WOMEN4IT
2020

TRAINING ROADMAP

Data Protection Officer

Iceland Liechtenstein Norway grants
Norway grants

About This Training Path

Total Hours

160

Training Objectives

The purpose of this training path is to provide you with the knowledge about the protection of personal data that is essential for anyone who handles personal information as part of their job. You will learn about data protection legislation and how organisations are required to handle personal data, including procedures for collecting, storing and sharing personal data.

Upon successful completion of the training you will be able to:

- Understand the key requirements of GDPR legislation and how it applies to organisations.
- Design basic data impact assessments and privacy policies.
- Know the scope and responsibilities of the Data Protection Officer (DPO) in an organisation.
- Understand the elements and processes of a data protection compliance audit.
- Identify, monitor and control risks regarding data protection within the organisation.

Success Criteria

You are assessed continuously throughout the training, earning badges for every module you successfully complete. You must achieve all badges to successfully complete the training. A minimum attendance rate of 75% is required.

Accreditation

You may qualify, in full or in part, for credits towards future training courses or certification by an awarding body. Your mentor will explain these options to you before you begin.

Your Training Roadmap

Your trainer may conduct a pre-assessment exercise with you to determine your knowledge of the subject and your comfort level with technology. This may be in the form of a short online test, a paper survey or informal interview, either 1 to 1 or in a group with your fellow learners. A digital skills introductory course may be recommended for you to help you progress through the training roadmap.

UNIT 1

Data Protection basics.

Learning Objectives

- Provide a basic understanding of data protection rights and responsibilities, being able to explain what data protection is, and why it is important for business.
- Learn how to identify personal data.
- Identify tasks in your job where personal data is processed.
- Understand the key concepts of privacy and their implications to day to day business.
- Understand legitimate grounds for data processing and being able to apply them in practice.

UNIT 2

The organisation's responsibilities when collecting and processing personal data.

Learning Objectives

- Understand the organisation's responsibilities when collecting and processing personal data.
- Learn about the responsibilities organisations have when sharing data internally and externally.
- Understand the contractual relationship between Controller and Processor.
- Learn how to review and to develop relevant contractual clauses.

- Learn practical aspects of data assessment and data flow design enabling to ensure implementation of the relevant privacy measures into the organisations' daily business operations.
- Learn and understand how to record processing activities we document or link to the relevant documentation such as Privacy policy, consent record, records of data breach etc.
- Learn when, how and to whom organisation needs to notify the data breach.

Unit 3

Detailed data assessments and obligation to appoint a DPO.

Learning Objectives

- Understand the data protection risks, the principles for risk assessment and their influence to the organisations' data flow assessment.
- Understand when and why Data Protection Impact Assessment is required.
- Learn how to design the basic Data Impact Assessments.
- Understand when and why Organisations' need to appoint DPO.
- Understand DPO role and responsibilities.

Unit 4

Rights of the data subject and organisations' privacy policy.

Learning Objectives

- Learn about data subject rights – what they are and what their mean to your organisation.
- Understand the privacy best practices for communication with employees, clients, business partners etc.
- Understand the requirements for data subjects' consent, learn how to develop relevant consent forms and/or practices.

- Learn how to and when to review and/or design Organisations' Privacy policy.

UNIT 5

Data transfer across the borders.

Learning Objectives

- Learn about the responsibilities organisations have when sharing data across borders.
- Learn how to reflect the cross-border data transfers into the organisations' privacy policy, data subjects consent and contracts with the clients and suppliers.

UNIT 6

Data security.

Learning Objectives

- Understand the main challenges for safe data processing and learn how to identify the most vulnerable areas for risk assessment.
- Learn how employees internally determine risk level of their actions relating to everyday communications while using phone, e – mail, internet etc.
- Learn about identifying information assets that are sensitive to the business, individuals and/or subjects to legal requirements.
- Learn how to handle data with integrity and confidentiality.
- Understand how to reflect the relevant security risks and actions for risk minimisation into the organisations' Privacy Policy and other relevant documentation.

UNIT 7

Electronic communications and marketing.

Learning Objectives

- Learn about an organisation's obligations in privacy field when sending electronic marketing messages (by phone, fax, email or text), use cookies, or provide electronic communication services to the public.

UNIT 8

Data protection compliance assessment (audit).

Learning Objectives

- Understand when and why data protection compliance self- assessment is needed and how it can help organisation
- Learn the best practices how to prepare for self-assessment and to design organization data protection compliance checklists
- Understand and learn how to reflect self-assessment outcomes within organizations' relevant Privacy documentation

UNIT 9

Supervisory authority. Remedies, liability and penalties.

Learning Objectives

- Learn about the Supervisory Authorities role, competence, tasks and powers under GDPR.
- Understand organisations' rights and liabilities under GDPR case of non-compliance or any intervention by Supervisory Authority.