

Maltese Education Law and Data Privacy Implications in the Education Sector

Lecture Title: Data Privacy and Education
Implications Part II

Lecturer: Angelito Sciberras

Date: 29 November 2023



Diploma in Law (Malta)



CAMILLERI PREZIOSI
ADVOCATES

Controller

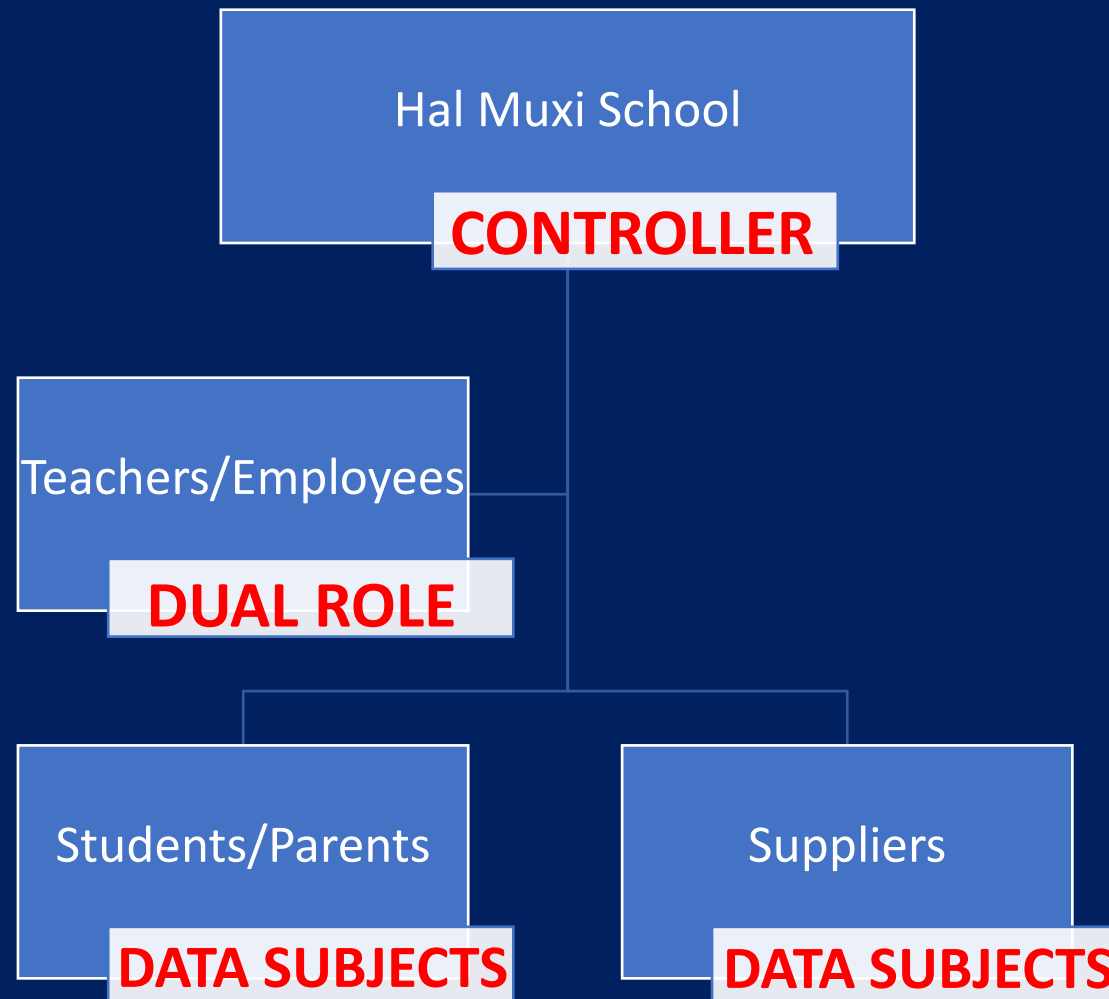
Art. 4(7)

‘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.

