



The Digital Skills Standard

ICDL Workforce

DATA PROTECTION

Syllabus 1.0



Learning Material

Provided by:
ICDL Malta

Copyright ICDL Foundation 2018 - 2019. All rights reserved. Reproducing, repurposing, or distributing this courseware without the permission of ICDL Foundation is prohibited.

ICDL Foundation, ICDL Europe, ICDL, ECDL and related logos are registered business names and/or trademarks of ECDL Foundation.

This courseware may be used to assist candidates to prepare for the ICDL Foundation Certification Programme as titled on the courseware. ICDL Foundation does not warrant that the use of this courseware publication will ensure passing of the tests for that ICDL Foundation Certification Programme.

The material contained in this courseware does not guarantee that candidates will pass the test for the ICDL Foundation Certification Programme. Any and all assessment items and / or performance-based exercises contained in this courseware relate solely to this publication and do not constitute or imply certification by ICDL Foundation in respect of the ICDL Foundation Certification Programme or any other ICDL Foundation test. This material does not constitute certification and does not lead to certification through any other process than official ICDL Foundation certification testing.

Candidates using this courseware must be registered with the National Operator before undertaking a test for an ICDL Foundation Certification Programme. Without a valid registration, the test(s) cannot be undertaken and no certificate, nor any other form of recognition, can be given to a candidate. Registration should be undertaken at an Approved Test Centre.

ECDL Data Protection

The ECDL Data Protection module sets out essential knowledge relating to data protection concepts and principles, data subject rights, the implementation of data protection policies and measures, and regulatory compliance.

On completion of this module you will:

- Understand concepts relating to personal data and its protection.
- Understand the rationale, objectives, and scope of the European Union General Data Protection Regulation
- Outline the key principles of the GDPR relating to the lawful processing of personal data.
- Understand the rights of data subjects and how they are upheld.
- Understand that company policies and methods should comply with data protection regulations, and outline key technical and organisational measures to achieve this.
- Understand how to respond to data breaches and the consequences of not complying with data protection regulations.

What are the benefits of this module?

Being familiar with data protection legislation and best practices is essential if you are involved in processing personal data. This module builds the foundational knowledge and introduces the relevant regulations underpinning data protection. Once you have developed the skills and knowledge set out in this book, you will be in a position to become certified in an international standard in this area - ECDL Data Protection.

ECDL DATA PROTECTION

LESSON 1 - THE RATIONALE FOR DATA PROTECTION	1
1.1 Defining Privacy	2
1.2 Recognising Risks	3
1.3 Privacy Rights.....	6
1.4 Data Protection	7
1.5 The General Data Protection Regulation.....	9
1.6 Review Exercise	12
LESSON 2 – DATA PROTECTION DEFINITIONS	13
2.1 Personal Data	14
2.2 Data Processing.....	16
2.3 Data Controller.....	17
2.4 Data Processor	17
2.5 Controller - Processor Example	18
2.6 Review Exercise	21
LESSON 3 – DATA PROTECTION PRINCIPLES	22
3.1 The Data Protection Principles.....	23
3.2 Lawfulness, Fairness and Transparency.....	24
3.3 Purpose Limitation	24
3.4 Data Minimisation	25
3.5 Accuracy.....	26
3.6 Storage Limitation	27
3.7 Integrity & Confidentiality	28
3.8 Accountability.....	29
3.9 Review Exercise	31
LESSON 4 – LAWFUL BASES FOR DATA PROCESSING	32
4.1 When is Data Processing Allowed?.....	33
4.2 The Lawful Bases	34
4.3 Appropriate Lawful Basis	36
4.4 Using Consent as a Lawful Basis	37
4.5 Issues Around Consent.....	39
4.6 Review Exercise	41
LESSON 5 – DATA SUBJECT RIGHTS	42
5.1 Data Subject Rights	43

5.2 The Right to be Informed	44
5.3 Privacy Notices	44
5.4 The Right of Access.....	48
5.5 Other Rights.....	49
5.6 Review Exercise	52
LESSON 6 – PERSONAL DATA BREACHES.....	53
6.1 Personal Data Breaches	54
6.2 Impact Of A Breach.....	54
6.3 Communicating a Data Breach	56
6.4 Minimising Data Breach Problems	58
6.5 Review Exercise	61
LESSON 7 – ORGANISATIONAL RESPONSIBILITIES	62
7.1 Accountability Requirement.....	63
7.2 Accountability Measures	63
7.3 Data Protection Officer.....	66
7.4 Privacy Planning	67
7.5 Review Exercise	72
LESSON 8 – ENFORCEMENT.....	73
8.1 Supervisory Authority	74
8.2 Tasks	75
8.3 Sanctions and Penalties.....	76
8.4 Review Exercise	80
References	81
ECDL SYLLABUS.....	82

LESSON 1 - THE RATIONALE FOR DATA PROTECTION

In this section, you will learn about:

- Defining privacy
- Recognising risks
- Privacy rights
- Data protection
- The General Data Protection Regulation

1.1 DEFINING PRIVACY

What is Privacy?

Everyone has an understanding of the concept of privacy and if asked, most people can offer a definition of what privacy means to them.

Take a moment to think about your own understanding of privacy. Try and come up with your own definition of privacy in one or two sentences.

There is no single definition of privacy. People's perspectives on privacy are influenced by many different factors. Here are some typical responses that people give when asked what privacy means to them:

- The right to be left alone.
- Freedom from interference by other people.
- The right to keep personal matters secret from others.
- A capacity to limit the sharing of personal information.
- The ability to act and communicate without intrusion by others.

People generally perceive privacy rights to cover a number of different aspects of their lives including, but not limited to:

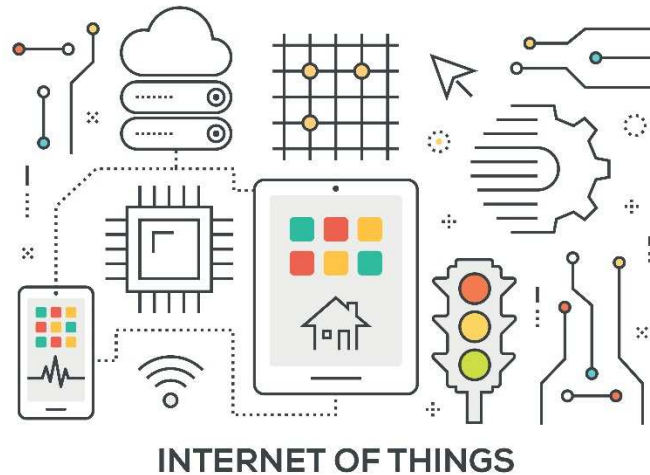
- Their bodies and personal space.
- Their physical movements and behaviours.
- Their political thinking, philosophies.
- Their sex lives and orientations.
- Their digital lives and communications.

Surveys of opinion provide evidence that people have different tolerances for sharing information about aspects of their personal lives and that views can be influenced by many factors including demographics, geography and societal norms.

Technology's Influence on Privacy

Technological developments often present new challenges to personal privacy. For example, over the last one hundred years, privacy debates have been provoked by the popular adoption and availability of technologies such as:

- Photography and the ready publication of illustrated newspapers.
- The telephone and the subsequent "bugging" of telephone conversations.
- The personal computer.
- DNA fingerprinting.
- The mobile telephone.
- The Internet.



In the past decade new privacy challenges have arisen with the public adoption of innovations such as:

- Drones.
- The Internet of Things.
- Wearable devices.
- Artificial intelligence systems.

Relationship between Privacy and Data Protection

The European Data Protection Supervisor (EPDS), the EU's independent data protection authority, offers the following definition of privacy.

Privacy is the ability of an individual to be left alone, out of public view, and in control of information about oneself. One can distinguish the ability to prevent intrusion in one's physical space ("physical privacy", for example with regard to the protection of the private home) and the ability to control the collection and sharing of information about oneself ("informational privacy").

(EPDS website accessed February 2018

edps.europa.eu/data-protection/data-protection/glossary_en)

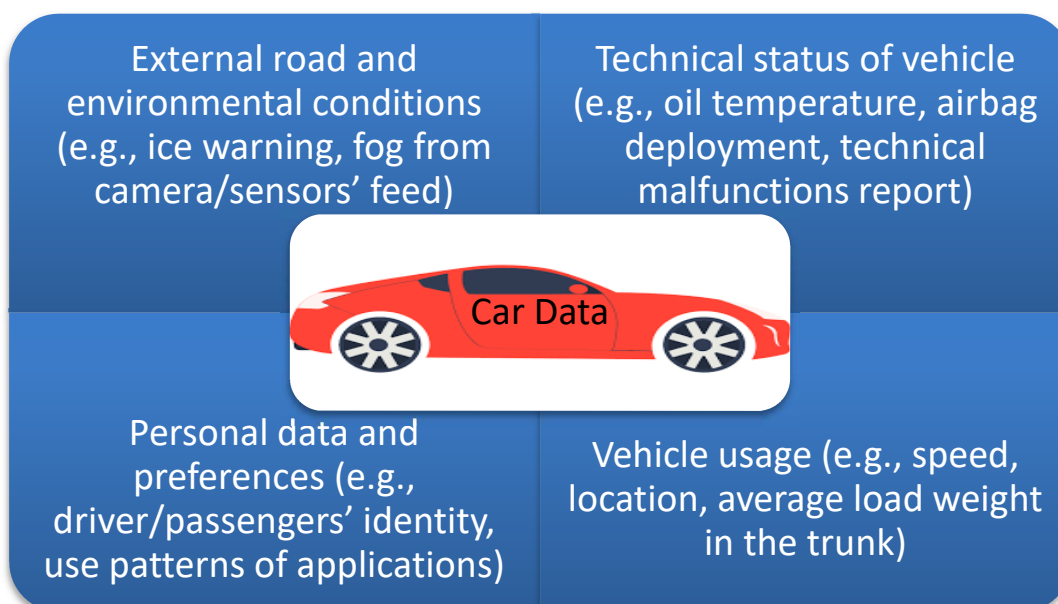
The concept of privacy therefore overlaps, but does not coincide with, the concept of data protection.

1.2 RECOGNISING RISKS

As computing power has grown, new challenges are prompted by the enormous volume of personal data that is being collected, used and stored. We are witnessing a so-called 'data deluge' effect: where the amount of personal data that exists is processed and is further transferred, continues to grow.

...the ever-increasing amount of personal information is accompanied by an increase in its value in social, political and economic terms. In some sectors, particularly in the on-line environment, personal data has become the de facto currency in exchange for on-line content. ... as personal information becomes more valuable for data controllers across sectors, citizens, consumers and society at large are also increasingly aware of its significance. This in turn reinforces the need to apply stringent measures to safeguard it. (Article 29 Data Protection Working Party Opinion WP173 on Accountability)

Data analytics, coupled with location and behavioural tracking, is generating more and more data points linked to individual citizens. This creative exploitation of personal data is helped by cheaper access to faster data processing, as well as innovations in areas such as machine learning and artificial intelligences. Such developments have a significant potential to contribute positively to society. However, there is also the need to consider their potential to impact on human rights and freedoms.



Categories of data generated by car usage

To choose just one example, developments in automotive technology now means that undertaking a car journey has the potential to generate a very large volume of data, at least some of which would be defined as “personal data.”

While this increased harvesting and connectivity of automotive data has the potential to contribute positively to road safety and provide other benefits (improved navigation and fuel efficiency) there also needs to be consideration of the potential risks.

It is important to recognise that privacy risks are not just related to innovations in physical hardware and infrastructure but also derive from new and unprecedented ways that personal data is now being mined and exploited. For example, inappropriate data profiling and exploitive use of personal data to capture insights

into individual and group trends, movements and activities has a real potential to damage civil liberties.



As more data is generated and travels across the globe, the risks of data breaches also increase. This emphasises the need for organisations, both in the public and private sectors, to implement real and effective internal mechanisms to safeguard the protection of individuals' information.

...breaches of personal information may have significant negative effects for data controllers in public and private sectors. Potential glitches in eGovernment, eHealth applications can have devastating consequences in both in economic and particularly in reputational terms. Thus, minimising risks, building and maintaining a good reputation, and ensuring the trust of citizens and consumers is becoming crucial for data controllers in all sectors. (Article 29 Data Protection Working Party Opinion WP173 on Accountability)



The consequences when privacy is lost are serious e.g. identity theft, fraud, financial loss, threat to professional secrecy.

In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage. (GDPR Recital 83)



In summary, when organisations are examining the possible collection and use of personal data it is important that consideration is given to any impact on “the rights and freedoms.” And while a risk evaluation will primarily concern the right to privacy, it may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

1.3 PRIVACY RIGHTS

The Right to Privacy

The right to privacy was enshrined as one of the articles of the *Universal Declaration of Human Rights* adopted by United Nations General Assembly in 1948.

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. (UDHR Article 12)

Privacy was also the subject of one of the articles when the Council of Europe drafted the *European Convention of Human Rights* in 1950.

Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. (ECHR Article 8)

One can distinguish the ability to prevent intrusion in one's physical space ("physical privacy", for example with regard to the protection of the private home) and the ability to control the collection and sharing of information about oneself ("informational privacy").



Recognition of an increasing automation and movement of data prompted the OECD to publish in 1980 what were in effect the first international set of privacy principles, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. These guidelines incorporated a set of core principles that had a significant influence on subsequent data protection provisions.

The *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* was adopted by the Council of Europe in 1981. This Convention 108 was the first legally binding international instrument in the area of data protection. Unlike the OECD Guidelines (which were non-binding) it required signatories to take steps in their domestic legislation to apply the principles.

In 1995, with the objective of better aligning data protection within the member states, the EU adopted Directive 95/46/EC *on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, usually referred to as the “1995 Directive”.

The EU *Charter of Fundamental Rights* (2009) in separate articles identifies both “privacy” and “data protection” as fundamental rights.

Respect for private and family life: Everyone has the right to respect for his or her private and family life, home and communications.
(EU Charter of Fundamental Rights, Article 7)

Protection of personal data: 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.
(EU Charter of Fundamental Rights, Article 8)

1.4 DATA PROTECTION

As the previous section has illustrated, the widespread adoption of computer technologies in the 1980s prompted heightened concerns about the increasing impact of new technologies on privacy. These concerns were addressed through

introducing legislation to govern the processing of personal data. These legal safeguards are now enshrined in an area of legislation known as “Data Protection.”

