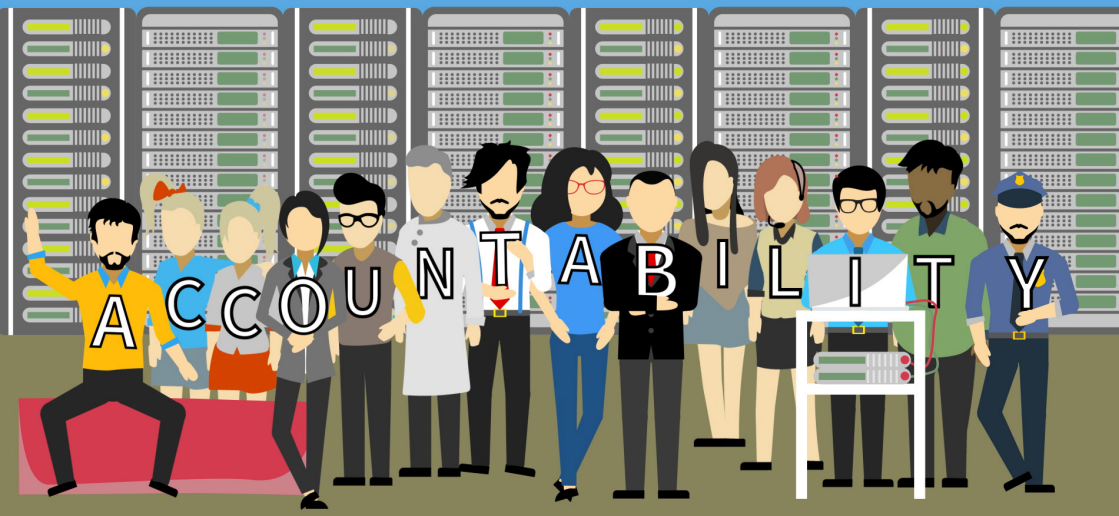
EDPS

New data protection rules for EU institutions and how they affect YOU



The way your institution deals with personal data has changed. These changes, introduced under the revised rules on data protection in the EU institutions, will affect you:

1 when you process personal data as part of your work at an EU institution;

2 when you draft legislative proposals, implementing or delegated acts (or international agreements) which might involve the processing of personal data;

3 when your EU institution processes your own personal data, in relation to recruitment, appraisal or sick leave, for example.

EU Data Protection rules:
accountability and transparency

The processing of personal data should be designed to serve mankind
(recital 4 of the General Data Protection Regulation - GDPR)

Personal data protection is about people. It is a fundamental right. The new rules give people more control over their personal data. They are designed to ensure that personal information is protected, no matter where it is sent, processed or stored.

The reform places the emphasis on **accountability**. This means that it is now the responsibility of your institution to comply with data protection rules *and* to be able to demonstrate this compliance. It follows that data protection is now everybody's business, independent of your place in the EU hierarchy.

Each EU institution, body and agency has a Data Protection Officer (DPO). Your DPO is your internal ally and can act as an adviser on data protection issues. If you want to avoid potential pitfalls, try to involve your DPO early on whenever you plan to work with personal data.

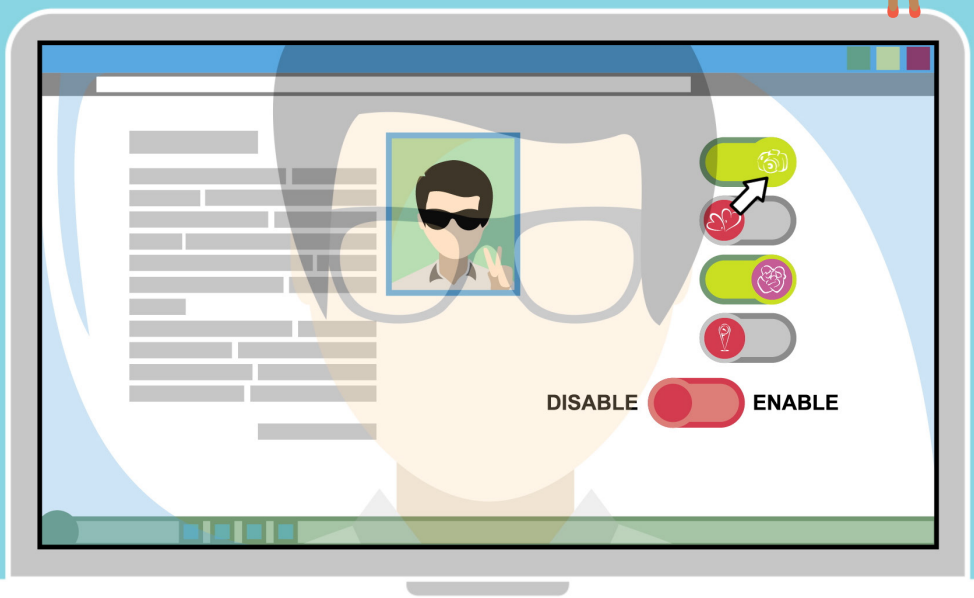
How the new rules affect you - Think data protection!

