Data Protection 1.0

Quick Reference

This quick reference is for the European Union General Data Protection Regulation.

Certification Test Goals

This 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.

Successful candidates will be able to:

- Understand concepts relating to personal data and its protection.
- Understand the rationale, objectives, and scope of the European Union (EU) 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.

1 Concepts

1.1 Personal Data

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.

- Privacy can be considered the ability to keep yourself ("physical privacy") and information about yourself ("informational privacy") secluded and free from unwanted or unnecessary intrusion from others, with the ability to choose what you make public.
- The right to privacy is typically considered a fundamental right and was declared in the Universal Declaration of Human Rights in 1948 and the European Convention of Human Rights in 1950.
- However, the right to privacy is not considered an absolute right and is typically balanced against societal needs and other fundamental rights, such as the freedom to conduct a business or the right to a fair trial, which in some cases may take precedence.
- Privacy laws vary globally but they aim to protect what is considered private in a particular jurisdiction, for example an individual's private and family life, their home and sensitive personal information about them.

1.1.2 Define the term personal data.

- "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)
- Personal data can be connected with or identify a living person.

1.1.3 Understand the term data processing.

- Data Processing is any operation or set of operations performed on personal data or on sets of personal data by manual or automated means.
- This broad definition includes the 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 of personal data.

1.1.4 Distinguish between automated and manual data processing.

- Automated data processing involves the processing of personal data by automated means, where the personal data are in digital format and processing is performed either partially or wholly by machines such as computers.
- Manual data processing involves processing of personal data by manual means, where the personal data are in physical format and are contained or are intended to be contained in a filing system.

1.2 Protecting Personal Data

1.2.1 Understand the term data protection.

- An area of legislation aimed at safeguarding an individual's privacy rights in relation to the processing of their personal data.
- It only applies to personal data.

1.2.2 Recognise some risks to personal data from data processing like: accidental or unlawful destruction, loss, alteration, unauthorised disclosure, unauthorised access.

- There are many risks to personal data from data processing particularly given the widespread adoption of technologies such as the internet, e-commerce, social media and mobile and the resulting increase in personal data processing.
- For example, personal data may be destroyed, lost, altered, disclosed or accessed without permission.
- This can be accidental, for example deleting personal information by mistake, or it can be unlawful, for example stealing and selling personal information to a third party.
- It is important to be aware of potential risks to personal data so that appropriate safeguards can be put in place to minimise the risks and keep personal data safe.

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.

- If personal data is not kept safe while being processed it may result in negative consequences for individuals.
- For example, if data is lost, stolen or disclosed it could be used to discriminate against an individual, to steal their identity, for fraudulent activity, to steal money from them, or to damage their reputation.
- It may also lead to loss of confidentiality, loss of privacy, loss of other rights, and a loss of control over their personal data.
- Personal data may also be used for profiling to analyse or predict something about the individual.

1.2.4 Understand data protection roles and responsibilities like:

- Data subject - A living person, known also as a natural person, to whom personal data relates.
- Data processor - A natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.
- This is typically an organisation or individual performing a task at the instruction of another organisation, for example, a website hosting company, an email service provider, a cloud storage company or an employee payroll company.
- Data processors are not employees of the data controller.
- Data controller - A 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.
- This is typically an organisation that makes decisions to collect or use personal data, for example, schools, charities, sports clubs, retail shops, government agencies, and multinational corporations.
- Data protection officer (DPO) - Responsible for informing, advising and monitoring data controllers, data processors and employees who carry out processing, to ensure that they comply with data protection regulations by various methods including advising on data protection impact assessments, staff training and internal audits.
- In addition, they act as the point of contact for the supervisory authority.
- Not all organisations are required to have a DPO - those that are required include public authorities; organisations whose activities involve the regular and systematic monitoring of data subjects on a large scale; and organisations who process special categories of personal data or data concerning criminal offences on a large scale.
- Supervisory authority - An independent public authority established by a member state responsible for monitoring and enforcing the application of data protection regulations in that member state.
- The supervisory authority is concerned with the processing of personal data when it is processed by data controllers or data processors established in the Member State, it belongs to data subjects residing in the Member State, or it relates to a complaint lodged with them.

