Q4INC.COM

GDPR - Overview

Data protection legislation has existed for decades to protect personal information. Changes in technology and business environments have seen this legislation updated and adjusted over the years.

The GDPR is the most recent example.

This **Q4 GDPR training** will **teach** you all you need to know in order to **comply with GDPR**.

- Describe the GDPR, its importance and the date it comes into effect.
- Identify the relevant data protection roles
- Determine when a task is within the scope of the GDPR
- Identify and differentiate between personal data and sensitive data.
- Summarise the **six data protection principles**.
- Summarise the legal obligation of data controller and a data processor.
- Describe data subject's rights under the GDPR.
- Identify when a data subject's personal data can be processed and shared.
- Process around Subject Access Request **(SAR)**
- Outline the process for **reporting a breach**.

General Data Protection Regulation (GDPR)

Introduction

The history of data protection and the GDPR

GDPR roles

Look at the different roles within the GDPR

GDPR scope

Identify which tasks fall within the scope of GDPR

GDPR principles

Examine the GDPR data protection principles

Applying the GDPR

Practical information on applying the GDPR.

Summary

Review the information we've covered in the Q4 GDPR course.

Introduction – The GDPR in a Nutshell

- **The EU GDPR** (European Union General Data Protection Regulation) provides a coherent and thorough personal data privacy law across all EU member states.
- The **GDPR aims** to **prevent security breaches** and the **loss of personal data** by organisations that hold or process **PII** (Personally Identifiable Information).
- **Impacts any organisation** that offers goods or services (even free ones) or monitors the behaviour of EU citizens.
- More prescriptive than the Data Protection Directive 95/46/EC (which it replaces)
- **Penalty** for breaking the regulations can be financially extreme and significantly detrimental
- **GDPR will be the lawful benchmark** that all organisations who process or store PII must adhere to
- **Effective date – May 25th 2018**

