

Maltese Education Law and Data Privacy Implications in the Education Sector

Lecture Title: Data Privacy and Education Implications Part I

Lecturer: Angelito Sciberras

Date: 11 November 2025



Diploma in Law (Malta)



CAMILLERI PREZIOSI
ADVOCATES

Rising Incidents:

Over the past three years, educational institutions in the EU have reported a **150% increase in data breach incidents**, highlighting the growing vulnerability of this sector.



Self-Assessment



The Self Assessment

- During this first sitting you **MUST** choose what you believe is the correct answer for each of the 20 questions by ticking the box next to the correct answer.
- In the second sitting you **MUST** either confirm your answer by ticking again the same box or tick a new box next to what you now believe is the correct answer.



The Self Assessment

- Correct answer in Session 1 receives 1 point
- Correct answer in Session 2 confirming answer in Session 1 additional 1 point
- Correct answer in Session 2 correcting wrong answer in Session 1 receives 2 points
- Wrong answer in Session 2 with wrong answer in Session 1 receives 0 points
- Wrong answer in Session 2 with correct answer in Session 1 receives -1 points



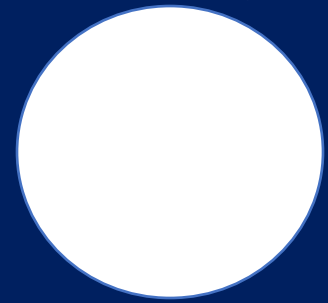
The Self Assessment

- There are 20 questions to be answered
- By now you should have received a link to a Google form where you are expected to input the answers which are correct
- Each slide - having the question and possible answers - will be displayed for 60 seconds
- Once you submit all the answers you will receive a copy of your answers by email.



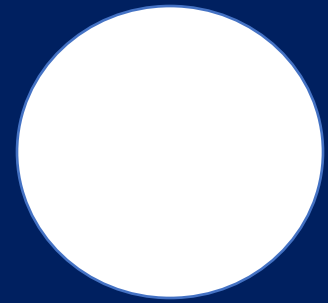
1. Personal Data is...

- a. Facts and statistics collected together for reference or analysis
- b. Any information relating to an identified or identifiable individual
- c. Anonymised Data
- d. None of the above



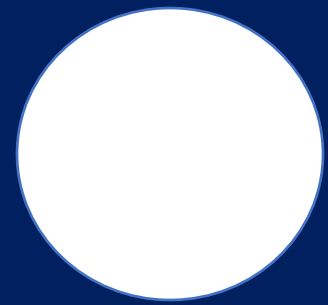
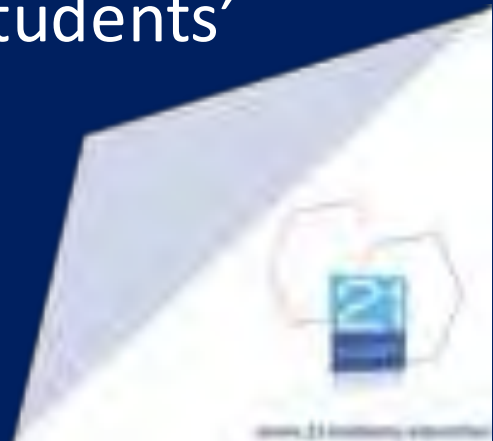
2. The General Data Protection Regulations came in force on?

- a. January 25th 2012
- b. April 14th 2016
- c. May 6th 1995
- d. May 25th 2018



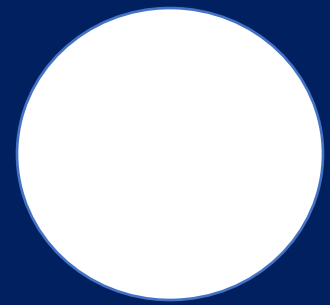
3. Which of the following does NOT constitute processing of personal data:

- a. Storing students data
- b. Modifying a teacher's status from single to married
- c. Sticking a circular to the school's notice board
- d. Informing the Education Department about each students' attendance



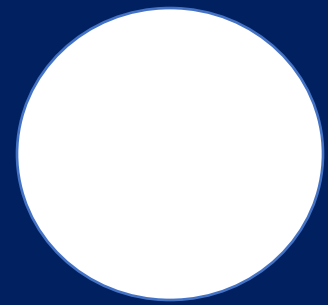
4. Which of the following is NOT personal data?

