

Maltese Education Law and Data Privacy Implications in the Education Sector

Lecture Title: Data Privacy and Education
Implications Part I

Lecturer: Angelito Sciberras

Date: 28 November 2022



Diploma in Law (Malta)



CAMILLERI PREZIOSI
ADVOCATES

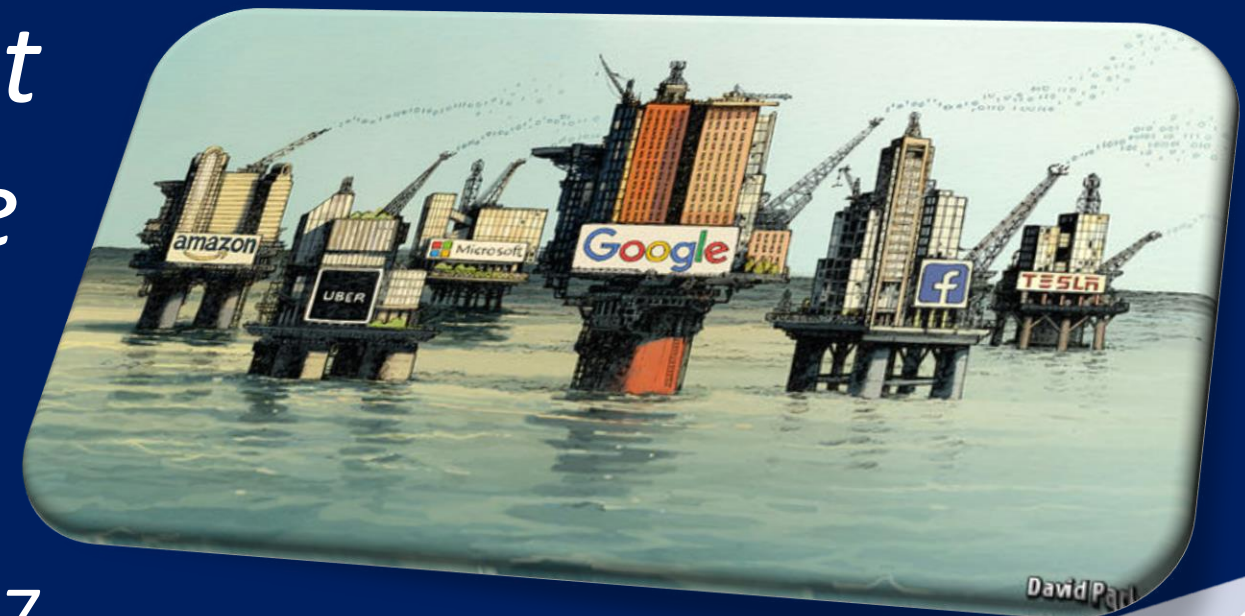
MAMO TCV
ADVOCATES

The power & value of DATA




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

- The Economist, May 2017



Pregnancy and Power of Data



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

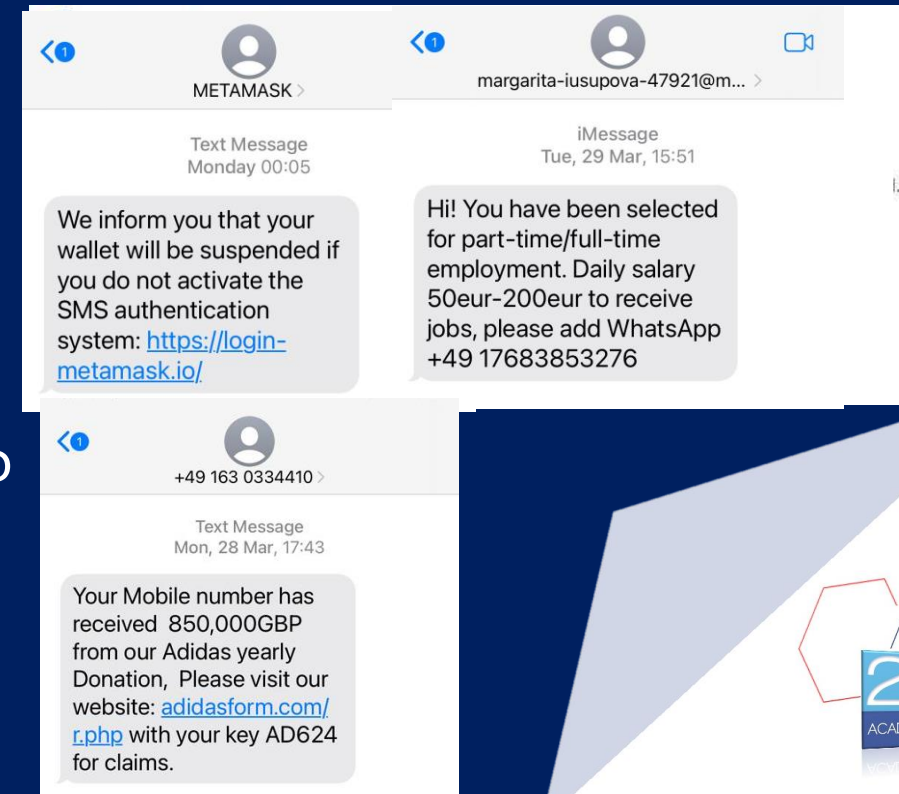
Value of Data

What value does personal data have?