Benefits both for the individual and for society

Data Protection regulations have a primary focus on the individual i.e. on protecting the informational privacy of citizens. Nowadays nearly all civic and economic activity is dependent on there being a sufficient level of trust in how personal data will be treated by all sorts of organisations, whether there to serve business, government or society in general.

Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data. (GDPR Recital 6)

While compliance with data protection legislation undoubtedly demands an investment of time and other resources from organisations, this brings benefits by helping to build trust without which it would be difficult for the digital economy to function and develop.

Privacy as a fundamental (but not an absolute) right

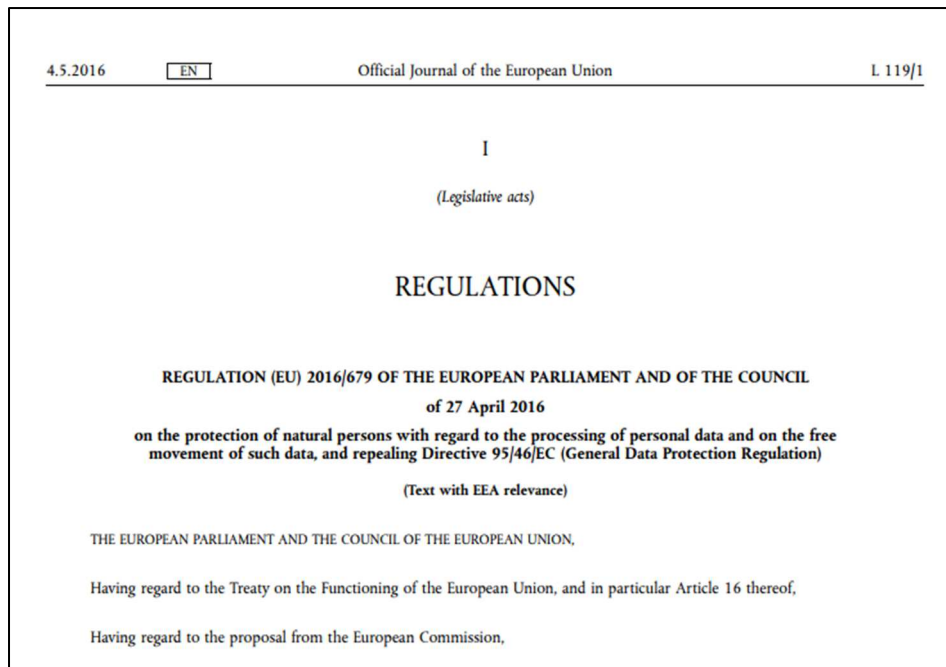
The right to the protection of personal data is not an absolute right. It needs to be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.

This means that sometimes other civil goods, such as freedom of speech or the prevention of crime, may take precedence over protecting personal privacy.

1.5 THE GENERAL DATA PROTECTION REGULATION

Rationale

The General Data Protection Regulation was adopted by the European Parliament in 2016 (with an enforcement date of 25th May 2018).



It replaced the European 1995 Directive on Data Protection.

A standard set of regulations

The GDPR is applicable as European law throughout the EU (in practice the European Economic Area, which is the EU plus Norway, Iceland, and Lichtenstein). As it is a “Regulation” (as opposed to a “Directive”) it provides for the first time a standard legal basis for protecting personal data across all the countries of the European Economic Area (EEA).

Additional Member State legislation

Just as there are many different dimensions to privacy, the rights of citizens, can stem from a number of different bases. For European residents, privacy rights also derive from legislation specific particular jurisdictions e.g. national laws and constitutions.

While GDPR imposes a standard in how personal data must be processed and protected throughout the EEA, there is scope for member states to provide additional legislation to clarify some aspects of data protection.

Member state legislation (usually in the form of a Data Protection Bill adopted by national parliament) sets out the structures that are required to support GDPR implementation within a particular country or jurisdiction such as the mechanisms for imposing sanctions and collecting fines.

When does GDPR apply?

GDPR applies in nearly all circumstances in which personal data is being processed. The regulation sets this out as follows:

This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. (GDPR Article 2, Material Scope)

So GDPR is applicable to personal data held in digital format (automated) and to nearly all manual data (i.e. personal data stored in hard copy format).

GDPR does not apply to the personal data of deceased persons (although the regulation does not prevent member states from addressing this in national legislation).

Where does GDPR apply?

One of the significant changes that has been implemented with GDPR relates to the territorial scope of data processing.

This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. (GDPR Article 3, Territorial Scope)



This means that GDPR has an extraterritorial scope in that its reach extends beyond Europe. Organisations located outside the EU fall within the scope of the regulation if they are undertaking processing activities that involve the offering of goods or services within the EU. For example, the processing and storage of a European Citizen's data through the cloud by a non-EU country is covered and subject to the regulations of the GDPR. This is the case irrespective of whether a payment is required, for example, GDPR will apply to companies who are monitoring behaviour, such as website tracking, if that behaviour takes place within the Union.

Data Controllers outside EEA are required to appoint a representative who is resident within the EEA.

In general, transfers of personal data to third countries or international organisations for processing are only permitted if the level of protection of the personal data in the third country or international organisation is at least equivalent to that provided by the GDPR.

Some GDPR exceptions

Where personal data is in a physical format and is also unstructured (i.e. lacking any form of organisation or indexation) then GDPR may not apply.

There are also a limited, but nonetheless very significant, number of processing activities to which GDPR does not apply. Examples include activities relating to:

- A purely personal or household activity.
- The prevention, investigation or prosecution of criminal offences.
- The prevention of threats to public security.

1.6 REVIEW EXERCISE

1. The right to privacy is one of the fundamental rights that is protected under European Charter. List some aspects of private life that the “fundamental right to privacy” might help to protect.

2. List some other fundamental rights that are protected under European Charter.

3. Explain the difference between a “Directive” and a “Regulation” under EU law. Into which category does the GDPR fall?

4. Look at each of the following examples and decide whether it comes within the scope of GDPR.
 - (i) Maintaining a home database (containing names, addresses and telephone numbers) for the purpose of communicating with friends and family.
 - (ii) Maintaining a database (containing names, addresses and telephone numbers) while acting as voluntary secretary to a sports club.
 - (iii) Maintaining in a home office a database containing a list of business names and addresses.

LESSON 2 – DATA PROTECTION DEFINITIONS

In this section, you will learn about:

- Personal data
- Data processing
- Data controller
- Data processor

2.1 PERSONAL DATA

Data Subject

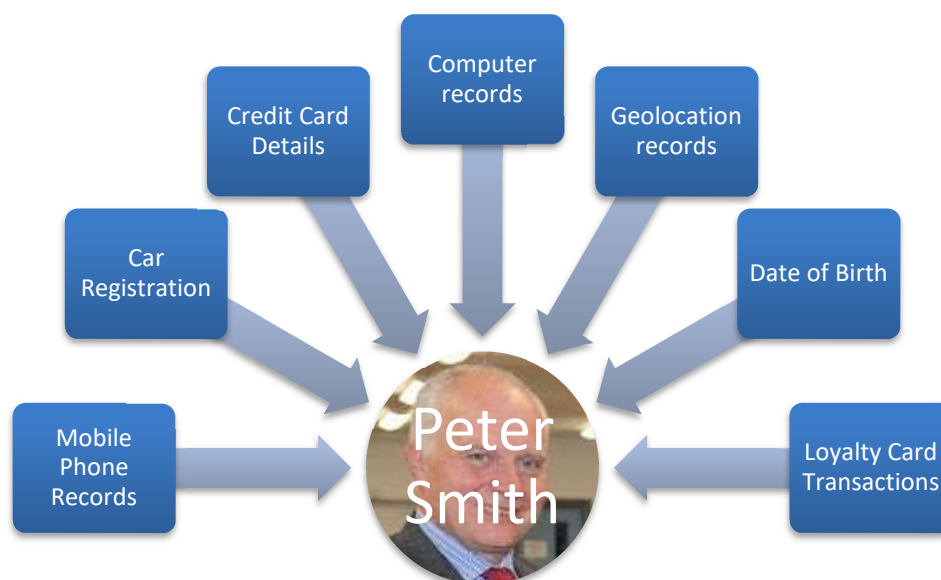
Data protection law is only relevant to **personal data**. This is data that can be linked to an identifiable living person. Living persons are known as **data subjects** under data protection legislation.

Natural Person and Legal Person

Data protection law uses the term **natural person** to refer to a living person. The term **legal person** is also used. This term refers to an organisation, for example a company or corporation, which can take on legal responsibility. Data protection law applies to natural persons only.

When is Data classified as Personal?

For data to be considered personal data, it must be possible to connect it to a living human being. Sometimes there is no doubt that we are dealing with personal data because the linkage between the data and an individual is very easy to see. On other occasions, the connection may not be as obvious, but if it is somehow possible to connect the data we are using to an identifiable person then we are in fact handling personal data.



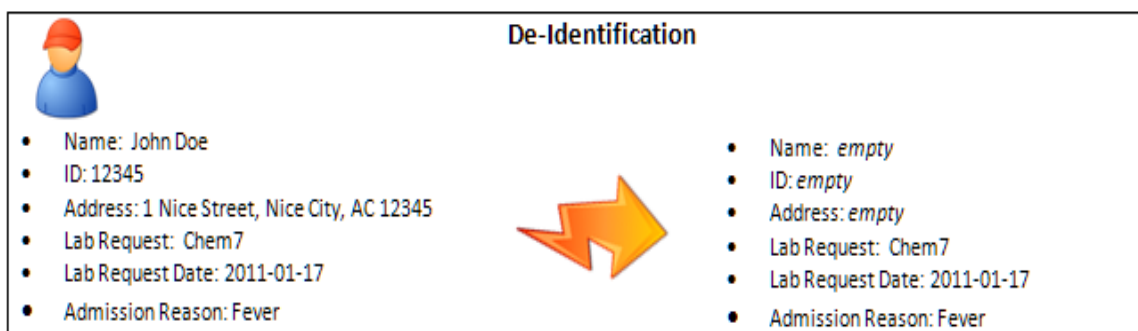
Personal Data can be linked with an Identifiable Person

The definition used in the GDPR makes it clear that personal data should be understood in very broad terms.

‘personal data’ means 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; (GDPR Article 4, Definitions)

Pseudonymisation

One way of protecting personal data during processing is to remove the most obvious identifiers, such as a person’s name. This helps to protect the data subject’s identity during processing.



Pseudonymisation of Personal Data

An example of pseudonymisation would be sending a blood sample for medical testing. The blood sample is identified with a code rather than by patient name. The results of the blood test are then sent back to the doctor using the same code as reference. The doctor then links the test results with the patient name so that the results can be given to the patient.

‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person; (GDPR Article 4, Definitions)

Anonymisation

The blood test results remain personal data because it is possible to use additional information to associate the results with the names of specific patients. If it were not possible to link the results with patient names then the data would have been anonymised (rather than pseudonymised).

If we anonymise personal data then it should never be possible in the future to re-establish a linkage between the data and the data subjects. Such data is no longer “personal data” and consequently the data protection regulations no longer apply to its processing.

Special Categories of Personal Data

Medical data (used in the previous example) is an example of a special category of personal data. GDPR defines special categories as personal data that reveals (or has the potential to reveal):

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic information.
- Biometric information.
- Health information.
- Information concerning a natural person’s sex life or sexual orientation.

The processing of personal data that falls into these categories is prohibited unless certain conditions are satisfied.

2.2 DATA PROCESSING

What is Data Processing?

The term *data processing* is defined in the GDPR as follows:

‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; (GDPR Article 4, Definitions)

This shows that data processing needs to be understood in very broad terms. It isn’t necessarily a complex activity. The simple act of viewing personal data in a paper file or on a computer screen is considered as a “data processing” activity. In fact, even if the personal data is simply being held in a file somewhere (and not being viewed or consulted in any way) this “storage” activity is likely to satisfy the GDPR definition of data processing.

2.3 DATA CONTROLLER

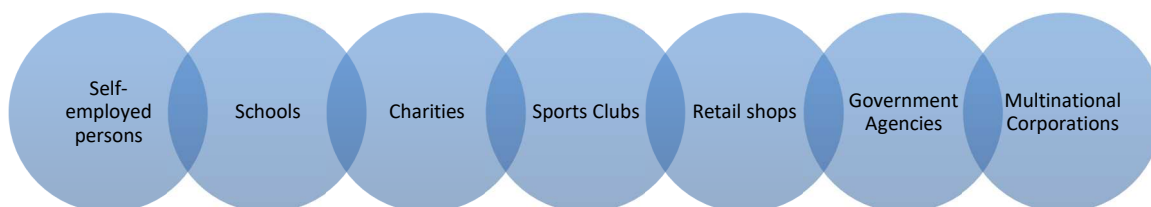
A Data Controller makes decisions about how personal data is collected and used. The term is defined within GDPR as follows.

‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; (GDPR Article 4, Definitions)

So, organisations that decide to collect or use personal data in any way are in fact acting as “Data Controllers”. These organisations, whether big or small, will all have responsibilities under GDPR.

While data controllers will often be organisations, individuals can also act as data controllers. Many self-employed people will control personal data obtained from their clients. For example, an accountant will usually hold personal data relating to individuals (or employees within organisations) for whom work is being undertaken.

A data controller – data subject relationship doesn’t have to be commercial. For example, many voluntary organisations will collect and use personal data to communicate with members.