2 GDPR Overview

2.1 Rationale and Objectives

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.

- The General Data Protection Regulation was adopted by the European Parliament in 2016.
- It automatically becomes law in European Economic Area (EEA) member states on 25 May 2018.
- The GDPR creates a standard for how personal data must be processed and protected but also allows scope for member states to provide additional legislation.
- It replaces the previous European Directive 95/46/EC on data protection, which was created before the growth of social media and e-commerce. Unlike the GDPR, the directive had to be adopted into national law.

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

- As the world is increasingly connected through technology and more personal data is processed in innovative ways, the GDPR responds to a need for increased legal certainty relating to personal data processing for organisations working across jurisdictions and individuals availing of goods and services from multiple jurisdictions.
- It also provides increased consumer confidence and trust relating to how personal data will be treated, which facilitates consumer engagement and economic growth.
- And it responds to a need for increased protection of growing volumes of electronic personal data and their international transfer.

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 – The GDPR aims to standardise data protection laws to provide the same protection for all citizens in the EU in relation to the processing of their personal data.
- Free flow of personal data throughout the European Union (EU) – The GDPR aims to ensure that there is a free exchange of personal data between member states and beyond by providing equivalent legal protection, legal certainty and by building trust.

2.2 Scope

2.2.1 Outline the scope of data processing activities covered by the GDPR:

- Automated and manual processing of personal data – The GDPR applies to nearly all activities where personal data is processed including automated processing and manual processing.
- Personal data processing activities exempted from the application of the regulation – The GDPR does not apply to certain personal data processing activities such as those that fall outside the scope of EU law; personal or household activities; criminal prevention, investigation and prosecution activities; national or EU security activities; where personal data is in a physical and unstructured format; and where personal data belongs to a deceased person.

2.2.2 Outline the territorial scope of the GDPR regarding the location of personal data processing and data subjects.

- The GDPR applies to the processing of personal data by a data controller or data processor established in the EU, regardless of whether the data processing occurs in the EU or not.
- The GDPR also applies to the processing of personal data by a data controller or data processor not established in the EU, if the processing involves the offering of goods or services to a data subject in the EU, regardless of whether a payment is involved; involves the monitoring of the behaviour of a data subject within the EU; or takes place where member state law applies by virtue of public international law.

3 Principles

3.1 Processing Personal Data

3.1.1 Define the principle of 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)
- This principle requires that processing of personal data should have a lawful basis; should be in line with what is considered fair; and should be transparent so that data subjects know when and to what extent their personal data is processed.

3.1.2 Define the principle of 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; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes" (GDPR Article 5)
- This principle requires a data controller to process personal data for specific purposes, which must be specified at the time of collection, and any further processing must be compatible with those purposes.
- For example, an email address collected for the purpose of delivering an electronic receipt to a customer may not be used for marketing purposes.

3.1.3 Define the principle of data minimisation.

- "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)
- This principle requires a data controller to collect the minimum amount of personal data needed to fulfil the specific purpose of the processing.
- For example, if a data controller needs to confirm that an individual is over a certain age, they may request confirmation of that information rather than requesting a date of birth.

3.1.4 Define the principle of accuracy.

- "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)
- This principle requires a data controller to have systems in place to ensure personal data is accurate and up to date and that inaccurate information is deleted or updated, unless maintaining inaccurate information is necessary for the purpose of processing.
- For example, a data controller should ensure a customer's postal address is accurate and up to date if the address is used for delivering goods or services; however an inaccurate medical diagnosis may need to be kept on a patient's records as part of their medical history.

3.1.5 Define the principle of 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; 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject." (GDPR Article 5)
- This principle requires a data controller to define the minimum duration needed to retain personal data for the purposes of processing, or a time to review this, and to delete any personal data after this duration. However personal data may be stored for longer if it is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
- For example, if a data controller collects a customer's date of birth to verify their age, the date of birth should be deleted from the record after the age verification is recorded.