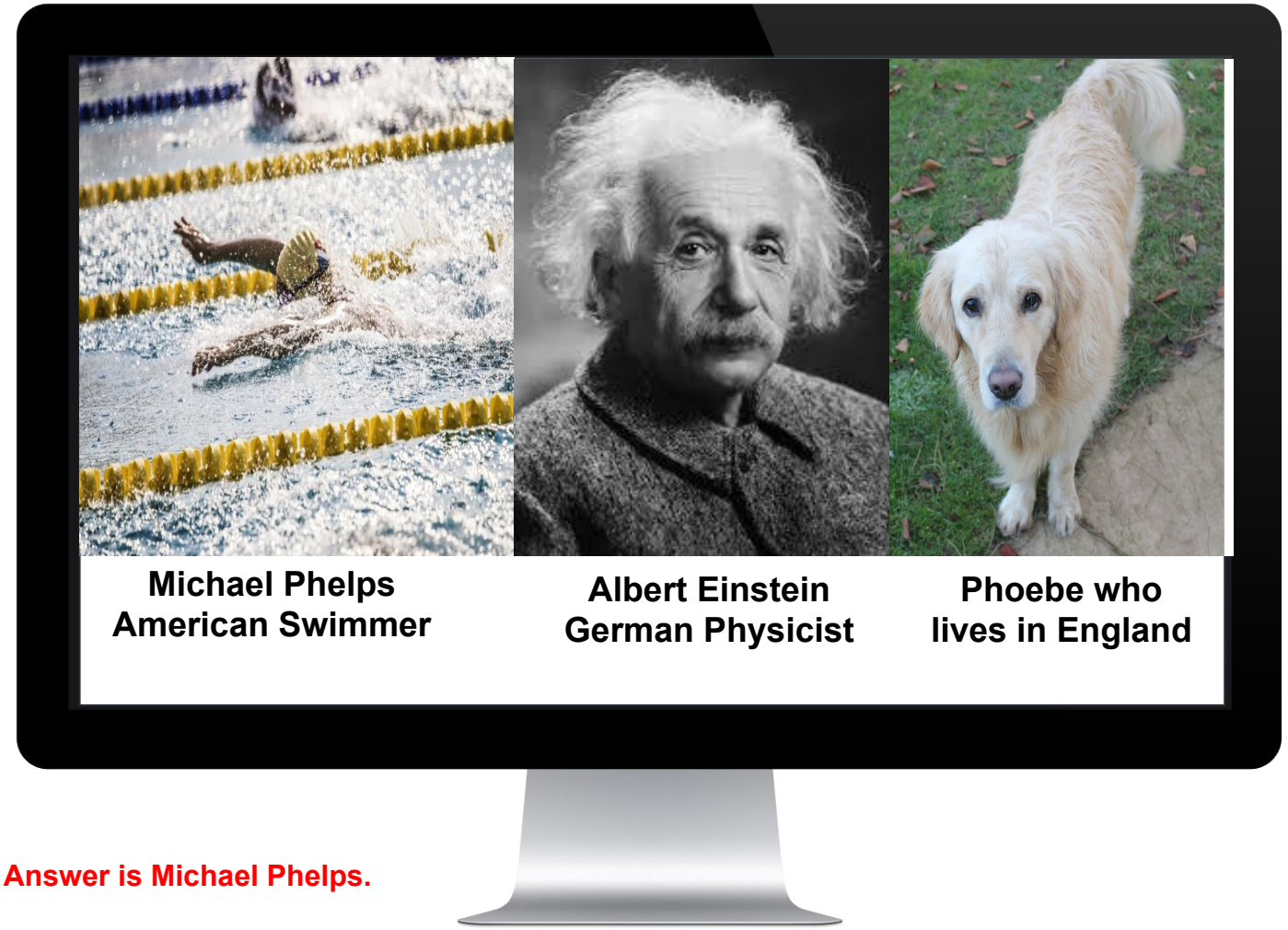
Introduction – The Focus of GDPR

- The GDPR is a legal set of rules that must be adhered to by organisations that "**process**" - harvest, store, or make use of personal information
- The focus is on **people** – they are the ones that have personal information (Personally Identifiable Information or PII)
- In an age of increasing globalisation and big data, PII has a value and can be exploited
  - ➢ **The GDPR is aimed at protecting people's PII** when it is in the hands of organisations
  - ➢ **The GDPR grants people rights** and places the obligation on organisations that hold their data

What is Personal Information?
GDPR Art.4(1) defines Personal Data as:
"Any information relating to an identified or identifiable natural person ("data subject"); an identifiable 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, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person."

- ➢ If you can identify an individual from the data held, then the data is "Personal Information" and it therefore **falls within the scope of the GDPR**.

Which of the following would be protected under the GDPR?



- **The correct Answer is Michael Phelps.**

- GDPR does not just cover EU citizens but the scope includes anyone in EU or who is processed by anyone in the EU.
- Albert Einstein is not alive and GDPR only covers living people. Phoebe is not human so she is out of scope for GDPR.

General Data Protection Regulation (GDPR)

Introduction

The history of data protection and the GDPR

GDPR roles

Look at the different roles within the GDPR

GDPR scope

Identify which task fall within the scope of GDPR

GDPR principles

Examine the GDPR data protection principles

Applying the GDPR

Practical information on applying the GDPR.

Summary

Review the information we've covered in the Q4's GDPR course.

GDPR roles

Role	Description
Data Subject	A living natural person – they have rights and PII refers to them
Data Controller	Specifies how PII is to be manipulated
Data Processor	Manipulates the PII on behalf of the Data Controller
Data Protection Officer (DPO)	A person charged with protecting PII and helping an organisation to meet the GDPR compliance requirements
Supervisory Authority (SA)	A national body who enforces the GDPR in EU member states.
EDPB	**European Data Protection Board:** The coordinating layer who provides consistency between SAs
Third Country	A country outside of the EU
Third Party	An individual linked in some way to the Data Subject or any company or organisation to who data is sent

Processing: GDPR Definition

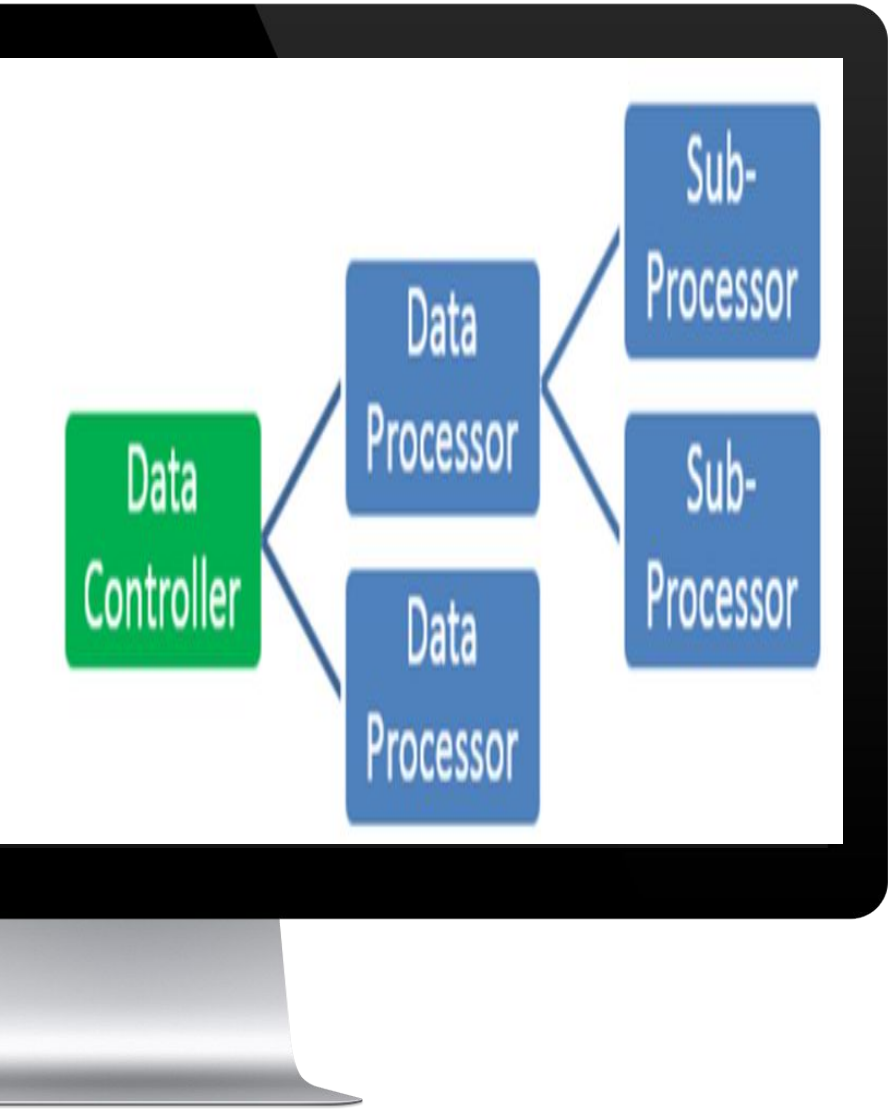
"Processing" in relation to information or data means **"obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data"**.