Data Controllers can vary in size and function

2.4 DATA PROCESSOR

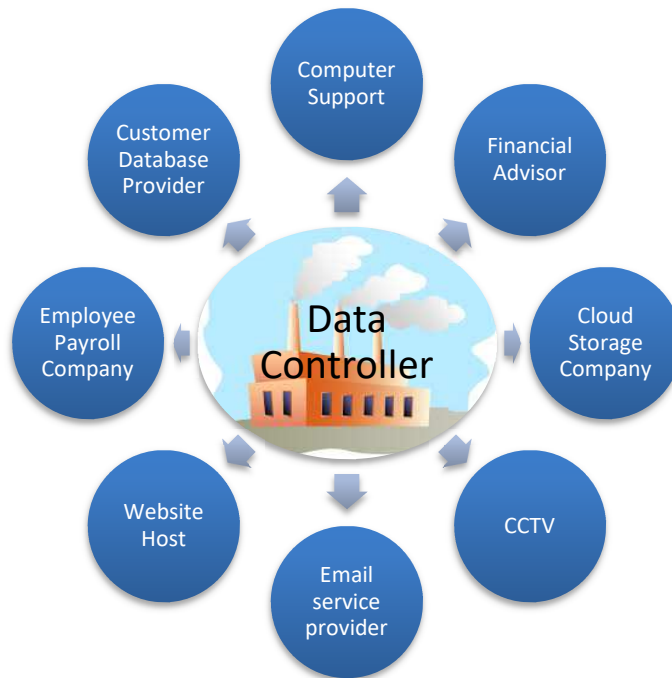
What does a Data Processor do?

A Data Processor acts on the instructions of a Data Controller.

‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; (GDPR Article 4, Definitions)

A Data Processor uses personal data under the direction of the Data Controller.

In practice a data processor is very often an organisation that is carrying out some task on the instructions of another organisation.



Examples of data processors used by a company (data controller)

2.5 CONTROLLER - PROCESSOR EXAMPLE

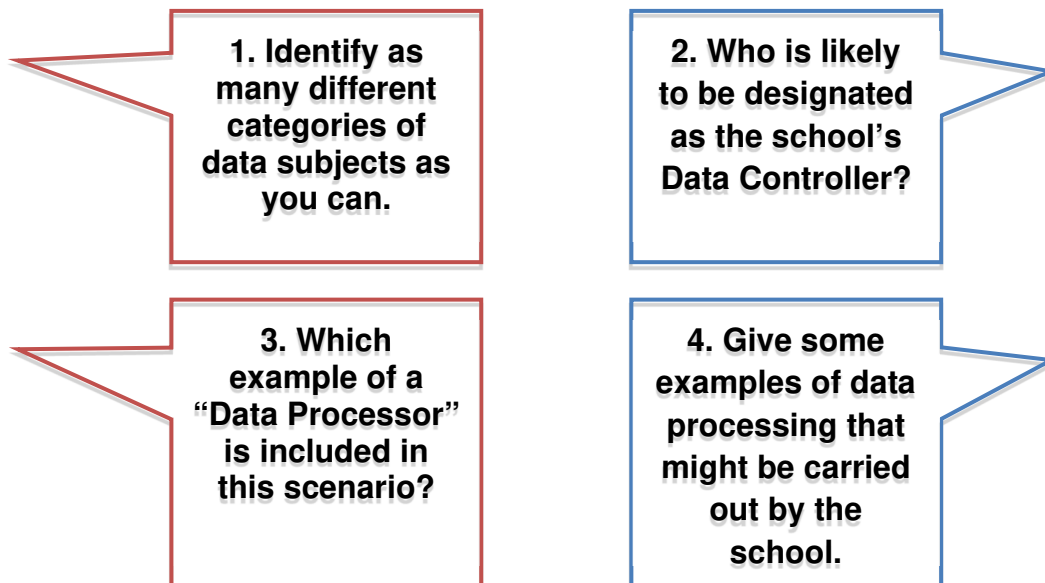
A school board employs a school principal and another 50 staff. The school has 500 students on its roll. Each year the school usually admits 50 new students. Another 50 students take the school leaving examination annually and leave to enter work, further training or higher education. The school secretary deals with a lot of tasks that involve handling personal data.



The school uses a company to look after its ICT system. The school principal supplies the ICT company with the names of students and staff, and the company uses this information to set up user accounts and permissions on the school's

network so that the school community can access the network and use it for tuition and administration purposes.

Use this example to answer the following questions.



Controller-Processor Example Discussion

1. Identify as many different categories of data subjects as you can.

This example contains lots of different categories of data subjects. The most obvious ones are the school staff and students as well as their parents. The school will hold some personal data on all these data subjects. If the school has received applications from families who want to come to the school in the future then it is also likely to hold some personal data for this category of data subject. The school may have to retain some records for past pupils and past staff so these would provide other data subject categories. Other data subjects would be members of the school board and volunteers who may assist with some school activities. You may have suggested some others!

2. Who is likely to be designated as the school's Data Controller?

A data controller has overall decision making power as to how and for what purposes personal data is collected and used. The school board is likely to fulfil this role. While the principal is in charge on a day to day basis (and likely to process much more personal data than the board members who normally only handle a very restricted amount) he or she is unlikely to hold ultimate authority. This responsibility would be reserved for the board and consequently it is the board that should be designated as data controller.

3. Which example of a "Data Processor" is included in this scenario?

The ICT Company is an example of a data processor. The school is likely to use a number of other data processors e.g. CCTV company, accountant, cloud storage

company, pupil database supplier, document storage company. While the school secretary, and indeed the principal, undertake a lot of tasks that involve “data processing”, neither are considered to be “data processors”. Under GDPR, employees are not data processors. Similar to controller, processor is a role that is typically assigned to an organisation, or a legal entity or a self-employed individual.

4. Give some examples of data processing that might be carried out by the school

All of the following examples are likely to involve the processing of personal data:

- The school board recruiting a new teacher.
- A teacher entering test results onto a class list.
- The secretary creating a class list of parental contact details.
- The principal entering students into a state exam.

2.6 REVIEW EXERCISE

1. List some examples of information that would be personal data.

2. Examine each of the following statements for personal data.

- (i) Mary Brown of 21 Main Street, Boston was born on 25th May 2001.
- (ii) John lived in Paris before moving to New York.
- (iii) Half the students leaving Catherine’s school entered university.

3. List some examples of special categories of personal data.

4. “Personal data that has been truly anonymised is no longer subject to the GDPR”.

- (i) True
- (ii) False

5. Think of an example of a work place that is familiar to you. Identify the following:

- (i) Data Controller
- (ii) Data Subjects
- (iii) Categories of Personal Data
- (iv) Examples of processing activities
- (v) Data Processors (if any)

LESSON 3 – DATA PROTECTION PRINCIPLES

In this section, you will learn about:

- The data protection principles
- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity & confidentiality
- Accountability

3.1 THE DATA PROTECTION PRINCIPLES

Data protection guidelines and regulations have been in place in Europe and elsewhere for many years. Since their first introduction, it has been accepted that data processing can only go ahead if certain guiding principles apply.

Although the laws governing the area of data protection have changed over the years, the areas that these principles govern have been fairly stable.

These principles are primarily designed to protect the fundamental rights and freedoms of natural persons whose personal data may be subject to processing.

The General Data Protection Regulation (GDPR) sets out 6 core principles and 1 special principle.

The following principles apply to the processing of personal data under GDPR:

1. **Lawful, Fair and Transparent**
2. **Purpose Limitation**
3. **Data Minimisation**
4. **Accuracy**
5. **Storage Limitation**
6. **Integrity & Confidentiality**
7. **Accountability**



The Data Processing Principles under GDPR

Each one of these principles must be considered anytime personal data is processed. This means that the data processing that is being undertaken cannot be considered lawful if any one of these principles is disobeyed.

3.2 LAWFULNESS, FAIRNESS AND TRANSPARENCY

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject; (GDPR Article 5, Processing Principles)

Personal data can only be processed if there is a lawful basis for doing so. (The legal basis for processing personal data is examined in Lesson 4).

This means that, amongst other things, people should understand how their personal data is being used.

It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. (GDPR Recital 39)

3.3 PURPOSE LIMITATION

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; (GDPR Article 5, Processing Principles).

When we share personal data with others we have an expectation about the purposes for which it will be used. Specification of purpose is an essential first step in applying data protection laws: “The specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data” (GDPR Recital 39).

The principle of purpose limitation prevents mission creep i.e. personal data being processed for purposes beyond those for which it was originally collected.

Purpose Limitation Example 1

A clothing store asks a paying customer for her email addresses for the purposes of supplying her with an electronic receipt. The customer subsequently receives an email from the company providing an e-copy of the receipt. This email also provides marketing information relating to broadband services. This use of the customer’s email address for marketing purposes is different to the original purpose for which her personal data was collected and is not appropriate.

So processing of personal data in a way that is incompatible with the purposes specified at collection is against the law and therefore prohibited. Purpose

limitation protects data subjects by setting limits on how data controllers can use their data.

Purpose Limitation Example 2

Tax authorities are seeking access to smart meter data from households. They want to detect whether any houses that are declared unoccupied actually have people residing in them. Commercial data provided for an entirely unrelated purpose is to be used for tax enforcement purposes. Such use may not be reasonably expected by the data subjects, especially if they have not done anything wrong and are not under any particular suspicion or investigation. These factors strongly indicate incompatibility.

At the same time the purpose limitation principle does offer some flexibility to data controllers. Processing for a different purpose may be acceptable if it is considered compatible with the purpose for which the data was originally collected.

Purpose Limitation Example 3

The electricity network operator implements an intelligent system, including an analytics tool, to detect anomalies in usage patterns which may give reasonable suspicion of fraudulent use (for example, tampering with the meters). The initial purposes for collecting smart meter data was for providing energy to the customers and charging them for the energy use. This further processing for the purpose of fraud prevention stems from, and is in furtherance of, the original purpose and is likely (with appropriate safeguards in place) to be compatible.

Compatibility always needs to be assessed on a case by case basis. Other examples where processing is likely to be considered compatible with the original purpose for collection may be when personal data is processed for archive purposes in the public interest, scientific or historical research purposes or statistical purposes.

3.4 DATA MINIMISATION

Controllers need be able to clearly explain and justify the need to collect and hold personal data. This must be clearly linked with the purpose(s).

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; (GDPR Article 5, Processing Principles)

Data Controllers must not fall into the trap of collecting personal data “just in case” it might be needed for some purpose in the future. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

Data Minimisation Example 1

The data controller might need to confirm that a data subject is a certain age. It may be sufficient to ask the data subject to confirm that they are “over 18 years old” rather than asking for their data of birth.

As technology evolves over time, there are increasingly new ways to collect more data. Cheaper storage costs and the ability to process large amounts of information can encourage organisations to collect more data than they need. The growth of the Internet of Things and the development of wearable devices have led to more and more ways to generate and process data.

Data Minimisation Example 2

A user installs a connected fire alarm in his apartment. The alarm uses an occupancy sensor, a heat sensor, an ultrasonic sensor and a light sensor. Some of these sensors are required to detect fire while some of them only provide additional features about which he was previously informed. The user should be able to disable these features to make use of the fire alarm only, hence disconnect the sensors used to provide these features.

Data minimisation is an essential principle in complying with the data protection law. As well as the legal implications, the data controller should consider all of the risks associated with collecting and holding too much data. This will include potential risks to the privacy of the data subject as well as their own exposure as data controller to the consequences of data loss and breaches.



3.5 ACCURACY

Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted.

Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; (GDPR Article 5, Processing Principles).

Personal data that is being processed for a particular purpose must be kept accurate and up to date. If the information is used for a purpose that relies on it remaining current, the “accuracy” principle requires that it should be kept up to date. In these circumstances controllers will need to ensure that they have systems in place to amend or delete inaccurate or outdated personal data.

Accuracy Example 1

Employee payroll records should be updated when there is a pay rise. Similarly, records should be updated for customers’ changes of address so that goods are delivered to the correct location.

In other circumstances, it may not be necessary, or indeed appropriate, to update information.

Accuracy Example 2

An individual moves job from Dublin to Paris. A record showing that she currently works in Dublin is obviously inaccurate. But a record showing that she once worked in Dublin remains accurate, even though she no longer works there.

Maintaining a record of “inaccurate” information may also be appropriate in other circumstances.

Accuracy Example 3

A misdiagnosis of a medical condition continues to be held as part of a patient’s medical records even after the diagnosis is corrected, because it is relevant for the purpose of explaining treatment given to the patient, or to additional health problems.

3.6 STORAGE LIMITATION

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (GDPR Article 5, Processing Principles).

Observing this principle requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. To ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

Data controllers need to:

- Define for how long they need to retain personal data.
- Regularly review the personal data that they hold.
- Delete any personal data whose storage purpose is no longer justified.

While a clear purpose (and lawful basis) may justify the initial collection and storage of personal data, that doesn't mean that data retention can continue indefinitely. The controller needs to be able to justify the length of the retention period for each piece of personal data that it holds.

Storage Limitation Example 1

While age verification may require that an actual date of birth is collected as part of the process, it may not be necessary that this data is retained as part of the data subject record. Confirmation that age verification has taken place may be sufficient and the birth record data should in those circumstances be deleted.

Data controllers should also recognise that data storage costs money and that limiting data storage will help to reduce costs. The dangers of data hoarding are similar to those of physical hoarding and can make it very difficult to find what we need when we need it.

Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

3.7 INTEGRITY & CONFIDENTIALITY

When we pass over our personal data to others, whether to an organisation or individual, we need confidence that they will endeavour to keep our data safe and secure at all times. Both controllers and the processors must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. (GDPR Article 5, Processing Principles)

Data protection laws make it abundantly clear that maintaining “Integrity & Confidentiality” is an onerous responsibility and one that needs to be taken seriously by all those who process personal data.

If you are a data controller, or a data processor, you need to plan very carefully so that the design and organisation of your security fits the nature of the personal data you hold. This means that you will need to:

- Assign clear responsibilities for information security.
- Plan for appropriate physical and technical security.
- Ensure robust policies and procedures and reliable, well-trained staff.
- Prepare to respond to any personal data breach swiftly and effectively.

Protecting against unauthorised or unlawful processing is something that must be considered from different perspectives. It applies equally to protecting data from employees who have no reason to handle the personal data as demonstrated by examples 1 and 2 (below).

Integrity and Confidentiality Example 1

An employee's sick certificate is hand delivered to a company's public receptionist with a request that it be passed on to the HR department. The receptionist places it on her desk noting that it is for delivery the following day to the human resource manager. The certificate which shows details of the employee's illness sits on the receptionist's desk overnight and is visible to a security guard amongst others.