3.1.6 Define the principle of integrity and confidentiality.

- "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)
- This principle requires a data controller and a data processor to protect personal data from security risks by implementing appropriate technical and organisational measures such as physical and technical security measures, information security roles and responsibilities, policies and procedures, and staff training.
- For example, a data controller should have measures in place to ensure physical and electronic files containing personal data are not lost due to events such as fires, floods, theft, or accidental deletion.
- For example, a data controller should have measures in place to ensure that a patient's medical file or an employee's personal file are kept private and not left in public view.

3.1.7 Define the principle of accountability.

- "The controller shall be responsible for, and be able to demonstrate compliance with, (the other principles)". (GDPR Article 5)
- This principle requires a data controller to implement appropriate measures to comply with the other 6 data protection principles and to be able to demonstrate these measures on request.
- Data processors also carry significant responsibilities for compliance under data protection legislation.

3.2 Lawfulness of Processing

3.2.1 Outline the conditions under which personal data processing is lawful:

Processing personal data is only lawful, and should only take place, when there is a valid lawful basis. There are six lawful bases, and which of them a data controller selects as the lawful grounds for processing depends on the purposes of the processing. They are:

- Consent by data subject - "The data subject has given consent to the processing their personal data for one or more specific purposes." (GDPR Article 6)
- This is when a data subject is given a real choice about whether their personal data is processed or not for an explicit reason and they agree.
- For example, an individual choosing to join an electronic mailing list.
- Performance of a contract - "Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract." (GDPR Article 6)
- This is when a data subject is already in or is planning to enter into a contract.
- For example, an individual agreeing to purchase a holiday from a travel agent.
- Compliance with a legal obligation – "Processing is necessary for compliance with a legal obligation to which the controller is subject." (GDPR Article 6)
- This is when a data controller is obliged by law to process personal data.
- For example, an organisation being obliged by law to deduct taxes from their employees' salaries.
- Protection of vital interests – "Processing is necessary to protect the vital interests of the data subject or of another natural person." (GDPR Article 6)
- This is when a data subject or someone linked to them needs protection or care.
- For example, an individual falling when hiking and needing medical attention and the emergency services finding them using location related mobile data and services.
- Performance of a task carried out in the 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." (GDPR Article 6)
- This is when a data controller needs to meet an obligation in the public interest or are acting in their capacity as an official authority.
- For example, a shop owner sharing CCTV information of an individual committing a crime or a police officer gathering information to solve a crime.
- Pursuance of legitimate interests by the controller or by a third party – "Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks." (GDPR Article 6)
- This is to fulfil a legitimate interest of a data controller or third party. However, a legitimate interest does not override the fundamental rights and freedoms of the data subject.
- For example, a credit card provider passing personal data to a debt recovery agency when a customer is in arrears on their credit card.

3.2.2 Be aware that consent can only be considered given by the data subject if certain conditions are met.

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

3.2.2 Outline the conditions for consent:

- Recorded - A data controller must demonstrate that a data subject, through a clear affirmative action (sometimes referred to as opt-in), has unambiguously consented to their personal data being processed.
- Consent can be demonstrated in a variety of ways such as a recorded written or verbal statement or behaviour, but it must clearly demonstrate that the data subject accepts the proposed processing of their personal data.
- For example, ticking a box on a website or setting preferences in a mobile app demonstrate consent whereas silence, pre-ticked opt-in boxes or inactivity do not.
- Clearly requested - A data controller must present the request for consent clearly, transparently and distinguishable from any other information so that the data subject's consent is clearly informed.
- For example, the request for consent should not be mixed with the terms and conditions for use of a product or service.
- If processing has multiple purposes, consent should be granular and specifically requested for each purpose so that the data subject's consent is specific.

