

LAW & DATA

2024/2025

University of Padova

20 December 2024



***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 Authorities
- Designate a Data Protection Officer (where required)

Contents of the RECORD

CONTROLLER

Name and contact details of the (joint) controller(s), the representative(s) and DPO(s)

Purposes

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

Envisaged time-limits for erasure of the different categories of data

General description of TOSMs

PROCESSOR

Name and contact details of the processor(s) and (joint) controller(s), the representative(s) and DPO(s)

Categories of processing

--

--

Transfer to third countries/international organisation and documentation of suitable safeguards

--

General description of TOSMs

DATA PROTECTION BY

DESIGN

the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects

DEFAULT

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons

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



- **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**