



E-LEARNING

Level 5



WA13: General Legislation

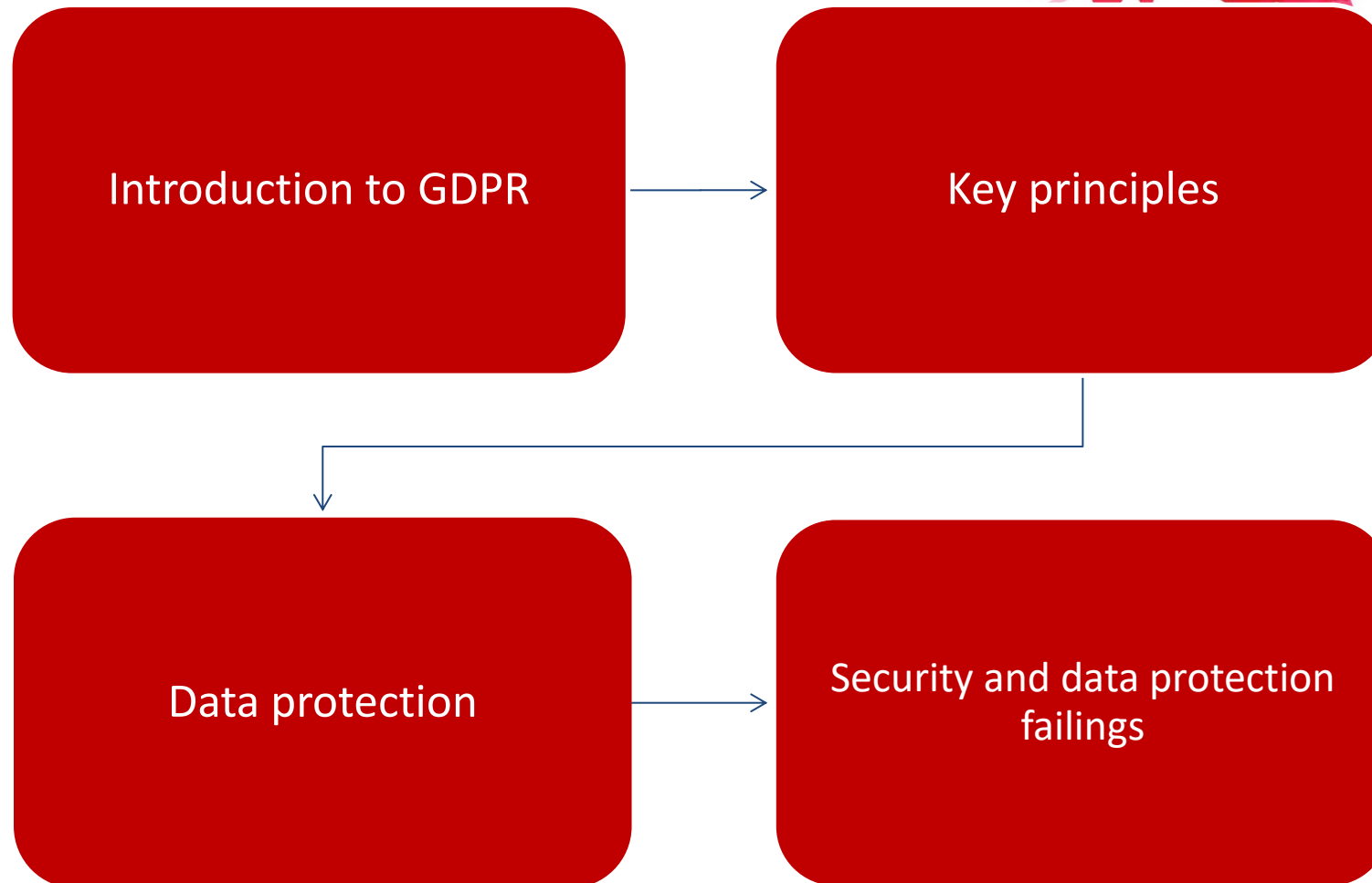
5.5 GDPR and data protection

LO5.27 Demonstrate a comprehensive knowledge regarding GDPR regulations and principles in a broad context to assist the company or organisation, to predict situations and to develop solutions to problems related to the data protection

LO5.28 Demonstrate the ability to implement GDPR regulations and principles in a context of company or organisation



Route Map



Introduction to GDPR

Key terms

The General Data Protection Regulation (GDPR) is a privacy and security law and it regulates the way of processing and managing personal data. It is related to all businesses and organisations (e.g. hospitals, public administrations, etc) in EU.