Integrity and Confidentiality Example 2

A resume from a job seeker that arrived in the morning post is sitting on a manager's desk. The contents of the resume are clearly visible to a large number of people who enter the manager's office during the course of the day.

Integrity and Confidentiality Example 3

A company is obliged to keep staff employment details for pension purposes. The records date from pre-computer times and are kept in paper format. The files are inadvertently left behind when the company moves to new offices. The new occupant has directed cleaners to shred any paper materials they come across and consequently the files are destroyed. No other copy exists.

Example 3 (above) is also an example of a breach of the "Integrity and Confidentiality" principle, one in which the data controller has failed to protect personal data from "accidental loss, destruction or damage."

3.8 ACCOUNTABILITY

The accountability principle places a responsibility on the data controller to be ready to demonstrate compliance with the other 6 data processing principles i.e.

1. Lawfulness, Fairness and Transparency
2. Purpose Limitation
3. Data Minimisation
4. Accuracy
5. Storage Limitation
6. Integrity & Confidentiality.

Accountability requires data controllers to implement appropriate and effective measures to effect the principles and obligations of the GDPR and to be able demonstrate this on request.

The controller shall be responsible for, and be able to demonstrate compliance with (the above principles). (GDPR Article 5, Processing Principles).

What does this accountability principle mean in practice? Well a data controller should be able to point towards explicit measures they have put in place. As with the other 6 principles, accountability is a legal responsibility and compliance has a statutory basis.

3.9 REVIEW EXERCISE

1. Accountability could be described as an “oversight” principle that governs the processing of personal data. List the other six principles.

2. An interviewer has collected personal data by carrying out a door-to-door survey. They leave their interview records behind after having lunch in a restaurant. Which of the data processing principles have they broken?

3. Who is legally responsible for ensuring that the 7 data processing principles are obeyed?

4. For each of the following statements, review and decide whether it is TRUE or FALSE.

- (i) A data controller may be able to process personal data for a purpose that is different from that for which it was first collected if that new purpose is compatible with the original purpose.
- (ii) A data controller must keep personal data up to date at all times and in all circumstances.

LESSON 4 – LAWFUL BASES FOR DATA PROCESSING

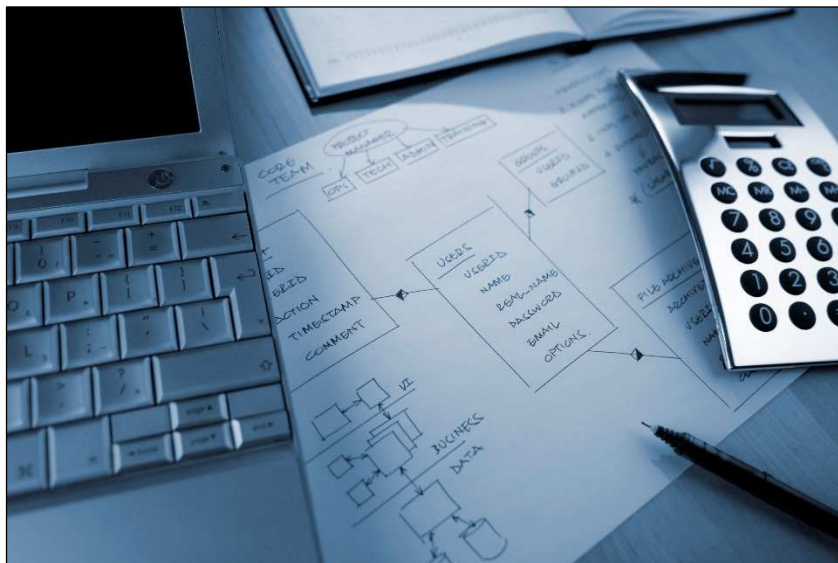
In this section, you will learn about:

- When data processing is allowed
- The lawful bases
- Appropriate lawful basis
- Using consent as a lawful basis
- Issues around consent

4.1 WHEN IS DATA PROCESSING ALLOWED?

A Lawful Basis is needed

The previous lesson (Lesson 3) set out the 7 principles that must be observed any time personal data is processed. The first principle established that personal data must be processed in a manner that is “lawful, fair and transparent”. This means that anytime a data controller intends to process personal data, they must establish the “lawful basis” for doing so. This lesson explains the 6 different bases that can be used to make data processing “lawful.”

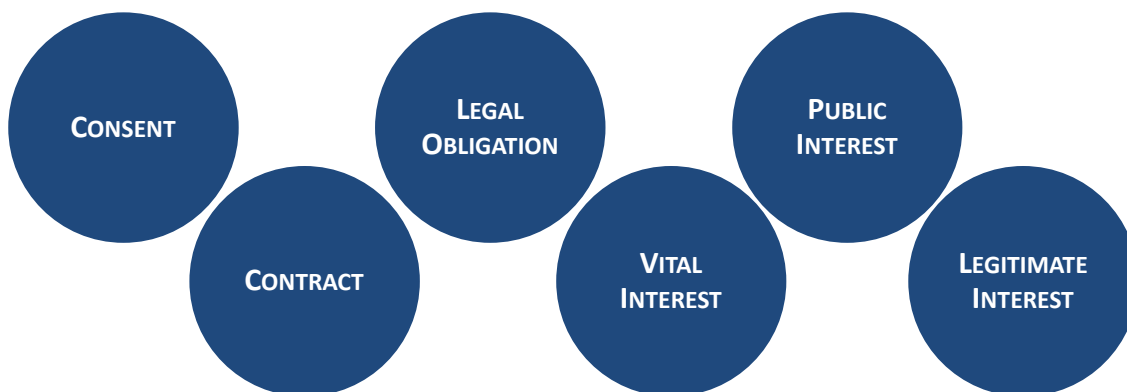


Restrictions on processing data

Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. Consequently, an assessment of its necessity and proportionality may need to be undertaken prior to commencement. This assessment would consider whether the processing is necessary to achieve the designated purpose, or whether some other less intrusive method is available.

The processing of “special categories” of data is more restricted than that of other personal data. In fact, the processing of special category personal data is forbidden unless certain conditions are met. (GDPR Article 9)

4.2 THE LAWFUL BASES

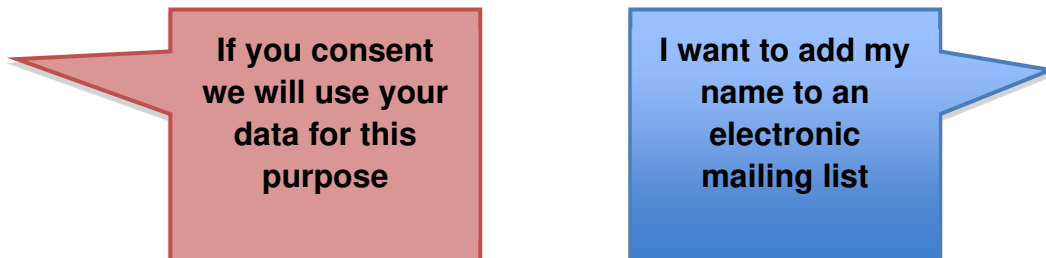


One of these Lawful Bases must apply to any data processing operation

Processing shall be lawful only if and to the extent that at least one of these applies.

(a) Consent

The data subject has given consent to the processing of his or her personal data for one or more specific purposes.



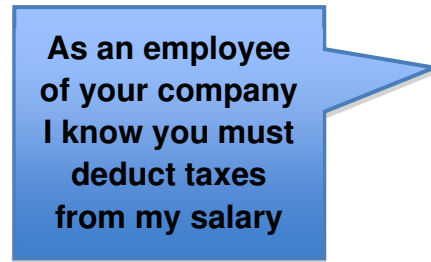
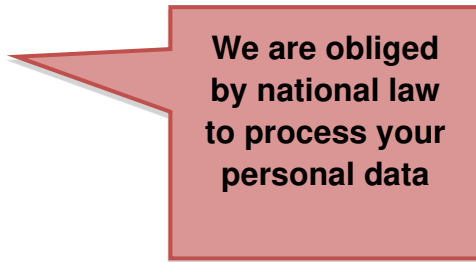
(b) Contract

Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract.



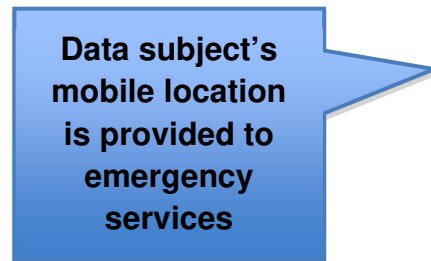
(c) Legal Obligation

Processing is necessary for compliance with a legal obligation to which the controller is subject.



(d) Vital Interests

Processing is necessary to protect the vital interests of the data subject or of another natural person.



(e) Public Interest

Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.



(f) Legitimate Interest

Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party,



4.3 APPROPRIATE LAWFUL BASIS

Before a data controller starts to collect and use personal data, they should be clear about which lawful basis they plan to use; not least because this forms part of the fair processing information that must be communicated to any data subject. It is therefore very important that controllers assess the purposes and the lawful grounds prior to collecting the data.

The choice of an appropriate lawful basis will be linked with the purpose for which the data is being processed.

Often organisations need personal data for several purposes, and the processing may rely on more than one lawful basis. For example for some purposes the processing of customer data might be lawfully based on “contract” and for in other purpose the lawful basis might be “consent”. Controllers therefore need to be clear from the outset about which purpose applies to each element of data and which lawful basis is being relied upon.

Lawful Basis Example 1

An employer might be obliged to install tracking technology in vehicles to demonstrate compliance with legal obligations, e.g. to ensure the safety of employees who drive those vehicles. The employer may also have a legitimate interest in being able to locate the vehicles at any time.

If the data controller is processing based on either public interest or legitimate interest, then the data subject has the right to object. Consequently it is possible that the processing will not go ahead if the data controller’s interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Another restriction is that “legitimate interest” cannot provide a basis for processing carried out by public authorities in the performance of their core tasks. This means that public authorities are likely to rely on public interest as the lawful for the majority most of their data processing.

4.4 USING CONSENT AS A LAWFUL BASIS

Consent is one of six lawful bases to process personal data. When initiating activities that involve processing of personal data, a controller must always take time to consider whether consent is the appropriate lawful ground for the envisaged processing or whether another ground should be chosen instead.

GDPR defines consent as:

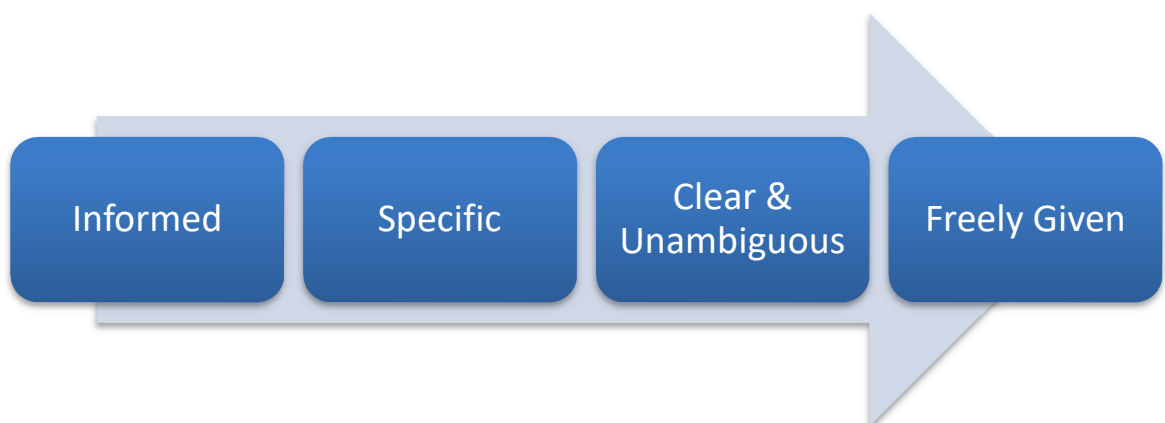
any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. (GDPR Article 4, Definitions).

Generally, consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment.

It is important to state that employees are seldom in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Unless in exceptional situations, employers will have to rely on another legal ground than consent — such as the necessity to process the data for their legitimate interest. However, a legitimate interest in itself is not sufficient to override the rights and freedoms of employees.

Certain conditions must apply if consent is being used as the lawful basis for processing personal data.

Consent must be...



Consent must be informed

The request for consent must be presented using clear and plain language, and the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. This demonstrates the importance of data controllers observing the data processing principle of “transparency”.

Consent must be specific

The request for consent must be presented in a manner which is clearly distinguishable from other matters.

When the processing has multiple purposes, consent should be given for all of them.

Consent Example 1

A cable TV network collects subscribers’ personal data, based on their consent, to present them with personal suggestions for new movies they might be interested in based on their viewing habits.

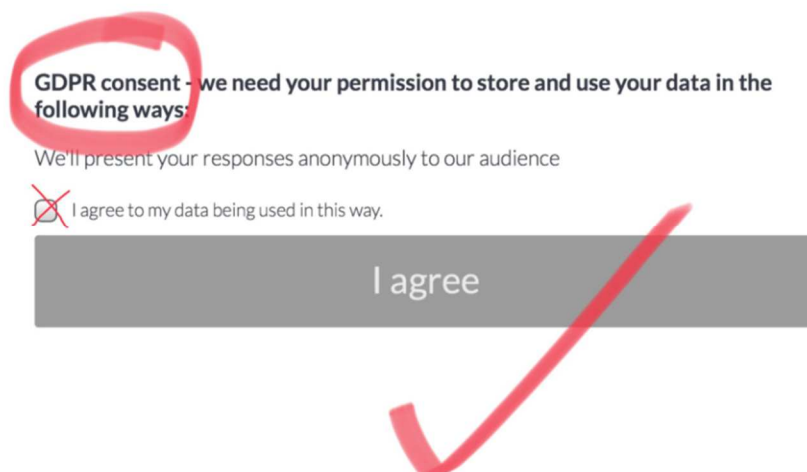
After a while, the TV network decides it would like to enable third parties to send (or display) targeted advertising on the basis of the subscriber’s viewing habits. Given this new purpose, new consent is needed.

