

Privacy Statement for Legal Entity and Bank Account Validation

In line with Article [63 of the rules of application of the Financial Regulation](#), the departments of the Commission's Accounting Officer will collect your personal data in a common file and record them in the Commission's accounting system only to the extent necessary to process and account for financial and contractual relations you have or will have, directly or indirectly, with the Commission.

The system of accounts is linked to:

- the early warning system (EWS) operated by the Commission on the basis of the [Articles 30 and 32](#) of the Financial Regulation on sound financial management and [Commission Decision 2008/969/EC, Euratom](#) on the early warning system for the use of authorising officers of the Commission and the executive agencies
- the central exclusion database operated by the Commission on the basis of Article [108 of the Financial Regulation](#) and [Commission Regulation EC/Euratom 1302/2008](#).

See also: [Protecting EU interests – Early Warning System and Central Exclusion Database](#), Privacy Statement of OLAF (European Anti-Fraud Office) [OLAF DPO-17.2](#) - [OLAF DPO 159](#) - [OLAF DPO 160](#) and [Privacy Statement for the central exclusion database](#) — available in EN only.

The EWS provides information on identified risks relating to potential and successful contract tenderers and grant beneficiaries via a system of 'flags' indicating the level of risk. Categories W1 to W4 are intended to encourage managers to reinforce monitoring of the contract or grant in question while category W5 indicates that the entity concerned has been excluded under Article [106\(1\)](#), [109](#) or [131](#) of the Financial Regulation (W5a) or under the Common Foreign & Security Policy Council Decisions (W5b). Data recorded in the W5 category are exported into the central exclusion database.

Who has access to or receives your information?

All authorised Commission, European External Action Service, consultative bodies and agencies users dealing with financial and accounting matters have access to your data, which may also be sent to the Internal Audit Service, the Court of Auditors, the Financial Irregularities Panel, the Anti-fraud Office and any other institution or entity responsible for audits or investigations. As the Commission uses the SWIFT network to make payments, your bank particulars will also be sent to this company whenever a payment is made in your favour.

In accordance with [Article 108 of the Financial Regulation](#), authorities and entities managing EU funds or the European Development Fund have access to information on situations justifying exclusion provided that those authorities and entities comply with the EU legislation on the protection of personal data.

How do we protect and safeguard your information?

The data collected in the Commission's accounts can be accessed by designated officials and staff of the Commission, consultative bodies and agencies, using a user ID and password. A Service Level Agreement with the organisational entities charged with operational execution of the budget ensures a level of confidentiality and technical and organisational security that complies with data protection law.

How can you check or amend your information?

You have no direct access to your personal data stored by the Commission. If you wish to check or amend any of your personal data, exercising your rights under Section 5 of Regulation (EC) No 45/2001

on the protection of personal data and the processing thereof, please write to your contact person in the institutions or agencies of the European Union. You can also write to the Commission's data protection officer (DATA-PROTECTION-OFFICER@ec.europa.eu) if you have any difficulties or questions regarding the processing of your data.

Please note that recorded data is only amended on compelling grounds supported by documentary proof.

How long do we keep your data?

To provide an audit trail and allow queries on past payments at all times, no recorded data are deleted from the accounts. The forms and documents you submit are archived electronically. The data recorded under the early warning system are rendered invisible to users of the system of accounts as soon as the corresponding warnings are deactivated. The personal data of natural persons are rendered illegible five years after deactivation.

Recourse

In case of disagreement with the Controller or data protection officer concerning the processing of your personal data, you have the right to submit a complaint at any time to the [European Data Protection Supervisor](#).