21 Academy
Course
Online Sessions
Data Protection Officer
Data Protection Officer/Lead
www.21academy.education
2099 5486
21
ACADEMY

Data Protection Officer/ Lead Course

Session No. 1 – 27.10.2026

1. **Background on GDPR**
2. **The role of the DPO – what it involves**
3. **What constitutes personal data**
4. **The 6 data protection principles – applying them and showing compliance**

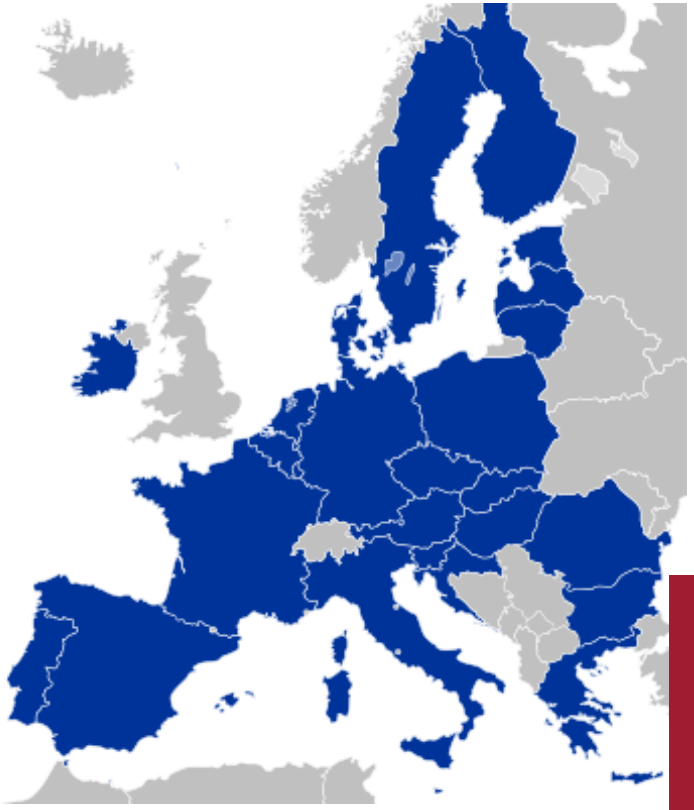
FENECH + FENECH
ADVOCATES

Av.Helene Kristensen
Helene.kristensen@fenechlaw.com

FENECH + FENECH
ADVOCATES

www.21Academy.education

Background on the GDPR



Background on the GDPR

A NEW EU REGULATION

BUT THIS

DID

NOT

REINVENT THE WHEEL

Background on the GDPR

WHY?

We have had a Data Protection Act since 2001

Chapter 440 Laws of Malta

FENECH + FENECH
ADVOCATES

www.21Academy.education

Background on the GDPR

Directive 95/46/EC

DIRECTIVE 95/46/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 24 octobre 1995

relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Background on the GDPR

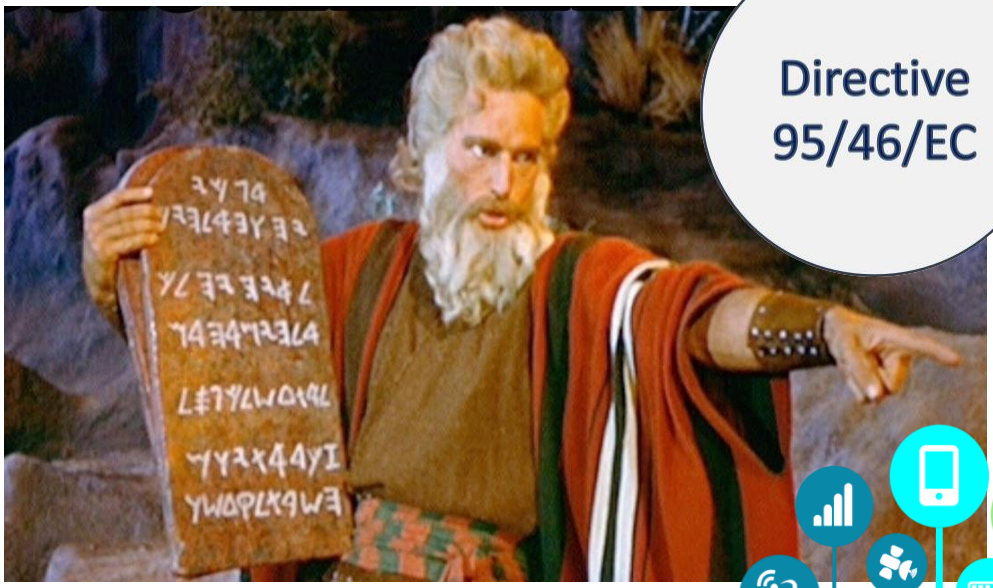
Directive 95/46/EC

1995

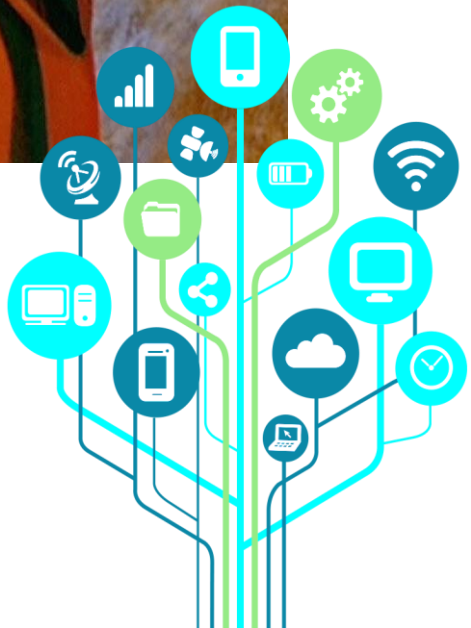
Background on the GDPR

1995

Background on the GDPR

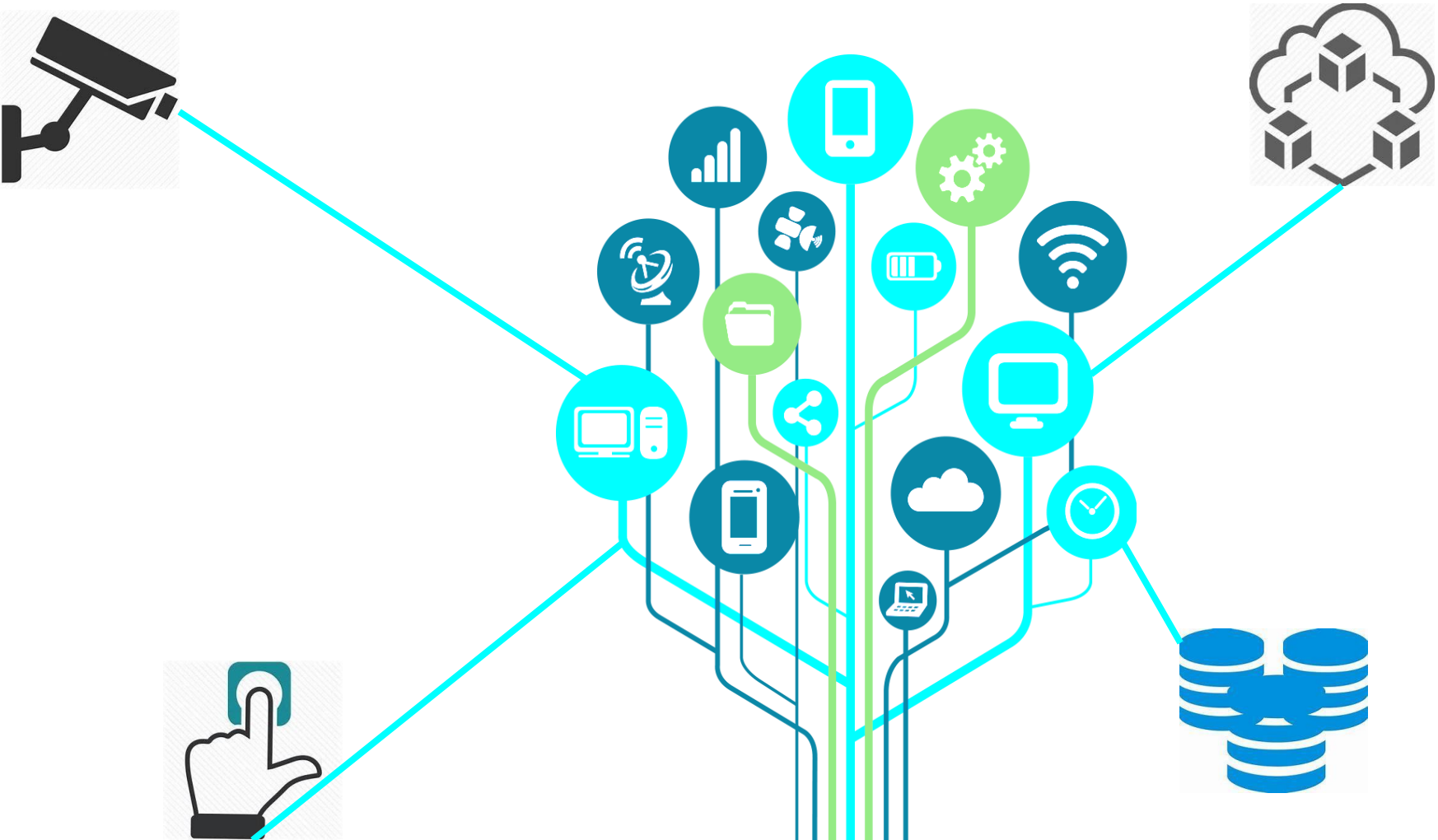


Directive
95/46/EC



technology
neutral

Background on the GDPR



Background on the GDPR

GDPR # Recital 6:

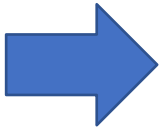
"*Rapid technological developments and globalisation have brought new challenges for the protection of personal data.* ***The scale of the collection and sharing of personal data has increased significantly.*** *Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities…*

Background on the GDPR

Date	
1995	Directive 95/46/EC
2012	European Commission publishes proposals to reform EU Data protection rules – including a draft Data Protection Directive
2015	EU General Data Protection Regulations (GDPR) agreed upon
25 May 2018	GDPR replaced the current Directive and became directly applicable in all Member States without the need for implementing national legislation.

Background on the GDPR

Directive 95/46/EC



GDPR

Background on the GDPR