This includes:

- Organising and retrieving data.
- Manipulating data.
- Adaptation, alteration, or modification of the data.
- Use of the information or data.
- Transmitting the data and making the data available.
- Destroying, blocking, or erasing data.

How does this apply to Q4: Q4 has around 1000 clients and we are processing data on behalf of our clients.

Who processes PII?



Data Controllers

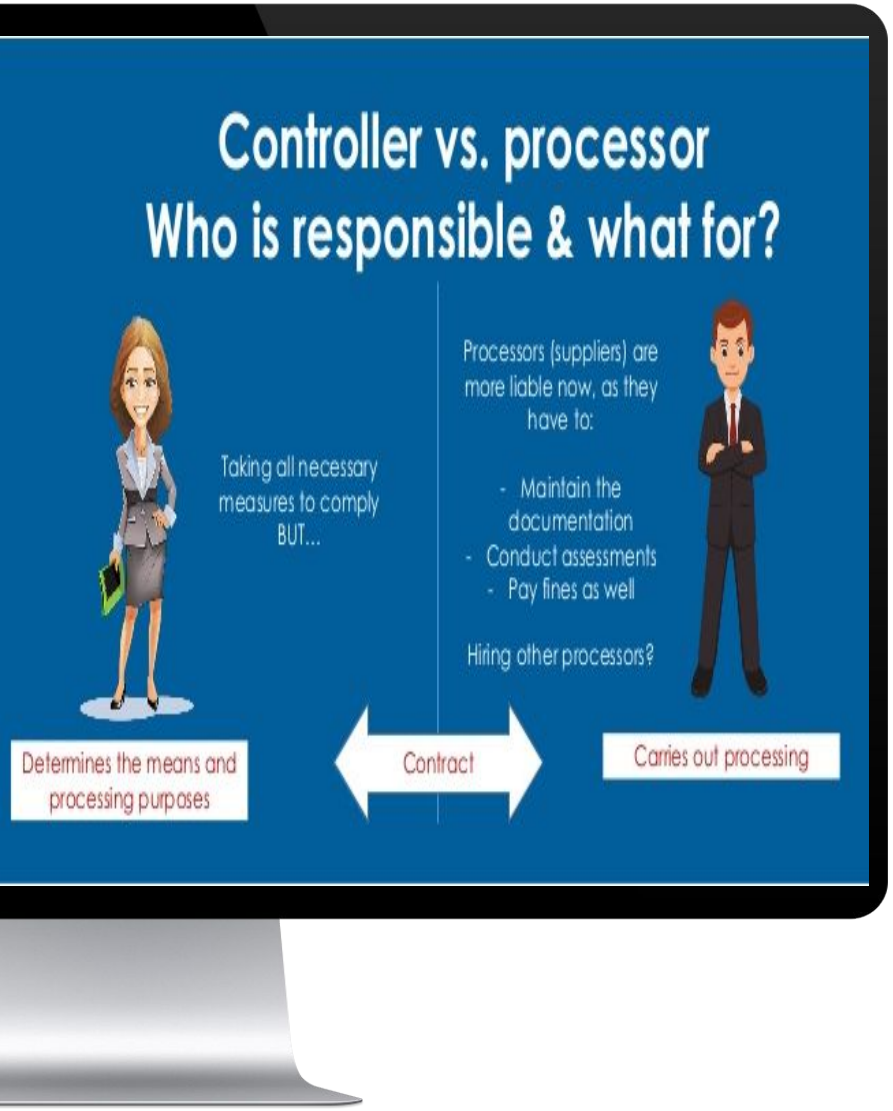
- *"A natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by EU or Member State laws, the controller (or the criteria for nominating the controller) may be designated by those laws".* **(Article.4(7))**

Data Processors

- *"A natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller"* **(Article.4(8))**

How does this apply to Q4: Our clients (eg: Intel) is the controller and Q4 is the data processor who processor their data as instructed by the controller.

Difference between Controller and Processor



As you may have realised, **it's not always easy** to draw distinct lines **between** the **roles** of data controller and data processor. In fact, in many situations, there may be more than one data controller involved, but there is usually a "main" data controller. Added to this, your particular role may change depending on the situation.

The important thing to **determine** is **whether you** or a particular party **has a say** in **what, how and why information** is **collected and processed.** If you do, then you are most likely a data controller.

Despite this, **both data controller and data processor are accountable** for ensuring compliance with the GDPR and are expected to take appropriate steps to be compliance.

