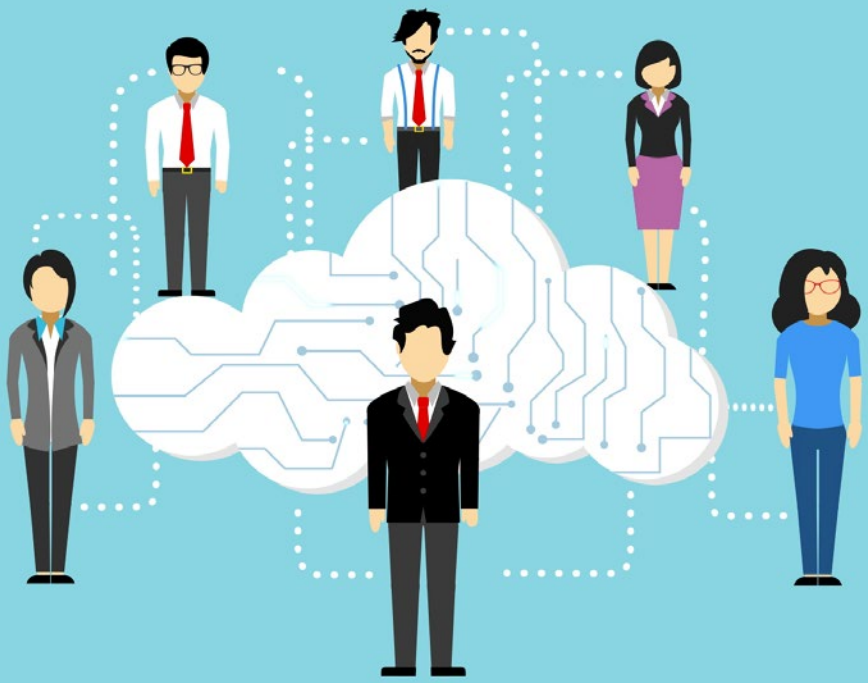
EDPS



Documenting data processing: The EDPS guide to ensuring accountability

Luxembourg: Publications Office of the European Union, 2019

© European Union, 2019

Reproduction is authorised provided the source is acknowledged.

Print ISBN 978-92-9242-396-4 doi:10.2804/58624 QT-04-19-045-EN-C
PDF ISBN 978-92-9242-397-1 doi:10.2804/717377 QT-04-19-045-EN-N



Accountability on the ground

Unlawful data processing can have serious implications for the lives and rights of the individuals whose data we process. For this reason, the principle of accountability, which involves demonstrating data protection compliance, must be at the core of every data processing activity we carry out.

The EU institutions, bodies and agencies must comply with certain rules when processing personal data.

If you are responsible for processing personal data on behalf of your EU institution, you are accountable for *what* you do, *why* you do it and *the way* you do it. This means that you need to make sure that you not only comply with data protection laws, but that you can demonstrate this compliance.

One way to demonstrate compliance is to document all processing operations which take place in your EU institution. Depending on the level of risk a processing activity might pose to the individual concerned, you will have to complete one or more of the following documentation requirements:

- **For all processing operations:** Compliance check and processing record
- **For *high risk* processing operations:** Data protection impact assessment (DPIA)
- **For *high residual risk* processing operations and processing operations listed under Art. 40(4) of the Regulation:** Prior consultation

The EDPS' *Accountability on the ground* toolkit will guide you through this process.

What are records?

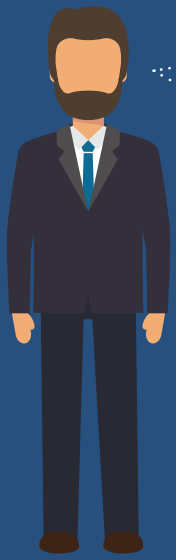


A record is the basic documentation needed for all your processing operations. All records feed into a central register kept by your EU institution, and are usually managed by the institution's *Data Protection Officer* (DPO). It is important to remember that, though the DPO is best-placed to manage this register, you remain responsible for the content of the records you produce.

The records register should be public. In this way your institution is able to effectively and transparently demonstrate compliance with data protection rules.



When should you carry out a Data Protection Impact Assessment?



Some risky processing operations require more than just a record. Examples include:

- the processing of large amounts of sensitive personal data, such as health data;
- the processing of data relating to disciplinary matters;
- the use of profiling techniques.

These cases, and others, require you to carry out a DPIA.

The EDPS provides a template to help you go through this assessment.



How do you carry out a Data Protection Impact Assessment?

DPIAs involve analysing your planned processing operation in detail, in order to determine the specific privacy risks involved and develop strategies to mitigate them. This process should lead to the production of a DPIA report. However, keep in mind that DPIAs are an ongoing process, so you should plan to carry out regular reviews.