- a. Pseudonymised data
- b. CCTV footage of the school's entrance
- c. Anonymised data
- d. The school's yearbook



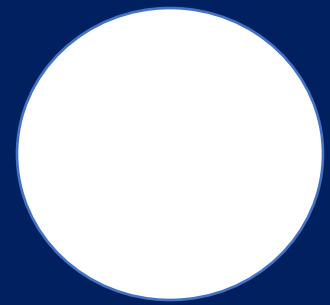
5. Which of the following is NOT special category of data?

- a. A student's sick certificate
- b. A teacher's union membership
- c. Attendance through facial recognition
- d. IP address



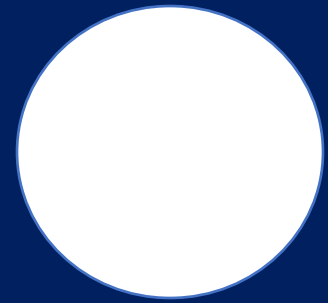
6. The Material Scope of the GDPR includes:

- a. Any information about a natural person which is not processed
- b. Personal data processed wholly or partly by automated means
- c. Personal data about purely personal activity
- d. Personal data used for crime prevention



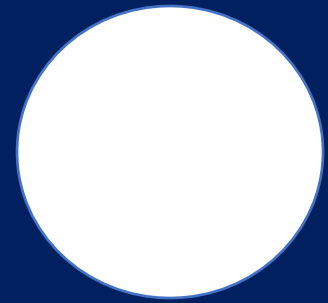
7. GDPR applies to Education Institutions

- a. Located in an EU member state only
- b. Providing services to EU citizens irrespective of where it takes place
- c. Located anywhere in the world
- d. Only if the supervisory authority dictates this



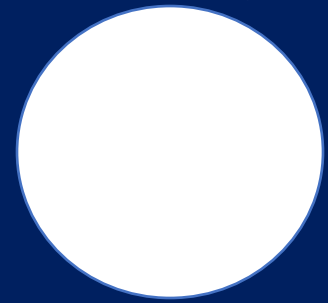
8. Data breaches must be notified to the Data Protection authorities:

- a. Within 24 hours
- b. Within 48 hours
- c. Within 72 hours
- d. Without undue delay

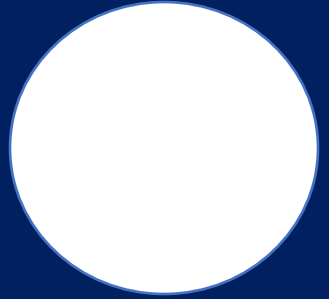


9. Employee's payroll data can be processed freely if the employee gives consent:

- a. True, but only if consent is written
- b. True only if consent is specific and employee informed how it will be used
- c. True if employee is given the right to withdraw at any time
- d. False



10. Upon termination an employee asks for the school to exercise their right to be forgotten

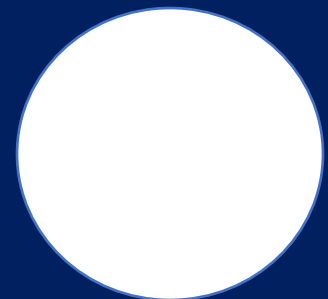


- a. All personal data has to be destroyed because employee has a right to be forgotten
- b. Approval to destroy data must be sought from Data Protection Officer
- c. Data not destroyed because of legitimate grounds and legal obligations
- d. Data has to be destroyed because it is not needed



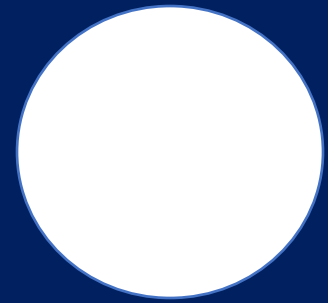
11. Which of the following is not a principle under data privacy legislation?

