Data Protection in Action

Thank you for your interest and active participation in the training on data protection rules under Regulation (EU) 2018/1725. We hope that you have found our training useful!

Here are the main takeaways from this training.

From theory...

Personal data means any information relating to an identified or identifiable natural person ("data subject").

Processing of personal data means any operation or set of operations performed on personal data - whether or not by automatic means - such as collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosure by transmission, dissemination or otherwise making available. This also includes data alignment or combination, restriction, erasure or destruction.

Controller or joint controller determines the purposes and means of the processing of personal data, decides why and how data will be processed, and has influence in law or in fact over the purposes and means for which data is processed.

Accountability

The controller shall be responsible for ensuring, verifying and demonstrating compliance with data protection rules and principles, as well as the effectiveness of implemented measures and safeguards.

Data protection by design and by default in practice

How to implement specific data protection principles throughout the processing operation:

A. *Lawfulness:*

Legal obligation

Is your data processing operation justified by a specific legal obligation?

Public Interest

Is your data processing operation necessary for the performance of the institutions' tasks?

Consent

Consent must be "freely given, specific, informed and unambiguous", by way of a clear and informative act.
The controller should be able to demonstrate that the data subject has given consent.
Relying on consent is, in most cases, not appropriate in the employment context.

B. *Purpose limitation:*

Personal data shall be collected for specified, explicit and legitimate purpose(s).

C. *Data minimisation:*

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

D. *Accuracy:*

Personal data must be accurate and kept up to date. Mechanisms should be established for individuals to be able to exercise their rights!

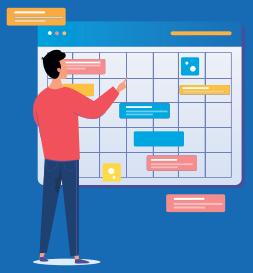
E. *Storage limitation (retention period):*

Personal data shall not be kept longer than necessary in relation to the purpose(s) of processing.

F. *Technical and organisational security measures:*

You should ensure the availability, integrity and confidentiality of the personal data you process.

To Practice...



Data Protection is about people: you have rights & obligations!

1) How to document your processing operations and keep individuals informed?

- Implement data protection by design & by default: check and implement data protection compliance from the outset of all your projects
- Create your records and update data protection notices relevant to each processing
- Check if your processing needs a DPIA and inform your DPO
- Follow the EDPS thematic Guidelines!

2) How to handle a transfer request within your EUI, within EUIs or to a third party?

- Transfers are possible, however conditions apply! Control what data is transferred by you or on your behalf!
- Always ask your DPO for advice.

3) What about data protection in procurement and outsourcing activities?

- The draft tender should include data protection specifications and updated data protection clauses, including as regards transfers.
- When entering into a contract to outsource the processing of data (IT services, HR services, expert selection, etc.), your external provider is a processor and Article 29 requirements must be included.
- Control the use of sub-processors and transfers!

4) In case of a joint controllership project:

- Determine with the other controllers your respective roles and responsibilities in a written arrangement
- Make the essence of this written arrangement available to data subjects via the data protection notice and
- Set up a contact point so that data subjects can exercise their rights.

5) What if there is a personal data breach?

- Immediately report the incident to your DPO/LISO and keep a record of the breach and mitigating measures. Notify the EDPS no later than 72h after having become aware of the breach if there are risks for data subjects.

6) What to do when people request to exercise their rights in relation to their personal data?

- People have the right to information, access, rectification, portability, right to erasure etc. When it is possible, these rights must be granted with the application of the necessary and justified restrictions and data subjects must be informed accordingly.
- Always keep your DPO informed throughout the process.

Useful links

Fact sheets:

- The GDPR for EU institutions: your rights in the digital era
- New data protection rules for EU institutions and how they affect YOU
- Documenting data processing: The EDPS guide to ensuring accountability
- e-brochure with the compilation of several checklists and flowcharts on data protection issues
- Data protection impact assessment in a nutshell
- The EDPS quick-guide to necessity and proportionality

Guidelines:

- Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies
- EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725
- EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data
- EDPS Necessity Toolkit
- Guidelines on Personal Data Breach Notification

If you have any questions or feedback to share with us, do not hesitate to contact your Data Protection Officer or Data Protection Coordinator (where applicable).

To keep up to date with the latest data protection news, please visit the EDPS website, subscribe to our monthly newsletter, and follow us on twitter.

www.edps.europa.eu

@EU_EDPS
EDPS
European Data Protection Supervisor