Erasmus+
Enriching lives, opening minds.

Day 4

Ecological and Sustainable Project Management in Erasmus+

EUROPEAN UNION

Ruggell | 10.-13. June 2024

Erasmus+
Enriching lives, opening minds.

PERSONAL DATA PROTECTION
Safeguarding personal information

Michal Osmenda

EUROPEAN UNION

WHAT IS PERSONAL DATA?

- **Identification details** - Any information that can directly identify an individual, such as name, address, email, phone number.
- **Digital Footprint** - Online data that can indirectly identify an individual, like IP addresses, browsing history, and device identifiers.
- **Sensitive Information** - Personal data revealing racial or ethnic origin, political opinions, religious beliefs, biometric data, or health information.

Legal framework

- Regulation (EU) 2016/679 – GDPR - on the protection of natural persons regarding the processing of personal data and on the free movement of such data

- Regulation (EU) 2018/1725 – EUDPR - on the protection of natural persons regarding the processing of personal data by the **Union institutions, bodies, offices and agencies** and on the free movement of such data

Main roles

- **Data subject** - the individual whose personal data is being processed; equipped with rights
- **Data controller** - the entity that determines the purposes and means of processing personal data; has obligations towards data subjects
- **Data processor** - the entity that processes data on behalf of the controller; has obligations towards the data controller

DATA PROTECTION PRINCIPLES

Storage limitation

Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary.

Integrity and confidentiality

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability

The controller must be responsible for, and be able to demonstrate compliance with, the data protection principles.

Lawfulness, fairness, and transparency

Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.

Purpose limitation

The collection of personal data must have clear, predetermined, and lawful objectives.

Data minimisation

Personal data processed must be adequate, relevant, and limited to what is necessary.

Accuracy

Accurate data is vital; correct inaccuracies promptly.

QUESTIONS TO ASK YOURSELF

- WHY
- FOR WHAT PURPOSE
- WHAT
- HOW LONG
- BY WHOM

DATA SUBJECT RIGHTS

- **Right to be informed**

Individuals have the right to be informed about the collection and use of their personal data.

- **Right of access**

Individuals have the right to access and obtain a copy of their personal data held by organisations.

- **Right to rectification**

Individuals have the right to correct inaccurate or incomplete personal data.

- **Right to erasure**

Individuals have the right to request the deletion of their personal data, this is also known as the 'right to be forgotten'.

- **Right to restrict processing**

Individuals have the right to restrict the processing of their personal data in certain circumstances.

- **Right to data portability**

Individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format.

- **Right to object**

Individuals have the right to object to the processing of their personal data for specific purposes.

SPECIAL CONSIDERATIONS

1. **Special categories of personal data** - data revealing race or ethic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric and health data, data concerning a natural person’s sex life or sexual orientation (Art. 9 of GDPR, Art. 10 of EUDPR) - national laws may introduce further conditions and limitations (Art.9(4) of GDPR)

2. **Age of consent** (above which parental approval for processing of personal data is not required) - 16 years but can go as low as 13 years old, if national law permits it (Art.8(1) of GDPR); Organisations must make reasonable efforts to verify that consent is given or authorised by the parent or guardian
    a. EU institutions - 13 years old (Art.8 of EUDPR)

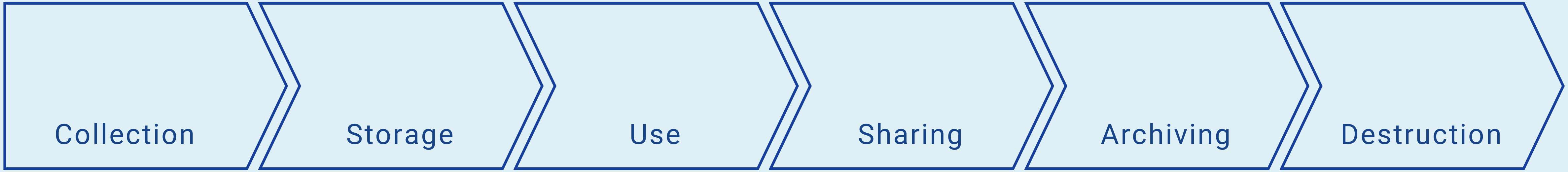
SPECIAL CONSIDERATIONS

3. **Data Protection Impact Assessment** (DPIA) is required in case processing carries out high risk to rights and freedoms of data subjects (Art.35 of GDPR, Art.39 of EUDPR)