- a. Subsidiarity
- b. Storage limitation
- c. Accurate & up to date
- d. Lawful, fair and transparent



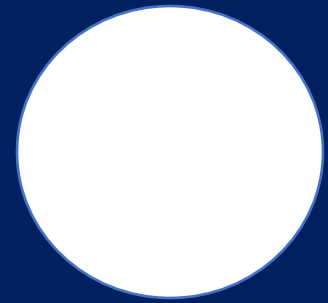
12. Which of the following does not regulate processing of personal data by Educational Institutions in Malta...

- a. Data Protection Act (Cap. 586)
- b. GDPR
- c. S.L. 9.07
- d. S.L. 586.07



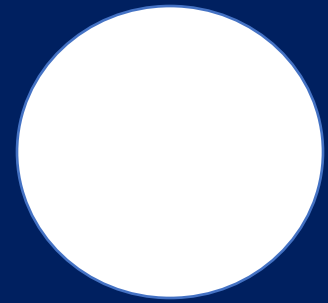
13. Educational Institutions cannot process...

- a. Attending students' special category of data
- b. Student's welfare data
- c. Medical data of past students
- d. Data for research and purposes

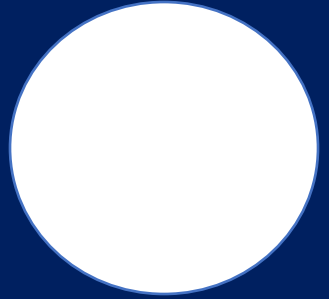


14. The age of consent in the Education sector is?

- a. 13+ years old
- b. 16+ years old
- c. 18+ years old
- d. Parents have to consent irrespective of the student's age



15. If processing is based solely on consent and student/parent/guardian withdraw it...

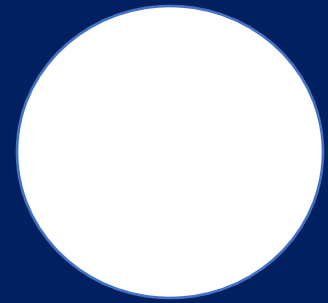


- a. The controller can still process the personal data without notification
- b. The controller can still process the personal data but needs to notify the data subject
- c. The controller has to stop processing and delete the data concerned
- d. The controller has to stop processing but may keep a copy of the data concerned



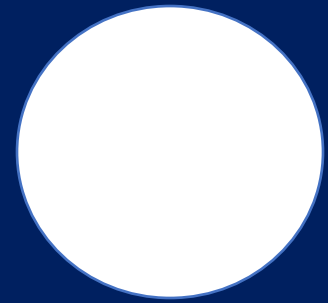
16. Pseudonymised data...

- a. Can be kept for ever
- b. Shall not be retained for a period which is longer than necessary
- c. Is another name of calling anonymised data
- d. Does not need adequate organisational and technical safeguards in place



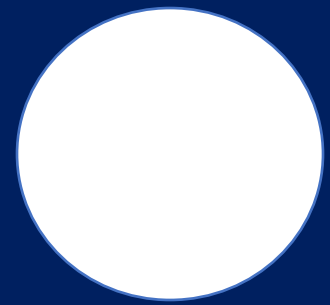
17. Which of the following is not a right of a data subject under data privacy legislation

- a. To Information
- b. To Data Portability
- c. To Object
- d. To Freedom



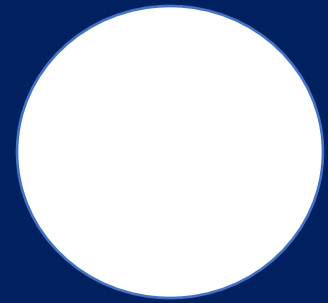
18. An access request has to be complied with within a period of...

