Learner Guide

Data Protection Act 2018 Training Course

Abstract

The one-day **Data Protection Act 2018 Training Course** provides a comprehensive introduction to the Data Protection Act 2018, and a practical understanding of the implications and legal requirements for organisations of any size. The course is part of the IT Governance data protection pathway.

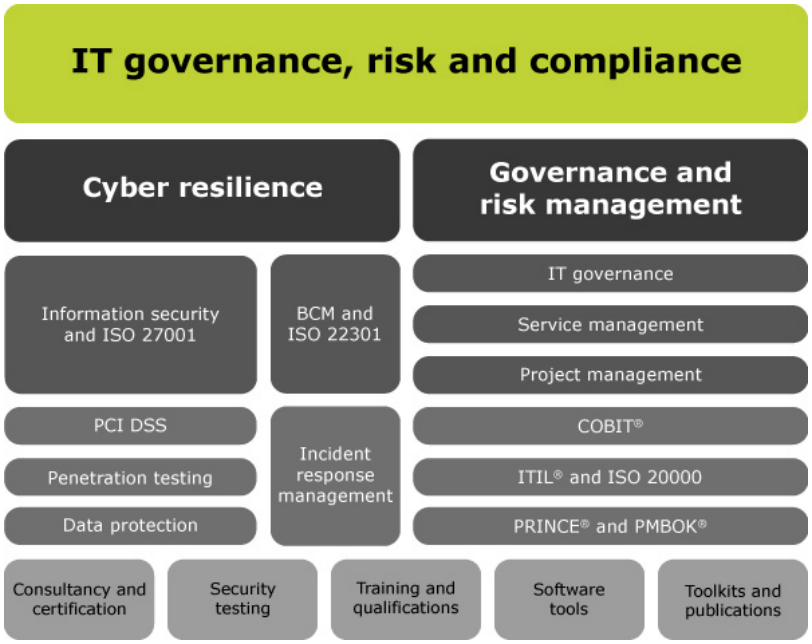
Table of Contents

Introduction

Introduction

Welcome to the Data Protection Act (DPA) 2018 Course. This course does not comprise specific legal advice – legal advice on specific points where the DPA impinges on your business should be sought from your own solicitor or other legal adviser.

IT Governance is a one-stop shop for all your risk and compliance needs. We provide a range of services – consultancy, training, data protection, information security and cyber security – as well as our own products, ranging from books to toolkits, to help you with your information security and data protection compliance.



This one-day course is designed to provide you with knowledge and an understanding of the DPA. It is not designed to teach you the implications and legal requirements of the General Data Protection Regulation (GDPR). For that, you need to take the Certified EU GDPR Foundation course.

Course objectives

By the end of this course you will be able to:

- Recognise the key differences between the DPA 1998, DPA 2018 and the GDPR
- Recognise the circumstances where special categories of data may be processed legitimately
- Recognise the controller's and processor's obligations with respect to the processing of personal data for law enforcement and intelligence services processing.
- Give examples of the exemptions to the rights individuals have over their own data.
- Explain when transfers of personal data to a third country can take place.
- Recall the functions and role of the Information Commissioner.

Introduction

IT Governance training pathway

Action plan

Throughout the course we will refer to the following action plan. The plan's aim is to create a resource that's relevant to you and your role within your organisation.

Timeframe	**Agreed action** – as a result of what I learned on this course, I'm going to…	**How will success be measured?** I'll know that I'm succeeding with this objective when…
Within one week		
Within one month		
Within three months		

90-day check-in: After 90 days, assess your progress.

1. How well did you accomplish your objectives?

2. What in your work environment supported you in achieving your goals?

3. What in your work environment blocked you from achieving your goals?

4. What ongoing goal(s) will you strive to achieve?

Module 1

Module 1 – Scope and definitions

By the end of this module you should be able to:

- Explain the terms and definitions within the DPA;
- Explain the lawful bases that can be applied to a processing activity; and
- Recognise the circumstances where special categories of data may be processed legitimately.

The DPA 2018 received royal assent on 23 May 2018 in the UK.
It modernised the DPA 1998 to accommodate the expansion of an increasingly digital society and of UK data protection laws in general (and the GDPR in particular).

The DPA 2018 provides a comprehensive and modern framework for data protection in the UK, with stronger sanctions for malpractice compared to DPA 1998. Additionally, it addresses data protection in relation to data processing that does not fall within EU law, such as immigration and law enforcement. It provides a framework tailored to the needs of UK law enforcement agencies and intelligence services, in order to protect the rights of victims, witnesses and suspects, including from the various forms of global threats that the UK faces.

