Presentation

On 25 May 2018, the General Data Protection Regulation (GDPR), aiming to improve data protection for individuals across the EU, became directly applicable. Now, organizations need to be compliant with the new rules and should act immediately. In addition, the 1148/2016 Directive concerning measures for a high common level of security of network and information systems across the Union became also applicable in order to establish security and notification requirements for operators of essential services and for digital service providers.

By developing good knowledge of the GDPR and understanding how it affects you, you will learn about the first steps for making your organization compliant and can immediately start taking them. You will explore data subjects' rights, data controllers' and processors' obligations, and enforcement and compliance notions in the context of the Regulation.

In this course, the topics that will be covered are general principles and basic concepts of the GDPR, rights of data subjects, obligations of data controllers and processors and law compliance measures, enforcement and compliance mechanisms, the Role of DPO, liabilities and sanctions and data breach.

Furthermore, you'll learn how to recognise security threats that could lead to data breach and explore the steps you can take to minimise your risk.

The course will improve your online safety in the context of the wider world, introducing concepts like malware, Trojan virus, network security, cryptography, identity theft, and risk management.

On one hand, participants will be able to identify the main positions of the GDPR, including key concepts, principles and data protection roles, explore rights of data subjects and their relevance in daily life and investigate obligations of data controllers and processors and related steps that need to be taken for complying with the GDPR. On the other hand, they will be able to recognize and minimize risks that could lead to data breach by implementing cyber security policies.

Objectives

The purpose of this educational unit is to enrich the knowledge in how to implement GDPR and Security Policies.

The trainees with the completion of their training they will have the ability to:

- Identify the main positions of the GDPR, including key concepts, principles and data protection roles
- Investigate obligations of data controllers and processors and related steps that need to be taken for complying with the GDPR
- Explore rights of data subjects and their relevance in daily life
- Implement Impact Assessment
- Identify data threats and risks
- Data Management
- Protect their Data using Cyber Security policies and tools

Pre-departure

Trainees will receive a questionnaire, which will provide information on their teaching background, qualifications, and previous experience with GDPR and Cyber Security, as well as their expectations of the course.

Target groups

The program is addressed to those who want to be informed about the GDPR and Data Security Policies and Tools. The specific targets groups are aspiring or experienced educators and teachers.

The Trainers

The trainers have a very deep knowledge of the principles and techniques of GDPR and Cyber Security particularly as part of the 21st-century skills.

Labs

The lessons will take place in modern full equipment laboratories.

Language of the course

English

Program

Day 1

Participant arrival, individual orientation and information about the venue and the city. Presentation of the course, the trainers, and participants.

- Introduction to the General Data Protection Regulation
- The Rights of the Data Subject

- Key concepts, approaches, methods and techniques to effectively participate in the implementation process of a compliance framework with regard to the protection of personal data File management, transfer and sharing
- Data Protection Impact Assessment and risk assessments

Day 2

- Security of personal data, data transfer and privacy by design
- Data breach
- The Role of DPO
- Internal Audits
- Case Studies
- Solve GDPR problems across a range of various scenarios

Day 3

- Introduction of cyber security
- Security Awareness
- Cyber Security threats and vulnerabilities

Day 4

- Phishing Simulation
- Common incidents
- Security Breaches

Day 5

- Back up and Disaster Recovery Solutions
- Network Security
- Incident response
- Case studies

Day 6

- Space for discussion of future cooperation and planning follow up activities
- Course roundup and final evaluation
- Validation of learning outcomes and certification ceremony
- Participants' departure

Fees

Course fee: 480,00€ (VAT included). It includes:

- ✔ Preparation for the course
- ✔ Training materials
- ✔ Administration costs
- ✔ Organizational costs

Follow-up

Trainees will be given soft and hard copies of all lesson materials, which they can review at their

leisure in addition to presenting them to their colleagues at their organizations. Also, an e-community of participants will be created to exchange ideas and experiences.

Erasmus+ KA1 Courses in Greece

🌐 **www.digitalidea.gr**

f **@digitalideagr   @coursesKA1**

✓ *Minimum number of participants: 6*
✓ *Maximum number of participants: 18*

If you have a group of 6 staff or more, please contact us for convenient dates