- a. 7 days
- b. 15 days
- c. 1 month
- d. 3 months



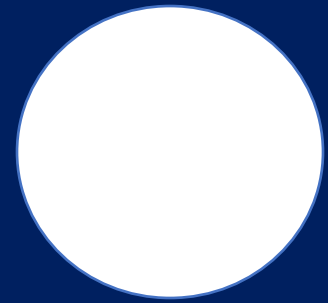
**19. CCTV footage must not be kept for longer than....
unless an authorisation for a longer period is sought
from the supervisory authority**

- a. 4 days
- b. 7 days
- c. 15 days
- d. 30 days



20. Which of the following is not a data breach

- a. Sending an emails to multiple recipients in BCC
- b. Sending personal data to the wrong recipient
- c. Misplacing the employees' attendance sheet
- d. Disposing of the school's beyond repair lap tops with the hard discs left intact



Rising Incidents:

Over the past three years, educational institutions in the EU have reported a **150% increase in data breach incidents**, highlighting the growing vulnerability of this sector.



Rising Incidents:

In the EU, the education sector typically ranks among **the top five most targeted sectors for data breaches**, often alongside healthcare, finance, retail, and government. While exact rankings can vary by year and specific reports, the education sector consistently faces significant threats due to its **large volumes of personal data and often limited cybersecurity resources**.



The power & value of DATA



Pregnancy and Power of Data



Why the hell are you sending these maternity coupons to my daughter?

*“The world’s most
valuable resource
is no longer oil,
but data”*

- The Economist, May 2017



Value of Data

What value does personal data have?

- Email addresses
- Mobile numbers

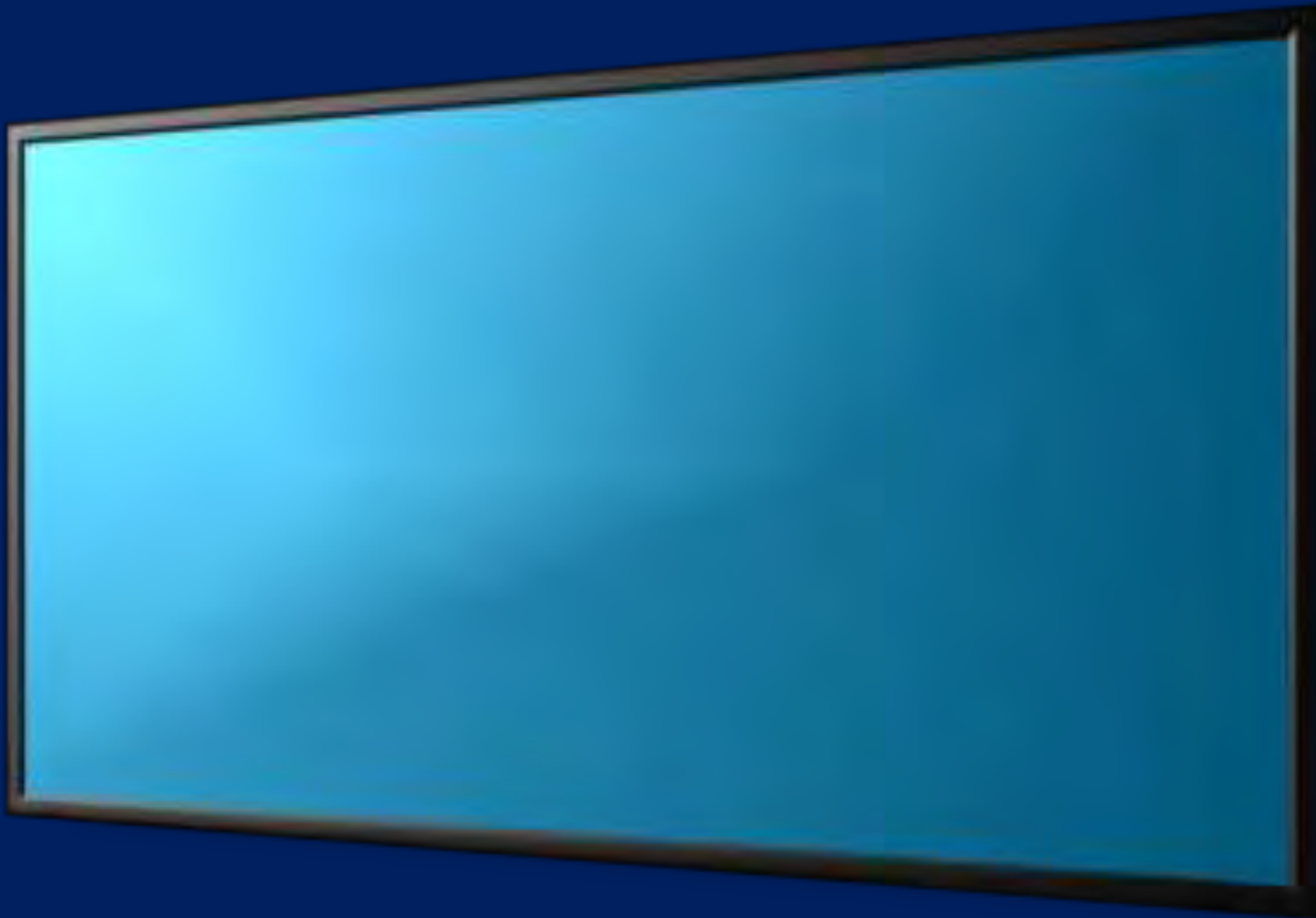
Do you keep copies of ID cards?