Quick Quiz:

- City Bank has a collection of archived customer data that is securely stored by Big-tech, an IT company it employees for this purpose.
- City Bank is looking for some insight into its existing customer base and has hired a research company called Intuit Research to sift through this archived data and provide a report on specific metrics that have been identified by City Bank.

Can you identify the data protection roles in this scenario?

C

City Bank is the data **Controller** in this scenario as it controls the customer data and determines how and why it is used.

S

City Bank's customers are the data **Subject** in this scenario as the archived data is about them

P

Both Big-tech and Intuit Research are data **Processors** in this scenario. Big-tech is responsible for securely storing customer data and Intuit has been hired to provide metrics of customer data provided by City Bank.

General Data Protection Regulation (GDPR)

Introduction

The history of data protection and the GDPR

GDPR roles

Look at the different roles within the GDPR

GDPR scope

Identify which task fall within the scope of GDPR

GDPR principles

Examine the GDPR data protection principles

Applying the GDPR

Practical information on applying the GDPR.

Summary

Review the information we've covered in the Q4's GDPR course.

GDPR scope

Another key factor to consider is whether the task you are performing is within the scope of the GDPR.

The GDPR applies to the processing of personal data by controller and processors with the EU; regardless of where the data subject resides. It also applies to the processing of an EU data subjects personal data by controllers and processors that are not established within the EU, if this processing is being carried out to provide services into the EU.

This means that **in order to determine whether the GDPR applies** to a particular task you must consider a few elements:

- Whether the **data** being processed is **considered** to be the **personal data** of a **living natural person**.
- Whether the **data** is **collected**, **held** or **processed within the EU**; and if not,
- Whether **services** are being **provided into the EU**.

Personal Data (PII)

- The GDPR considers **personal data** to be **any information** that can be used to, directly or indirectly, **identify an individual**. This includes information that is stored digitally or manually indexed and filed.

- In addition to this, the **GDPR identifies certain personal data as sensitive.** Any data controller or data processor looking to collect or make use of sensitive data is required to obtain the explicit consent of the data subject before doing so.

How does this apply to Q4: Q4 stores email subscriber list, first names, last names, and other Personal data so we need to ensure there is adequate security to protect this data and Q4 is GDPR compliant.

Sensitive or Special Data (PII)

- **This is PII** that is particularly sensitive to the person concerned.

- The GDPR gives examples of **'Special Categories'** of personal data in Article (9):
  - Racial or Ethnic origin
  - Political opinion/affiliation
  - Religious or political beliefs
  - Trade Union membership
  - Genetic/biometric data (for the purpose of uniquely identifying a natural person)
  - Health related
  - Sex-life/sexual orientation

- Special categories of data have additional rules and processing restrictions.

How does this apply to Q4: Q4 does not store any Sensitive Data for any of our products.

GDPR Scope

Now that you have a better idea of what constitutes personal and sensitive data, **look** at the **scenarios that follow and determine whether** the particular **task is within the scope of the GDPR.**

Remember, **the GDPR is applicable to:**

1) Any **personal data** of a **living** natural **persona** that is collected, held or processed **within the EU** (regardless of the location of subject);

2) Any **personal** data that is collected, held or processed **outside the EU**, if done for the **purpose** of **providing services** in the EU.

Scenario 1

Q1) You work for a telecommunication company that operates in the E.U. Your marketing team is conducting customer research to determine the purchasing trends of the EU customers based on their demographic.

You are responsible for collecting and consolidating the survey information with the aim of informing future marketing strategy

Scenario 2

Q2) Last year you launched your own business providing consulting service to large corporate clients throughout the EU.

Your company has gone from strength to strength since you launched and it is now time to upgrade your branding to align with your professional offering.

You approach a local graphic design company, based in the E.U, for assisting updating your logo.

Scenario 1

Ans1) In Scenario 1, the survey information you are collecting and consolidating is considered personal data as it can directly identify the data subjects – who are living natural individuals.

You organization is the data controller and processor in this situation and is based within the EU, which, together with the personal data being processed, makes **it part of GDPR scope.**

Scenario 2

Ans2) Although your business, as the data controller, and the graphic design company, as the data processor, are both based in the E.U, Intellectual property (such as logo) is not considered personal data.

Additionally, the logo can only be used to identify your business, which in its own right, is not considered a data subject and **is not part of GDPR scope.**

Scenario 3

Q3) You work for EU-based company that provides payroll solutions to organization looking to outsource this function.

One of the accounts you're in charge of is headquartered in the USA. This head office provides you with the payroll information for the EU arm of its business, which you then run at the month end.

Scenario 4

Q4) Your company, based in Canada, sells business literature online to organizations around the world. You use a local Canadian courier service to deliver the literature to your customers, promising delivery within five working days worldwide.

You have just received an order from an individual within the EU which you must take payment for and process.

Scenario 3

Ans3) The payroll information in this scenario is considered personally identifiable and your company, as the data processor, is based in the E.U. This is **part of GDPR scope** despite the data controller being in the USA.