Stronger rights for individuals

Before you collect any personal data, use a data protection notice to inform people about how your institution intends to process their personal data. Individuals have the right to request access to their own personal data and to receive a copy of any personal data being processed by your institution. They also have the right to have their personal data rectified and, in some cases, deleted. The new right to data portability allows people to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

Ensure compliance and document it

Identify the processing operations under your responsibility and inform your DPO. Keep a written record of why and how your institution processes personal data.



Think data protection from the outset - *data protection by design and by default*

Embed data protection into your manuals, procedures and all processing operations before you begin to process personal data. You need to ensure the effective implementation of data protection principles whenever the operation is performed. Relevant principles include fair and lawful processing, data minimisation, limited conservation periods and appropriate security measures. Ask your DPO for advice from the outset. Periodically review the technical and organisational measures in place while the processing operation remains in use. Your DPO can also help you to identify the processing operations that require a Data Protection Impact Assessment and provide you with information on how to carry it out.

Risk-based assessment

Assess the risks that each of your processing operations may pose to the rights and freedoms of the individuals concerned and choose appropriate safeguards.

Data Protection Impact Assessments (DPIAs)

In some cases, you will have to carry out a formal DPIA, analysing the risks caused by your planned processing operations in more detail, choosing controls and documenting them. This is the case for large-scale processing of sensitive data, such as medical data, for example.

Outsourcing, procurement, SLAs and MoUs

Your institution is also responsible for any processing of personal data carried out on its behalf by external parties or contractors. Identify the risks of the processing operation, include data protection requirements from the drafting stage of the call for tender, choose appropriate contractors and include **contractual data protection clauses**. Similar considerations apply when you share a processing operation with one or several EU institutions, through a Service Level Agreement or a Memorandum of Understanding. Revise your existing contracts and update them to reflect the new obligations.

Transferring data to countries outside the EU

Transfers of personal data to countries outside the EU and the European Economic Area are only allowed on the basis of an adequacy decision, issued by the Commission, or if appropriate safeguards are implemented, such as specific contractual clauses.

The DPO: your internal ally and adviser

While the institution and all members of staff are responsible for respecting data protection rules, every institution must also appoint a Data Protection Officer (DPO). The DPO works as an independent internal adviser to all staff working at the institution. They are also the point of contact should any individual wish to exercise their data protection rights or make a complaint, and can launch investigations into data protection issues at their EU institution.

Detect and report personal data breaches

As soon as you become aware that a personal data breach has occurred, inform your institution's hierarchy! Your institution must inform the DPO, assess the incident and mitigate its impact. Most personal data breaches must also be reported to the EDPS no later than 72 hours after your institution becomes aware of the breach. Data breaches might include theft of personal data, loss of a USB key containing names or accidental publication of internal staff directories.

Liability and penalties

Failure to comply with data protection rules may result in disciplinary sanctions for EU staff members. If you suffer from material or non-material damage because of an infringement of personal data protection rules, you have the right to receive compensation from your institution. The EDPS may exercise corrective powers, such as a warning or a ban on processing. The EDPS will also be able to fine EU institutions (up to €500 000 per year).


ensure compliance
implement safeguards
demonstrate
safeguards are effective
verify compliance
measure compliance

Personal data means any information relating to an identifiable (directly or indirectly) **natural person**. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Examples: name, e-mail address, annual appraisal file and medical health records, but also indirectly identifiable information such as a personnel number, IP address, connection logs, fax number, biometrics etc.

Processing refers to any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Examples: recruitment procedure, grant award procedure, list of external experts, managing an event, publication of pictures, creating a collaborative online platform for citizens or staff members.

Processing also occurs in situations where European institutions provide Member States with a technical tool or solution to facilitate information exchange, while retaining access to the personal data concerned or keeping a register of connection logs relating to the platform.

To learn more about the new data protection rules read our other factsheets:

- **The GDPR for EU institutions: your rights in the digital era**
- **New data protection rules for EU institutions and how they affect YOU**

or consult the EDPS website: **www.edps.europa.eu**

This factsheet is issued by the European Data Protection Supervisor (EDPS) - an independent EU authority established in 2004 to:

- monitor the processing of personal data by EU institutions and bodies;
- give advice on data protection legislation;
- cooperate with similar authorities to ensure consistent data protection.

www.edps.europa.eu


@EU_EDPS


EDPS


European Data Protection Supervisor