For what purpose?



<https://globallegitdocs.com/product/maltese-id-card>





Data vs Personal Data



60sec



Data vs Personal Data

facts and statistics collected together for reference or analysis

VS

any information relating to an identified or identifiable individual



Data

NETFLIX

amazon
prime video

HBOmax



Data

NETFLIX

- Committed to 26 episodes
- @ \$3.8million per episode
- Without watching a single episode

HOW?

NB: Netflix premiered the first episode of *House of Cards* on **1st February 2013**.
The final season, which was the sixth, was released on **2nd November 2018**.



Data

NETFLIX

You have been employed by Netflix...

...your friends ask you, what is Netflix? What does it do?

How would you answer?



Data

NETFLIX RESEARCH

Home

Netflix Research

Dr.

About

Netflix has been a **data-driven** company since its inception. Our analytic work arms decisions, makes ensure the company with useful metrics, insights, predictions, and analytic tools so that everyone can be a part of the data in their function. Partnering closely with business teams in product, content, studio, marketing, and business operations, we perform context-rich analysis to provide insight into every aspect of our business, our partners, and of course our members' experience with Netflix.



Personal Data



Personal Data

1

In 2014 a Facebook quiz invited users to find out their personality type

2

The app collected the data of those taking the quiz, but also recorded the public data of their friends

3

About 305,000 people installed the app, but it gathered information on up to 87 million people, according to Facebook

4

It is claimed at least some of the data was sold to Cambridge Analytica (CA) which used it to psychologically profile voters in the US



Personal Data



Why GDPR?



Legislation

Directive 95/46/EC



GDPR

What changed on an Organisational Level?



Directive 95/46/EC



Macintosh Performa 6200



IBM Personal Communicator



Kodak DCS 460 Camera



Iomega Zip Drive



Motorola Tango Pager



IBM ThinkPad 701C



DVDs



Sony Handycam DCR-VX1000



Legislation

Directive 95/46/EC



GDPR

What changed on a School Level?



Office Tools Evolution



Personal Data

Directive 95/46/EC



GDPR

What changed on an Personal Level?



Personal Data





Why are Educational Institutions more at risk?