Scenario 4

Ans4) You, the data controller, and the courier company, as the data processor, are both based in Canada meaning the personal data is held outside the EU, but because you are providing service to a data subject within the EU, its **part of GDPR scope.**

General Data Protection Regulation (GDPR)

Introduction

The history of data protection and the GDPR

GDPR roles

Look at the different roles within the GDPR

GDPR scope

Identify which task fall within the scope of GDPR

GDPR principles

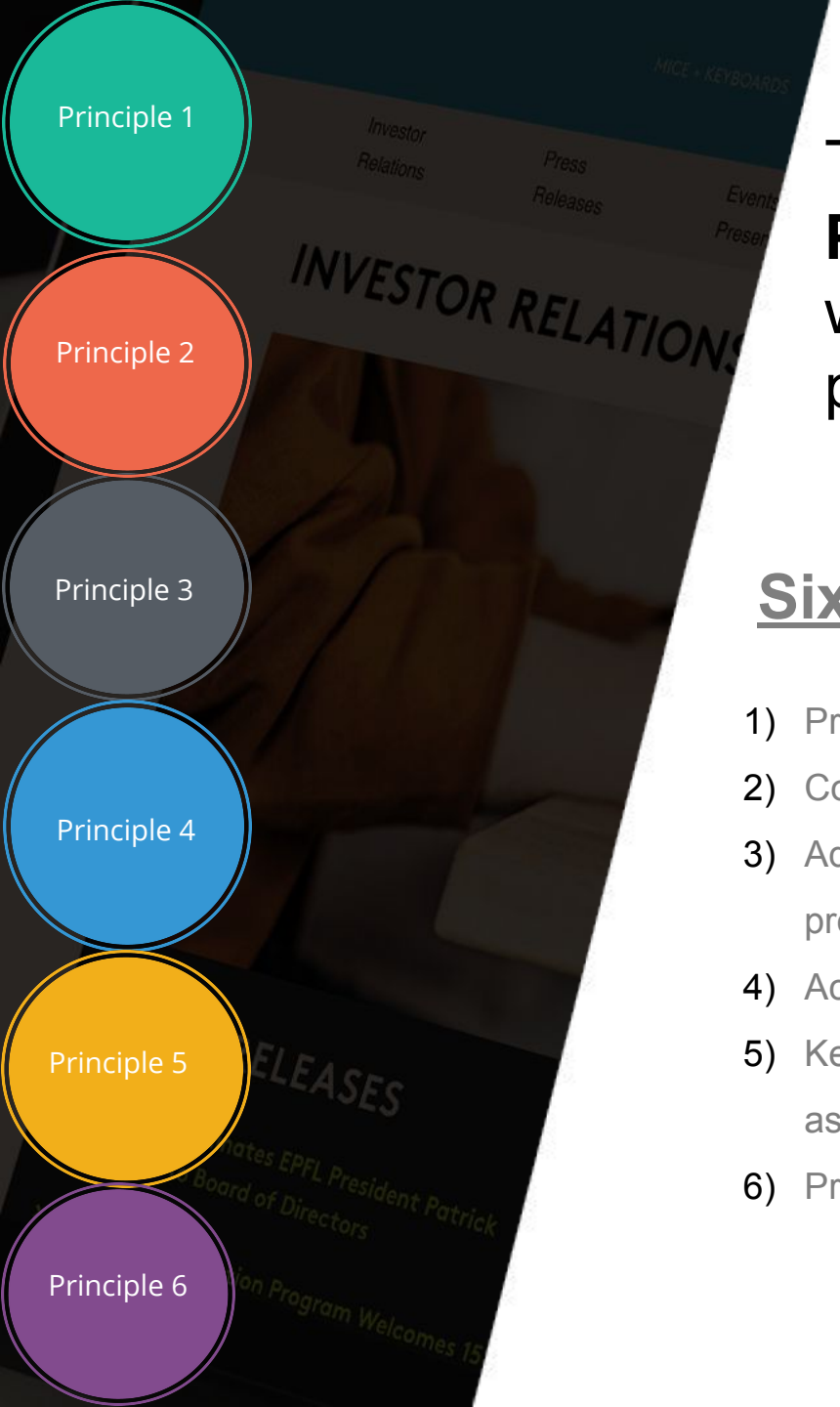
Examine the GDPR data protection principles

Applying the GDPR

Practical information on applying the GDPR.

Summary

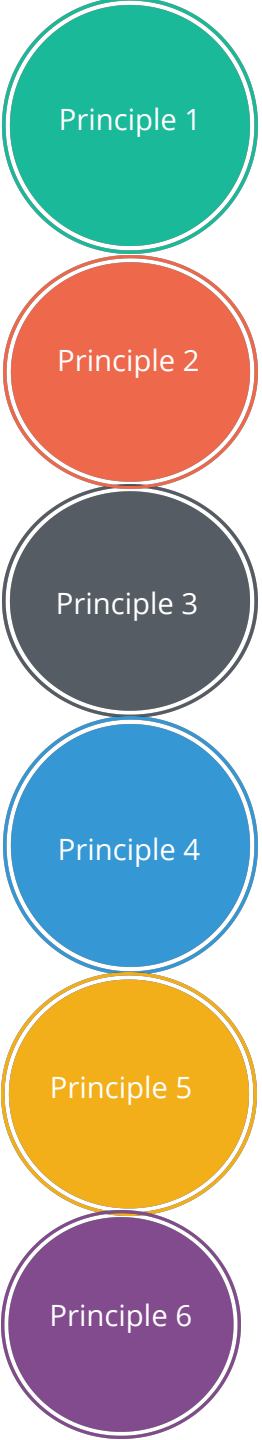
Review the information we've covered in the Q4's GDPR course.