- For example, a request for consent by a content streaming company to gather information to provide personalised content should be separate from a request for consent to provide this information to third parties to display targeted advertising.
- Withdrawable - A data controller must ensure that the data subject can easily withdraw consent at any time. The withdrawal of consent should not affect the lawfulness of the processing that took place before the withdrawal.
- Given freely – Consent must be given freely and should not be a precondition for the performance of a contract or accessing a service, if the personal data processing is not specifically needed for the performance of the contract or service.
- Consent is not considered given freely if the data subject has no real choice or is unable to refuse or withdraw consent without negative consequences

3.2.3 Understand the conditions applicable to a child's consent in relation to online services.

- Processing of personal data belonging to a child in relation to online services such as online shopping, streaming, and social networking services, is only considered lawful when consent is given by the person with parental responsibility for the child.
- A child is considered a person who is less than 16 years old, although Member States can set the digital age of consent as low as 13 years old.
- A data controller must make reasonable efforts to verify that consent is provided by the person with parental responsibility for the child.

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.

- A data controller is legally required to have data processing agreements in place with data processors (or data processors with sub-processors) to ensure that appropriate and necessary controls are in place anytime a processing activity is carried out for one organisation by another organisation.
- A data controller should only use data processors who can guarantee they use appropriate technical and organisational measures to secure personal data processed by other organisations and individuals.

3.2.5 Identify special categories of personal data that are typically prohibited from processing:

These are types of personal data that reveal or have the potential to reveal:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic information.
- Biometric information.
- Health information.
- Sex life.
- Sexual orientation.

3.2.5 Recognise that special categories of data can be processed lawfully under certain conditions like explicit consent.

- Special categories of personal data can be processed in certain situations, such as when a data subject gives their explicit consent to the processing.

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.

- 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.

4 Data Subject Rights

4.1 Facilitate Rights

4.1.1 Recognise the importance of clearly communicating to the data subject information relating to processing like: privacy notice, fair processing notice.

- A data subject has the right to be informed in relation to how their personal data is processed and for what purpose.
- The data controller must provide the data subject with comprehensive information in relation to the processing of their personal data to facilitate this right.
- This information is typically provided in the form of a privacy notice or fair processing notice at the same time when personal data is collected.
- All information and communication in relation to processing must be clear, concise, transparent, easily understood, easily accessible and appropriate for the audience.

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 – A data subject should be informed about who the data controller is and how to contact them or their representatives.
- The purpose and legal basis of processing - A data subject should be informed about why their personal data is being processed as well as the legal basis for the processing.
- The data retention period - A data subject should be informed about the length of time the data will be stored or if this is not known, the criteria for determining the retention period.
- The data subject's rights - A data subject should be informed about their applicable rights under the legislation in relation to personal data processing.

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 - If a data controller intends to transfer personal data to a third country or international organisation, they should inform the data subject of this along with relevant information about adequacy decisions and safeguards.
- Contact details for any DPO - If there is a DPO, the data subject should be informed about their contact details.
- Any other recipients – If a data controller intends to pass personal data to any other recipients they should inform the data subject of the other recipient's information.
- Any other information to make the processing fair – For example if a data controller intends to process the personal data for anything other than the original purpose, they must inform the data subject before processing the personal data further.

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.

- 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.

4.2 Exercise Rights

4.2.1 Define the term subject access request. Understand a data subject's right of access.

- A data subject has the right to obtain from a data controller confirmation if their personal data is being processed, a copy of the personal data being processed, and information about how their personal data is processed including the purposes of processing, the categories processed, any recipients, the data retention period, the data subject's rights, the source of the data if it was collected indirectly, any automated decision-making, and any safeguards if data is transferred to a third country or international organisation.
- This information is requested by a data subject via a subject access request, also known as a data access request and the data controller must respond to the request within one month of receipt free of charge.

4.2.2 Understand the right to rectification.

- A data subject has the right to obtain from a data controller, without undue delay, the rectification or revision of incorrect personal data, as well as the completion of any incomplete personal data, including by providing additional information.

