# Managing Data and its Implications

## Lecture Title: General Data Protection Regulation


Lecturer: Angelito Sciberras

Date: 17 June 2023

Undergraduate Diploma in Business Administration

# Last Lectures

- What constitutes data - Qualitative vs Quantitative data
- Different types of data and how they’re measured
- Storage
- What is big data and the 7Vs of big data
- How companies use big data and data using different tools
- Why data has become important
- Profiling - Demographic, Psychographic, Geographical, Behavioural
- Digital Footprint
- Risks with data at companies
- Phishing and Spear Phishing


*to give individuals more control over their personal data*

# GDPR

- May 2018 replaced Directive 95/46/EC
- applies to any organisation, regardless of their location, that processes the personal data of EU citizens
- severe fines – up to €20 million or 4% of the organisation's annual global turnover
- major catalyst for organisations worldwide to take data protection seriously and implement stricter privacy policies and practices

# What was different from 1995?

# Directive 95/46/EC

Macintosh Performa 6200

IBM Personal Communicator


Kodak DCS 460 Camera

Iomega Zip Drive

Motorola Tango Pager

IBM ThinkPad 701C

Sony Handycam DCR-VX1000


DVDs

# GDPR vs Directive 95/46/EC

- Data was less portable
- Data was less accessible from the outside world
- No social media
- No emails
- No cloud storing
- Paper filing was still common practice

# GDPR vs Directive 95/46/EC

- Less risk of data breaches
- Less risk of identity thefts

# Data Breaches

15:00

Give examples of data breaches

How do they happen?

# Data Breaches

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.

# Data Breaches

Ransomware (inaccessible files)

Business Email Compromise

Stolen information

Password Guessing

Distributed Denial of Service (Ddos Attack) (crash servers)

Malware (control over device)

Keystroke loggers

PHISHING

# Data Breaches

Lost or stolen devices

Sending an email with multiple recepients not in BCC

Email sent to the wrong recepient

Accidental destruction of data

Unintended publication

Data of wrong person shown

# Data Breaches

August 2013 - 3 billion accounts

January 2018 - 1.1 billion Indian citizens

November 2019 - 1.1 billion

https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

# Last year - 2022

- The number of cyberattacks increased significantly
- Phishing attacks and ransomware being the most common types of attacks
- Stolen or compromised credentials were the leading cause of data breaches

# Last year - 2022

- Healthcare and finance were the most targeted industries
- Remote work and the use of personal devices for work purposes contributed to the increase in cyberattacks.
- Small and medium-sized businesses were targeted more frequently