The **GDPR identifies Six Principles** that should be applied when persona data is collected or processed.

Six Principles:

1) Processed lawfully, fairly, and transparently
2) Collected for specified and legitimate purpose.
3) Adequate, relevant and limited to what is necessary for processing
4) Accurate and kept up to date
5) Kept in a form that allows the identification of data subjects only as long as necessary for purpose
6) Processed in a manner that ensure its security

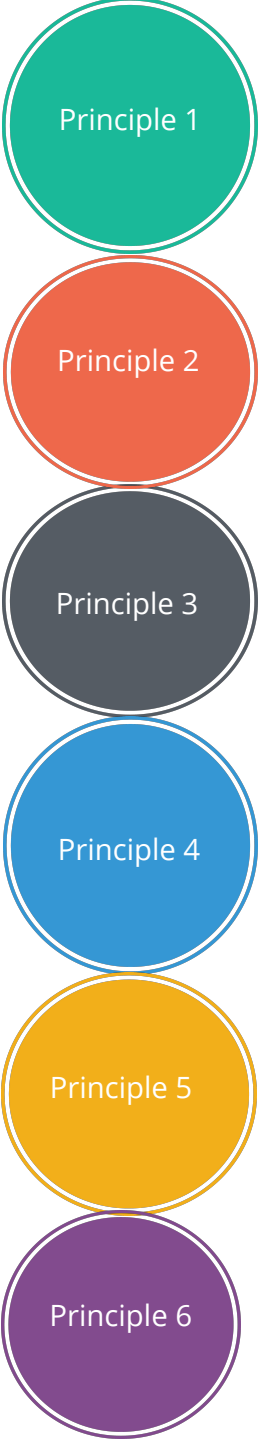


Principle 1

Processed lawfully, fairly and transparent

- This means ensuring that you have **met the conditions required** to **process personal and sensitive data**. In other words, you have obtained consent to process personal data (or explicit consent for sensitive data).
- When collecting personal data, you should also tell the data subject who you are, how the data will be processed and if the data will be disclosed to any other parties.

How does this apply to Q4: Q4 has updated its privacy statement which describes how we store and use personal data and what we disclose to third parties. The privacy policy is on the Q4 website.



Principle 2

Collected for specified, explicit and legitimate purpose

- You must only **collect personal data** for **legitimate** and **specified reasons**, and you must inform the data subject of these reasons.
- Personal data may, however, be achieved in the public interest, for scientific or historical research purpose or for statistical purpose.

How does this apply to Q4: Q4 collects data to provide service to its clients which is clearly detailed in our privacy policy.

Principle 1
Principle 2
Principle 3
Principle 4
Principle 5
Principle 6

Principle 3

Adequate, relevant and limited to what is necessary for processing

- Make sure you **only collect enough personal data** as is **necessary for processing**. You should not collect more personal data than you need to meet the requirements of the task at hand.

How does this apply to Q4: Q4 has made changes to its form to collect the minimum personal information required to provide service to its customers.

Principle 1
Principle 2
Principle 3
Principle 4
Principle 5
Principle 6

Principle 4

Accurate and Kept up to date

- You must take reasonable steps to **ensure personal data** is **accurate and kept up to date.**
- This includes amending or erasing personal data when it is found to be inaccurate, or when a data subjects informs you of any changes.

How does this apply to Q4: The clients can use CMS or send a request to Q4 support team to update or delete any inaccurate information.

Principle 1
Principle 2
Principle 3
Principle 4
Principle 5
Principle 6

Principle 5

Kept in a form that allows the identification of data subjects only as long as necessary for processing

- Personal data must only be kept in an identifiable form for as long as necessary for its intended purposes. Q4 has data retention policy that identifies when particular records may be destroyed and a systematic way of doing so.
- Personal data may, however, be stored for long periods if archived in the public interest, for scientific or historical research purposes, statistical purposes or for legal requirements.

How does this apply to Q4: Q4 keeps the data in the system as long as the service is required by the user. The end users can unsubscribe at any time or send a request to Q4 support team to remove their data from Q4 systems.

Principle 1
Principle 2
Principle 3
Principle 4
Principle 5
Principle 6

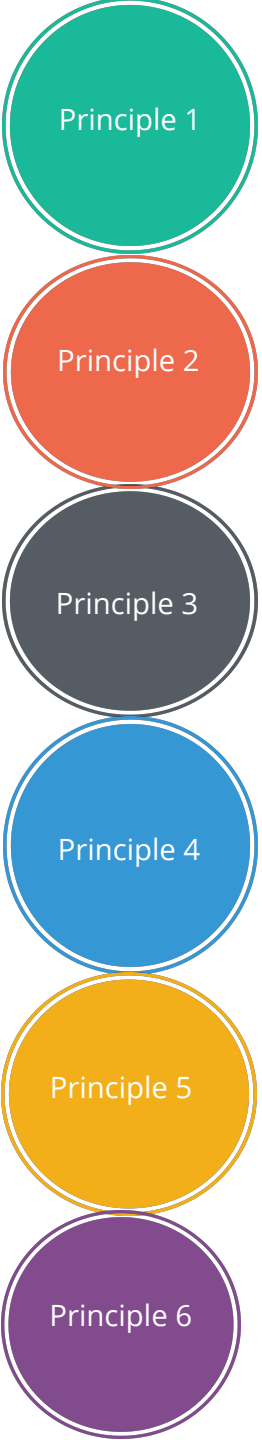
Principle 6

Processed in a manner that ensures its security

- Using appropriate technical and organisational measures, **personal data must be kept secure** to:

- Ensure protection against unauthorised or unlawful processing;
- Prevent accidental loss, damage or destruction
- Access control policy to ensure limited access to production.
- Implement Data Protection Principle by design and data protection by default.
- Data minimization, Pseudonymization, Transparency and improving security on an ongoing basis.
- Data should be encrypted both in transition and at-rest. PII data should not be transmitted in plain text or through email. It should be transferred through a web portal using SSL encryption.
- Implement an ISMS security program which follows ISO27001 and SOC2 security standards in securing data.
- End-to-End Security – Life Cycle protection – Nothing should be missed in terms of protection or accountability. Privacy must be consistently protected throughout the life cycle of all realms.

How does this apply to Q4: Q4 has Security processes and procedures in place to protect clients personal data.



Accountability

- The **data controller** is **responsible** for demonstrating compliance with GDPR data protection principles and must therefore ensure that any data processors have measures in place to enable compliance with GDPR.
- If there is a **breach**, however, **both the data controller and the processor are liable.**
- This makes it important to specify responsibilities and liabilities in any contractual arrangements between data controller and data processor.
- **Note: The ISO 27001 standards** is internally recognised as an effective way of demonstrating that the appropriate technical and organisational measures have been implement.

General Data Protection Regulation (GDPR)

Introduction

The history of data protection and the GDPR

GDPR roles

Look at the different roles within the GDPR

GDPR scope

Identify which task fall within the scope of GDPR

GDPR principles

Examine the GDPR data protection principles

Applying the GDPR

Practical information on applying the GDPR.

Summary

Review the information we've covered in the Q4's GDPR course.

We've covered the **concept** behind the **GDPR** and you should have a better idea about why it's been implemented, the different roles involved, and the scope and **principles of the GDPR**. But **what do you actually have to do?** Have a look at the **below section for more information**.

Collecting and processing personal data

Requesting personal data

Data breaches and security incidents

What are the data subjects under the GDPR?

- **The GDPR** provides **data subjects** with more control over their data as well as a better understanding of what their data is being used for?

- As a result, data subjects have certain **data protection rights** under the GDPR that, if infringed, allow the data subject to take legal action against data controllers and data processors, and seek compensation for damages. Make sure you abide by these rights when collecting or processing personal data:

1) The right to be informed
2) The right of access
3) The right to rectification
4) The right to erasure (to be forgotten)
5) The right to restrict processing
6) The right to data portability
7) The right to object
8) Rights in relation to automated decision making.

How does this apply to Q4: The data subjects (customers) can exercise any of their above rights at any time. For eg: a customer can request to remove their data from Q4 systems by sending an email to our support team. Q4 needs to respond within 1 month to ensure compliance. This service needs to be provided free of charge.

Subject Access Request (SAR)

- Often called “Access Request”
- Under the **GDPR Data Subjects** have the **legal right** to ask a Data Controller or a Data Processor what PII they hold on them, a description of any data which is being processed by reference to them.
- **Data Subjects also have the right to stop data processing** or terminate it and have their PII erased.
- Q4 has built templates for our multiple products so we can reply using a templated approach. Each request must receive a response within a month or we can face penalties by E.U Supervisor Authority. Link to the template.

Master Subject Access Request doc:
https://docs.google.com/document/d/11sg2ixiRFxpOFzVgMknlrnuzvGdf78OuJs4NRqZ9pwU/edit?usp=sharing

Consent

As a **data controller**, you **must:**

- Obtain clear and unambiguous consent.
- Obtain explicit consent for any sensitive data being processed.
- Obtain consent for each processing activity.
- Allow data subjects to remove consent.

How does this apply to Q4: Q4 has updated its email templates to get clear consent from the end users.

Data Breaches

- "**Data Breach**" means a breach of security leading to the:
  - Accidental or unlawful destruction
  - Loss
  - Alteration
  - Unauthorised disclosure of
  - Or access to personal data that has been transmitted, stored, or otherwise processed

- **Data Controllers** & **Data Processors** have **joint liability** for Data Breaches

- **Data Subjects have the right to sue:**
  - For material **and** non-material damage
  - Separately or jointly (class actions)
  - The Data Collector and/or the Data Processor
  - The Supervisory Authority if they do not take action when a complaint is raised
  - The regulations do not give an upper limit that can be awarded by the courts

- **The Supervisory Authority can impose administrative fines if not notified within 72 hours:**
  - Maximum fine – **€20M or 4%** previous year's global turnover for tier 1 breaches (Article 83), whichever is higher

  - These fines can be mitigated by demonstrating that an effective and robust framework is in place to protect personal data

How does this apply to Q4: Q4 has an Information System Security Incident response policy in place which follows 72 hour response time for any data breaches.