Consent can cover all processing activities carried out for the same purpose or purposes.

Consent must be a clear affirmative act

Consent can be a statement or conduct which clearly indicates the data subject’s acceptance of the proposed processing of his or her personal data.

As consent requires a clear affirmative act, silence, pre-ticked boxes or inactivity cannot constitute consent.



Consent must be unambiguous

The controller must be able to demonstrate that the data subject has consented to processing of his or her personal data.

Consent can be demonstrated through a written statement, including by electronic means, or an oral statement. It might include ticking a box when visiting an internet website or choosing technical settings on a mobile app.

Consent must be freely given

The fact that consent must be freely given means that data controllers who are in positions of power must be very careful that the data subject felt able to decline. Therefore schools must be careful in terms of processing the personal data of students and employers must be careful if processing the personal data of employees.

Consent Example 2

A public school asks students for consent to use their photographs in a printed student magazine. Consent in these situations would be a genuine choice as long as students will not be denied education or services and could refuse the use of these photographs without any detriment.

Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

Consent Example 3

A film crew is going to be filming in a certain part of an office. The employer asks all the employees who sit in that area for their consent to be filmed, as they may appear in the background of the video. Those who do not want to be filmed are not penalised in any way but instead are given equivalent desks elsewhere in the building for the duration of the filming.

4.5 ISSUES AROUND CONSENT

Consent must be easy to withdraw

It should be as easy to withdraw as to give consent and the data subject has the right to withdraw his or her consent at any time.

The fact that consent can be so easily withdrawn and relevant processing having to stop, means that data controllers must be careful not to carry out processing based on consent when another legal basis may be appropriate.

Digital Age of Consent

The GDPR defines certain conditions that apply to consent where a child is using information society services, for example, accessing a social media website.

in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. (Article 8, GDPR)

When relying on parental consent, the data controller is required to make “reasonable” efforts (taking into consideration available technology) to verify that consent is being given or authorised by a holder of parental responsibility.

This is an example of one area where GDPR allows for variation across Europe, as member states are free to set the digital age of consent lower than 16 (provided that such lower age is not below 13 years).

Explicit Consent

The term explicit refers to the way consent is expressed by the data subject. Explicit consent is required in certain situations, for example where the processing of special categories of data is based on consent.

An obvious way to make sure consent is explicit is for the controller to make sure a written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future.

However, a signed statement is not the only way to obtain explicit consent. For example, in the digital or online context, explicit consent might be achieved by the data subject filling in an electronic form, sending an email, uploading a scanned document carrying the signature of the data subject, or by using an electronic signature. Two stage verification of consent can also be a way to make sure that consent is explicit.

4.6 REVIEW EXERCISE

1. Give the definition of consent under GDPR.

2. Suggest an appropriate legal basis for each data processing activity.

- (i) An employer obliged to send details of employee earnings to the national tax authority.
- (ii) A business wishing to email marketing information to a potential customer.
- (iii) A hotel processing credit card details to take a payment for a vacation.

3. A shop plans to install a CCTV system within its premises. Which legal basis would you suggest it rely on to process personal data? What other factors would the data controller need to take into consideration as part of its planning?

4. For each of the following statements, review and decide whether it is TRUE or FALSE.

- (i) Valid consent is needed to process personal data under GDPR.
- (ii) The rights and freedoms of a data subject may prevent processing by a data controller who is relying on “legitimate interest” as the lawful basis.

LESSON 5 – DATA SUBJECT RIGHTS

In this section, you will learn about:

- The rights of data subject
- The right to be informed
- The privacy notice
- The right of access
- Other rights

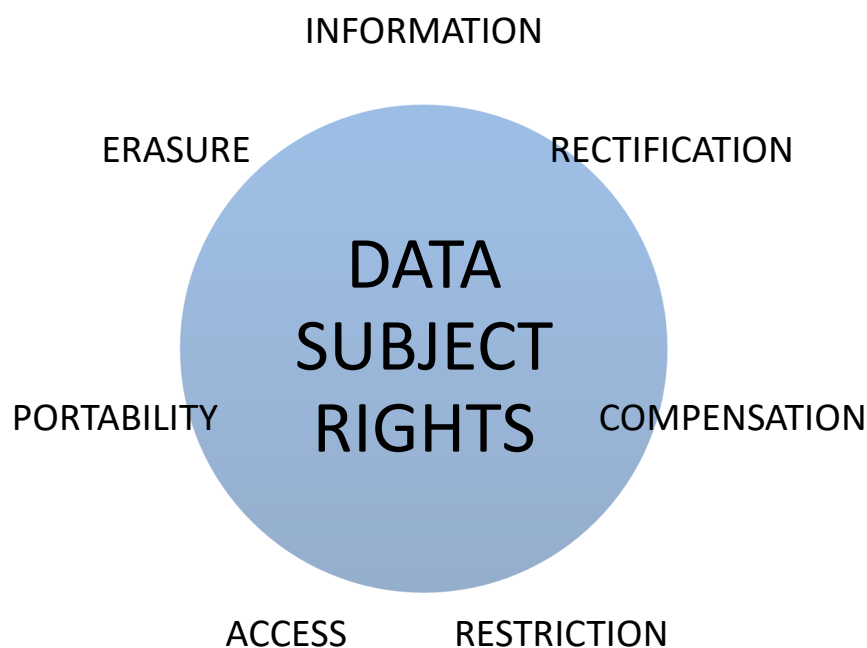
5.1 DATA SUBJECT RIGHTS

Data protection law is designed to protect the fundamental rights and freedoms of living individuals. The preservation of the rights of data subjects is a key foundation underlying European data protection legislation.

As well as being a unifying theme throughout the general data protection regulation legislation, the rights of individuals also feature in a number of specific contexts.

Amongst those rights identified as fundamental are the following:

- The right to be informed
- The right of access
- The right of rectification
- The right of erasure
- The right to restrict processing
- The right to data portability
- The right to compensation.



It is the responsibility of the Data Controller to ensure that data subjects are aware of their rights. Controllers must respond without undue delay to data subjects who are seeking to exercise their rights, and in any event, within one month of receipt of a request.

Most of these rights have some restrictions on their application i.e. they are not “absolute” rights. However in general they serve to provide data subjects with

significant protections to their rights and freedoms. The first of these rights, the right to information, could be said to be very close to an “absolute” right, in that it applies to nearly all processing of personal data.

5.2 THE RIGHT TO BE INFORMED

The need for transparency is an essential part of the first data processing principle (Lesson 3). It is obviously important whenever an individual is being asked to trust their personal data to the safe keeping of another person or organisation.

It should be transparent to natural persons that personal data concerning them are (being) collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. (GDPR Recital 39)

Amongst other things, data subjects need to be told:

... the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing. (GDPR Recital 39)

Data subjects should be informed of any risks, rules and safeguards as well as being given information about their rights and how those rights can be exercised.

5.3 PRIVACY NOTICES

Fair Processing or Privacy Notice

The principle of transparency requires that any information and communication relating to the processing of those personal data is easily accessible and easy to understand and that clear and plain language should be used. There is an onus on whoever is collecting the personal data to clearly communicate all necessary information to the data subject.

The information is usually communicated to the data subjects in the form of a “fair processing” or a “privacy” notice. This notice should be provided at the same time as the personal data is being collected.



It is often good practice for the privacy notice to be delivered using the same medium as is being used to collect the personal information. So, if the data controller is collecting information through an online form then a privacy notice could be provided just as the individual is being asked to fill out the form.

The different ways to communicate a privacy notice

Widespread online access can provide a ready means of communicating privacy information to data subjects. However, a wide variety of media may be used for privacy notices:

- Hard-copy written format: - written explanations, leaflets, information in contractual documentation, cartoons, infographic, and flowcharts printed media.
- Signage: visible notice boards, public signage, public information campaigns, newspaper/ media notices.
- Electronic screens: in text messages; on websites; in emails; in mobile apps.
- Screenless technology: icons, QR codes, voice alerts, written details or videos incorporated into set-up instructions, written information on smart devices;
- Telephonic: oral explanations by a real person, automated or pre-recorded information with options to hear further more detailed information;
- Person to person: oral explanations, written explanations provided in hard or soft copy format.

What information must be communicated to the Data Subject?

Data subjects need to know how their personal data will be used and, in nearly all cases, data controllers must provide this information in advance of collecting any personal data.

The GDPR provides clear guidance as to what information must be provided to data subjects, prioritising:

...information on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. (GDPR Recital 39)

In summary then, data subjects will always need to know:

- The identity and contact details of the Data Controller.
- The purpose and legal basis of the processing.
- How long the data will be held (or the criteria used to determine retention period).



In addition, whenever applicable, data subjects must also be provided with information about:

- Any transfer of data outside the EEA (and safeguards) such as third countries.
- The contact details of any data protection officer.
- Any recipients of the personal data.
- The identity of any controller's representative.
- Other relevant information such as the rationale for any processing based on legitimate interests; the existence of automated decision-making, including profiling etc.

It is important to remember that regardless of the circumstances that apply to the processing, data subjects must always be informed of their rights.

Other Transparency Communications

Transparency needs to be considered not only when personal data is being collected, but also at key times throughout the life cycle of any processing, for example when there is some significant change to the processing or when a data breach occurs.

It may be that a data controller, sometime after initially collecting the personal data, wishes to further process the data for a purpose other than that for which the personal data were collected. In such circumstances the controller is required to inform the data subject about that new purpose prior to undertaking any additional processing.

Sometimes data controllers may be recipients of personal data, not having obtained it directly from the data subjects themselves. In these circumstances the data controllers must contact the data subjects directly and provide them with all the standard information set out above as well as informing the data subjects of the source from which the personal data has been obtained.

When a data controller obtains personal data about a data subject from a source other than the data subject, they must still provide the data subject with the standard information about processing, as well as additional information such as the source of the personal data.

This information should be provided to a data subject in a reasonable time, at the latest one month after obtaining the data, or before communicating with the data subject, or before disclosing the personal data to another recipient.

Information appropriate to the audience

A controller must assess the audience that is providing personal data to their organisation and ensure that “transparency” information is presented in a manner that is understandable by that audience.

For example, if the targeted audience includes data subjects that are underage, the controller is expected to make sure that the information is understandable for minors.

Where a data controller is offering goods or services that are particularly utilised by children then the vocabulary, tone and style of the language used must be appropriate to that audience.

Equally, if services are availed of by other vulnerable members of society, including people with disabilities or people who may have difficulties accessing information, this fact needs to be considered in light of the transparency obligations.

5.4 THE RIGHT OF ACCESS

Any data subject can ask a data controller if personal data concerning him or her are being processed, and the purposes of the processing. The data subject can also seek a copy of whatever personal data is being held.

This “right of access” is exercised by an individual making a “data access request” or a “subject access request”. The controller is required to respond to such a request within one month of receipt.

Right of Access Example

Right of access includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided.

In general, a data controller cannot apply a charge for processing a data access request (although a reasonable fee based on administrative costs may be charged for any further copies requested).



Where the controller processes a large quantity of information concerning the data subject, the controller can request that the data subject specify the information or processing activities to which the request relates.

Where the data subject makes the request by electronic means, the data controller is expected to provide the information in a commonly used electronic form.

It is important to recognise that there are some restrictions on a data subject’s right of access to their personal data. For example, no data subject’s right of access should adversely affect trade secrets, intellectual property or the rights and freedoms of others.

5.5 OTHER RIGHTS

Right to Rectification

A data subject can ask that a controller rectify, without undue delay, any inaccurate personal data that hold about him or her. This could also involve the adjustment of a personal record where the data might not be complete.



Right to Erasure ('right to be forgotten')

A data subject can ask a controller to erase his or her personal data. This will particularly be relevant where:

- The personal data are no longer needed in relation to the purposes for which they are collected, or where.
- A data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her.



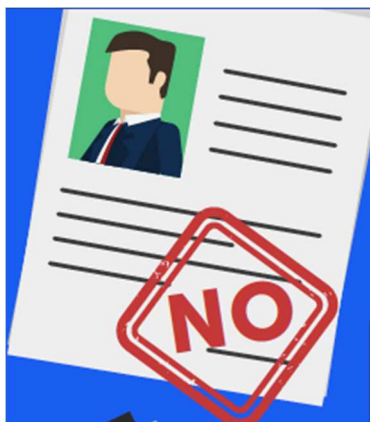
The right to erasure may also be used by a data subject who gave as a child his or her consent to processing (for example, on the internet) but was not fully aware of the risks involved and is now seeking the removal of such personal data.

A data controller is not always obliged to erase personal data. Examples of grounds for retention could include:

- Compliance with a legal obligation.
- The defence of legal claims.
- Exercising the right of freedom of expression and information.
- Performance of a task carried out in the public interest.
- Research purposes and public archiving.

Right to restrict processing

In some circumstances a data subject has the right to restrict processing. For example where the accuracy of the personal data is contested, the processing may be restricted for a period to enable verification of the accuracy of the personal data.



Right to data portability

The right to portability generally applies where the processing is carried out by automated means. This right allows a data subject to request that a copy of their personal data is provided in a “machine-readable format” for transmission to another controller.

Right to object

A data subject has the right to object to the processing of his or her data.

In many (but not all) circumstances, processing will need to stop as a consequence of an objection. For example where personal data are being used for direct marketing purposes, a data subject’s objection means that processing for such purposes must cease.



When a controller is processing personal data based on “legitimate interest”, a data subject’s objection will mean that processing must cease unless the controller can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject.

Automated individual decision-making, including profiling

The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects him or her.

Legal restrictions of data subject’s rights

The rights of a data subject and the obligations of the data controller in relation to data protection may be restricted as a result other legislation in the European Union or Member States that takes precedence such as those in relation to national security.

5.6 REVIEW EXERCISE

1. List the different rights of a data subject under GDPR.

2. What media might be used to communicate privacy information concerning use of CCTV to a data subject?

3. A data subject has been asked to provide personal data by completing an online form. The text of the privacy notice provided is as follows: “If you give your consent we will use your personal data to provide you with information about our products”. To what other information should the data subject have ready access, in order to make this processing legal?

