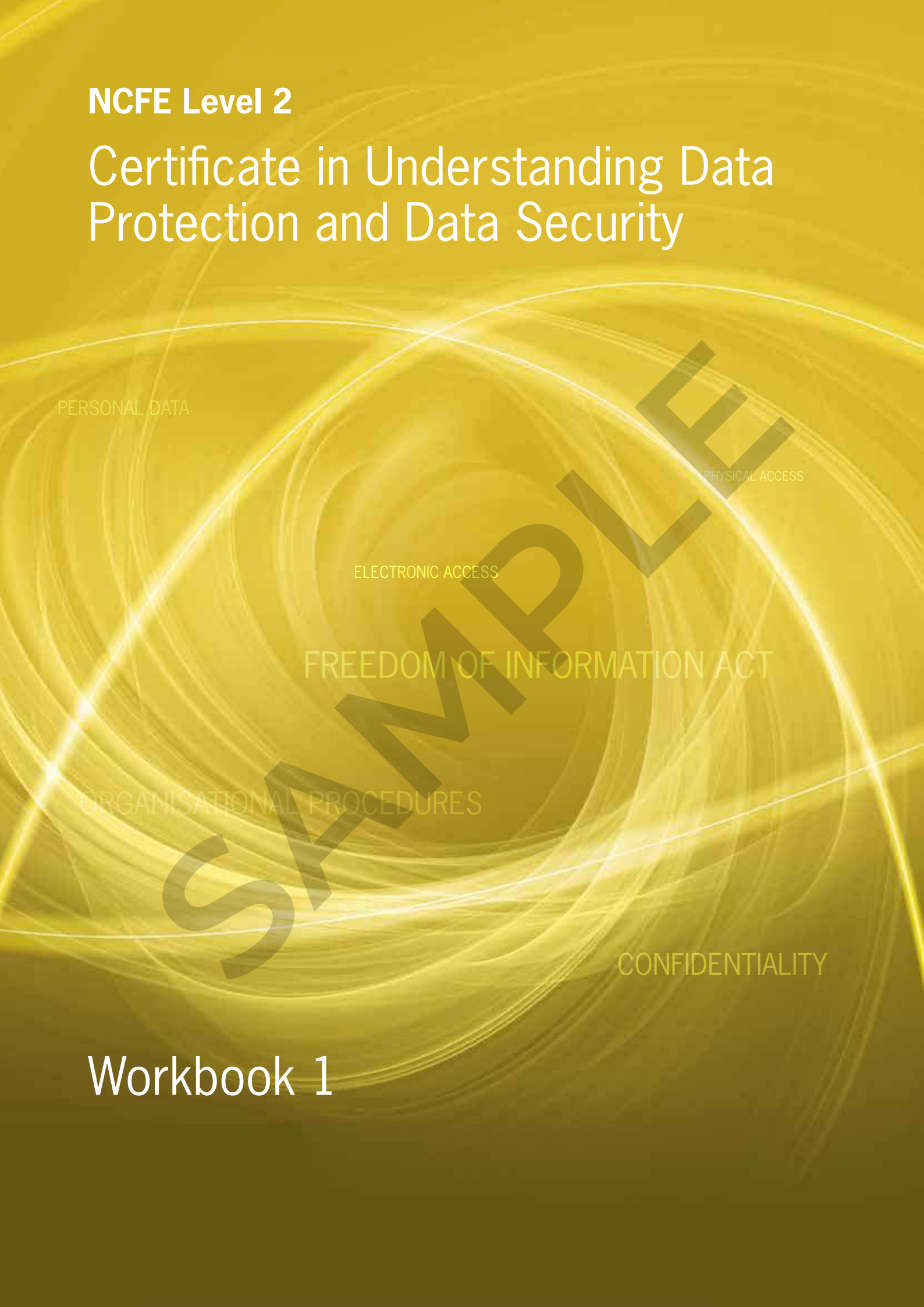
NCFE Level 2

Certificate in Understanding Data Protection and Data Security



Workbook 1

In this section, you will learn about the GDPR, including what it is, its purpose and what organisations need to do to meet the associated legal requirements.

Personal data

Please read the following as it will help you to answer question 1.

Personal data is any information that can be used to identify a specific person, for example:

- a name
- address
- date of birth
- IP address (a computer's unique identification number)
- genetic or biometric data, e.g. fingerprints
- information about criminal convictions

There isn't a definitive list about what is considered to be personal data under the General Data Protection Regulation (GDPR) 2018; however, personal data is defined in the Regulation as:

> "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

For example, a name on its own such as Jack Jones may not be considered personal data because there are thousands of people with that name, but a name with a date of birth and address would allow an individual to be identified.

The purpose of the General Data Protection Regulation

Please read the following as it will help you to answer question 2.

The GDPR is European legislation that was brought into effect in May 2018 to replace the Data Protection Act 1998. It is used alongside the new Data Protection Act 2018, which will be used in the UK after it leaves the EU. The main purpose of the GDPR is to create data protection laws that will protect all members of the European Union.

Additionally, the GDPR:

- increases privacy
- extends EU residents' data rights
- provides authorities with powers to take action against any organisation that breaches the regulation
- ensures that all new businesses that use personal data follow the regulation
- ensures that businesses outside the EU collect and process the personal data of EU residents according to the regulation

The role of a data controller and a data processor

Please read the following as it will help you to answer question 3.

The GDPR applies to two different groups: data controllers and data processors.

A **data controller** is a: "natural or legal person, public authority, agency or other body" which decides how and why personal data will be processed.

A **data processor** is a: "natural or legal person, public authority, agency or other body" which processes data for the controller.