The important thing to note is that organisations cannot just look at the GDPR in isolation. Reference will need to be made to the DPA as well. This is particularly true of organisations handling **health data**, **education establishments** and **law enforcement agencies**.

The new act:

- Repeals and replaces the DPA 1998;
- Incorporates the GDPR into UK law and applies GDPR standards to areas not covered by EU data protection law;
- Provides a foundation for the free flow of data between the UK and the EU post-Brexit;
- Sets out permitted derogations under the GDPR;
- Implements the Directive (EU) 2016/680 (the Law Enforcement Directive);
- Provides a framework for data protection for the intelligence services;
- Sets out the duties and powers of the UK Information Commissioner's Office (ICO); and
- Sets out enforcement provisions.

Further reading:

The Data Protection Act 2018: www.legislation.gov.uk
The GDPR: www.itgovernance.co.uk/articles-of-the-gdpr

Module 1

The DPA has seven **parts**, followed by numerous **schedules**, which provide supplementary information to chapters within the parts:

Key definitions

Controller	A "data controller" is responsible for complying with data protection law. They are defined in Article 4 of the GDPR as the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.
Processor	A "data processor" means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.
Public authority	For the purposes of the GDPR, the following (and only the following) are "public authorities" and "public bodies" under UK law: a) A public authority as defined by the Freedom of Information Act 2000.

Module 1

	b) A Scottish public authority as defined by the Freedom of Information (Scotland) Act 2002 (asp 13). c) An authority or body specified or described by the Secretary of State in Regulations.
Health professional	Includes a registered: a) Medical practitioner b) Nurse or midwife c) Dentist d) Optician e) Osteopath f) Chiropractor g) Pharmacist h) Psychotherapist
Education data	Personal data consisting of information that constitutes an educational record, but is not data concerning health.
Certification provider	A person who issues certification for the purposes of Article 42 of the GDPR.
National accreditation body	The national accreditation body for the purposes of Article 4(1) of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.
Freedom of Information (FOI) public authority	A public authority as defined in the Freedom of Information Act 2000, or a Scottish public authority as defined in the Freedom of Information (Scotland) Act 2002 (asp 13).
Competent authority	A person specified or described in Schedule 7 of the DPA, and any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes.
Automated or structured processing of personal data	The processing of personal data wholly or partly by automated means, and the processing otherwise than by automated means of personal data that forms part of a filing system or is intended to form part of a filing system.
Manual unstructured processing of personal data	The processing of personal data that is not the automated or structured processing of personal data.

Notes section:

Module 1

Fill in learner guide

Quick question 1: Which of these definitions under the DPA are incorrect?

a) *A "processor" means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.*

b) *Education data is personal data consisting of information that constitutes an educational record, and data concerning health.*

c) *A certification provider is a person who issues certification for the purposes of Article 42 of the GDPR.*

d) *A "controller" is responsible for complying with data protection law.*

_____

Answer

The DPA 2018 and the GDPR

Part	Heading
1	Preliminary
2	General processing
3	Law enforcement processing
4	Intelligence services processing
5	The Information Commissioner
6	Enforcement
7	Supplementary and final provision
8	Schedules

Chapter	Heading
I	General provisions
II	Principles
III	Rights of the data subject
IV	Controller and processor
V	Transfer of personal data to third countries
VI	Independent supervisory authorities
VII	Cooperation and consistency
VIII	Remedies, liabilities and penalties
IX – XI	Various specific provisions

The DPA 2018 provides a comprehensive and modern framework for data protection in the UK, with stronger sanctions for malpractice compared to DPA 1998. Additionally, it addresses data protection in relation to data processing that does not fall within EU law, such as immigration and law enforcement. It provides a framework tailored to the needs of UK law enforcement agencies and intelligence services, in order to protect the rights of victims, witnesses and suspects, including from the various forms of global threats that the UK faces.

The important thing to note is that organisations cannot just look at the GDPR in isolation. Reference will need to be made to the DPA as well. This is particularly true of organisations handling **health data**, **education establishments** and **law enforcement agencies**.

