**Course:**
**GDPR Compliance: From Principles to Practice - A Practical Guide for Organisations**

## Course Description

This course provides a comprehensive and practical overview of the key requirements that organisations need to understand and implement in order to comply with the General Data Protection Regulation (GDPR). It introduces the fundamental concepts and principles of personal data protection and explains what constitutes the processing of personal data, when such processing may be unlawful, and how organisations can meet the GDPR's specific requirements. The course also highlights the potential consequences of non-compliance, including examples of fines imposed for infringements of GDPR provisions.

A significant part of the course focuses on Consent and the rights of Data Subjects. It describes in brief what constitutes valid Consent, the conditions that must be satisfied for Consent to be lawful, and the specific requirements applicable to children's Consent. Through examples, the course demonstrates how organisations can obtain and document valid Consent and avoid common mistakes when relying on Consent as a legal basis for processing personal data.

The course also provides guidance on how organisations should respond to requests from Data Subjects exercising their GDPR rights. The course explains the various rights available to Data Subjects, understand the applicable restrictions, and refers to how to handle rights requests appropriately and within the required framework. Examples and scenarios are used to demonstrate how Data Subjects' rights requests can be managed effectively in real-life situations.

Another key area covered is the retention of personal data and the importance of establishing appropriate retention periods. The course explains how to determine how long personal data should be retained, what should happen when personal data is no longer needed, and what a Personal Data Retention Policy may include. The course provides guidance on applying retention periods and identifies key points that organisations should consider when managing the lifecycle of personal data.

The course also introduces Data Protection Impact Assessments (DPIAs), explaining what a DPIA is, when it should be performed, and what it should contain. It provides examples of processing activities that may require a DPIA and review a practical DPIA structure that can be used as a basis for a DPIA implementation. Attention is given to the key considerations that organisations should take into account when assessing and managing personal data protection risks associated with their processing activities.

The final section focuses on the management of personal data breaches and the procedures organisations should have in place to respond effectively to such incidents. It describes what constitutes a personal data breach, when affected Data Subjects and the relevant Supervisory Authority may need to be informed, and how breach notification requirements apply in practice. The course also explains how to develop and implement a Personal Data Breach Management Procedure and provides examples to support an effective organisational response.

Finally, the course addresses the key internal policies, procedures, agreements and documentation that organisatons should consider developing and implementing as part of their GDPR compliance framework. These include privacy policies and notices, cookies policy, employee guidance, confidentiality and processing agreements, Consent declarations, a DPO job description and a Record of Processing Activities (RoPA). The course provides a practical understanding of the key measures, processes and documentation required to establish and maintain an effective GDPR compliance framework.

## Topics covered

The course is split into the following sections:

**Section 1: Does your Company comply with the GDPR requirements?**

- Key Terms.
- The GDPR in summary.

- Comply with the GDPR Principles.
- When processing of personal data is unlawful.
- What does the Processing of Personal Data Involve?
- How to comply with GDPR specific requirements.
- Avoid being penalised for the infringement of GDPR provisions (Examples of fines imposed).

**Section 2: Understand how to receive valid Consent and meet Data Subjects' rights**

- General provisions of Consent.
- Understand when a Consent is valid.
  - Conditions for valid Consent.
  - Conditions applicable to children's Consent.
  - Examples of obtaining valid Consent.
  - Valid Consent – Summary.
- Understand how to meet Data Subjects rights.
  - What rights do Data Subjects have?
- Restrictions on responding to Data Subjects' rights requests.
  - Key points regarding restrictions.
- Practical guidance on handling Data Subjects' rights requests.
  - Examples on handling Data Subjects' rights requests.
  - Respond to Data Subjects' rights requests.
  - Data Subjects Rights Request (DSRR) Procedure.
  - What forms a company may develop and implement for handling Data Subjects' rights requests.