4. **Transfers to third countries or international organisations** - transfer of data to countries other than EU/EEA and those not listed in the EC adequacy decisions list is generally forbidden, unless specific rules are fulfilled (Chapter V of GDPR/EUDPR)

Erasmus+
Enriching lives, opening minds.

DATA PROCESSING LIFECYCLE



Collection	Storage	Use	Sharing	Archiving	Destruction
Collecting personal data.	Securely storing collected personal data in databases, cloud storage, or other appropriate systems.	Utilising personal data for specific purposes.	Disclose personal data only with consent and necessity.	Retaining personal data for legal or regulatory requirements, following data retention policies and procedures.	Properly dispose of personal data after retention period ends.

EUROPEAN UNION

IMPLEMENTING DATA PROTECTION

Think about data processing approach	Role, purpose, means, security
Implement technical and organisational measures	Deploy appropriate security controls and processes to safeguard personal data.
Maintain records of processing activities	Document the purposes, types of data, and other details of data processing operations.
Follow the process	Collect, safeguard, process, archive, dispose

POOR DATA PROTECTION

Data breaches

Unauthorised access to sensitive information leading to exposure and misuse.

Identity theft

Stolen personal data used for fraudulent activities, damaging credit and reputation.

Financial loss

Costly fines, lawsuits, and expenses from data breach recovery efforts.

Damage to reputation

Loss of customer trust and brand value, impacting business growth and success.

Legal penalties

Severe regulatory fines and potential criminal charges for non-compliance with data protection laws.

Key factor: risk

- Data protection regulations mandate a focus on risk reduction.
- Risk reduction applies to both data subjects and data controllers/processors.
- Risk management is essential in designing data processing activities.
- Every step in the process should maximise efforts to minimise risk.

Erasmus+
Enriching lives, opening minds.

IN ERASMUS+
you may become

data subject

- you're an applicant, mobility participant, expert, partner contact person, legal representative
- your data will be processed by others (EC, National Agency)
- you have a right to know how and for what purpose (application, project, mobility data)
- you want to know how long it will be processed (1 year, 5 years, 10 years)
- be aware of your rights as well as limitations of those rights (right to be forgotten is not absolute and may be limited by the rules protecting budget of the EU)

data controller

- you need to design the processing (purpose, actors, transfers, retention period, security)
- Your processing must have solid legal basis (relevant laws and regulations, consent or legitimate interest)
- you need to document everything (description of processing activities, categories of data and data subjects)
- you choose your processors/partners wisely
- you respect the rights of the data subjects (but the are boundaries too!)
- you are transparent to all parties (data subjects, processors, authorities)

data processor

- you're a beneficiary and you process personal data in line with the Erasmus+ privacy statement
- process personal data in the way defined in a contract (GA) or become a controller yourself (Art.29 of EUDPR)
- document your processing (use templates)
- know what to do at the end of the retention period (return or delete the data)
- Have sound policies in case of data breach situations
- Know your responsibilities towards the data subjects

EUROPEAN UNION

What’s in it for me? Lessons learned

Sustainability – practice of meeting the needs of the present without compromising the ability of future generations to meet their own needs

Environmental Sustainability – Ensuring that natural resources are used responsibly and preserved for future generations.