Quick Quiz:

Which of the following would be classified as Data Breaches under GDPR?

A. A laptop, with customer details, is left on a train, it has no password and the hard drive is not encrypted

B. A laptop, with customer details, is left on a train, it is password protected but the hard drive is not encrypted

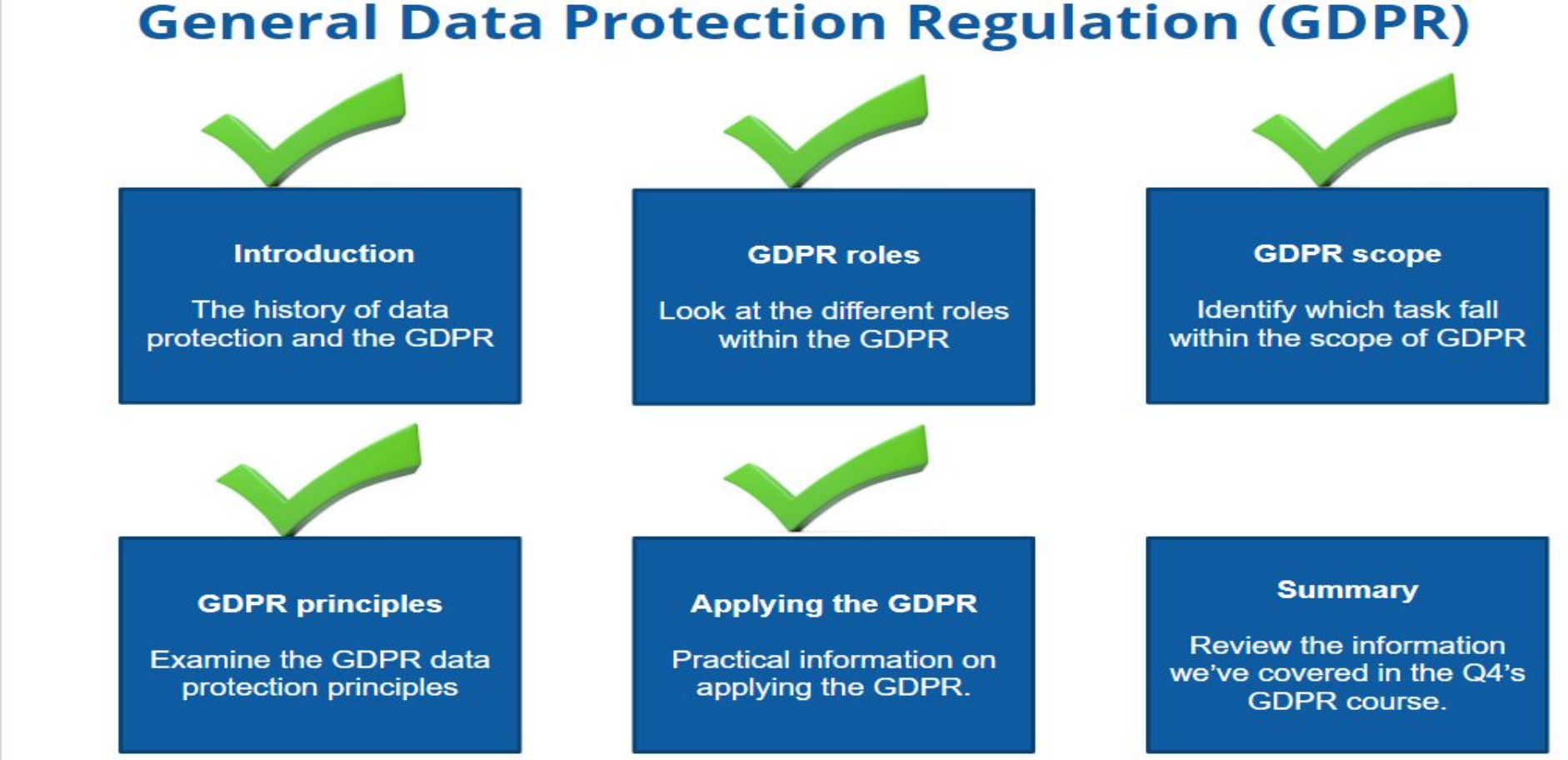
C. A laptop, with customer details, is left on a train, it is password protected and the hard drive is strongly encrypted

D. A file of patients and their associated medical histories is accidently deleted and there is no backup file.

E. A file of patients and their associated medical histories is accidently deleted and there is a backup file.

A B D

A, B & D if the data is not in recoverable format then there is no escape or leak. B ensure data is encrypted so it can't be viewed by anyone so it's not a breach. E – Since there is backup and the data can be restored quickly without any effect to end users, it will be not part of the breach.



Summary

Congratulations, you've completed the GDPR e-learning staff awareness course :

The GDPR can be complex topic, **buts its important that you:**

- **Know the role you play in a particular task:**
- **Understand if** the **task** is **within scope** of the GDPR;
- **Can identify personal and sensitive data and their processing requirements**; and
- **Apply** the **GDPR principles** when processing personal data.