

# Data protection guide for beneficiaries in the EU programmes Erasmus+ and European Solidarity Corps (ESC)

The protection of personal data has become increasingly important in recent years. The sensitive handling of personal data also plays an important role in the current programme generation of Erasmus+ and the European Solidarity Corps. The respective principles are laid down in the EU data protection regulation 2018/1725 of the European Commission, which is mentioned in all grant agreements.

As a beneficiary, you are obliged to take over the role of a "processor" when handling personal data in Erasmus+ and the ESC. This results in the following obligations when implementing your projects: ensuring technical and organizational measures to protect all personal data, notifying participants about how their personal data are being processed, and maintaining documentation of all processing activities.

The European Commission has published the following guidelines to help you better understand the data protection obligations as a beneficiary. The first part explains what it means to be a processor in Erasmus+ and ESC projects. The second part contains a security checklist with the most important measures to ensure the protection of personal data. The third part describes the main actors in the processing of personal data in Erasmus+ and the ESC programmes. And the fourth part provides a template for the documentation of your processing activities.

Please adhere to the following guidelines during the implementation of your projects.

## Index

- Part I: Duties and Responsibilities of the Processor
- Part II: Security Checklist for the Protection of Personal Data
- Part III: Main Actors in the Processing of Personal Data
- Part IV: Template for the Record of Categories of Processing Activities

## Part I: What does being a processor in Erasmus+ and European Solidarity Corps programmes mean for the beneficiary?

- 1. Acting on instructions:** you can only process the personal data fulfilling the purposes described in the privacy statement available at <https://webgate.ec.europa.eu/erasmus-esc/index/privacy-statement>. If you process the data for your purposes, you will step outside your role as a processor and become a controller for that processing. A description of the main actors is provided on the following pages of this document.
- 2. Bound by a contract:** you have a grant agreement with the Erasmus+ or European Solidarity Corps National Agency which describes your obligations of a processor. This contract sets the legal framework for your role as a processor, in line with Regulation 2018/1725 explaining the obligations of the processor in Article 29.
- 3. Use of sub-processors:** you must not engage another processor without prior written authorisation from the controller. Please contact the data controller for more information on this topic. You can find the controller's contact details in the privacy notice. Please keep your National Agency in copy of this communication.
- 4. Applying data security:** you must implement technical and organisational measures that are appropriate to the risk of the processing to ensure the security of personal data, including protection against accidental or unlawful destruction or loss, alteration, unauthorised disclosure, or access. (See the security checklist below).
- 5. Notifying of personal data breaches:** You must notify the controller without undue delay if you become aware of a personal data breach. You must also assist the controller in complying with its obligations regarding personal data breaches - providing all necessary information about the breach, steps already taken to contain the breach, and assessing the likely consequences to the data subjects. You can find the controller's contact details in the privacy notice. Please keep your National Agency in copy of this communication.
- 6. Notifying of potential data protection infringements:** you must notify the controller immediately if the purposes and means of processing would lead to a breach of the Regulation (EU) 2018/1725 or local data protection laws.
- 7. Being accountable:** you must comply with accountability obligations, such as creating and implementing data protection policies (policies standardising the use, monitoring, and management of personal data in your organisation), maintaining documentation of your processing activities (see an example of a template for the record of categories of processing activities attached).

8. **Restricting international transfers:** the data protection regulation sets very strict rules on transferring personal data to 3rd countries. You must ensure that the controller authorised any transfer outside the EU/EEA beyond the transfers defined in the grant agreement with the Erasmus+ or European Solidarity Corps National Agency and the transfer complies with the regulation provisions on international data transfers. This concerns situations when you directly transfer data without the support of the European Commission IT tools towards other organisations outside EU/EEA or when you give access to such organisations in the IT tools of the European Commission. Please contact the data controller for more information on this topic. You can find the controller's contact details in the privacy notice. Please keep your National Agency in copy of this communication.

## Part II: Security checklist

- **We understand the requirements of confidentiality, integrity, availability and resilience** for systems and services where the data is being processed.
  - **Confidentiality** is similar to privacy. Confidentiality measures are designed to prevent sensitive information from unauthorised access attempts.
  - **Integrity** involves maintaining data's consistency, accuracy, and trustworthiness over its entire lifecycle. Data must not be changed in transit, and you must take steps to ensure data cannot be altered by unauthorised people (for example, in a breach of confidentiality).
  - **Availability** means information should be consistently and readily accessible to authorised parties. This requirement means appropriately maintaining hardware and technical infrastructure and systems that hold and display the data.
  - **Resilience** refers to your organisation's ability to continue operating during a disruption and its ability to restore its systems to an effective state in a “timely manner”.
- **We know who has access to the data under our control**, and we regularly check the list of authorised persons – this applies to both the European Commission-provided IT tools as well as IT tools used by ourselves. The persons are under an appropriate statutory obligation of confidentiality.
- **We transmit the data only via secure transmission protocols** (for example, secure Internet browser connections, but not email – unless encrypted).
- **We store data in secure locations** when we export the data from the European Commission IT tools, ensuring only authorised personnel have access (good examples: local drive of a password-protected computer, network drive (file server) with access control; bad examples: local drive of a publicly available computer, a USB drive, cloud storage – unless your organisation security policy

allows it).

- **We are aware of the limited data retention period** and stop processing personal data related to the purposes defined in the privacy statement outside of the IT tools provided by the European Commission once the period is over.

### Part III: Who are the main actors in the processing of personal data in Erasmus+ and European Solidarity Corps programmes?

For the processing activities defined in the privacy statement available at <https://webgate.ec.europa.eu/erasmus-esc/index/privacy-statement>:

1. The European Commission, Directorate-General for Education and Culture acts as **data controller**.
2. The Erasmus+ and European Solidarity Corps National Agencies act as **processors**.
3. Organisations and individuals signing and taking over the rights and obligations stemming from the grant agreement with the Erasmus+ and European Solidarity Corps National Agencies take over the role of processors (also called sub-processors).

### Part IV: Template for the Record of categories of processing activities

In accordance with Article 31 (2) of the Data Protection Regulation (EU) 2018/1725, every beneficiary is obliged to maintain a record of all processing activities when handling personal data in Erasmus+ and ESC. All processing operations shall be documented in this record. Here you can find a template that fulfils the requirements of the regulation: [Template for the record of categories of processing activities](#)