# Data Breaches - March 2023

# Identity Theft

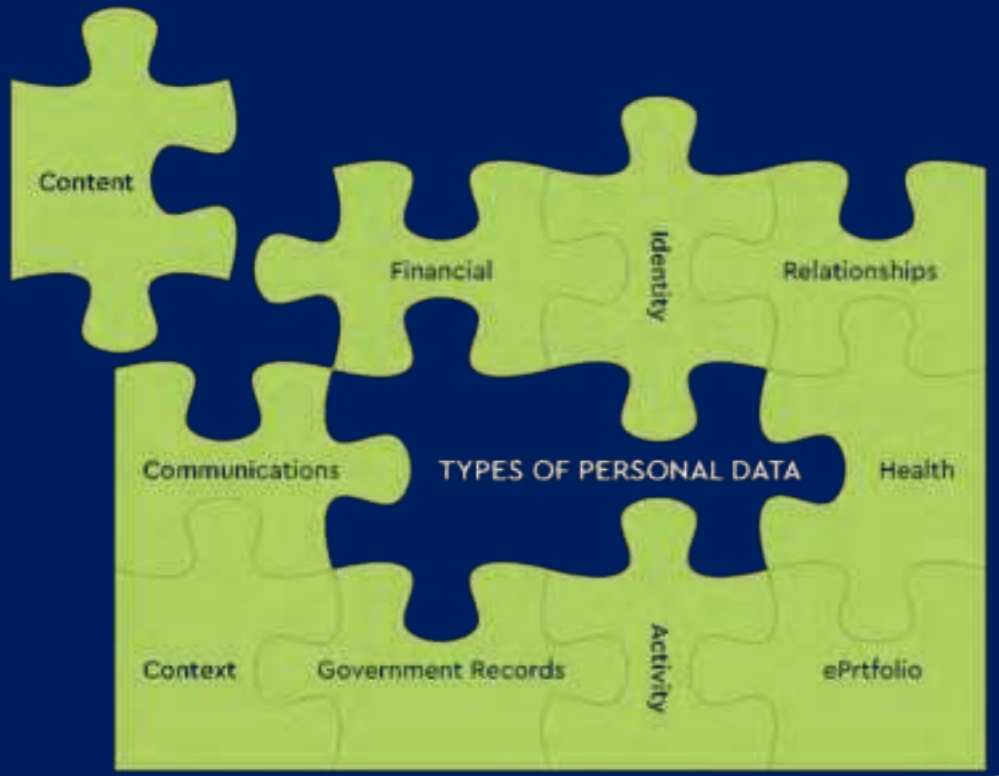
10:00

Give examples of identity theft

How do they happen?

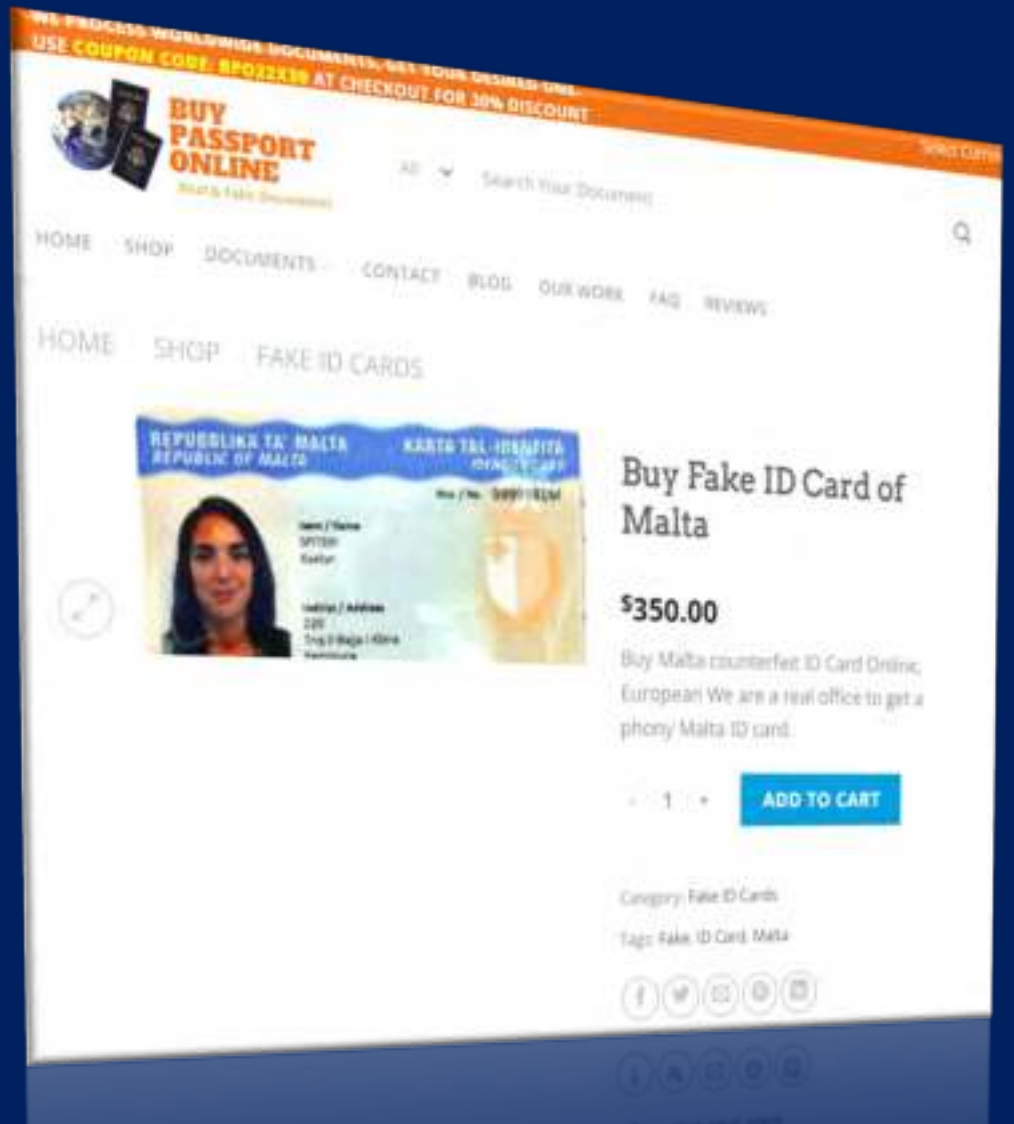
# Identity Theft

all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.