- Regulation of the business environment in context of processing and controlling personal data
- Data Protection legislation across the EU

Introduction to GDPR

Key terms

Personal data - any information that relates to an individual who can be directly or indirectly identified

Data controller - the person who decides why and how personal data will be processed

Data processing - any action performed on data, whether automated or manual (e.g. collecting, recording, organizing, structuring, storing, using, erasing)

Data processor - a third party that processes personal data on behalf of a data controller

Data subject - the person whose data is processed (e.g. customers)

Key principles of data protection

There are seven protection and accountability principles related to data protection:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Designation of The Data Protection Officer required:

- Public authority
- Large-scale, regular monitoring
- Large-scale special data categories

What are the necessary professional qualities of The Data Protection Officer:

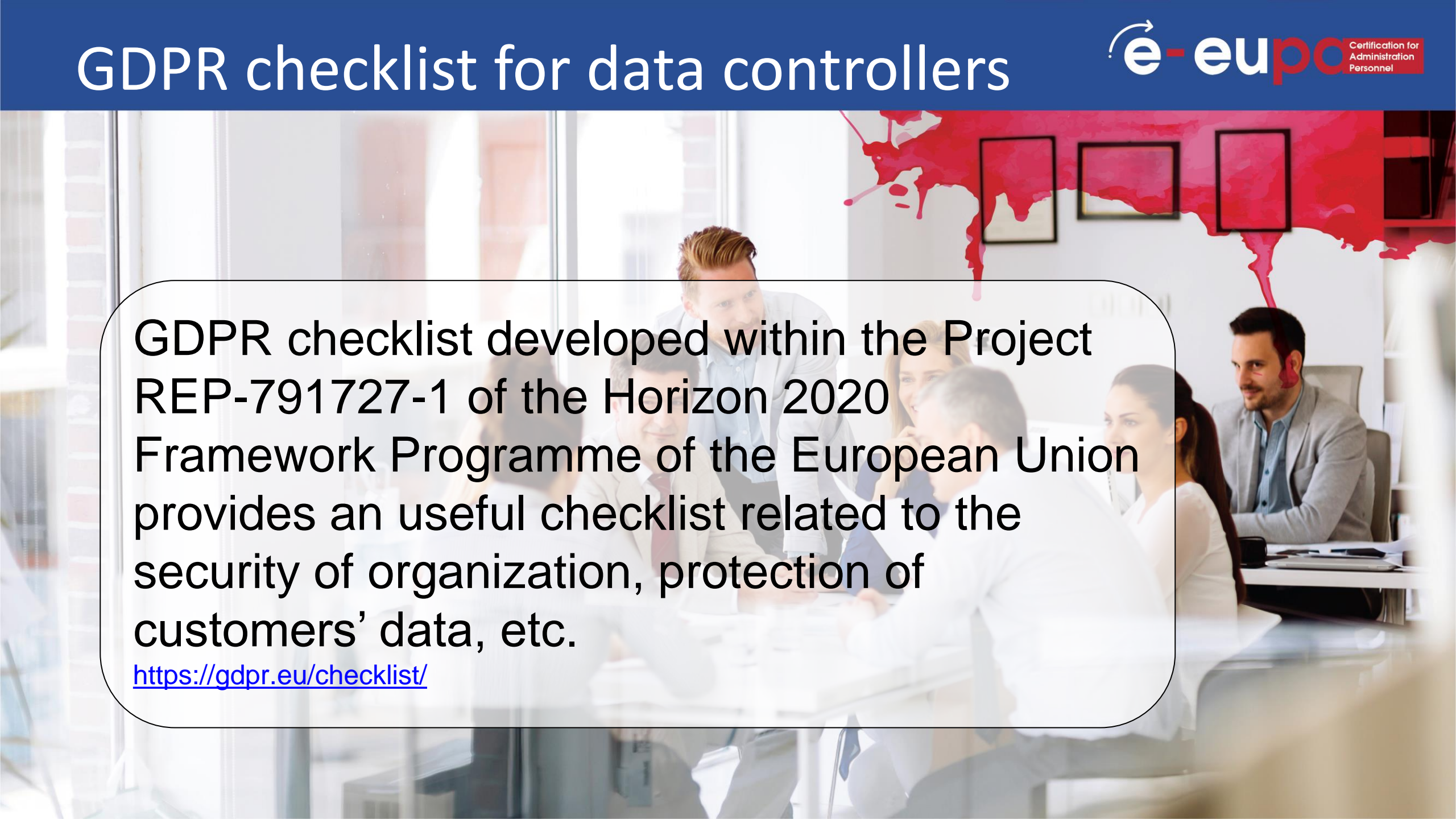
- Expert knowledge of data protection law and practices
- Expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR
- Understanding of the processing operations carried out
- Understanding of information technologies and data security
- Knowledge of the business sector and the organisation
- Ability to promote a data protection culture within the organisation