4.2.3 Understand the right to be forgotten.

- A data subject has the right to obtain from a data controller the erasure or deletion of personal data without undue delay in certain circumstances.
- These include when personal data is no longer needed for the original purpose, the data subject withdraws consent and there is no other lawful basis for processing, the data subject objects to processing and there are no overriding legitimate grounds for processing, the personal data has been unlawfully processed, or the data controller must meet a legal obligation.
- A data controller must make a reasonable attempt to inform any other data controllers processing the personal data that the data subject has requested that it is deleted along with any links to it or copies of it.

4.2.4 Understand the right to restriction of processing.

- A data subject has the right to obtain from a data controller restriction or suspension of processing in certain circumstances.
- These include when the data controller needs to address a claim from the data subject that their personal data is inaccurate, processing is unlawful but the data subject does not want their personal data deleted, the data controller no longer needs the personal data for processing but the data subject needs it for a legal claim, or there is a decision pending about the legitimate grounds of processing.

4.2.5 Understand the right to data portability.

- A data subject has the right to receive their personal data in a structured, commonly used and machine-readable format and to transfer it from one data controller to another.
- This generally applies where the processing is carried out by automated means.

4.2.6 Understand the right to object.

- A data subject has the right to object at any time to the processing of their personal data and in many circumstances, the data controller must stop processing as a result.
- For example, if a data controller is processing personal data for direct marketing and a data subject objects, then the data controller should stop processing.
- However, if a data controller is processing personal data based on "legitimate interest", and a data subject objects, the data controller can continue processing if they can demonstrate legitimate grounds for the processing which override the interests, rights and freedoms of the data subject.

4.2.6 Understand the right not to be subject to a decision based solely on automated processing, including profiling.

- A data subject has the right not to be subject to a decision based solely on automated processing, including profiling if it has a legal effect or similarly significant effect on them.
- Exceptions include when the decision is necessary for a contract between the data subject and a data controller, is authorised by law or is based on the data subject's explicit consent.

4.2.7 Understand that the rights of the data subject may not be met if there are legal restrictions.

- 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 EU or Member States that takes precedence such as those in relation to national security.

5 Implementation

5.1 Policies and Methods

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.

- Data protection guidelines and policies that govern personal data processing throughout an organisation must be compliant with data protection regulations as required by the principle of accountability.
- Examples include policies governing data processing operations such as security policies; procedures to manage access, correction and deletion requests; procedures to manage reporting of security breaches; procedures for creating new personal data processing operations; procedures such as audits to verify that measures are implemented in practice; and mechanisms to handle complaints.
- Demonstrated adherence to organisational data protection guidelines and policies is important because it demonstrates accountability and compliance with data protection regulations and it also avoids infringements and potential consequences.

5.1.2 Understand that data processing should incorporate data protection by design and by default.

- Data protection by design, also known as privacy by design, requires organisations to adopt a holistic approach to data protection where privacy is embedded into any new projects from the planning stage.
- The data controller must apply data protection by design by implementing technical and organisational measures that address data protection obligations both when planning new data

processing activities and at the time of data processing.

- Examples of measures include pseudonymisation and data minimisation.
- Data protection (privacy) by default, also known as privacy by default, requires organisations to ensure that personal data is processed with the highest privacy settings and protection from the start.
- The data controller must apply data protection by default by implementing appropriate technical and organisational measures that ensure, by default, that only relevant personal data are collected and processed for specific purposes, are stored for no longer than necessary, and are accessed only by authorised people.
- For example, a social media platform should by default set profile settings to be as private as possible and allow the data subject to decide whether to make their profile more public.

5.1.3 Understand the term data protection impact assessment and when it is required.

- A data protection impact assessment (DPIA), also known as a privacy impact assessment, should be carried out by a data controller to assess the impact of any new processing activities when they are considered a high risk to the rights and freedoms of data subjects.
- A DPIA is mandatory for certain types of processing such as automated decision making producing a legal or significant effect on data subjects; any large-scale processing of special categories of data or personal data relating to criminal convictions and offences; and any large scale systematic monitoring of data subjects in public areas.
- For example, a DPIA should be carried out in the case of a data controller gathering public social media profile data to be used by private companies generating profiles for contact directories.