- Student and Teacher Data Hold Value
- Institutions Often Have Limited Security Protections
- Academic Institutions May Use New, Untried Technology
- Attackers Value Email Addresses Ending in .edu
- Academic Staff Often More Exposed to Phishing
- Some Institutions Have Paid Ransoms





Diploma in Law (Malta)



CAMILLERI PREZIOSI
ADVOCATES

GENERAL DATA PROTECTION REGULATION



“What must be recognised is that GDPR is an evolution in data protection, not a total revolution... GDPR is building on foundations already in place for the last 20 years.”

– Steve Wood - Deputy Commissioner for Policy, ICO

25 August 2017



Problem Solved?



Problem Solved?



Problem solved?

1.2 billion euro fine for Facebook as a result of EDPB binding decision

22 May 2023 **GDPR**

Brussels, 22 May - Following the EDPB's [binding dispute resolution](#) decision of 13 April 2023, Meta Platforms Ireland Limited (Meta IE) was issued a 1.2 billion euro fine following an inquiry into its Facebook service, by the Irish Data Protection Authority (IE DPA). This fine, which is the largest GDPR fine ever, was imposed for Meta's transfers of personal data to the U.S. on the basis of standard contractual clauses (SCCs) since 16 July 2020. Furthermore, Meta has been ordered to bring its data transfers into compliance with the GDPR.



Andreea Jelinek, EDPB Chair, said: "The EDPB found that Meta IE's infringement is very serious since it concerns transfers that are systematic, repetitive and continuous. Facebook has millions of users in Europe, so the volume of personal data transferred is massive. The unprecedented fine is a strong signal to organisations that serious infringements have far-reaching consequences."

In its binding decision of 13 April 2023, the EDPB instructed the IE DPA to amend its draft decision and to impose a fine on Meta IE. Given the seriousness of the infringement, the EDPB found that the starting point for calculation of the fine should be between 20% and 100% of the applicable legal maximum. The EDPB also instructed the IE DPA to order Meta IE to bring processing operations into compliance with Chapter V GDPR, by ceasing the unlawful processing, including storage, in the U.S. of personal data of European users transferred in violation of the GDPR, within 6 months after notification of the IE SA's final decision.

The IE DPAs final decision incorporates the legal assessment expressed by the EDPB in its binding decision, adopted on the basis of Art. 65(1)(a) GDPR after the IE DPA, as lead supervisory authority (LSA), had triggered a dispute resolution procedure concerning the



Problem Solved?



Fines - Malta

What was the highest fine under GDPR
in Malta so far?

60sec



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





Diploma in Law (Malta)



CAMILLERI PREZIOSI
ADVOCATES



Diploma in Law (Malta)



CAMILLERI PREZIOSI
ADVOCATES

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.

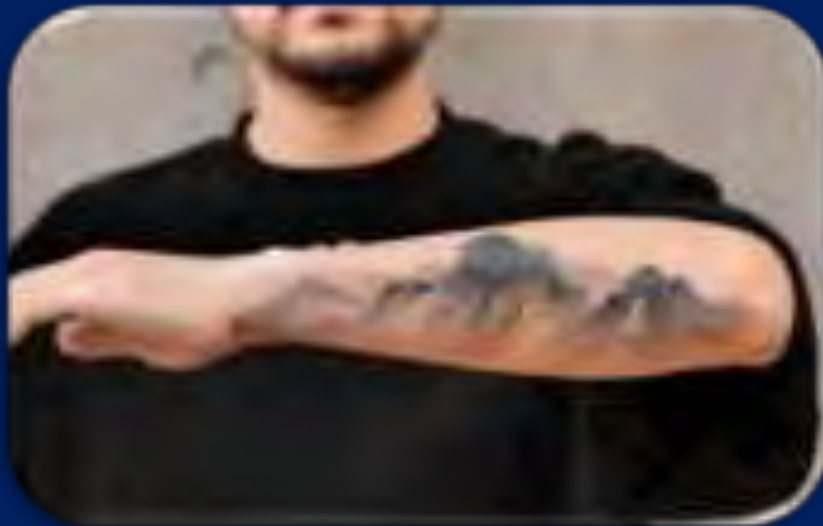


Personal Data

- 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?