# Identity Theft

# Identity Theft




https://buypassportsonline.com

21 ACADEMY

# Undergraduate Diploma in Business Administration

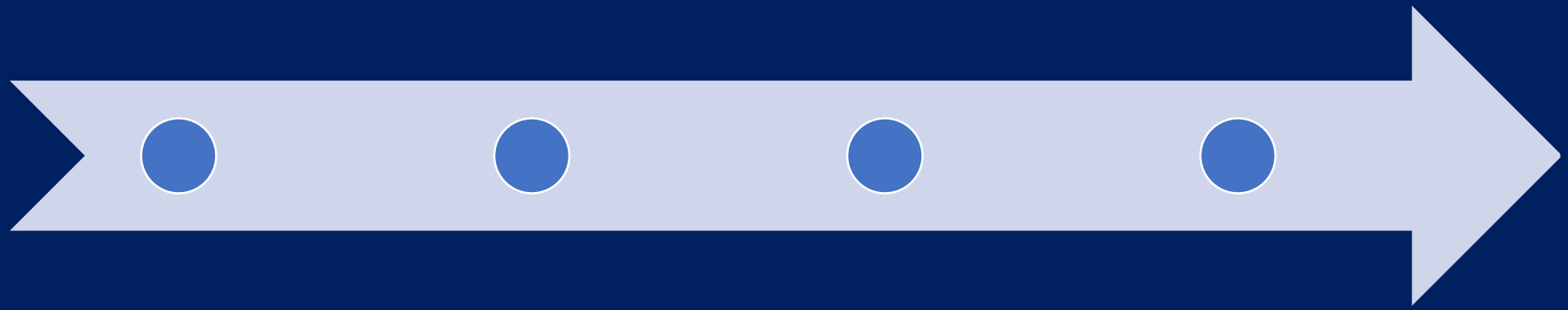
15:00

21 ACADEMY

Undergraduate Diploma in Business Administration

# How can data breaches be mitigated?

# How can data breaches be mitigated?



# GDPR

- Same legislation in all EU Member states
  - Regulation not Directive
- Member states may have additional legislation
  - Malta Data Protection Act Cap. 586
- Member states may have
  - additional legislation - Malta Data Protection Act Cap. 586
  - different supervisory authority setup - Malta IDPC
- It applies to ALL organisations processing EU citizen's personal data

# GDPR

- Address concerns related to data breaches, cyber-attacks, and misuse of personal data by organisations.

- Strengthen the rights of individuals with respect to their personal data and to harmonise data protection laws across the EU.

# GDPR

Severe fines

- up to €20 million or 4% of the organisation's annual global turnover

- moral damages

# Highest Fines

Meta

€1.2 billion

- Ireland's Data Protection Commission
- Transfer of data to the United States
- Meta used basis to transfer data which do not comply with EU Law - Privacy Shield

# Highest Fines

Meta

# Highest Fines

€746 million


- Luxembourg National Commission for Data Protection (CNDP)
- how Amazon processes personal data of its customers
- complaint filed by 10,000 people in 2018
- infringements regarding Amazon's advertising targeting system that was carried out without proper consent

# Highest Fines

Meta

€405 million

Ireland's Data Protection Commission

- processes personal data of teenagers between the ages of 13 and 17
- Instagram accounts automatically displayed the contact information (email addresses and/or phone numbers) of children publicly
- Meta failed to take measures to
  - provide child users with information using clear and plain language,
  - lacked appropriate technical and organizational measures, and
  - failed to conduct a Data Protection Impact Assessment.