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.

Principles, Lawful Processing & Rights



Principles

Art. 5

1	lawful, fair and transparent
2	specific, explicit and legitimate purpose
3	adequate, relevant and limited to what is necessary
4	accurate & up to date
5	storage limitation
6	integrity and confidentiality



Principles, **Lawful Processing** & Rights



Lawfulness of processing

Art. 6

Processing is lawful if based on one of the following legal basis



Exercise

Go to:

<https://www.enforcementtracker.com>

In Controller/Processor filter type School

View the list



Why GDPR?

Most fines issued on the basis of:

“Insufficient legal basis for data processing”

OR

“Insufficient technical and organisational measures to ensure information security”



Why GDPR?

Swedish SA fines Board of Education in the City of Stockholm

24 November 2020

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 in Stockholm. 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 School Platform allowed large parts of the staff to access information about students, for example, on other children concerning, for example, their health.



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




Schools issued formal reprimand by ICO

13 August 2018

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 fully around the use of images and children's personal data.

A class photograph was taken at a school in Humberstone. The parents of the pupil concerned had stated on the complaint that the photograph was taken for use 'outside of school'. A class photograph was taken for use 'outside of school'. The parents of the pupil concerned had stated on the complaint that the photograph was taken for use 'outside of school'. The parents of the pupil concerned had stated on the complaint that the photograph was taken for use 'outside of school'.

The school failed to implement an appropriate procedure for the use of images and children's personal data. The school failed to implement an appropriate procedure for the use of images and children's personal data. The school failed to implement an appropriate procedure for 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

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 the KSSIP, and thus 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.



Lawfulness of processing

SL 586.07

4.(1) **Education authorities** may process personal data in relation to students and, where specifically required in the best interest of the students, personal data of parents and legal guardians may also be processed to carry out their functions as provided under the Education Act.

2.(1) "**education authorities**" means the Directorates constituted in terms of Part II of the Education Act, as well as the Malta Further and Higher Education Authority established in terms the Further and Higher Education Act;

4.(2)(a) In the course of executing their functions subject to sub-regulation (1), **education authorities** may, from time to time, and by means of a written request, require **educational institutions** to furnish, in such manner as may be requested and within a reasonable time, personal data in relation to students attending such educational institutions, and their parents or legal guardians.(b) **Special categories** of data listed in Article 9 of the Regulation shall be requested only with the **explicit consent** of the parent or legal guardian.

2.(1) "**educational institutions**" means any licensed school or other institution or entity offering educational services



Lawfulness of processing

SL 586.07

5.(1) **Educational institutions** may process personal data in relation to students, parents and legal guardians for administration purposes and for the daily operations and efficient running of such institutions for the purpose of providing their students with the necessary educational services as required under the Education Act.

5.(2) Personal data in relation to students may also be processed for the following purposes:

(a) academic progress monitoring which includes performance data, examination and, or assessment results associated with the students;

(b) organisation of functions and, or activities which may form part of curricular and extra-curricular requirements, provided that where the processing is related to informal activities the consent is obtained from the students themselves if applicable, or from their parents or legal guardians



Lawfulness of processing

SL 586.07

Other personal data which may be processed:

Medical

separate distinctive files
forwarded to another educational institution to which students are transferred
destroyed once the students stop attending the institution concerned

Welfare

separate distinctive files
forwarded to another educational institution to which students are transferred
destroyed once the students stop attending the institution concerned

Visual Images

consent must be obtained



Lawfulness of processing

SL 586.07

Other personal data which may be processed:

Historic Purposes

no special categories of data and student welfare data are retained for such purposes

Research and Statistics

to perform tasks which are required by the education authorities in terms of regulation
legitimate interest of the educational institution to provide the necessary education to
their students