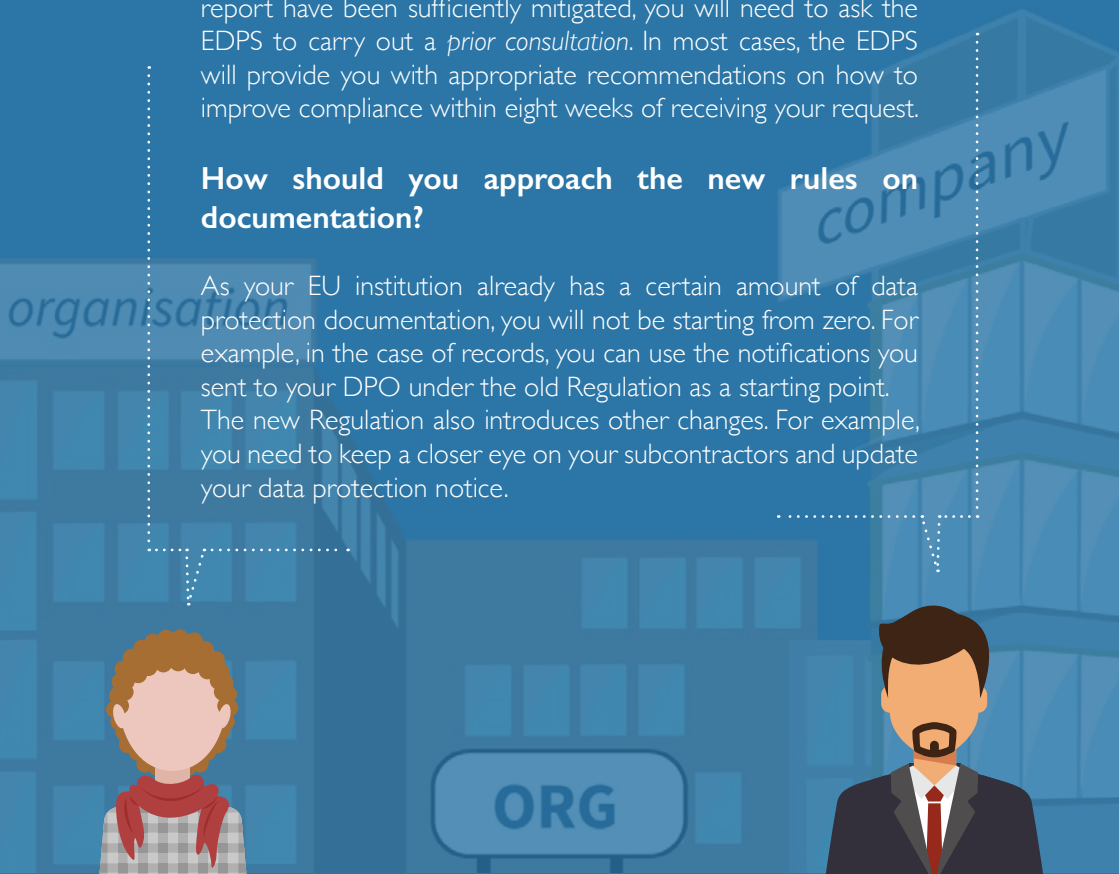
The EDPS provides templates for carrying out DPIAs, designed to help you in this process. However, any methodology that complies with the requirements of the Regulation or the GDPR can be used.

When should you request a prior consultation?

If you are not sure whether the risks identified in your DPIA report have been sufficiently mitigated, you will need to ask the EDPS to carry out a *prior consultation*. In most cases, the EDPS will provide you with appropriate recommendations on how to improve compliance within eight weeks of receiving your request.

How should you approach the new rules on documentation?

As your EU institution already has a certain amount of data protection documentation, you will not be starting from zero. For example, in the case of records, you can use the notifications you sent to your DPO under the old Regulation as a starting point.
The new Regulation also introduces other changes. For example, you need to keep a closer eye on your subcontractors and update your data protection notice.



How can your DPO help?



In every EU institution, there is at least one Data Protection Officer. The DPO acts as a reference point for all matters related to data protection. In some larger EU institutions, such as the European Commission, you will also have Data Protection Coordinators or Contacts (DPCs). DPOs and DPCs can provide you with guidance on how to generate records and carry out DPIAs. You should also contact them if you have any other questions relating to data protection. Keep in mind that the responsibility for ensuring compliance lies with you, as the data controller.



How can the EDPS help?



The EDPS is the supervisory authority responsible for data protection in the EU institutions and bodies. Our job is to monitor and check that the EU institutions comply with data protection rules. This might involve investigating complaints, carrying out *inspections*, replying to prior consultations or carrying out investigations on our own initiative. We produce *Guidelines* and provide training to help you ensure compliance and implement best practice, all aimed at ensuring that the EU institutions are able to lead by example on data protection.



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