€390 million

Forced Consent

€265 million

Data breach disclosing the personal data of 533 million users

# Highest Fines

€225 million

- Ireland's Data Protection Commission
- whether WhatsApp supplied enough information to users about how their data was processed and if its privacy policies were clear enough.
- What's more of interest
  - Original proposed fine was €30 to €50 million
  - Objections from 8 countries

# Highest Fines - Employment Related


€35.3 million

- Hamburg Data Protection Authority
- The company recorded and stored gigabytes of recorded one-on-one conversations with employees - back to work interviews
- Personal Data included vacation experiences, symptoms of illness, diagnosis, family issues and religious beliefs
- Details provided in those conversations were used in decisio regarding the employees

# Highest Fines - Employment Related

€10.4 million


- State Commissioner for Data Protection in Lower Saxony
- The company had been using video surveillance to monitor its employees for at least two years with no legal justification
- Some of the areas recorded by the illegal cameras included workspaces, sales floors, warehouses and staff rooms
- Many of the recordings were saved for 60 days

# Highest Fines - Employment Related


€5 million

- UK Information Commissioner Office (ICO)
- Cyber attack in 2020
- Personal data of up to 113,000 employees was encrypted and rendered ‘unavailable’

# Highest Fines - Employment Related


€5 million

- An Interserve employee who was working from home forwarded a phishing email to another employee, who opened it and downloaded the contents
- The ICO found that Interserve:
  - failed to follow-up on the original alert of a suspicious activity;
  - used outdated software systems and protocols; and
  - had a lack of adequate staff training and insufficient risk asses

# Highest Fines Malta

€250,000

- 2022
- Information and Data Protection Commissioner
- Controller infringed principles of security regarding personal data of data subjects and failed to implement appropriate technical and organisational measures
- Infringements of Articles 32(1) and 32(2) of the GDPR

# Highest Fines Malta


€65,000

- 2022
- Information and Data Protection Commissioner
- Controller infringed principles of security regarding personal and special categories of data of many data subjects
- Infringements of Articles 6(1), 9(1), 9(2), 14, 32(1), 5(1)(f), 33(1) and 34(1) GDPR

# Highest Fines Malta

€20,000

- 2020
- Information and Data Protection Commissioner
- Personal data undergoing processing was partially provided following a right of access request. Privacy Policy not satisfying the transparency requirements
- Infringement of Articles 13 and 15 GDPR

21 ACADEMY

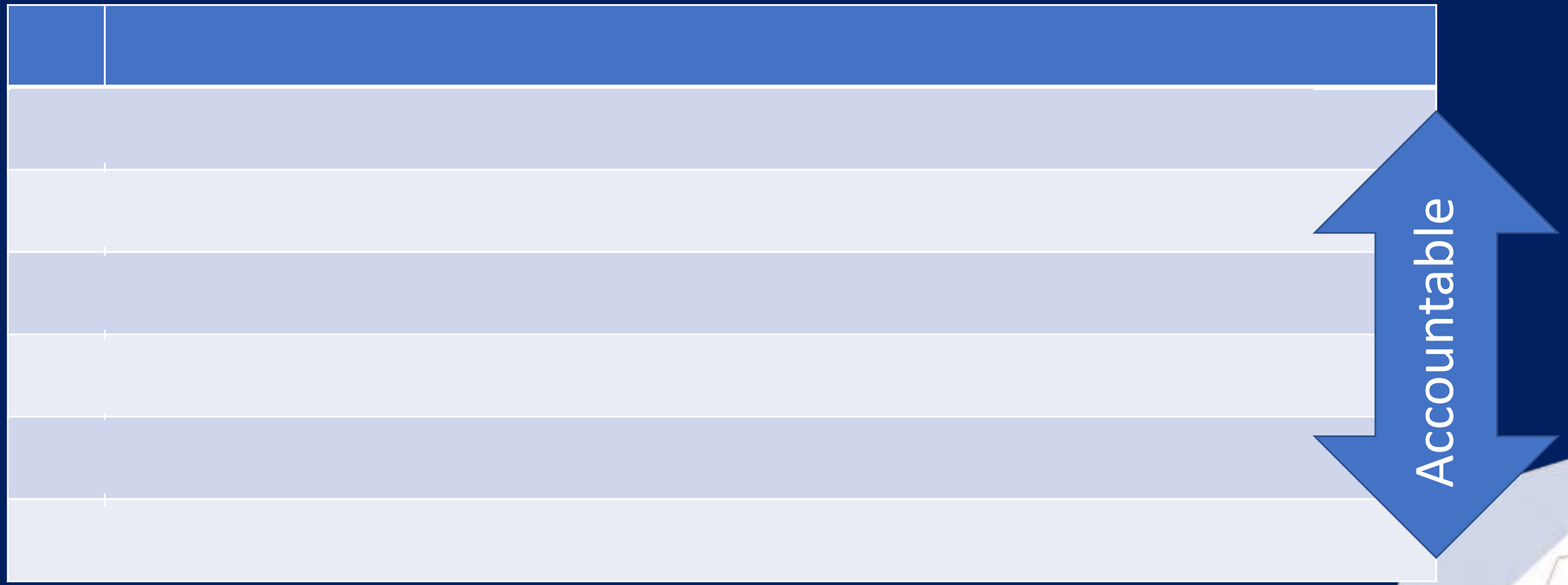
# Undergraduate Diploma in Business Administration

