

# Personal data protection policy

---

## What are personal data

There is a broad legal definition of personal data.

Any information relating to an identified or identifiable person is considered personal data (for a full definition see Article 2 paragraph a) of [Regulation \(EC\) No 45/2001](#) (pdf 234KB). It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be “personal data”.

The categories of personal data are broadly drawn so that, for example personal data are considered to be telephone numbers, addresses, financial information, photographs, satellite images, car registrations, ID numbers, e-mail addresses, health records, etc.

Personal data can be contained in computer files (e.g. in databases, on the Internet or other closed networks) or in paper records. Data protection is a fundamental right, protected not only by national legislation, but also by European Law.

---

## Legal basis

The legal basis for data protection is Regulation (EC) No 45/2001.

This regulation aims to protect the liberties and fundamental rights of individuals and in particular their right to privacy with respect to the processing of personal data about them.

It only applies within the institutions and bodies set up by, or on the basis of, the Treaties establishing the European Communities. The legal basis for data protection concerning the general public is not ruled by this Regulation.

The Regulation applies to the processing of personal data by all Community institutions and

bodies, insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law (Article 3.2.)

---

## Legal background

- 1 | Charter of Fundamental Rights of the EU - Article 8
  - 2 | Treaty establishing the European Community - Article 286
- 

## Collection of personal data by EIGE

A number of EIGE's activities involve the collection and processing of personal data, for instance as part of the recruitment procedures, or collection of data for salaries or reimbursements, contractual arrangements with suppliers or organization of events, etc.

It shall be noted that collecting and processing of personal data and its subsequent utilization should be done "fairly and lawfully" (Article 4 paragraph 1a).

---

## Purpose of the collection

Whenever personal data are requested, it is essential that the data subject (the person whose personal data are collected, held or processed) knows for what purposes the data is being collected. According to the Article 4 Paragraph 1b of the Regulation, personal data "must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."

Moreover, personal data must be adequate, relevant, and not excessive in relation to the purpose and kept for no longer than is necessary for the purposes for which they were collected.

---

## Rights of data subjects

When personal data are requested, data subjects have the right

- to be informed of the processing operations (Articles 11 and 12)
  - to access, rectify, block or erase the data (Articles 13-16)
  - to object to the processing on compelling legitimate grounds (Article 18)
  - to compensation for any damage (Article 32)
- 

## Other principles

- 1 Processing of personal data is only lawful, if the purpose(s) is legitimate and if it is necessary either:
  - for the performance of a task carried out in the public interest or in the legitimate exercise of official authority (Article 5(a))
  - for compliance with a legal obligation (Article 5(b))
  - for the performance of a contract to which the data subject is party (Article 5(c))
  - if the data subject has unambiguously given his or her consent (Article 5(d))
  - in order to protect the vital interests of the data subject (Article 5(e)).
- 2 The Data Controller (i.e. the person who is responsible for the processing operation) must ensure that all provisions of the Regulation (EC) 45/2001 are complied with.
- 3 According to the principles of confidentiality and security, only those people who need access shall have it. By analogy:
  - access to basic personal data shall be limited to staff who need it for their work (such as security guards).
  - access to a staff evaluation report should be limited to the particular employee in question, as well as to a restricted number of people in the human resources department.
- 4 Sensitive data, such as medical files or an arrest warrant shall be treated even more carefully (Article 10). The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with even greater care than other personal data.
- 5 Personal data should in general be transferred neither internally nor externally, unless it is necessary for the legitimate performance of tasks covered by the competence of the recipient – the necessity of the transfer must be evaluated. In certain cases data subjects

must be informed of the transfer.

- 6 Unauthorized access to personal data should be prevented by ensuring appropriate safeguards, both:
- in terms of barriers that secure the system technically and logistically
  - by selecting a limited and appropriate number of people who have authorized access

---

## The main players

Besides the data subject, there are three main data protection players:

The [European Data Protection Supervisor](#) (EDPS) is responsible for the monitoring of Community institutions and bodies on their compliance with data protection rules, in particular to ensure that the fundamental rights and freedoms of natural persons, especially their right to privacy, are respected by the Community institutions and bodies. The EDPS is an independent supervisory authority.

The **Data Protection Officer** (DPO) ensures that data controllers and individuals know their rights and obligations, co-operates with the EDPS, ensures internal application of the regulations and keeps a register of processing operations notified by the controllers. EIGE has one designated DPO, who can be contacted via e-mail at: [dpo@eige.europa.eu](mailto:dpo@eige.europa.eu)

The **Data Controller** is the person who determines how personal data is processed, and is the person that grants the rights to the data subject. For each processing operation, a Data Controller must be identified and prior notice must be given to the DPO of the institution.

---

## Who should you contact for more information about the processing of your personal data by the Institute?

If you feel that your personal data are being misused by the Institute, or their processing by the Institute is otherwise not compliant with Regulation (EC) No 45/2001, you should first notify the Data Controller for the processing in question and ask him or her to take action.

You may also contact the Institute's DPO at [dpo@eige.europa.eu](mailto:dpo@eige.europa.eu) to inform him or her of any issues related to the processing of your data.

If the problem cannot be solved this way, you may lodge a complaint with the EDPS. The EDPS is empowered to hear and investigate complaints and to conduct inquiries, including on his or her own initiative. If a breach of data protection rules is found to have occurred, the EDPS may exercise the powers assigned to him or her under Article 47 of Regulation (EC) No 45/2001.

---

## User Privacy

EIGE is committed to user privacy. The policy on 'protection of individuals with regard to the processing of personal data by the Community institutions' is based on Regulation (EC) No. 45/2001. This general policy covers the European Union's family of institutional websites, within the 'europa.eu' domain.

Although you can browse through EIGE's web pages without giving any information about yourself, in some cases, personal information is required in order to provide the e-services you request.

Web pages that require such information treat it according to the policy described in the Regulation mentioned above and provide information about the use of your data in their specific privacy policy statements.

The European Union's family of institutional websites, within the 'europa.eu' domain, provides links to third party sites. Since we do not control them, we encourage you to review their privacy policies.

---

## Further information on specific data protection operations

[Protection of personal data in relation to procurement procedures and contract management \(.pdf\)](#) →

[Protection of personal data in relation to the organisation of events \(.pdf\)](#) →

[Protection of personal data in relation to EIGE's contacts relationship management \(CRM\) and newsletter \(.pdf\)](#) →

[Protection of personal data in relation to the procedure applicable to the use and selection of outside experts Art.204 of the Financial Regulation \(FR\) and the 287 of the Rules of Application \(RA\) \(.pdf\)](#) →