4. For each of the following statements, review and decide whether it is TRUE or FALSE.

- (i) A data controller must respond to a subject access request within 1 month.
- (ii) The “right to erasure” is commonly known as the “right to rectification”.
- (iii) Data subject rights are absolute rights and a data controller must always do as asked.

LESSON 6 – PERSONAL DATA BREACHES

In this section, you will learn about:

- What a data breach is
- How to deal with a data breach
- Preventing data breaches

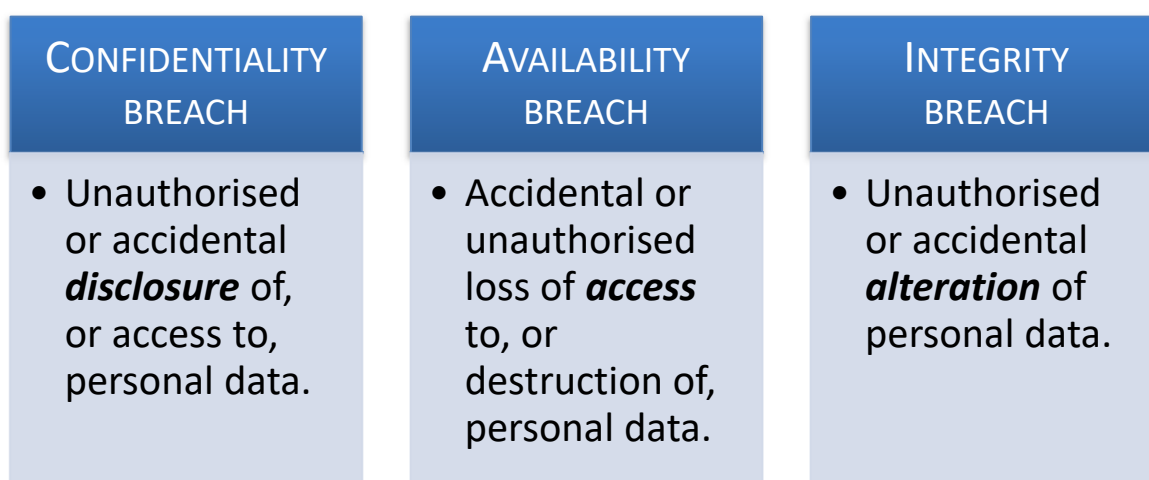
6.1 PERSONAL DATA BREACHES

Data protection legislation helps to keep personal data safe. The principle of “integrity and confidentiality” means that controllers must have appropriate security in place to protect data from unauthorised access or accidental loss.

Controllers need to implement measures to help protect against a “personal data breach” which is defined as:

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. (GDPR Article 4, Definitions)

Any personal data breach can fall into one or more of the following categories:



If a controller hasn’t taken appropriate steps to ensure that “technical and organisational measures” are in place to keep personal data secure, then they are likely to be in breach of the law.

6.2 IMPACT OF A BREACH

A personal data breach can have a range of adverse effects and potentially result in significant physical, material, or non-material damage to individuals.

Personal Data Breach Example

Four laptop computers were stolen from a "Children’s Healthcare Institute"; they stored sensitive health and social welfare data as well as other personal data concerning 2050 children.

This personal data breach concerns confidentiality and (if no backup of the data was available to the controller) availability and integrity of the data.

Potential consequences and adverse effects of the **confidentiality** breach:

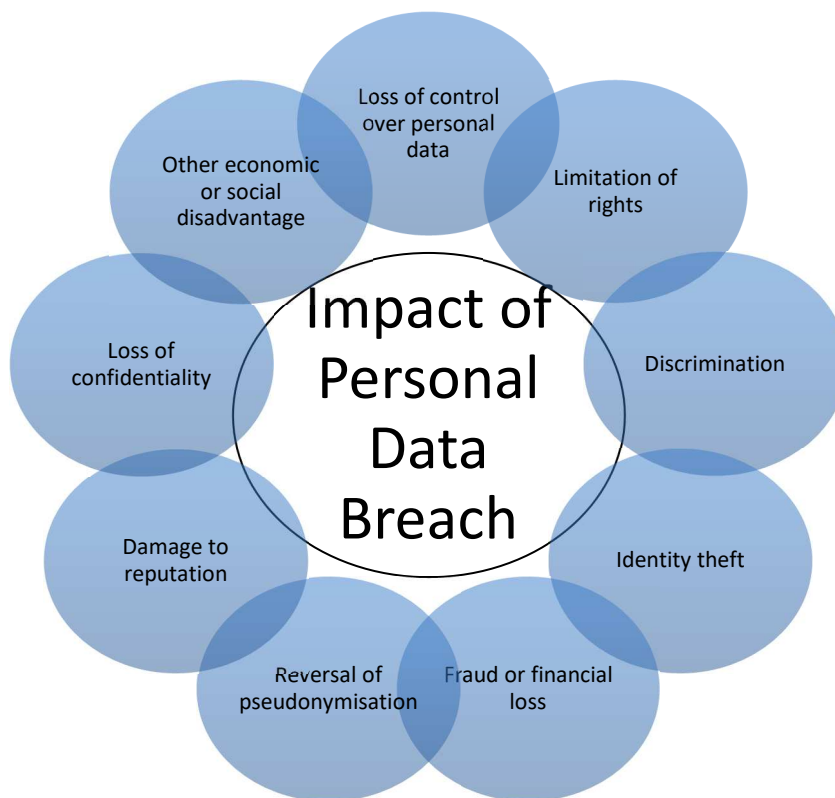
- The first impact is a breach of medical secrecy: the database contains intimate medical information on the children which are available to unauthorised people.
- The data may impact the school and/or family environment of the children (e.g. data on assault, long terms diseases, mental problems, social or financial difficulties of the family, etc.).
- It may emotionally affect children and parents.
- Data may be used to blackmail parents and children (depending on their age).
- Parents of critically ill children may be targeted by people eager to profit from their weakness.

Potential consequences and adverse effects of the **availability** breach:

- It may disturb the continuity of children's treatment leading to aggravation of the disease or a relapse.
- It may lead to accidental poisoning by drug allergy or by conflicting drugs, which may result in various health problems or death.
- It may lead to undue delay in reimbursement or financial assistance to the data subjects which would have financial impacts on the concerned families.

Potential consequences and adverse effects of the **integrity** breach:

- The lost data may affect the integrity of the medical records and disrupt the treatments of the children. For example, if only an old back-up of the medical records exists, all changes to the data that were made on the stolen computers will be lost, leading to corruption of the integrity of the data. The use of medical records that are not up-to-date may disrupt the continuity of children's treatments leading to aggravation of the disease or a relapse.



6.3 COMMUNICATING A DATA BREACH

Breaches can cause significant damage to those individuals whose personal data has been compromised. For this reason, data controllers are required by law to take action when a personal data breach has occurred.

The data controller should report personal data breaches to the supervisory authority as soon as possible and, where possible, within 72 hours.

If reporting after 72 hours, they shall also report the reasons for the delay.

Data controllers must evaluate the potential impact on the individuals who may be affected by the data breach. Data controllers do this by considering the level of risk that has resulted from the data breach. The actions that must follow depend on this perceived level of risk.

When a personal data breach occurs, the law requires data controllers to consider communicating with both:

1. The Supervisory Authority.
2. The individual Data Subjects.

Notification to the competent supervisory authority is triggered where a breach is likely to result in a risk to the rights and freedoms of individuals.

Communication of a breach to the individual is triggered where it is likely to result in a high risk to their rights and freedoms.

The level of risk associated with any personal data breach will therefore need to be assessed on a case-by-case basis and a decision reached about (i) notifying the supervisory authority and (ii) communicating with the data subjects.

Personal Data Breach Example 1

A sailing club sent an email reminder to members about an upcoming event. The organiser neglected to use the “blind carbon copy” (BCC) field and consequently all email addresses were inadvertently shared with all recipients. The number of people affected was less than 100 and all were known to each other.



Personal Data Breach Example 2

A school management system database became corrupted and had to be recreated from a backup copy. All personal data were successfully restored except for the parental email addresses for one student class. The school wrote to the parents concerned and asked that they update their email address. The impact was that the school was prevented from contacting parents by email for a week or so until the school’s email database was repopulated.

Both of the above cases constitute personal data breaches, the first relating to “confidentiality” and the second to “availability”. In both these cases the data controllers examined the breaches and reached the view that there was unlikely to be a risk to individual rights and freedoms and that no supervisory authority notification was necessary.

Neither of the examples above involved personal data that would be classified as “special category.” This fact would also have helped to lower any potential risk or damage. In general, when the breach involves personal data that reveal racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, the level of risk or potential for damage is increased.

Personal Data Breach Example 3

In the context of a hospital, if critical medical data about patients are unavailable, even temporarily, this could present a risk to individuals' rights and freedoms; for example, operations may be cancelled.

Although a loss of availability of a controller's systems might be only temporary and may not have an impact on individuals, the fact that there has been a network intrusion could still be considered a potential confidentiality breach and notification might be required. Therefore, it is important for the controller to consider all possible consequences of a breach.

Personal Data Breach Example 4

Infection by ransomware (malicious software that encrypts the controller's data until a ransom is paid) could lead to a temporary loss of availability if the data can be restored from backup. However, a network intrusion still occurred, and notification could be required if the incident is qualified as a confidentiality breach (i.e. personal data is accessed by the attacker) and this presents a risk to the rights and freedoms of individuals.

In some cases it may involve a disproportionate effort to contact individuals. In these circumstances the controller may only be able to notify the data subjects through some form of public communication.

Personal Data Breach Example 5

The warehouse of a statistical office has flooded and the documents containing personal data were stored only in paper form. The data subjects contact details have been lost. The controller initiates a publicity campaign in an attempt to notify the data breach to the individuals concerned.

6.4 MINIMISING DATA BREACH PROBLEMS

A key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner.

Appropriate Technical and Organisational Measures

Controllers (and processors) need to ensure an appropriate level of security through implementing appropriate technical and organisational measures. These measures should reflect the risk posed to the personal data being processed.

This means taking account of the state of the art, the costs of implementation and the nature, the scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

Appropriate technical and organisational measures taken prior to any event can serve to protect personal data in the event of data breach.

<h2 style="text-align: center;">Technical and Organisational Measures to Secure Personal Data</h2>			
<p>Pseudonymise and encrypt personal data.</p>	<p>Check availability and resilience of processing systems and services.</p>	<p>Ensure capacity to restore access after a physical or technical incident.</p>	<p>Regularly test and evaluate effectiveness of security.</p>

State-of-the-art encryption can render personal data unintelligible to any person who is not authorised to access it. In other cases it may be that, immediately following a breach, the controller can take steps to ensure that the high risk posed to individuals’ rights and freedoms is no longer likely to materialise. For example, the controller may have immediately identified and taken action against the individual who has accessed personal data before they were able to do anything with it.

Personal Data Breach Example 6

A breach that would not require notification to the supervisory authority would be the loss of a securely encrypted mobile device, utilised by the controller and its staff. Provided the encryption key remains within the secure possession of the controller and this is not the sole copy of the personal data then the personal data would be inaccessible to an attacker. This means the breach is unlikely to result in a risk to the rights and freedoms of the data subjects in question. If it later becomes evident that the encryption key was compromised or that the encryption software or algorithm is vulnerable, then the risk to the rights and freedoms of natural persons will change and thus notification may now be required.

Data Processing Agreements

Data processing agreements are contractual agreements that are made between controllers and processors (or processors and sub-processors). They ensure that appropriate and necessary controls are in place anytime a processing activity is carried out for one organisation by another organisation.

Data processing agreements are a legal requirement under GDPR. They mean that, for example, a controller can only use a processor who has guaranteed to implement appropriate technical and organisational measures. In addition to other benefits, these agreements help to enhance the security of data processing activities that are being carried out by other organisations and individuals.

6.5 REVIEW EXERCISE

1. Give the definition of a “personal data breach” under GDPR.

2. How many of the following examples constitute a personal data breach?
- (i) The loss of a file containing a financial statement of a company.
 - (ii) The theft of a laptop secured with industry standard encryption.
 - (iii) The accidental destruction of the only copy of a file containing medical records.

3. A company accidentally publishes a list of its customer details on its website. This list of personal data includes bank account details. Identify the actions that the company must take in terms of (i) the supervisory authority (ii) the data subjects.

4. For each of the following statements, review and decide whether it is TRUE or FALSE.
- (i) Data subjects must always be contacted in the event of a data breach.
 - (ii) The notification regulations do not apply if the data controller has taken every reasonable step to prevent a data breach.
 - (iii) Notification of a data breach to the supervisory authority by a data controller is not necessary if there is no risk to the data subjects.

LESSON 7 – ORGANISATIONAL RESPONSIBILITIES

In this section, you will learn about:

- Accountability
- The importance of record keeping
- Policies and guidelines
- Training and awareness
- The role of a data protection officer
- Privacy by design and by default
- Data protection impact assessment

7.1 ACCOUNTABILITY REQUIREMENT

Accountability is one of the principles that govern data processing activities. It obliges organisations to be ready to demonstrate their compliance with the law.

Data controllers, in particular, have a key role in terms of any data processing operation. It is data controllers who decide on the purposes for which data is collected and used. Consequently, a legal responsibility of accountability rests very much with data controllers.

Accountability means that controllers need to be ready to demonstrate the measures they have taken to ensure compliance with the various data processing principles.

Data processors (i.e. organisations or individuals - not employees of the data controller - who process personal data on behalf of the controller) also carry significant responsibilities for compliance under data protection legislation. Many of the accountability measures that are described in this lesson are just as applicable to processors as to controllers.

This lesson identifies some of the ways that an organisation can demonstrate its accountability. Some of these measures may be statutory requirements under the General Data Protection Regulation.



7.2 ACCOUNTABILITY MEASURES

Good governance from a data protection perspective requires effective organisational policies, procedures and guidelines as well as thorough and rigorous record keeping. It also requires appropriate “buy-in” from a human resource perspective, and this should pervade the organisation as a whole.



Examples of Actions that Contribute to Accountability

Policies, Guidelines and Procedures

A key way for organisations to show accountability is through the development of appropriate data protection policies. Demonstrated adherence to internal guidelines and procedures will also assist with this purpose.