# Identify the 6 principles of GDPR

00:00

Explain each

# Principles



# Principles

# Principles

# Principles

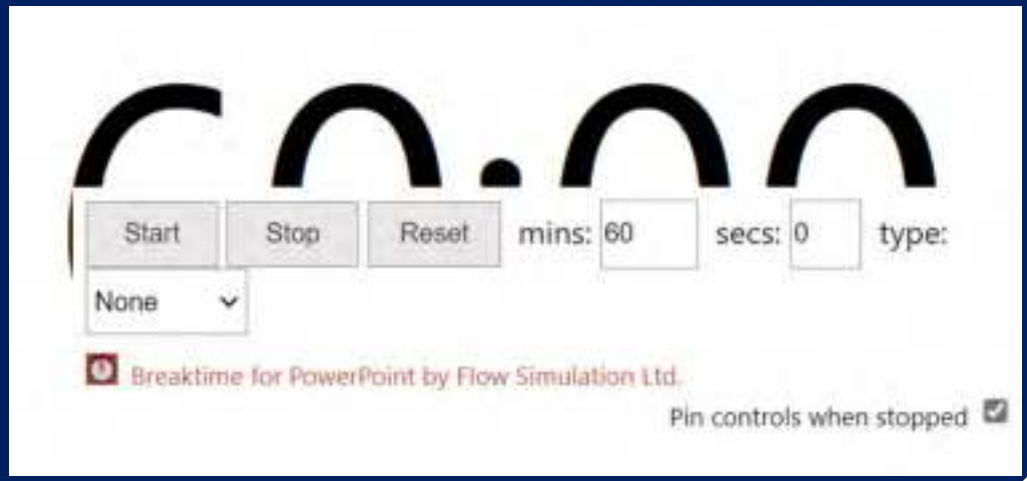
# Principles

# Principles

# Principles

21 ACADEMY

# Undergraduate Diploma in Business Administration




21 ACADEMY

# Undergraduate Diploma in Business Administration

# Definitions

# Data vs Personal Data

00:00

Explain each

# Data vs Personal Data

# Data vs Personal Data

facts and statistics collected together for reference or analysis

vs

any information relating to an identified or identifiable individual

# Definitions

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

# Is this personal data?

# Is this personal data?

# Is this personal data?

# Is this personal data?

# Is this personal data?

21 ACADEMY

# Undergraduate Diploma in Business Administration

# Special Category of Data

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation

# Special Category of Data

- Criminal Convictions & Offences

# Special Category of Data

| PERSONAL DATA | SPECIAL CATEGORIES | NOT PERSONAL DATA |
| --- | --- | --- |
| • name<br>• email address (name.surname@domain.com)<br>• phone number<br>• Internet Protocol (IP) address<br>• home address | • criminal records<br>• personal data related to racial or ethnic origin<br>• medical records<br>• religious or philosophical beliefs<br>• trade-union membership<br>• blood type<br>• political stands... | • a company registration number;<br>• an email address as info@company.com<br>• anonymiZed data<br>• information about legal entities<br>• data related to a deceased individual |

# Identify (a) personal data, (b) special category of data and (c) out of scope



- Mr Ramesh Kumar
- 21 Academy
- info@21academy.education
- High blood pressure
- Police conduct certificate
- +356 2099 5486

