

Certified GDPR-KVKK Foundation and Practitioner

Learn via: **Classroom/AFA**

Duration: **5 Day**

Overview

This Five day comprehensive practitioner course, with independent APMG exam, will provide a practical guide to planning, implementing and maintaining compliance with the new General data Protection Regulation (GDPR) Regulations.

Under the new EU data protection regulations, the appointment of a Data Protection Officer (DPO) will be mandatory for controllers and processors in the public sector. The obligations for this new and challenging role will require insight into cyber threats, risks, data breach management, secure design and secure by default principles, privacy compliance and the legal spectrum of the GDPR-KVKK.

This course is suitable for data protection officers, HR Professionals, compliance officers, auditors, IT & security Professionals.

Who Should Attend

This GDPR-KVKK Practitioner course is primarily aimed at professionals working with IT, Risk, Security, Governance and Compliance roles across public and private sectors. It is also aimed at Marketing Professionals and Project Managers.

What You Will Learn

Learn to solve GDPR-KVKK problems to new privacy situations by applying acquired knowledge, facts, techniques, and rules in a learnt from the GDPR Practitioner course.

- Apply the implementation pathway for GDPR-KVKK compliance
 - Privacy Impact Assessments
 - Incident Response
 - Policy Frameworks
 - E-discovery and data auditing
 - Privacy by Design / Default
- Identify the key differences between the Data Protection Act and the GDPR-KVKK
- Understand the role of the data Protection Officer (DPO) and the new obligations
- Develop a plan to address the challenges of building a privacy programme across your organisation
- Prepare for managing and reacting to a data breach both from a regulator and commercial perspective
- Identify the changing rights of data subjects, consent, data in the cloud and third parties
- Model about the enforcement aspects of the GDPR-KVKK to your organisation

Business Outcomes

- Act in a more...responsible, ethical and well informed manner,to GDPR compliance issues and scenarios.
- Adapt your communication style...to being one of a knowledgeable, capable Privacy Professional and or Practitioner.
- Build effective working relationships....by being able to articulate and determine GDPR-KVKK compliance issues, via the logical interpretation and application of the GDPR-KVKK Articles and Recitals, to real world and hypothetical work/life scenarios.

Training Outline

Day 1 GDPR-KVKK & Privacy Legislation

- Module 1: Introduction to data protection & privacy
- Module 2: GDPR-KVKK Fundamentals & principles
- Module 3: GDPR-KVKK Rights of the data subject
- Module 4: GDPR-KVKK Controllers & processors
- Module 5: GDPR-KVKK Transfers of personal data to 3rd countries or international organisations

- Module 6: GDPR-KVKK Remedies, liabilities & penalties
- Module 7: GDPR-KVKK Supervisory authorities, co-operation, specific situations
- Module 8: Summary of changes

Day 2: Information Governance, Risk Management & Security

Module 1: Information Governance, management, assurance & accreditation

- Outline the importance of governance and having some kind of assurance & accreditation program in place if appropriate
- Cover different approaches to governance e.g. ISO27001 and NIST
- Cover the importance of information asset management control
- Outline what assurance and accreditation is and how organisations can use this as part of demonstrating compliance with the GDPR-KVKK requirements for due diligence

Module 2: Risk management frameworks

- Cover what risk is, emphasise the requirement of risk management in GDPR-KVKK
- Cover different risk methodologies that are available and what the objective is
- Cover residual risk, risk registers and how organisations need to continually monitor risk

Module 3: Information security, monitoring & incident management

- Cover baseline controls
- Cover where organisations can find advice and guidance on implementing cyber security e.g. 10 steps, Cyber Essentials, ICO information security recommendations, ISO27032 etc
- Cover the importance of monitoring – when not if people get in the network and the importance of having good incident management
- Cover incident management process – what is required, how it feeds into the risk process, how it should be used to improve security
- Cover reporting procedure

Day 3: Implementation

Module 1: Transitioning from DPA to GDPR-KVKK

- Having covered the law delegates should have a solid understanding of this but cover the changes in depth here for them to understand everything that is changing
- Summary of changes based on legal overview document
- Use the online ICO self-assessment toolkit for them to understand how they can use that to baseline where they currently are to give them their starting point
- Data streaming/data mapping
- Auditing current compliance – use of tools like e-Discovery to facilitate this
- Identification of policies & procedures which need to be reviewed to bring in line with minimising privacy impact and ensuring compliance

Module 2: Privacy by Design & Data Protection Impact Assessments (DPIA)

- Cover requirement to build in appropriate security from the start
- Cover DPIAs
- Cover impact for failing to do this (business costs – enforcement of failure to do this will be covered later)
- Privacy notices
- Bring Your Own Device (BYOD) & privacy

Module 3: Direct marketing & Online profiling

- Cover consent with regard to direct marketing – what it means
- Cover the issue of online profiling and tracking cookies and what it will require to be compliant with GDPR-KVKK
- The EU PECR is currently in a consultation phase to bring it into line with GDPR-KVKK – discussion of the implications this will have for organisations

Module 4: Obligations of controllers & processors

- How organisations need to ensure that a data subject can exercise their rights
- The obligations on controllers and information they need to provide to data subjects when collecting data from data subjects
- The obligations when they buy data in
- The requirements of notification – to data subjects and others they have passed the data to when a data subject exercises their rights
- The obligations on the controller to ensure a processor is compliant with the GDPR-KVKK
- How the change to liability for a breach still doesn't absolve the controller of their accountability
- Records required
- Exemption for small organisations although it is likely most will adhere – the records are what best practice and good management require or is information that should be on a DPIA anyway

Day 4: Implementation

Module 1: Cloud & Big Data

- Geographic location of cloud
- Legal and jurisdictional issues
- What big data is
- Should we do this vs we can do this – consider repurposing of data issues

Module 2: Staying compliant

- Steps and quick wins to achieve compliance
- Steps to remain compliant

Module 3: Enforcement & supervisory authority powers

- Enforcement regime – summary of the 2%/10 million and 4%/20 million fines
- Summary of enforcement powers the ICO will have – urgency requirements to stop all processing of personal data immediately
- One stop shop – simplification of administration across the EU
- Main establishment determines the supervisory authority
- Legal requirement to co-operate with the supervisory authority

Day 5

Independent APMG GCT Certified GDPR-KVKK Foundation & Practitioner Examination. In class candidates will take a paper based version of the course exam, whilst our AFA delegates will take a remotely proctored exam both to be taken at the end of the course.

Exam Information

Candidates will receive individual emails to access their APMG GCT candidate portal, typically available two weeks post exam. If you experience any issues, please contact the APMG GCT technical help desk on 01494 4520450.

| | |
|-----------|----------------------------------------------------------------------------|
| Duration | 70 minutes |
| Questions | 70, multiple choice (4 multiple choice answers only 1 of which is correct) |
| Pass Mark | 50% |