



## **INFORMATION NOTICE ON THE PROTECTION OF PERSONAL DATA**

Everyone has the right to the protection of personal data.

The processing of personal data by the institutions, bodies, offices and agencies of the European Union is governed by Regulation (EU) 2018/1725 (OJ 2018 L 295, p. 39).

This notice explains how and why your data are used in the context of the processing operation concerned.

### **PROCESSING IN SAP IN THE CONTEXT OF BUDGETARY AND FINANCIAL MANAGEMENT**

#### **Who is the data controller?**

The data controller is the Directorate for the Budget and Financial Affairs.

#### **Why do we need your data?**

Personal data are used solely for the performance of legal and contractual obligations relating to financial processes, as defined by the applicable legislation.

The SAP integrated system is used for budget implementation and associated processing and financial transactions.

The system manages the following processes:

- management and budget accounting,
- management and financial accounting,
- management and fixed asset accounting,
- management of banking operations,
- payments,
- inventory management,
- cost accounting,
- management of public procurement procedures,
- contract and purchasing management,



- management of receipts for goods received and services provided,
- production of statistics of financial operations carried out,
- production of financial reports.

In order for the processes listed above to be executed in accordance with the Financial Regulation and legal obligations, personal data of the following persons must be recorded:

- designated natural persons involved in financial or contractual relationships with the Court;
- natural persons designated as representatives or acting on behalf of economic operators and contractors in the context of public procurement procedures and contracts;
- designated members of the Court's staff using the SAP system to perform tasks associated with financial transactions, such as the initiation, recording, updating, verification and approval of transactions in the system, including participation in the electronic workflows which are mandatory for the performance of their duties;
- named natural persons involved as authors or contributors in the development and adjustment of the SAP software.

The activities of all SAP users are recorded in the technical security logs which may be used solely for the purposes of verification and investigation in the event of suspicious activity in the system or if there are doubts as to the authenticity of the data. The data linked to operations initiated and changes made are recorded in the audit logs, which enable the source of changes made to the data or to financial documents to be documented, and financial operations and their chronology to be verified.

If you are a developer or contributor, your name or identifier associated with changes to the source code, customisation of modifications, and design documentation may be used for technical verification for 10 years after implementation, and to document the fact that you are their author if rights are applicable.

This notice summarises the part of the processing of personal data that is carried out technically within the SAP system. The data protection files and associated privacy statements for the full processing of personal data required for the relevant financial processes are documented separately in the following information notices:



- legal entities information notice,
- public contracts information notice,
- EDES information notice,
- ex ante and ex post verification information notice.

### **How did we obtain your data?**

Certain data have been obtained directly from you for the purposes of managing the various processes set out above. Only data that you have been asked to provide strictly for the purposes of these processes are recorded in our SAP system databases.

We have obtained your data via:

- the information sheet that you sent us if you require payment from the Court;
- the documents which you sent in connection with tender procedures;
- the documents requesting access to the SAP system that you sent if you require access to the system.

Other data are recorded automatically by the SAP system to make up the security and audit logs which ensure that all operations carried out in the SAP system are traceable.



Categories of data subject and categories of personal data processed.

Category	Information relating to data subject	Origin
Legal entity	Name, address, email, VAT number, bank account(s), holder(s) of the account(s), supporting documentation relating thereto.	Sent by the representative of the entity
	Framework contracts, specific contracts setting out the services, goods, quantities ordered, prices and other features of the order, documents relating thereto (bids, ...).	Recorded by the Court
	Receipt of goods received and services provided, delivery documentation.	Recorded by the Court
	Invoices or equivalent payment demands received from a third party, payments received, documents annexed.	Sent by the representative of the entity
	Debit notes issued, payments made, payments received, other accounting operations linked to the legal management of accounts.	Recorded by the Court
Economic operator	Name, address, email, VAT number.	Sent by the representative of the operator
	Procurement procedures and lots, information on non-exclusion, technical and financial capacity, and characteristics of the bid.	Sent by the representative of the operator
	Evaluation of the bid and acceptance or rejection.	Recorded by the Court
Natural person representing a legal person or an economic operator (point of contact, employee, delivery person, etc.)	Name, professional contact details (email, telephone), employer, position.	Recorded by the Court