(Article 37(5) of the GDPR)

Company's obligations under the GDPR

“Personal data can be processed under certain conditions (fair, transparent, specified, legitimate purpose etc), it must be based on one of the following legal grounds:

- The consent of the individual concerned
- A contractual obligation between company and the individual
- To satisfy a legal obligation
- To protect the vital interests of the individual
- To carry out a task that is in the public interest
- For the company's legitimate interests, but only after having checked that the fundamental rights and freedoms of the individual whose data is processed, is not seriously impacted
- If the person's rights override company's interests, then company cannot process the data



GDPR checklist developed within the Project REP-791727-1 of the Horizon 2020 Framework Programme of the European Union provides an useful checklist related to the security of organization, protection of customers' data, etc.

<https://gdpr.eu/checklist/>

Processing data based on consent

- Strict rules for processing data based on consent
- Ensuring the individual understands what he or she is consenting to
- The consent given freely, specific, informed, presented in clear and plain language
- Consent given by an affirmative act, e.g. checking a box online or signing a form
- Keeping documentary evidence of consent

Protection of individuals' rights

- Provision of transparent information about the company
- The right to request access to own personal data, free of charge and in an accessible format
- Right to be forgotten
- Right to correct and right to object

Acting in accordance with the GDPR means:

Keeping detailed records:

- Name and contact details of the business involved in data processing
- Reason(s) for processing personal data; description of the categories of individuals
- Providing personal data
- Categories of organisations receiving the personal data
- Transfer of personal data to another country or organisation
- Storage period of the personal data; description of security measures used when
- Processing personal data
- Maintaining and updating written procedures and guidelines for the employees

Data breach

A data breach means that the personal data for which the company is responsible, is disclosed, either accidentally or unlawfully, to unauthorised recipients or is made temporarily unavailable or altered.

Procedure in case of data breach:

- notification of the supervisory authority (Data Protection Authority)
- notification of individuals affected in case of high risk



GDPR and key principles

E-EUPA_LO_5.27_M_001



GDPR and data protection

E-EUPA_LO_5.28_M_001

Revision Questions

Revision Question 1

Which operations performed on personal data cover data processing?

Revision Question 2

What does General Data Protection Regulation ('GDPR') regulate?

Key Point 1

Key principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Key Point 2

- Getting consent to use personal data
- Securing the personal data which are processed

Key Point 3

- Provision of transparent information
- right to access and right to data portability for those giving the data
- right to erasure data (right to be forgotten)

WELL DONE



You have completed Unit 5.5!



**Co-funded by
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