- Email addresses
- Mobile numbers

Do you keep copies of ID cards?

For what purpose?





All ▾ Search Your Document

HOME SHOP DOCUMENTS ▾ CONTACT BLOG OUR WORK FAQ REVIEWS

HOME / SHOP / FAKE ID CARDS



Buy Fake ID Card of Malta

\$350.00

Buy Malta counterfeit ID Card Online, European We are a real office to get a phony Malta ID card.

- 1 +

ADD TO CART

Category: Fake ID Cards

Tags: Fake, ID Card, Malta



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

The logo for Amazon Prime Video, featuring the word "amazon" in a small, dark font above "prime video" in a larger, blue font. Below the text is the iconic Amazon smile arrow.

HBOmax



Data

NETFLIX

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

HOW?



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

RESEARCH AREAS ▾

BUS

About

Netflix has been a **data-driven** company since its inception. Our analytic work arms decision-makers around the company with useful metrics, insights, predictions, and analytic tools so that everyone can be stellar 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



Personal Data

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

Personal Data

Directive 95/46/EC



GDPR

What changed on an Personal Level?

Personal Data





ment Opportunities
operations
bus service throughout the Borough
& City

Weekends
Trains will not run to
Brooklyn all weekend
Please take
to Atlantic Av-
Barclays Ctr for

NETFLIX

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



Why GDPR?



Why GDPR?



Central Bank served with a reprimand by Information and Data Protection Commissioner

Friday, 21 February 2020, 11:42

Last update: about 12 days ago



H&M fined €35 million for illegally storing employees' personal data

IT firm C-Planet fined €65,000 over massive voter data breach

Private information on some 337,000 Maltese voters was leaked online

National Elections Data Privacy

January 17, 2022 | Ivan Martin | 64

3 min read



Ombudsman website is probed over security risk

Attackers could view complaints submitted by citizens

National Daphne Caruana Galizia

February 21, 2020 | Jacob Borg | 44



Why GDPR?

Polish school hit with GDPR fine for using fingerprints to verify students' lunch payments

Swedish SA fines Board of Education in the City of Stockholm

24 November 2020 Sweden

The Swedish Data Protection Authority has reviewed the so-called School Platform, the IT system used for, among other things, student administration of schools in the City of Stockholm. The review shows an insufficient level of security of such grave nature that the authority issues an administrative fine of four million SEK against the Board of Education in the City of Stockholm.

The Swedish Data Protection Authority has received a number of personal data breach notifications from the City of Stockholm's Board of Education. The incidents all relate to the School Platform, which is the IT system used for, among other things, student administration of schools. The school platform contains information of up to 500 000 pupils, guardians and teachers. The system contains sensitive data, including special categories of personal data, as well as information about pupils and teachers with classified information or protected identity.

The Swedish Data Protection Authority has found serious shortcomings. In one of the subsystems, information on other children has been allowed large parts of the staff to access information about students' personal data. The Informa' their proc with da'



Schools issued formal reprimand by ICO

Facial recognition: School ID checks lead to GDPR fine

27 August 2019

The Information Commissioner's Office (ICO) has announced that it has issued reprimands to two separate schools over photographs. The decision puts into context the importance of ensuring that schools comply with the use of images and children's personal data.

Polish DPA fines the National School of Judiciary and Public Prosecution (KSSIP) for breaching the GDPR

11 February 2021 Poland

The President of the Polish DPA found the breach of GDPR and imposed an administrative fine in the amount of PLN 100 000 (nearly EUR 22 000) on KSSIP for failing to fulfil its obligations as a controller.

According to the Personal Data Protection Office, the controller did not take the necessary technical and organisational measures, which would allow to ensure the confidentiality of the processing services, KSSIP failed to test and did not carry out the impact assessment of effectiveness of the technical and organisational measures in order to ensure the security of personal data contained in the copy of the database of the training platform of personal data. The controller improperly took into account the risks associated with changes in the processing of personal data.

In addition, it should be pointed out that the controller entrusted the processing of personal data to a processor without contractual commitment to process personal data only on documented instructions from the controller.



... school in Humberside. The parents of the pupil concerned had stated on the complaint was raised to the school in response to which it took steps to address the issue raised was that the proof sent home was in the context of the use of the image that the parents had failed to implement an appropriate procedure for the school to consider reporting the matter to the ICO as a data breach under Article 5(1)(f) GDPR.



Why GDPR?

1. Amazon – €746 million (\$823.9 million)



Year Issued: 2021

The online retailer's Luxembourg EU headquarters was found to be [tracking user data](#) without acquiring appropriate consent from users or providing the means to opt out from this tracking – resulting in Amazon being hit with the **largest GDPR fine to date**.

3. Google Ireland – €90 million (\$99 million)



Year Issued: 2021

France's CNIL fined Google Ireland for failing to give users an [easy way to refuse cookies](#) under both the GDPR and the ePrivacy Directive.