Example

A plumbing supply company has 50 employees. It signs a contract with a payroll firm that provides the IT system and stores all of the company's staff data, including employee names and addresses, National Insurance numbers, wage amounts and when wages should be paid. This agreement makes the plumbing supply company the **controller** and the payroll firm the **processor**.

Did you know?

The more information we provide online, the more companies can tailor advertisements to what we like and who we are. Online advertising in the UK generates over £10 billion in revenue by monetising people's online activities.

The key principles of the general data protection regime

Please read the following as it will help you to answer question 4.

The GDPR provides a range of key principles that organisations must include in their data protection regime (policies and procedures) to stay compliant. Read the information in the following table to learn about each of the principles.

Principle	Description
Lawfulness, fairness and transparency	Lawful: data subjects should be told what data processing will be done. Fair: data must be processed in the way described to the data subject. Transparent: processing must meet the tests described in the GDPR.
Purpose limitation	Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
Data minimisation	Only data that is relevant and limited to what is necessary in relation to the purposes for which they are processed should be gathered.
Accuracy	Data must be accurate and kept up to date, and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.
Storage limitation	Data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Integrity and confidentiality	Data must be processed in a way that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
Accountability	The organisation is responsible for complying with GDPR and must be able to show compliance if asked to do so. Compliance includes creating and implementing data protection policies, creating contracts with organisations that process personal data, reporting personal data breaches and putting security measures in place.

[Source: Article 5, GDPR]

A lawful basis for processing personal data

Please read the following as it will help you to answer question 5.

Under the GDPR, an organisation must have a lawful reason for processing personal data. There are 8 lawful bases for processing personal data in the GDPR, and organisations must choose the lawful basis that is most appropriate to the purpose and relationship with the individual.

Processing personal data must be necessary to a company's purpose, otherwise it will not be permitted to process. Whichever basis is chosen, it should be included in the organisation's privacy notice.

Read the information in the following table to learn about each lawful basis.

Lawful basis	Explanation
Consent	● A consent basis means that an organisation must offer individuals choice and control over their personal data. ● This basis requires individuals to 'positively opt in', which means they have to select a box themselves, not de-select a pre-ticked box. ● Consent requires a clear and specific statement of consent and requests should be kept separately from other terms and conditions. ● Blanket consents are not acceptable – individual consents have to be received for separate things. ● Consents must be clear and concise. ● It must be easy for an individual to withdraw consent at any time. ● Organisations must keep evidence of consent and review consent on a regular basis, updating it with any changes as necessary. ● Consent shouldn't be made a precondition of a service.
Contract	This basis is used when an organisation processes personal data because it has a contractual obligation to them or because the individual has asked the organisation to do something before entering into a contract, e.g. providing a quote. The organisation should document the decision to use this basis and be able to provide an appropriate justification, if asked.

Legal obligation	To use this basis, an organisation must be processing personal data to comply with a common law or statutory obligation. The organisation should document the decision to use this basis and be able to provide the appropriate law that requires personal data to be processed.
Vital interests	This is a very limited basis that can only be used to justify processing personal data to "protect the vital interests of the data subject", i.e. in life or death situations. For example, if a hospital needs to access a new patient's medical records in an emergency.
Public task	Public task requires that the task being carried out has a clear legal basis. Personal data can be processed "in the exercise of official authority", which includes legal powers and functions. Personal data can also be processed if doing so will be in the public's interest. This basis is used most often by public authorities.
Legitimate interests	This basis is described as "the most flexible" for processing; data must be used in a reasonable way and its processing should not have much of an impact on the individual's privacy. There must also be a "compelling justification", i.e. a good reason, for the processing. To use this basis, an organisation must be able to: ● identify a legitimate interest, e.g. your own interests or those of third parties ● show that the processing is necessary to achieve the legitimate interest ● balance the legitimate interest against the individual's interests, rights and freedoms
Special category data	Under the GDPR, sensitive data, such as information on an individual's race, gender, trade union membership and sexual orientation, falls into this lawful basis. Using this basis, organisations also have to prove that there is a lawful reason to process personal data. There are 10 conditions for processing special category data in the GDPR.
Criminal offence data	Criminal offence data includes information on criminal allegations, proceedings or convictions. To process personal data about criminal offences, there must be a lawful basis and the organisation must also have legal or official authority.

[Source: **www.ico.org.uk**]

SECURITY CHECKS

PROTECT ICT SYSTEMS

Disclaimer

Every effort has been made to ensure that the information contained within this learning material is accurate and reflects current best practice. All information provided should be used as guidance only, and adapted to reflect local practices and individual working environment protocols.

All legislation is correct at the time of printing, but is liable to change (please ensure when referencing legislation that you are working from the most recent edition/amendment).

Neither Learning Curve Group (LCG); nor their authors, publishers or distributors accept any responsibility for any loss, damage or injury (whether direct, indirect, incidental or consequential) howsoever arising in connection with the use of the information in this learning material.

Whilst NCFE has exercised reasonable care and skill in endorsing this resource, we make no representation, expressed or implied, with regard to the continued accuracy of the information contained in this resource. NCFE does not accept any legal responsibility or liability for any errors or omissions from the resource or the consequences thereof.

If you have any queries, feedback or need further information please contact:

Learning Curve Group
1-10 Dunelm Rise
Durham Gate
Spennymoor, DL16 6FS
info@learningcurvegroup.co.uk
www.learningcurvegroup.co.uk

This resource has been endorsed by national Awarding Organisation, NCFE. This means that NCFE has reviewed it and agreed that it meets the necessary endorsement criteria.

ncfe. endorsed

LCG-DPDS November 2018
Version 1 (603/3639/0)