Special Categories 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 Categories of Data

Art. 9 (2)

- **Explicit consent**
- Necessary for the purposes of **carrying out the obligations and exercising specific rights** of the controller or of the data subject in the field of **employment** and **social security** and **social protection** law
- To protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- **Legitimate activities** by an association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members
- Manifestly **made public** by the data subject

Continued...



Special Categories of Data

Art. 9 (2)

- Necessary for the establishment, exercise or defence of **legal claims** or whenever courts are acting in their judicial capacity
- Necessary for reasons of substantial **public interest**
- Purposes of **preventive or occupational medicine**, for the **assessment of the working capacity of the employee**, **medical diagnosis**, the **provision of health or social care** or **treatment** or the management of health or social care systems and services
- **Public interest in the area of public health**
- Archiving purposes in the public interest, **scientific or historical research purposes** or statistical purposes



Special Categories of Data

Art. 10

[B] Criminal Convictions & Offences

- only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects



Personal Data and Data

PERSONAL DATA	SPECIAL CATEGORIES	NOT PERSONAL DATA
<ul style="list-style-type: none">• name• email address (name.surname@domain.com)• phone number• Internet Protocol (IP) address• home address	<ul style="list-style-type: none">• criminal records• personal data related to racial or ethnic origin• medical records• religious or philosophical beliefs• trade-union membership• blood type• political stands...	<ul style="list-style-type: none">• a company registration number• an email address as info@company.com• anonymized data• information about legal entities• data related to a deceased individual

Exercise

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

- J. Borg
- Hal Muxi School
- Class Senior II
- High blood pressure

60sec

The information/data above is fictitious and is being used for training purposes only



Controller

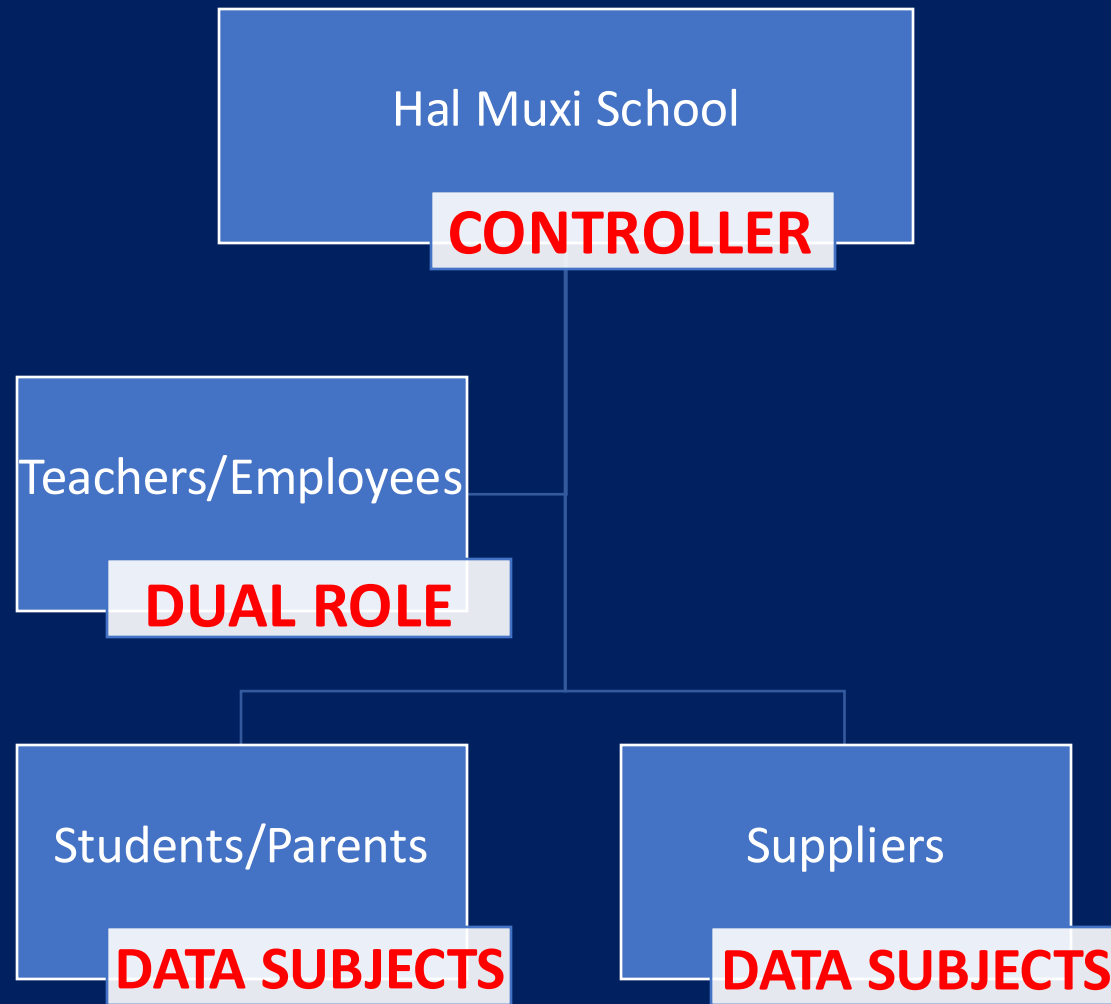
Art. 4(7)