2. WhatsApp – €225 million (\$247 million)



Year Issued: 2021

Ireland's Data Protection Commission fined WhatsApp for [unclear privacy policies](#) and a lack of transparency in how it was using user data.




Why GDPR?

FBI POLITICO PRO

Instagram fined €405M for violating kids' privacy

The fine is the third for a Meta-owned company handed down by the Irish regulator.



Christophe Simon/AFP via Getty Images

BY VINCENT MANANCOURT
SEPTEMBER 5, 2022 | 4:20 PM

The Irish Data Protection Commission has fined Meta-owned social media platform Instagram €405 million for violations of the General Data Protection Regulation.

The fine, which is the second-highest fine under the GDPR after a €746 million penalty against Amazon, is the third for a Meta-owned company handed down by the Irish regulator.





Diploma in Law (Malta)



CAMILLERI PREZIOSI

ADVOCATES

MAMO TCV

ADVOCATES

Definitions



Processing

Art. 4(2)

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

Art. 4(1)

- **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?



Hal Muxi School Newsletter
Student's personal data hit by cyber attack



Special Categories of Data

Art. 9 (1)

- 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) sensitive data and (c) out of scope

- A. Sciberras
- 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

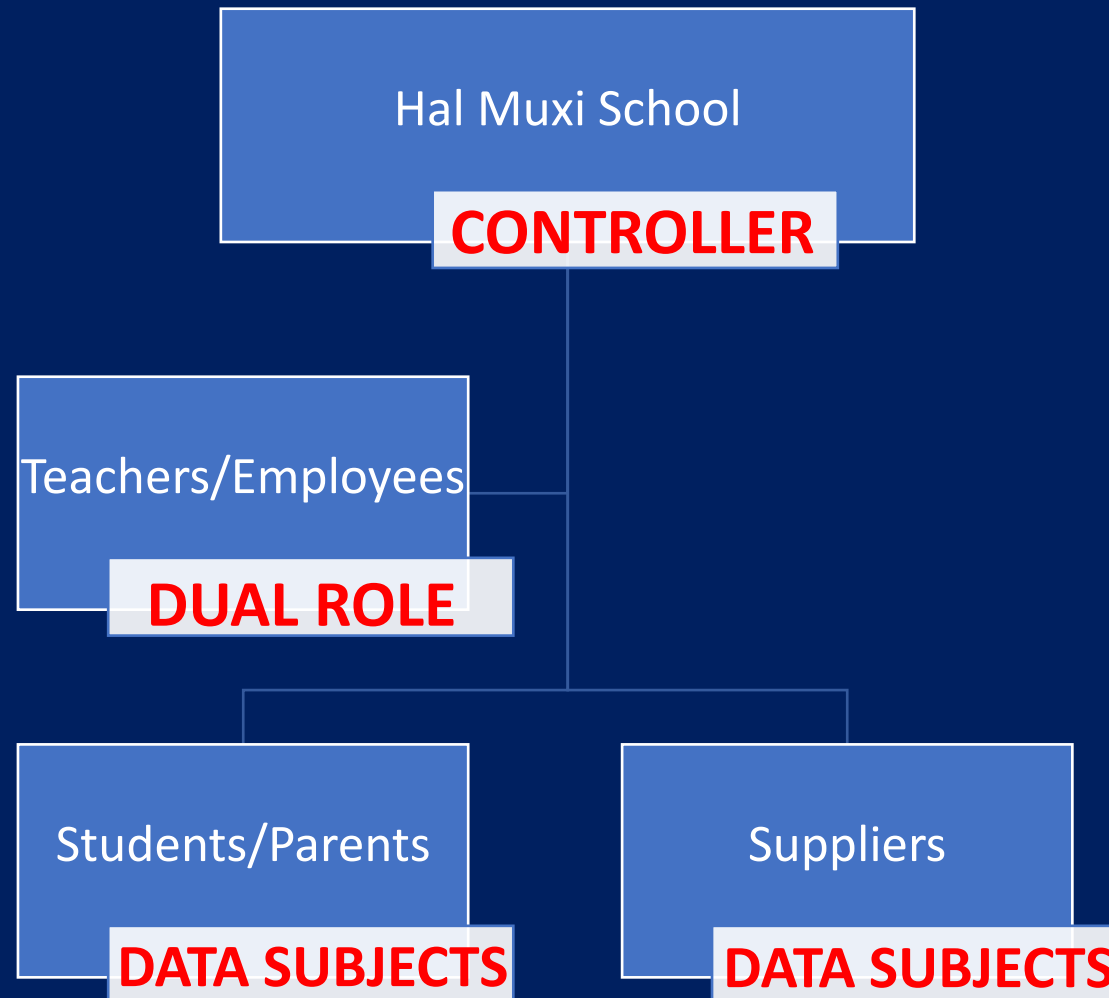
Art. 4(7)

‘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)

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.

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



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.

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





Diploma in Law (Malta)



CAMILLERI PREZIOSI
ADVOCATES

MAMO TCV
ADVOCATES