Economic Sustainability – Promoting economic growth and development that does not deplete natural resources or cause severe ecological damage

Social Sustainability – Ensuring that all members of society have their basic needs met and can live healthy, productive lives.

Environmental Sustainability – Ensuring that natural resources are used responsibly and preserved for future generations preserved for future generations.

Reduce amount of data being used/transferred/stored – positive impact on amount of energy and resources used by data centres, network devices, your company, organisation, household

Rethink categories of personal data processed – with sensitive data comes greater responsibility and greater cost of maintaining it

Create simple processes – less complications leads to faster processing and less resources used

Be transparent towards data subjects, processors and authorities – reduction in requests from data subject, clarifications from the contractors and authorities with clearly written privacy policy, reduced risk in data processing and categories of personal data

Economic Sustainability – Promoting economic growth and development that does not deplete natural resources or cause severe ecological damage

Transparent and simple data processing builds trust – data protection should enhance security and confidence, not create administrative burdens. Simple processes attract, while complex ones deter data subjects and partners.

Storing data costs money and excessive data collection wastes users' time – why collect more than you need?

Avoid penalties by correctly applying data protection principles and safeguarding your Erasmus+ project from careless data handling.

Reduce risks with clear, secure, and transparent data processing.

Create and document policies for data protection to ensure operational continuity and ease during audits.

Social Sustainability – Ensuring that all members of society have their basic needs met and can live healthy, productive lives.

Building Trust – Protecting personal data fosters trust between individuals and institutions.

Transparency – Transparent practices ensure individuals know how their data is used and protected.

Respecting Privacy – Data protection upholds individuals' right to privacy.

Preventing Discrimination – Robust protection prevents data misuse that could lead to discrimination or social exclusion, promoting fairness and equity.

Empowering Individuals – Data protection gives individuals control over their personal information, empowering informed decisions about their privacy.

Examples of unsustainable personal data processing practices

- **Storing ID documents**

  What? National IDs, passports, student IDs, driving licences

  Why? Because of data minimisation principle violation - you only process information you require

  Alternatives? For checking identity - validation of the identity by presentation of the ID by the data subject

- **Sending databases/lists of personal data by email**

  What? Excel files, list of participants, several CVs in attachment sent outside of your organisation

  Why? Lack of access control, data retention policy difficult to apply, security no longer verifiable

  Alternatives? Centralised storage - cloud or local network, your local computer storage

- **Treating health data the same way as other types of data**

  What? Data revealing race or ethic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric and health data, data concerning a natural person’s sex life or sexual orientation

  Why? Because of the requirement for special conditions for treatment and requirement for appropriate safeguards

  Alternatives? No processing or special security arrangements

Examples of unsustainable personal data processing practices

- **Not paying enough attention to security of data**

  What? Data breaches happen, it’s a question of time

  Why? Data breaches may have fatal consequences to business (ask British Airways - 20 million GBP fine, Marriott - 18 million GDB fine, H&M - 35 million EUR fine, Vodafone Spain - 8 million EUR fine, Austrian Post - 18 million EUR fine, etc, etc)

  Alternatives? DPIA, implementation of appropriate security, create data breach policy, follow up the incidents and submit report within 72 hours to data protection authority, be accountable

- **Disrespecting data subjects rights**

  What? Data subjects rights for information, restriction of processing, right to be forgotten

  Why? Personal data protection is a fundamental right and freedom of natural persons; not respecting the data subject rights may lead to problems with data protection authorities

  Alternatives? Data controllers must create procedures to respond to data subject requests

Data protection in Erasmus+

1. Data protection by default and by design in the entire project lifecycle
2. Data minimisation
3. Special consideration for personal data of minors (school education sector)
4. Special consideration for health data (force majeure)
5. Choose your partners wisely (3rd country transfers)
6. Document your processing (use template)
7. Know where to get information - E+ privacy statement, grant agreement, obligation of data processors (Art. 29 of EUDPR)
8. Think about personal data processing like it was processing *your own data*