‘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;



Controller

Art. 4(7)



Joint Controllers

Art. 27

Where two or more controllers jointly determine the purposes and means of processing

Reflect the respective roles and relationships vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

The data subject may exercise his or her rights in respect of and against each of the controllers.



Joint Controllers



Data Subjects



Controller



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.

Processor

Art. 4(8)

‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (sub-contractor)



Controller & Processor



Data Subjects



Controller



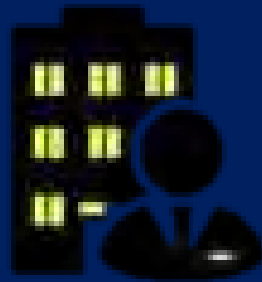
Processors



Controller & Processor & Sub Processor



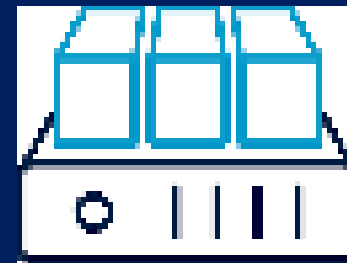
Employees
(DATA SUBJECT)



School
(CONTROLLER)



External Payroll Provider
(PROCESSOR)



OneDrive
(SUB-PROCESSOR)





Diploma in Law (Malta)



CAMILLERI PREZIOSI
ADVOCATES

Examples

A state school contracts a private market-research company to carry out some research. The school's brief specifies its budget and that it requires a satisfaction survey based on the views of a sample of its students' population. The school leaves it to the research company to determine sample sizes, interview methods and presentation of results.

What is the relationship?

60sec



Examples

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



Examples

A private company provides software to process the daily pupil attendance records of a state-maintained school. Using the software, the company gives attendance reports to the school.

What is the relationship?

60sec



Examples

The company's sole purpose in processing the attendance data is to provide this service to the school. The school sets the purpose - to assess attendance. The 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 company is likely to be a processor.**



Examples

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

What is the relationship?

60sec



Examples

The school 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 student'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 the school makes the final decision on the tracking service to be provided and the delivery company merely follows the school's instructions, then the school 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 students without the school's sign-off, it will be a controller.





Diploma in Law (Malta)



CAMILLERI PREZIOSI
ADVOCATES

Maltese Education Law and Data Privacy Implications in the Education Sector

**Lecture Title: Data Privacy and Education
Implications Part I**

Lecturer: Angelito Sciberras

Date: 11 November 2024



Diploma in Law (Malta)



CAMILLERI PREZIOSI
ADVOCATES