**Section 3: Learn how to comply with the Retention Period and how to develop a Data Protection Impact Assessment (DPIA)**

- Develop and implement a Retention Period.
  - What Retention Period means.
  - How long should a Company retain personal data?
  - What should a Company do with personal data that is no longer needed?
  - Apply Retention Period in practice.
  - What a "Personal Data Retention Policy" may include.
  - Key points to consider when implementing Retention Period.
- Develop a Data Protection Impact Assessment (DPIA).
  - What a DPIA is.
  - What a DPIA shall at least include.
  - When a DPIA shall be performed.
  - Examples of processing activities subject to DPIA.
  - Example of a DPIA structure.
  - Key points to consider when performing a DPIA.

**Section 4: Be prepared to manage a personal data breach and the various policies and procedures to keep internally**

- Be prepared to manage a personal data breach.
  - What a personal data breach is.
  - Informing affected Data Subjects for a breach.
  - Examples
  - Notify the personal data breach to the Supervisory Authority.
  - Examples
  - Develop and implement a "Personal Data Breach Management Procedure".
  - What a "Personal Data Breach Management Procedure" may include.
- Policies, Procedures and Agreements to Develop and Implement.

## Course Duration

This course may take up to 5 hours to be completed. However, actual study time differs as each learner uses their own training pace.

## The course is addressed to:

This course is addressed to all individuals who are involved in the processing of personal data in an organisation:

- Designated DPOs in Investment Firms, Investment Funds, ASPs, Trust Service Corporate Providers, Banks, Law Firms, Accounting Firms, Auditors, insurance companies, hospitals, schools and in general DPOs of all organisations.
- Employees of Investment Firms, Investment Funds, ASPs, Trust Service Corporate Providers, Banks, Law Firms, Accounting Firms, Auditors, insurance companies, hospitals, schools and in general of all organisations involved in the processing of personal data.
- Executive Directors, Non-executive directors, Senior Managers, Compliance Officers, Risk Managers, Product Managers, etc.
- Internal Auditors
- Consultants
- Lawyers

It is also suitable for professionals pursuing CPD for the renewal of CySEC Certificate (CySEC Basic or CySEC Advance Certificate or CySEC AML Certificate) or other relevant professional certificates in other jurisdictions.

## Training Method

The course is offered fully online using a self-paced approach. The learning units consist of power point presentations. Learners may start, stop and resume their training at any time.

At the end of the course, participants take a Quiz to complete the course and earn a Certificate of Completion once the Quiz has been passed successfully.

## Accreditation and CPD Recognition

The course can be accredited by regulators and other bodies for 5 CPD Units that require CPD training in financial and other regulation.

Eligibility criteria and CPD Units are verified directly by your association or other bodies in which you hold membership.

## Registration and Access

To register to this course, click on the *Take this course* button to pay online and receive your access instantly. If you are purchasing this course on behalf of others, please be advised that you will need to create or use their personal profile before finalizing your payment.

Access to the course is valid for 90 days.

If you wish to receive an invoice instead of paying online, please Contact us by email. Talk to us for our special Corporate Group rates.

## Instructor

Andreas Nicolaides has more than 10-years experience in the financial Industry. He is the Operations Manager of G.P. GLOBAL LTD offering consulting services and training courses to Investment Firms, Administrative Service Providers and Funds focuses in Internal Audit, compliance & AML issues. He is a member of the

Internal Audit team of G.P. GLOBAL LTD and is involved in numerous Internal Audits of Cyprus Investment Firms, Administrative Service Providers and Funds where he is engaged, among others, in the audit for compliance with the GDPR regulatory framework. He has completed a number of trainings on GDPR regulatory framework and assisted a number of Cyprus Investment Firms, Administrative Service Providers and Funds to comply with their GDPR legal obligations.

Andreas Nicolaides holds a BA in Business Management from the Northumbria University (Newcastle - UK). Andreas also holds an Advance and Money Laundering certificate from the Cyprus Securities and Exchange Commission for the provision of investment services/activities.