5.2 Measures

5.2.1 Recognise some appropriate technical and organisational measures to manage risks when processing personal data like:

- The pseudonymisation of personal data - This replaces any data that identifies the data subject directly with a pseudonym or value so that additional information is needed to identify the data subject. The additional information should be stored separately so it cannot be used to identify the data subject directly.
- The encryption of personal data - This involves ensuring that personal data is encoded so that it is unreadable by unauthorised people.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services - This involves ensuring that systems and services used to store personal data are secure and resilient.
- The ability to restore personal data in a timely manner - This involves ensuring that personal data is backed up to a secondary storage location so that in the event of loss, theft or damage, the data can be returned quickly and intact to its original location or a new location.
- A process for determining the effectiveness of technical and organisational measures - This involves implementing a process for evaluating the effectiveness of the measures in meeting data protection obligations, for example an auditing process.

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.

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.

5.2.4 Distinguish between the pseudonymisation and anonymisation of personal data.

- Pseudonymisation of personal data – This helps protect the identity of a data subject while the personal data is processed but because it may be possible to identify the data subject by reference to additional information it may not completely protect the identity of the data subject.
- For example, a medical sample identified by a code for processing in a lab may be connected to a person by linking the code to the person's name.
- Anonymisation of personal data – This is when the data has been processed so that the data subject can no longer be identified from the data or from any further analysis of any related data.
- Data which has been irreversibly anonymised is no longer considered personal data and is no longer subject to data protection regulations.

6 Compliance

6.1 Data Breaches

6.1.1 Understand the term personal data breach.

- "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)
- A personal data breach can be considered a confidentiality breach where there is unauthorised or accidental disclosure of, or access to, personal data; an availability breach where there is accidental or unauthorised loss of access to, or destruction of, personal data; an integrity breach where there is unauthorised or accidental alteration of personal data.

6.1.2 Be aware when the data controller must report personal data breaches to the supervisory authority.

- The data controller must report personal data breaches to the supervisory authority when it might result in a risk to the data subject's rights and freedoms.
- The report should include the categories and number of data subjects and personal data records affected, the name and contact details of the data protection officer or other relevant contact, the potential consequences of the breach, and the measures taken to address and reduce any negative consequences of the breach.

6.1.2 Be aware of the associated time frame for reporting.

- 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.

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.

- The data controller shall inform the data subject, without undue delay, when there is a personal data breach if there is a high risk to the data subject's rights and freedoms
- For example, where personal data is not encrypted, and that data is lost or stolen there is a high risk to the data subject's rights and freedoms.

6.2 Enforcement

6.2.1 Identify the supervisory authority in your jurisdiction and recognise the requirement to cooperate with it when requested.

- The supervisory authority in each Member State's jurisdiction is concerned with the processing of personal data in that jurisdiction when it is being processed by data controllers or processors established in that Member State, when it belongs to data subjects residing in that Member State, or when it is related to a received complaint.
- The data controller and the data processor are obliged to cooperate with the supervisory authority when requested, for example, by providing records of processing activities, to enable the supervisory authority to carry out its role in monitoring and enforcing the data protection regulations.
- The supervisory authority has very significant investigative, corrective, authorisation and advisory powers.

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.

- 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.

6.2.3 Understand possible consequences for organisations that fail to implement relevant data protection regulations like:

- Fines - A supervisory authority has the power to impose fines for breaches of the data protection regulation. Organisations may be liable for fines up to 20 000 000 EUR or 4% of total worldwide annual turnover of the preceding financial year, whichever is higher.
- Litigation - 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.
- Data subjects have the right to receive compensation from the controller or processor for damages suffered.
- Reputational damage - Organisations may suffer damage to their reputation, which may lead to loss of consumer trust and business.