LAW & DATA
2024/2025

University of Padova

18 December 2024

Fiorella Dal Monte, PhD
Adjunct Professor
University of Padova | Department of Mathematics

Lessons in January

Wednesday, 8th 12:30-16:30 (2)

Friday, 10th 16:30-18:30 (1)

Wednesday, 15th 12:30-16:30 (2)

Possible precall:

Thursday 16th OR Monday 20th

GDPR | CONTROLLER

the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing of personal data**

JOINT CONTROLLERS

Obligations of the Controller

As a general rule, it is responsible and liable for any processing of personal data carried out

- By itself
- On its behalf

Main obligations of the Controller

- Adoption of appropriate ***TOMs*** (technical & organizational measures)
- (+ protection policies)
- Record of processing activities
- Cooperation with Data Subjects
- Cooperation with Supervisory Authorities

- DPMS -
DATA PROTECTION MANAGEMENT SYSTEM

risk-based internal compliance system

typically consisting in an IT security concept that introduces and monitors technical and organisational conduct of data processing activities, and records/documents processing activities to achieve compliance with the GDPR

Aim = achieve compliance with GDPR, by adopting appropriate TOMs

GDPR | PROCESSOR

a natural or legal person, public authority, agency or other body which **processes* personal data** on behalf of the controller

*PROCESSING OF PERSONAL DATA

ANY OPERATION OR SET OF OPERATIONS WHICH IS 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

Main obligations of the Processors

- Act upon instructions of the Controller
- Implement TOMs
- Appoint a Representative within the EU
- Maintain a record of processing activities
- Cooperate with Supervisory Authotiries
- Designate a Data Protection Officer (where required)

Contents of the RECORD

CONTROLLER	PROCESSOR
Name and contact details of the (joint) controller(s), the representative(s) and DPO(s)	Name and contact details of the processor(s) and (joint) controller(s), the representative(s) and DPO(s)
Purposes	Categories of processing
Description of the categories of data subjects and categories of personal data	--
Categories of recipients to whom personal data are or will be disclosed (including outside EU and/or international organisations)	--
Transfer to third countries/international organisation and documentation of suitable safeguards	Transfer to third countries/international organisation and documentation of suitable safeguards
Envisaged time-limits for erasure of the different categories of data	--
General description of TOSMs	General description of TOSMs

GDPR | DATA PROTECTION OFFICER

Person who advises on compliance with data protection rules in organisations undertaking data processing

Voluntarily appointed by controllers, unless:

- a public authority or body carries out the processing
- the controller's or processor's core activities consist of processing operations requiring the regular and systematic monitoring of data subjects on a large scale
- the core activities consist of large-scale processing of special categories of data or personal data relating to criminal convictions and offences

GDPR | SUPERVISORY AUTHORITIES

Independent public authority which is established by each Member State pursuant to Article 51

- data subjects' complaints
- be responsible for monitoring the application of the GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union
- contribute to the consistent application of the GDPR throughout the Union and collaboration with the EU Commission

GDPR | MAIN NOTIONS

- PERSONAL DATA
- SENSITIVE DATA
- PURPOSES
- CONSENT
- PROCESSING
- TRANSFER
- CROSS-BORDER PROCESSING
- DATA PROTECTION IMPACT ASSESSMENT

GDPR | PERSONAL DATA

means any information relating to an identified or identifiable natural person ('data subject'); 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

GDPR | SENSITIVE DATA

special categories of personal data

personal data revealing **racial or ethnic origin**, **political opinions**, **religious or philosophical beliefs**, or **trade union membership**, and the processing of **genetic data**, **biometric data** for the purpose of uniquely identifying a natural person, data concerning **health** or data concerning a natural person's **sex life or sexual orientation**

SENSITIVE DATA - Processing

In principle: PROHIBITED

Exceptions:

- ✓ Explicit consent (specified purposes)
- ✓ Employment law / social security and social protection law
- ✓ Protection of vital interests
- ✓ Legitimate activities of foundations, associations, non-profit bodies – members or former members
- ✓ Manifestly made public by DS
- ✓ Legal claims
- ✓ Substantial public interest
- ✓ Preventive / occupational medicine
- ✓ Health - public interest
- ✓ Scientific and historical research – public interest

GDPR | PURPOSES

(not expressly defined by GDPR)

aims for which data are collected and processed

GDPR | CONSENT

(OF THE DATA SUBJECT)

any **freely given**, **specific**, **informed** and **unambiguous indication** of the data subject's **wishes** by which he or she, by a statement or by a **clear affirmative action**, signifies **agreement** to the processing of personal data relating to him or her

GDPR | PROCESSING

any operation or set of operations which is 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

GDPR | DPIA
DATA PROTECTION IMPACT ASSESSMENT

assessment of the impact of the envisaged processing operations on the protection of personal data

CONTROLLER ← → DPO

GDPR | DPIA Contents

- systematic **description** of the envisaged processing operations + purposes + legitimate interest of the Controller (if any)
- assessment of the **necessity and proportionality** of the processing operations **in relation to the purposes**
- an assessment of the **risks** to the rights and freedoms of data subjects
- the **measures envisaged to address the risks**, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance

GDPR

MAIN PRINCIPLES FOR PERSONAL DATA PROCESSING

- LAWFULNESS
- FAIRNESS & TRANSPARENCY
- PURPOSE LIMITATION
- DATA MINIMISATION
- ACCURACY
- STORAGE LIMITATION
- INTEGRITY & CONFIDENTIALITY
- ACCOUNTABILITY