Organisational policies, guidelines and procedures will reflect the underlying data processing functions specific to each organisation but may address areas such as:

- Policies governing data processing operations (e.g. Data quality, security etc.)
- Procedures to manage access, correction and deletion requests.
- Procedures for the management and reporting of security breaches.
- Procedures prior to creation of new personal data processing operations (internal review, assessment, etc.)
- Procedures to verify that measures are implemented in practice (internal or external audits, etc.)
- Mechanisms to handle complaints.
- Contracts to enforce data protection.
- Managerial oversight.

Record Keeping

Organisations can demonstrate accountability by maintaining records of their processing activities. The nature of the records that need to be maintained may be derived from internal organisational policies or stem from legal requirements.

The GDPR identifies schedules of records that must be maintained by organisations. These record-keeping requirements can be influenced by factors

such as the size of organisation, the type of processing, and whether the organisation is a controller or processor.

Note: GDPR record-keeping requirements allow some discretion to SMEs (Small to Medium Enterprises) in certain limited circumstances.

In general, a controller may need to maintain records that include the following factors (this list is not complete but provides an example of some of the GDPR requirements):

- The categories of data subjects and the purposes of the processing.
- Any sharing or disclosure of the personal data.
- Any transfer of data outside the EEA and the associated safeguards.
- Time limits for erasure of the different categories of data.
- A description of the technical and organisational security measures in place.

Similarly, processors are also expected to maintain records and to be ready to demonstrate their accountability by making these records available to the supervisory authority on request.

Categories of personal data and data subjects	Elements of personal data included within each data category	Source of the personal data	Purposes for which personal data is processed	Legal basis for each processing purpose (non-special categories of personal data)	Special categories of personal data	Legal basis for processing special categories of personal data	Retention period	Action required to be GDPR compliant?
List the categories of data subjects and personal data collected and retained e.g. current employee data; retired employee data; customer data (sales information); marketing database; CCTV footage.	List each type of personal data included within each category of personal data e.g. name, address, banking details, purchasing history, online browsing history, video and images.	List the source(s) of the personal data e.g. collected directly from individuals; from third parties (if third party identify the data controller as this information will be necessary to meet obligations under Article 14).	Within each category of personal data list the purposes for the data is collected and retained e.g. marketing, service enhancement, research, product development, systems integrity, HR matters, advertising.	For each purpose that personal data is processed, list the legal basis on which it is based e.g. consent, contract, legal obligation (Article 6).	If special categories of personal data are collected and retained, set out details of the nature of the data e.g. health, genetic, biometric data.	List the legal basis on which special categories of personal data are collected and retained e.g. explicit consent, legislative basis (Article 9).	For each category of personal data, list the period for which the data will be retained e.g. one month? one year? As a general rule data must be retained for no longer than is necessary for the purpose for which it was collected in the first place.	Identify actions that are required to ensure all personal data processing operations are GDPR compliant e.g. this may include deleting data where there is no further purpose for retention.

Template Example for SME Processing Records¹

Lesson 6, concerning the handling of personal data breaches, demonstrated that controllers will often need to issue notifications (to the supervisory authority) and communications (to data subjects). In cases where no notification is necessary, the controller must still document the breach, comprising the facts relating to the

¹ Irish Data Protection Commissioner – www.GDPRandYOU.ie

breach, its effects and the remedial action taken. Controllers are therefore encouraged to establish an internal register of breaches, regardless of whether they are required to notify or not.

Staffing, Training and Awareness

An understanding of appropriate data protection responsibilities should apply at all organisational levels, relevant to members of boards or senior management as well as to operational staff. This means ensuring that adequate data protection, training and education has been offered to, and availed of by, staff members (for example, by implementing ECDL Data Protection!).

Organisation or legal requirements may necessitate the appointment of a data protection officer and/or other individuals to discharge specific data protection responsibilities.



7.3 DATA PROTECTION OFFICER

The primary role of a data protection officer (DPO) is to ensure that his or her organisation processes the personal data of its staff, customers, providers or any other individuals in compliance with the applicable data protection regulations.

A DPO should have expert knowledge of data protection law and practices so that they can help a controller or processor to monitor internal compliance with the applicable regulations.

When is a DPO needed?

According to the GDPR an organisation (whether a controller or processor) must appoint a data protection officer when one of the following circumstances applies:

- Processing is carried out by a public authority or body.
- Core processing activities require regular and systematic monitoring of data subjects on a large scale.
- Core activities consist of processing on a large scale of special categories of data (i.e. Sensitive data) or data concerning criminal offences.

Organisations that fall outside these categories are also free to appoint a DPO should they wish to do.

What is the role of the DPO?

The key role of the DPO is to inform and advise the organisation on its obligations under the data protection legislation. In addition, DPOs act as intermediaries between relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organisation).

Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights. It is within their right to request contact details of any DPO.

In addition to these responsibilities, the GDPR sets out a number of other tasks where a data protection officer must be involved. Examples include

- Monitoring organisational compliance in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits.
- Providing advice where requested as regards any data protection impact assessment and monitoring its performance.

The organisation must support the data protection officer by providing the resources needed to carry out these tasks. The DPO role is expected to be independent in nature.

The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor (GDPR Article 38, Position of Data Protection Officer).

7.4 PRIVACY PLANNING

Traditionally privacy protection has often been reactive in nature. For example, policies that address the handling of personal data breaches respond to a privacy issue after the event has occurred. More recent approaches to data protection have tried to take a more proactive approach to protecting the privacy of individuals.

Risk Assessment

The assessment and management of risk is presented throughout the GDPR as an important skill for those who handle personal data. In order to maintain security, organisations need to evaluate the risks inherent in their processing and implement measures to mitigate those risks.



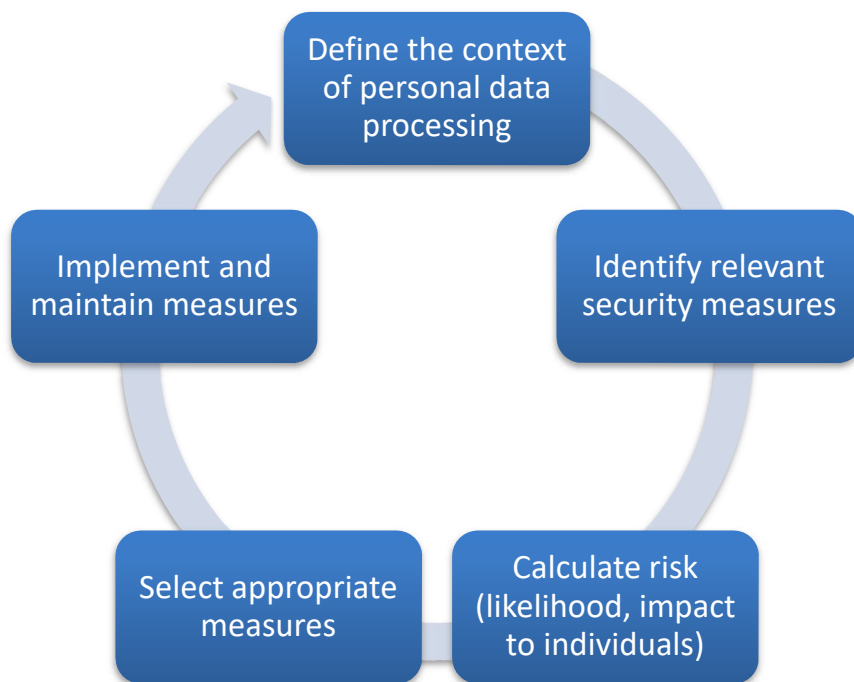
Example of a Resource to Support Risk Assessment: www.enisa.europa.eu

The first step in any risk-management process is likely to involve identifying the potential risks through taking account of factors such as:

- The nature of personal data (e.g. sensitive or not.)
- The category of data subject (e.g. minor or not.)
- The number of data subjects affected.
- The purpose of the processing.

Secondly, identified risks need to be assessed in terms of their likelihood and the potential severity of any impact on the data subject.

Finally, measures to mitigate these risks need to be identified so that the risks to individual rights and freedoms can be managed.



Security Risk Management for Personal Data

Security should be appropriate to the risk represented by the processing, and this approach will help to design a set of technical and organisational controls.

Data Protection (Privacy) by Design

The “Privacy by Design” principle requires organisations to build data protection considerations into their processing operations and systems from the ground up, rather than as a last-minute compliance issue. Hence organisations need to take early account of data protection rights whenever they are developing and designing products, services and applications.

In practice this really means that privacy must be embedded into organisational design processes from the very start and before any adoption of new business processes, physical spaces, information technologies or network infrastructures.

Privacy by design (PbD) also means that whenever data controllers are determining the means for processing, they should adopt appropriate technical and organisational measures (such as pseudonymisation or data minimisation) to integrate the necessary safeguards.

A PbD approach will also mean that developers and designers will minimise the amount of collected data to that required to provide the service.

In summary, the PbD concept assumes a holistic approach by transforming how an organisation manages privacy. Organisations should adopt PbD principles into all aspects of their operations wherever and whenever personal information is collected, used, disclosed, retained, transferred, and/or disposed.

Data Protection (Privacy) by Default

The “Privacy by Default” principle requires organisations to ensure that from the start personal data is processed with the highest privacy settings and protection. The data collected is the minimum needed for the service to be offered to the data subject. Similarly, the data should be stored for the shortest possible retention period and with minimum accessibility so that by default personal data isn’t made accessible to an indefinite number of other people.

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. (GDPR Article 25, Data Protection by Design and Default).

The principle of “privacy by default” is seen as particularly important in protecting the data subject in situations in which there might be a lack of understanding or control on the processing of their data, especially in a technological context.

Data Protection by Default Example

A social media platform should be encouraged to set users’ profile settings in the most privacy-friendly setting by, for example, limiting from the start the accessibility of the users’ profile so that it isn’t accessible by default to an indefinite number of persons.

Achieving transparency with regard to the functions and processing of personal data is a critical element in terms of meeting the requirements of privacy by default.

In summary this principle means that the privacy intrusive features and settings of a certain product or service are initially set to those needed for its most basic use. The data subject is then left to decide whether to allow use of his or her personal data in a broader way.

Data Protection (Privacy) Impact Assessment

A Data Protection Impact Assessment (DPIA), also known as a Privacy Impact Assessment, aims to identify the potential privacy risks of new or redesigned programs, systems or products.

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (GDPR Article 35, Data Protection Impact Assessment)

The GDPR provides some circumstances where a DPIA would be mandatory. For example: (a) processing that involves automated decision making that produces a significant effect on data subjects; (b) systematic monitoring of data subjects in a publicly accessible area; or (c) large scale processing of sensitive data (special categories of data and data regarding criminal offences).

Examples where DPIA are needed²

A hospital processing its patients' genetic and health data as part of a hospital information system. (Sensitive data; vulnerable data subjects.)

A camera system to monitor driving behaviour utilising an intelligent video analysis system to single out cars and automatically recognise license plates. (Systematic monitoring; Innovative technological solutions)

The gathering of public social media profiles data to be used by private companies generating profiles for contact directories. (Evaluation or scoring; Data processed on a large scale).

The above examples all illustrate cases where the processing is likely to present a high risk to the rights and freedoms of natural persons, and consequently a DPIA is needed to evaluate, in particular, the origin, nature, particularity and severity of the risks.

² These examples are derived from *WP 248*, Article 29 Data Protection Working Party.

7.5 REVIEW EXERCISE

1. Give three strategies that an organisation can use to help show its accountability with regard to its data protection responsibilities.

2. Who is responsible for record keeping under GDPR?

- (i) Data Controller.
- (ii) Data Processor.
- (iii) Both Controllers and Processors.

3. Give three examples of technical and organisation measures that can help to minimise risk during data processing.

4. For each of the following statements, review and decide whether it is TRUE or FALSE.

- (i) The Data Protection Officer is in charge of all of an organisation's data processing activities.
- (ii) Privacy by design is defined as the process for making sure that data protection websites are easy to understand.
- (iii) A data protection impact assessment (DPIA) is mandatory under certain circumstances.

LESSON 8 – ENFORCEMENT

In this section, you will learn about:

- Supervisory authorities
- Sanctions

8.1 SUPERVISORY AUTHORITY

Within each EU member state there exists a “Supervisory Authority”, a body that has a responsibility to oversee the implementation of the data protection legislation within its jurisdiction.

Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of (GDPR), in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (“supervisory authority”). (GDPR Article 51. Supervisory authority).



Supervisory authorities of the 3 largest European states

Some member states may have more than one supervisory authority (SA). This arrangement reflects different constitutional, organisational and administrative structures. And while there may be some local variations in terms of supervisory arrangements, the core functions are defined by the General Data Protection Regulation and consequently are common to all the states of the European Union.

For example, each supervisory authority must have its own staff who operate independently of any other state function. This is a safeguard to help ensure that each SA performs its tasks and exercises its powers with complete independence.

It is worth noting that data subjects have the right to lodge a complaint with a single supervisory authority in the Member State where they live, work or where the alleged infringement of their rights occurs.

8.2 TASKS

The tasks assigned to each supervisory authority are significant and derive from the legislative responsibilities.

Enforce	• Application of the law (GDPR).
Provide	• Information on data subject rights.
Investigate	• Complaints from data subjects and others.
Promote	• Awareness of controller & processor obligations.
Create	• Public awareness and understanding.
Advise	• Government and other institutions.
Monitor	• Developments that impact on data protection.

Examples of supervisory authority responsibilities

SAs are also required to cooperate with each other and are facilitated in this in being represented on a pan-European body, the European Data Protection Board (EDPB). The EDPB is an independent body that helps to ensure the consistent application of data protection legislation across the Union.



Supervisory authorities possess very significant powers and these can be either investigative or corrective in nature.

A temporary or definitive ban on processing.

Compliance to be achieved within a specified period.

Communication of a data breach to data subject(s).

Compliance with data subject requests.

Rectification, erasure or restriction of processing.

Suspension of data flow outside EEA.