Staff	Name, bank account(s), holder(s) of the account(s), supporting documentation relating thereto.	Sent by the person
	Identifier, NUP (unique payroll number) and department to which the individual is assigned.	Recorded by the Court
	IT equipment provided (laptop, mobile telephone, ...).	Recorded by the Court
	Mission expenses.	Sent by the person
	Calculation of salaries and allowances.	Drawn up by the Court
	Request for advance payment, payment made to the person, payment received from the person, other accounting operations linked to the legal management of accounts.	Recorded by the Court
Users (staff or similar)	Identifier, name, department, roles and authorisations in the system, roles in the financial circuit, email address, office number and telephone number.	Recorded by the Court on the basis of the SAP access request made
	Contract award procedures and lots in which the user serves as a member of the evaluation committee.	Recorded by the Court
Developers (internal or external)	Same information as users of a service provider or staff users	Recorded by the Court;
	+ changes made in the configuration, source code of the software created or modified in the system, transport orders linked to that change, with timestamps.	Recorded automatically by the system.
	Name or initials of the author/contributor in the preparatory design documents within the meaning of Directive 2009/24/EC, which are kept outside the SAP system.	
Any SAP user	Any financial file created by the user, with the timestamp of the action; any financial file or any value modified by the user with the timestamp of the modification; any financial file approved by the user with the timestamp of approval.	Recorded automatically by the system
	Security log: user ID, network ID of the user's workstation; name of the transaction or of the report launched (including connection transactions), timestamp of the operation.	Recorded automatically by the system

In addition, the system may store names or other data that could potentially identify natural persons in a free text field, either following data entry by members of the



Court's staff, or following automatic transmission from third parties (via electronic invoice or bank account extracts). This potential personal information cannot be processed automatically and is not generally sufficient to identify a natural person clearly and unambiguously.

Personal information and data included in invoices, fee notes or any other form of payment demand, as well as those set out in the documents sent to us that are annexed to those payment demands, are not recorded in the databases. However, all documents received are stored in the SAP system in digital format and are annexed to the financial transactions to which they refer.

Statistical summaries enabling budget and financial activity reports to be drawn up in respect of the various authorising services of the Court are extracted from the SAP system on the basis of operations carried out by those involved in the financial circuit.

### **Who has access to your data?**

Those involved in finance at the Court of Justice (originating agents, verification agents, authorising officers), the accounting officer and other members of staff involved in handling financial processes, as well as the auditors of the Court of Justice and of the European Court of Auditors within the framework of the task entrusted to it by Article 287 TFEU.

If you are a user of the SAP system, IT security experts and investigators may access the audit and security logs in order to check system security and security of user accounts.

A limited number of individuals involved in technical management and system support (support team within the Financial Directorate, SAP consultants, database administrators, network engineers) may access some or all of those data, but only in connection with their technical support tasks; they are not authorised to extract or to use the data for other purposes.

Your data are not transferred to third countries or to other international institutions.



### **How long are your data stored for?**

In accordance with the document storage periods adopted by the Institution, personal data, whether in paper or in electronic form, are stored for a period of 10 years from the 1st of January following the year in which the last financial transaction with you was concluded.

Paper or electronic files are deleted in the year following the end of the storage period.

The security log is stored for two years after the year in which the user's action was recorded.

In both cases, depending on the planning constraints of the data storage management programme, the data may be stored for a further year.

### **What are your rights?**

In accordance with the applicable rules, you have the right to request from the data controller access to your data and, if necessary, rectification or erasure of your data or restriction of processing.

You are also entitled to object to the processing of your data on grounds relating to your particular situation.

### **How do you exercise your rights? Whom to contact?**

You can contact the data controller, the Court of Justice of the European Union, as follows:

Contact / [dataprotection\\_finance@curia.europa.eu](mailto:dataprotection_finance@curia.europa.eu)

Postal address:                      Court of Justice of the European Union  
Directorate for the Budget and Financial Affairs  
Accounting Unit  
Rue du Fort Niedergrünwald  
L-2925 Luxembourg

We will respond to your request as soon as possible and, in principle, within one month. That period may be extended if necessary.



You can also contact the Data Protection Officer of the Court of Justice of the European Union:

[Contact](#) / [DataProtectionOfficer@Curia.europa.eu](mailto:DataProtectionOfficer@Curia.europa.eu)

### **European Data Protection Supervisor**

You have the right to lodge a complaint with the European Data Protection Supervisor if you consider that the processing of personal data concerning you does not comply with Regulation 2018/1725.