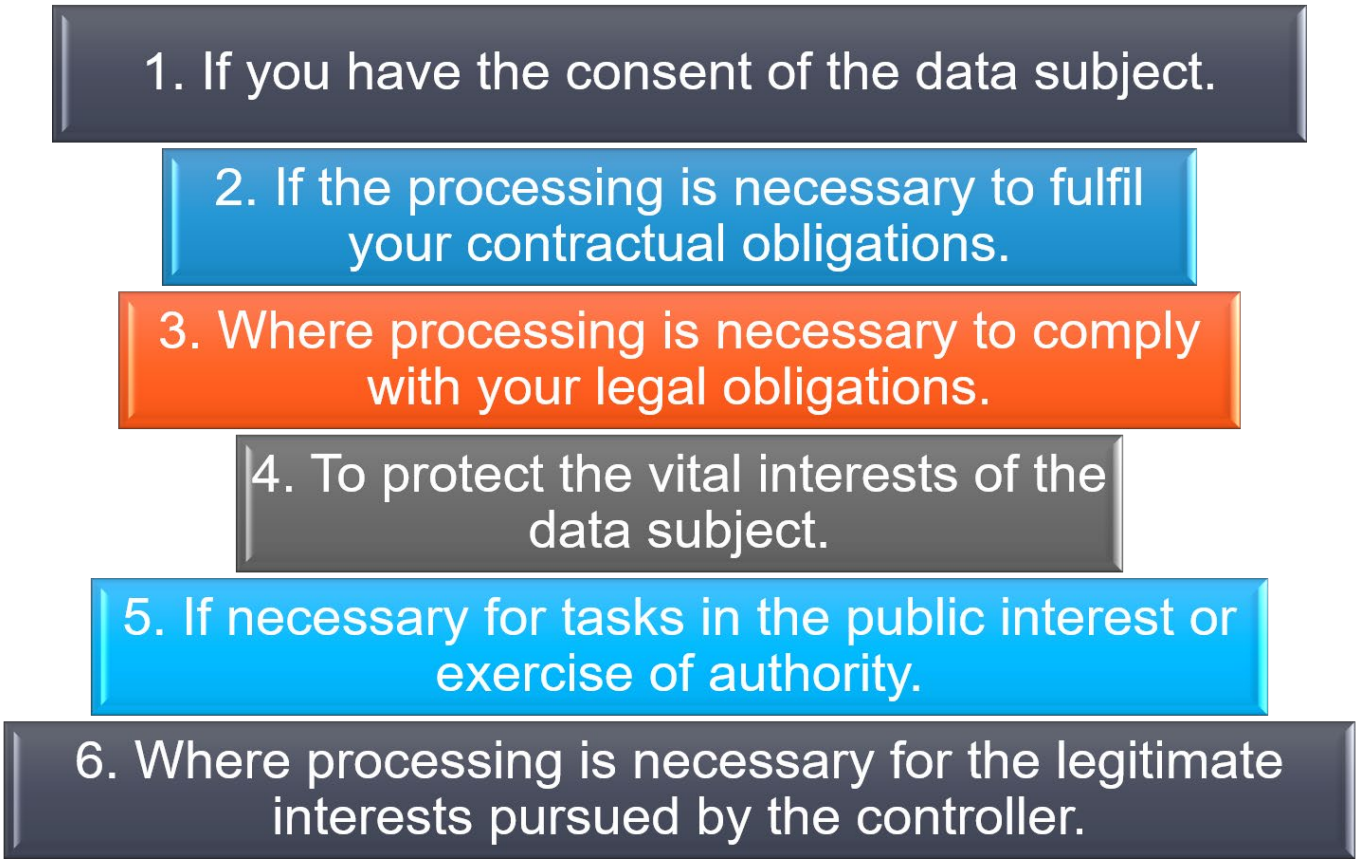
The DPA 2018 should be read in tandem with the GDPR.

Module 1

A comprehensive comparison between the DPA 1998, the GDPR and the DPA 2018 can be found at Appendix 1.

The six lawful bases for processing personal data

Article 6 of the GDPR explains what lawfulness is in the context of processing personal data.



Quick question 2:

The DPA offers further clarification regarding the use of the lawful basis 'processing is necessary for tasks in the public interest'. This processing must be necessary for one of five reasons – what do you think the five reasons could be?

_____

_____

_____

Answer

Resource Section

Learner guide answers

Quick question 1: Which of these definitions under the DPA are incorrect?

a) *A "processor" means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.*

b) *Education data is personal data consisting of information that constitutes an educational record, and data concerning health.*

c) *A certification provider is a person who issues certification for the purposes of Article 42 of the GDPR.*

d) *A "controller" is responsible for complying with data protection law.*

Answer: b) is incorrect

The correct wording of the incorrect definition is:

Education data	Personal data consisting of information that constitutes an educational record, **but is not** data concerning health.

Quick question 2

The DPA offers further clarification regarding processing of personal data using the lawful basis of necessary for tasks in the public interest. This processing must be necessary for one of five reasons – what do you think the five reasons could be?

Answer:

1. The administration of justice;
2. The exercise of a function of either House of Parliament;
3. The exercise of a function conferred on a person by enactment or rule of law;
4. The exercise of a function of the Crown, a Minister of the Crown or a government department; or
5. An activity that supports or promotes democratic engagement.