Lawfulness of processing

SL 586.07

Transferring of Students' Personal Data

Consent is required unless

- education authorities
- another educational institution where the student is transferred
- examination bodies
- health authorities
- hospitals, clinics and other medical professionals where students need medical attention
- Police in cases of criminal investigations
- Social workers or support agencies or authorities where there is suspicion or where it is alleged that the welfare of the student is not being protected
- Jobsplus in accordance with the Employment and Training Services Act
- any court, as required in judicial proceedings



Lawfulness of processing

SL 586.07

- Age of Consent above 16 years old (Art. 7(1))
- In writing or by a clear indication of opting in where consent is required to be given through on-line applications (Art. 7(2))
- May be withdrawn in writing, and the data controller shall remove such consent and stop such processing operation for which the consent has been withdrawn and delete or destroy the data concerned. (Art. 7(2))



Lawfulness of processing

SL 586.07

Processing for research and statistics purposes

- all identifiable data shall be rendered **anonymous**, unless in the case of research, the identification of the data subject is required to fulfil the purposes of such research (Art. 8(1))
- where... the research being conducted would require the identification details of students, data controllers shall process such data by replacing personal identification data with **pseudonymous** data (Art. 8(2))



Anonymous vs Pseudonymisation



60sec

Anonymous vs Pseudonymisation

Anonymous information is a data set which does not relate to an identified or identifiable natural person (Recital 26 of the GDPR)

VS

‘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 (Article 4(5))



Anonymous vs Pseudonymisation



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: ██████████
Medical data: migraine



Anonymous data

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

Lawfulness of processing

SL 586.07

When pseudonymous data are processed:

- personal data are not processed for any other purpose that is incompatible with the specific purpose;
- kept separately from the other data;
- adequate organisational and technical safeguards are in place
- personal data shall not be retained for a period which is longer than necessary

Article 8(4)





Diploma in Law (Malta)



CAMILLERI PREZIOSI
ADVOCATES



Diploma in Law (Malta)



CAMILLERI PREZIOSI
ADVOCATES

Principles, Lawful Processing & **Rights**



1 Right to information

2 Right of access

3 Right to rectify

7 Right to object

5 Right to restrict

4 Right to be forgotten

6 Automated processing

8 Data portability

Subject Access Request

Art. 15

What is a SAR?

- A right granted and regulated by the GDPR
- A data subject has the right to obtain all personal data pertaining to them which is held and/or processed by an organisation
- The requested organisation must comply with such a request within a period of 1 month (which may be extended up to a maximum of a further 2 months if the situation so warrants)



Subject Access Request

- Form
- Procedure
- Policy



Subject Access Request

- Procedure



Subject Access Request

Response

- confirm that you're processing their personal data
- provide them with a copy of it
- give details of how the data is collected, used and disposed of



Subject Access Request

You must let them know:

- what category of data you hold
- what it is being used for
- where you got it from
- who it has been disclosed to
- how long you will keep it for
- how it is being kept safe
- details of any automated decision making



Subject Access Request

You must also tell them they have the right to:

- complain to the regulator
- object to you processing their personal data
- ask you to erase, restrict, change or remove their personal data





Diploma in Law (Malta)



CAMILLERI PREZIOSI
ADVOCATES

Internal Processes



Documentation

- Privacy Standard
- Privacy Notices - Employees, Candidates, Students & Web
- Data Processing Agreements
- Joint Controllers Agreements
- SAR Policy, Forms and Procedures
- Data Breach Policy and Procedure



Documentation

- Retention Policy/Guidelines
- Consent Forms
- DPIA Policy & Template
- IT use policy (Emails & Disposal)
- CCTV Policy



Privacy Standard

- A privacy standard is an 'inward-looking' document, recently replacing what was previously known as a "privacy policy".
- Today, this has become an essential document which regulates an organisation's handling of personal data (whether obtaining, controlling, processing, transport, or storage) and also informs employees of their duties under data protection legislation.