Examples of supervisory authority powers

One of the most significant corrective powers is that a supervisory authority can order an organisation to stop all processing of personal data. In extreme cases this could mean that an organisation (commercial, not for profit, or public body) would have to immediately cease all its operations.

8.3 SANCTIONS AND PENALTIES

Administrative Fines

A supervisory authority has the power to impose fines for breaches of the data protection regulation. The GDPR states that fines must be “effective, proportionate and dissuasive.”



...fines must be
effective,
proportionate
and dissuasive...

The maximum level of sanction that can be imposed depends on the type of breach that has occurred. Two different breach categories are defined, both having the potential to lead to very high fines but with one having a higher maximum fine than the other.

The fact that two different maximum amounts of administrative fine (10/20 million Euros) have been defined indicates that a breach of some provisions of the GDPR may be treated more seriously than a breach of other provisions.

However, the precise level of fine will depend on the circumstances of each individual case. Some of the factors that will be taken into account in determining the level of a fine are listed below.

Nature, gravity and duration of the infringement.

Number of data subjects affected and the damage suffered by them.

Intentional or negligent character of the infringement.

Any action taken to mitigate the damage suffered by data subjects.

The degree of responsibility of the controller or processor.

Previous infringements by the controller or processor.

Degree of cooperation with the supervisory authority.

Manner in which the infringement became known.

Measures previously ordered against the controller or processor.

Other aggravating or mitigating factors.

Factors likely to influence the level of fine

The most serious category of breaches generally relates to non-observance of the processing principles (lesson 3), the lawful processing requirements (lesson 4) or data subject rights (lessons 5). Examples would be a controller who has been processing personal data without a lawful basis to do so, or a processor who has failed to implement security measures appropriate to the identified risks.

This first category of breaches has the potential to trigger sanctions at the highest level leading to fines of up to €20 million or 4% of the organisation's total worldwide annual turnover in the previous financial year (the ceiling being whichever is higher).

The second category generally relates to breaches of the regulation that concern non-observance of GDPR requirements such as those set out in lessons 6 and 7: For example a processor or controller might have failed to appoint a Data Protection Officer or neglected to carry out a Privacy Impact Assessment.

The ceiling for this type of breach is set at €10 million or 2% of total worldwide annual turnover, whichever is highest.

With regard to public authorities and bodies, GDPR allows each Member State to set its own rules as to what extent administrative fines will be imposed.

Level I Fines

- €10 million 2% of worldwide annual turnover. Whichever is highest.

Level II Fines

- €20 million or 4% of worldwide annual turnover. Whichever is highest.

Two levels of administrative fines within GDPR

Other Penalties including Judicial Remedies

All organisations, including public authorities and bodies, need to be aware that exposure to administrative fines is only one of the potential sanctions that may result from a GDPR breach.

For example, data subjects are free to exercise their right to seek remedy through the courts.

...each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation. (GDPR Article 79, Right to a Judicial Remedy)

Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. (GDPR Article 82, Right to Compensation)

GDPR also allows for the possibility that other penalties might apply for a breach of data protection legislation. These penalties can include criminal sanctions. Each member state has the discretion to decide how such additional penalties will be imposed in practice.

Data subjects have the right to bring legal proceedings against a data controller or data processor in the Member State where the controller or processor has an establishment or where the data subject lives. This is called **litigation**.

Data subjects also have the right to receive compensation from the controller or processor for damages suffered. Another key consequence of an organisation that fails to implement relevant data protection regulations is that they may suffer

damage to their reputation, which may lead to loss of consumer trust and business.

8.4 REVIEW EXERCISE

1. What is the primary function of a supervisory authority?

2. Which of the following powers can a supervisory authority exert?

- (i) A temporary ban on all personal data processing.
- (ii) Communication of a data breach to data subjects.
- (iii) Suspension of all data flow outside the EEA.
- (iv) All of the above.

3. Name the Supervisory Authority responsible for data protection in your jurisdiction.

4. List three possible consequences for an organisation that can result from a breach of the GDPR

5. What is the maximum fine that could result from each of the following:

- (i) A data controller fails to notify a data breach to the supervisory authority.
- (ii) A data processor causes personal data to be leaked to outside agencies.
- (iii) An organisation undertaking data processing fails to keep a record of its processing activities.

REFERENCES

- European Data Protection Supervisor. (2018). Glossary - European Data Protection Supervisor. [online] Available at: https://edps.europa.eu/data-protection/data-protection/glossary_en [Accessed 08 Mar. 2018].
- Hustinx, P. (2013). EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation. 1st ed. [ebook] p.9. Available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf [Accessed 08 Mar. 2018].
- UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III), Available at: <http://www.refworld.org/docid/3ae6b3712c.html> [accessed 08 March 2018]
- Coe.int. (2017). European Court of Human Rights (ECtHR). [online] Available at: http://www.coe.int/t/democracy/migration/bodies/echr_en.asp [Accessed 08 Mar. 2018].
- European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, Available at: <http://www.refworld.org/docid/3ae6b3b70.html> [accessed 08 March 2018]
- Guidelines for SMEs on the security of personal data processing. (2018). [ebook] ENISA. Available at: <https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing> [Accessed 08 Mar. 2018].

ECDL Syllabus

Ref	ECDL Task Item	Location	Ref	ECDL Task Item	Location
1.1.1	Understand the term privacy and its associated rights. Be aware that privacy is not an absolute right and other rights may take precedence.	<i>1.1 Defining Privacy</i> <i>1.3 Privacy Rights</i> <i>1.4 Data Protection</i>	2.1.1	Understand that the General Data Protection Regulation (GDPR) is a data protection regulation that is enforceable as law in all European Economic Area (EEA) member states.	<i>1.5 The General Data Protection Regulation</i>
1.1.2	Define the term personal data.	<i>2.1 Personal Data</i>	2.1.2	Recognise the rationale for the introduction of the GDPR: increased legal certainty, increased consumer confidence and trust, increased protection of growing volumes of electronic personal data and their international transfer.	<i>1.5 The General Data Protection Regulation</i>
1.1.3	Understand the term data processing.	<i>2.2 Data Processing</i>	2.1.3	Outline the primary objectives of the General Data Protection Regulation: equivalent level of protection of natural persons with regard to the processing of personal data, free flow of personal data throughout the European Union (EU).	<i>1.4 Data Protection</i>
1.1.4	Distinguish between automated and manual data processing.	<i>1.5 The General Data Protection Regulation</i>	2.2.1	Outline the scope of data processing activities covered by the GDPR: automated and manual processing of personal data, personal data processing activities exempted from the application of the regulation.	<i>1.5 The General Data Protection Regulation</i>
1.2.1	Understand the term data protection.	<i>1.4 Data Protection</i>	2.2.2	Outline the territorial scope of the GDPR regarding the location of personal data processing and data subjects.	<i>1.5 The General Data Protection Regulation</i>
1.2.2	Recognise some risks to personal data from data processing like: accidental or unlawful destruction, loss, alteration, unauthorised disclosure, unauthorised access.	<i>1.2 Recognising Risks</i> <i>3.7 Integrity & Confidentiality</i>	3.1.1	Define the principle of lawfulness, fairness and transparency.	<i>3.2 Lawfulness, Fairness and Transparency</i>
1.2.3	Recognise some risks for data subjects from personal data processing like: discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality, loss of privacy, loss of rights, loss of data control, profiling.	<i>1.2 Recognising Risks</i> <i>1.3 Privacy Rights</i> <i>6.2 Impact of a Breach</i>			
1.2.4	Understand data protection roles and responsibilities like: data subject, data processor, data controller, data protection officer (DPO), supervisory authority.	<i>2.1 Personal Data</i> <i>2.3 Data Controller</i> <i>2.4 Data Processor</i> <i>7.3 Data Protection Officer</i> <i>8.1 Supervisory Authority</i>			

Ref	ECDL Task Item	Location	Ref	ECDL Task Item	Location
3.1.2	Define the principle of purpose limitation.	<i>3.3 Purpose Limitation</i>	3.2.4	Recognise that where processing is carried out on behalf of a data controller, a legal agreement must be in place between the data controller and data processor that ensures compliance with data protection regulations and protects the rights of data subjects.	<i>7.2 Accountability Measures</i>
3.1.3	Define the principle of data minimisation.	<i>3.4 Data Minimisation</i>			
3.1.4	Define the principle of accuracy.	<i>3.5 Accuracy</i>			
3.1.5	Define the principle of storage limitation.	<i>3.6 Storage Limitation</i>			
3.1.6	Define the principle of integrity and confidentiality.	<i>3.7 Integrity & Confidentiality</i>	3.2.5	Identify special categories of personal data that are typically prohibited from processing: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic information, biometric information, health, sex life, sexual orientation. Recognise that special categories of data can be processed lawfully under certain conditions like explicit consent.	<i>2.1 Personal Data 4.5 Issues Around Consent</i>
3.1.7	Define the principle of accountability.	<i>3.8 Accountability</i>			
3.2.1	Outline the conditions under which personal data processing is lawful: consent by data subject, performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a task carried out in the public interest, pursuance of legitimate interests by the controller or by a third party.	<i>4.2 The Lawful Bases 4.5 Issues Around Consent</i>	3.2.6	Recognise that in general personal data can only be transferred outside the EU for processing when the external data protection regulations are compliant with the GDPR.	<i>1.5 The General Data Protection Regulation</i>
3.2.2	Be aware that consent can only be considered given by the data subject if certain conditions are met. Outline the conditions for consent: recorded, clearly requested, withdrawable, given freely.	<i>4.4 Using Consent as a Lawful Basis 4.5 Issues Around Consent</i>	4.1.1	Recognise the importance of clearly communicating to the data subject information relating to processing like: privacy notice, fair processing notice.	<i>5.3 Privacy Notices</i>
3.2.3	Understand the conditions applicable to a child's consent in relation to online services.	<i>4.5 Issues Around Consent</i>			

Ref	ECDL Task Item	Location	Ref	ECDL Task Item	Location
4.1.2	Outline key information that must be provided to a data subject when personal data is obtained like: the data controller's identity and contact details, the purpose and legal basis of processing, the data retention period, the data subject's rights.	<i>5.3 Privacy Notices</i>	4.2.7	Understand that the rights of the data subject may not be met if there are legal restrictions.	<i>5.5 Other Rights</i>
4.1.3	Outline additional information that may need to be provided to a data subject when personal data is obtained by the data controller like: data transfer to a third country, contact details for any DPO, any other recipients, any other information to make the processing fair.	<i>5.3 Privacy Notices</i>	5.1.1	Understand that organisational data protection guidelines and policies must be compliant with data protection regulations. Be aware of the importance of adhering to organisational data protection guidelines and policies.	<i>7.1 Accountability Requirement</i> <i>7.2 Accountability Measures</i>
4.1.4	Be aware that additional information should be provided to the data subject when data is not obtained directly by the data controller.	<i>5.3 Privacy Notices</i>	5.1.2	Understand that data processing should incorporate data protection by design and by default.	<i>7.4 Privacy Planning</i>
4.2.1	Define the term subject access request and understand a data subject's right of access.	<i>5.4 The Right of Access</i>	5.1.3	Understand the term data protection impact assessment and when it is required.	<i>7.4 Privacy Planning</i>
4.2.2	Understand the right to rectification.	<i>5.5 Other Rights</i>	5.2.1	Recognise some appropriate technical and organisational measures to manage risks when processing personal data like: the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services; the ability to restore personal data in a timely manner; a process for determining the effectiveness of technical and organisational measures.	<i>6.1 Personal Data Breaches</i> <i>6.4 Minimising Data Breach Problems</i>
4.2.3	Understand the right to be forgotten.	<i>5.5 Other Rights</i>			
4.2.4	Understand the right to restriction of processing.	<i>5.5 Other Rights</i>			
4.2.5	Understand the right to data portability.	<i>5.5 Other Rights</i>			
4.2.6	Understand the right to object and not to be subject to a decision based solely on automated processing, including profiling.	<i>5.5 Other Rights</i>			

Ref	ECDL Task Item	Location	Ref	ECDL Task Item	Location
5.2.2	Be aware of specific technical measures to manage risks when processing personal data like: encryption, secure digital storage, back up data, secure digital communications, secure physical environment, secure disposal of data.	6.3 <i>Communicating a Data Breach</i> 7.4 <i>Privacy Planning</i>	6.2.3	Understand possible consequences for organisations that fail to implement relevant data protection regulations like: fines, litigation, reputational damage.	8.3 <i>Sanctions and Penalties</i>
5.2.3	Be aware of specific organisational measures to manage risks when processing personal data like: training, processes and procedures, legal contracts, managerial oversight.	7.2 <i>Accountability Measures</i>			
5.2.4	Distinguish between the pseudonymisation and anonymisation of personal data.	2.1 <i>Personal Data</i>			
6.1.1	Understand the term personal data breach.	6.1 <i>Personal Data Breach</i>			
6.1.2	Be aware when the data controller must report personal data breaches to the supervisory authority. Be aware of the associated time frame for reporting.	6.3 <i>Communicating a Data Breach</i>			
6.1.3	Be aware that the data controller should report personal data breaches to the data subject when there is a high risk to their rights and freedoms.	6.3 <i>Communicating a Data Breach</i>			
6.2.1	Identify the supervisory authority in your jurisdiction and recognise the requirement to cooperate with it when requested.	8.1 <i>Supervisory Authority</i>			
6.2.2	Be aware of the data subject's right to lodge a complaint to their supervisory authority, regardless of where their data is processed.	8.1 <i>Supervisory Authority</i>			

Congratulations! You have reached the end of the ECDL Data Protection book.

You have learned about key aspects of data protection, including:

- Understanding concepts relating to personal data and its protection.
- Understanding the rationale, objectives, and scope of the European Union General Data Protection Regulation.
- Outlining the key principles of the GDPR relating to the lawful processing of personal data.
- Understanding the rights of data subjects and how they are upheld.
- Understanding that company policies and methods should comply with data protection regulations, and outline key technical and organisational measures to achieve this.
- Understanding how to respond to data breaches and the consequences of not complying with data protection regulations.

Having reached this stage of your learning, you should now be ready to undertake ECDL certification testing. For further information on taking this test, please contact your ECDL test centre.