00:00

21 ACADEMY

# Undergraduate Diploma in Business Administration

# Definitions

**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

# Definitions

**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;

# Pseudonymisation vs Anonymisation

# Pseudonymisation vs Anonymisation

| Personal data | |
|---|---|
| Name: | Jane Doe |
| Birth: | 13.07.1975 |
| Email: | j865@mail.com |
| Medical data: | migraine |

| Pseudonymous data | |
|---|---|
| Name: | 764566 |
| Birth: | x1.j4.874f |
| Email: | [redacted] |
| Medical data: | migraine |

| Anonymous data | |
|---|---|
| Sex: | female |
| Age: | 37-50 |
| Medical data: | migraine |

21 ACADEMY

# Undergraduate Diploma in Business Administration

15:00

21 ACADEMY

Undergraduate Diploma in Business Administration

# Definitions

**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**; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

# Definitions

**Joint Controllers**: where two or more controllers jointly determine the purposes and means of processing

# Definitions

## Joint Controllers

Data Subjects


Controller


Meta

Controller

- Facebook's purpose is to improve its ad targeting.
- The Page admin's purpose is to learn about how people interact with its Facebook Page.

# Definitions

**Processor**: means a natural or legal person, public authority, agency or other body which **processes personal data on behalf of the controller**

# Controller & Processor


Data Subjects


Controller

Processors


# Controller & Processor & Sub Processor

Employees
(DATA SUBJECT)



Company
(CONTROLLER)



External Payroll Provider
(PROCESSOR)

OneDrive
(SUB-PROCESSOR)

# Controller vs Processor vs Joint Controller

# Examples

Your company contracts a private market-research company to carry out some research. Your brief specifies the budget and that you requires a satisfaction survey based on the views of a sample of your clients' population. You leave it to the research company to determine sample sizes, interview methods and presentation of results.

What is the relationship?

00:00

# Examples

The research company is processing personal data on your behalf, but it is also determining the information that is collected (what to ask the clients) and the manner in which the processing (the survey) will be carried out. It has the freedom to decide such matters as which clients to select for interview, what form the interview should take, what information to collect from clients and how to present the results. This means the market-research company is a joint controller with you regarding the processing of personal data to carry out the survey, even though you retain overall control of the data because you commission the research and determines the purpose the data will be used for.

Adapted from: https://ico.org.uk/

# Examples

A private company provides software to process the daily employee attendance records of your company. Using the software, the private company gives attendance reports to you on a weekly basis.

What is the relationship?

00:00

# Examples

The private company's sole purpose in processing the attendance data is to provide this service to your company. Your company sets the purpose - to assess attendance. The private company has no need to retain the data after it has produced the report. It does not determine the purposes of the processing; it merely provides the processing service. This private company is likely to be your processor and your company the controller.

https://ico.org.uk/

# Examples

Your company contracts a mail delivery service to deliver orders to clients such as books. The clients can use a website to check the status of their order and track its delivery.

What is the relationship?


# Examples

Your company will be the controller for any personal data inside the package. The delivery company will not be a controller or a processor for any personal data contained inside the package, as it has no control over or access to that data.

However, the delivery company will be processing some personal data (eg the client's name and address) in order to deliver the books and provide the tracking service.

**Whether it is a controller or a processor for the tracking element of the service will depend on who makes the decisions.**

If your company makes the final decision on the tracking service to be provided and the delivery company merely follows your instructions, then your company will be the controller and the delivery company is likely to be a processor.

But if the delivery company independently decides on the tracking service provided to the clients without the school's sign-off, it will be a controller.

Adapted from: https://ico.org.uk

21 ACADEMY

# Undergraduate Diploma in Business Administration

# Data Protection Officer


the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

# Data Protection Officer


the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale;

# Data Protection Officer


the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

# Data Protection Officer


## Tasks

to **inform** and **advise** the controller or the processor and the employees who carry out processing **of their obligations** pursuant to this Regulation and to other Union or Member State data protection provisions;

# Data Protection Officer

## Tasks


to **monitor compliance** with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor 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;

# Data Protection Officer


## Tasks

to provide **advice** where requested as regards the **data protection impact assessment** and monitor its performance pursuant to Article 35;

to **cooperate** with the **supervisory authority**;

# Managing Data and its Implications

## Lecture Title: General Data Protection Regulation


Lecturer: Angelito Sciberras

Date: 17 June 2023

Undergraduate Diploma in Business Administration