Controller mentioned in point 1.
Contractors (contracted external audit firms) are contractually obliged to keep all working material related to audits during the whole duration of the framework contract plus two years after the end of the framework contract. ERCEA staff members in charge of audits give instructions concerning the deletion of personal data after this retention time.

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

4. 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 services in charge of ex post audits and controls and/or contracted external audit firms, if applicable, without prejudice to a possible transmission to the authorizing officer responsible for the project and to the bodies in charge of monitoring or inspection tasks in accordance with Community law (OLAF, Court of Auditors, Ombudsman, EDPS, IDOC, Internal Audit Service of the Commission and ERCEA).

5. 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 ERCEA and on local servers of the ERCEA. During the audit, documents are also stored at the Contractor's premises and on their local servers.

The Commission and ERCEA premises and operations of all servers abide by the Commission's security decisions and provisions established by the Directorate of Security of DG HR establishes the regulatory framework and overall information source for all IT and non-IT security related matters and their management in the ERCEA within the context of the corporate policies set in the Commission. ERCEA staff members in charge of audits give instructions to the contracted external audit firms concerning processing of personal data security measures.

6. 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.

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: ERC-C4-SECRETARIAT@ec.europa.eu.
For any clarification on your rights under the data protection Regulation (EU) 2018/1725, please contact the ERCEA Data Protection Officer: ERC-DATA-PROTECTION@ec.europa.eu.

8. Recourse
In case of conflict, complaints can be sent to the European Data Protection Supervisor (EDPS).