Privacy Standard

- written in simple language and presented in an accessible form
- comprehensive
- easily accessible



Privacy Standard

- Principles
 - Lawfulness, Fairness, Transparency
 - Purpose Limitation
 - Data Minimisation
 - Accuracy
 - Storage Limitation
 - Security Integrity & Confidentiality
 - Reporting a Data Breach
 - Transfer Limitation
 - Data Subject's Rights and Requests
- Accountability
 - Technical and Organisational measures
 - Record Keeping
 - Training and Audit
 - Privacy by Design
 - Data Protection Impact Assessment
 - Automated Processing
- Direct Marketing
- Sharing Personal Data
- Changes to the Privacy Standard



Privacy Standard

Having these duties set out in writing does not exempt the employer from being bound to **educate & train employees on good data practices** in order to comply with the law.



Notice to Data Subjects

Can you name a list of an educational institutions' data subjects?

1 minute



Notice to Data Subjects

- Potential Students
- Students
- Parents/Guardians
- Candidates
- Employees/Contractors
- Website Visitors
- Service Providers
- Suppliers



Notice to Data Subjects

- Who is processing the data
- What legal basis allow you to collect user data
- What are the purposes of collecting the personal data
- What types of personal data you collect
- How long will the data be stored for
- The contact details of the data protection officer, where applicable;
- The right to lodge a complaint with a supervisory authority;
- Whether you transfer the data internationally
- Whether you use the data in automated decision-making
- With what third parties you share the data
- What are the data subject rights
- How you'll inform users that your notice has changed



Monitoring

*"Employers have legitimate interests in monitoring in order to improve efficiency and protect company assets. However, workplace monitoring becomes intrusive and unjustifiable if it is not limited or **transparent**."*

- Working Party 29



Monitoring

- Data subjects must be informed:
 - of the existence of monitoring;
 - about the purposes for which their data is processed; and
 - of any other information necessary to guarantee fair processing.



Monitoring



Caution
CCTV in operation

is affixed in an office. It is
ng employees & visitors that
ing is being carried out

1 minute

Is this enough? Why?



Monitoring



A yellow rectangular sign template for CCTV monitoring. At the top center is a black triangle containing a white silhouette of a CCTV camera. Below the triangle, the word "Caution" is written in a large, bold, black font, followed by "CCTV in operation" in a slightly smaller, bold, black font. Underneath, there are three sections, each with a label and a white rectangular input box:

- The first section is labeled "This scheme is operated by:" and has a single input box.
- The second section is labeled "For the purpose of:" and has a larger input box.
- The third section is labeled "For more information and access requests contact" and has two stacked input boxes.

www.21academy.com



1 minute



**CCTV
IN
OPERATION**

IMAGES ARE BEING MONITORED AND
MAY BE RECORDED FOR THE
PURPOSE OF CRIME PREVENTION
AND PUBLIC SAFETY

This scheme is operated by:
YOUR COMPANY NAME HERE

For further information contact
The Data Controller
TEL: YOUR NUMBER HERE

What is missing in this notice from an HR perspective?



Data Breach

A breach is not hacking only

- Sending personal data to to the wrong recipient
- Sending emails to multiple recipients who are not in BCC
- Losing employee data
- Others

3.1 Nature of the incident - Tick as appropriate

- | |
|---|
| a) Paper lost or stolen or left in insecure location. |
| b) Device lost or stolen or left in insecure location. |
| c) Mail lost or opened. |
| d) Hacking. |
| e) Malware (e.g. ransomwares). |
| f) Phishing. |
| g) Incorrect disposal of personal data. |
| h) E-waste (personal data still present on obsolete device). |
| i) Unintended publication. |
| j) Data of wrong data subject shown. |
| k) Personal data sent to wrong recipient. |
| l) Verbal unauthorized disclosure of personal data. |
| m) Other. |
| n) Summary of the incident that caused the personal data breach including the storage media involved. |

Data Protection Impact Assessment



is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan.



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 II

Lecturer: Angelito Sciberras

Date: 29 November 2023



Diploma in Law (Malta)



CAMILLERI PREZIOSI
ADVOCATES