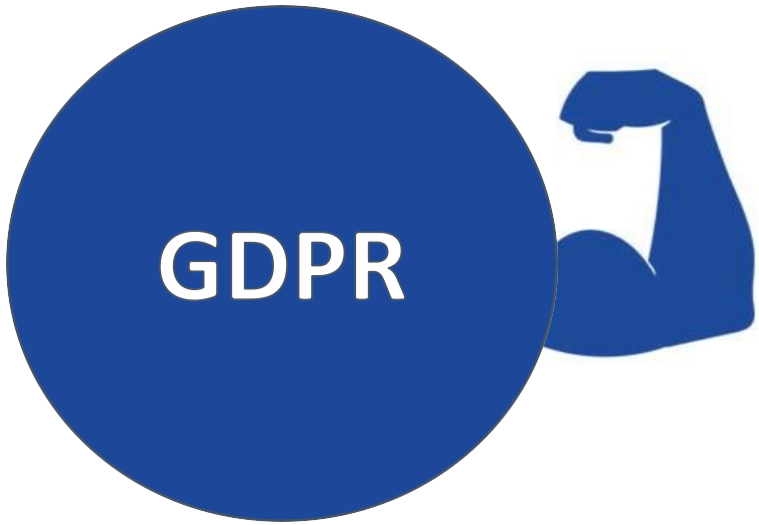
GDPR RECITAL 9

"The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union"

FENECH + FENECH
ADVOCATES

www.21Academy.education

Background on the GDPR



1. WIDER REACH
2. MORE RIGHTS
3. MORE OBLIGATIONS
4. HIGHER POTENTIAL FINES

Background on the GDPR

- WIDER REACH

Directive Vs Regulation

- 1 Law for all M-States ***[?]***

Background on the GDPR

WIDER REACH

Directive Vs Regulation

- 1 Law for all M-States ***[?]***
- One-Stop-Shop
  - An entity with several subsidiaries in other M-States may choose to deal with the DPA in the MS of its "**main establishment**" (***where decisions are being taken***).

Background on the GDPR

WIDER REACH

BUT

1. GDPR allows for some additional rules to be determined by local authorities;

2. Co-decision making process can be triggered in cross-border complaints.

LEAD vs **CONCERNED AUTHORITIES**

vs

EDPB European Data Protection Board

Background on the GDPR

WIDER REACH

EXTENDED SCOPE

Applicability (1)

Processing in the Context of Activities of an **EU-based Establishment** of controllers/processors

even if processing takes place outside the EU

Background on the GDPR

WIDER REACH

EXTENDED SCOPE

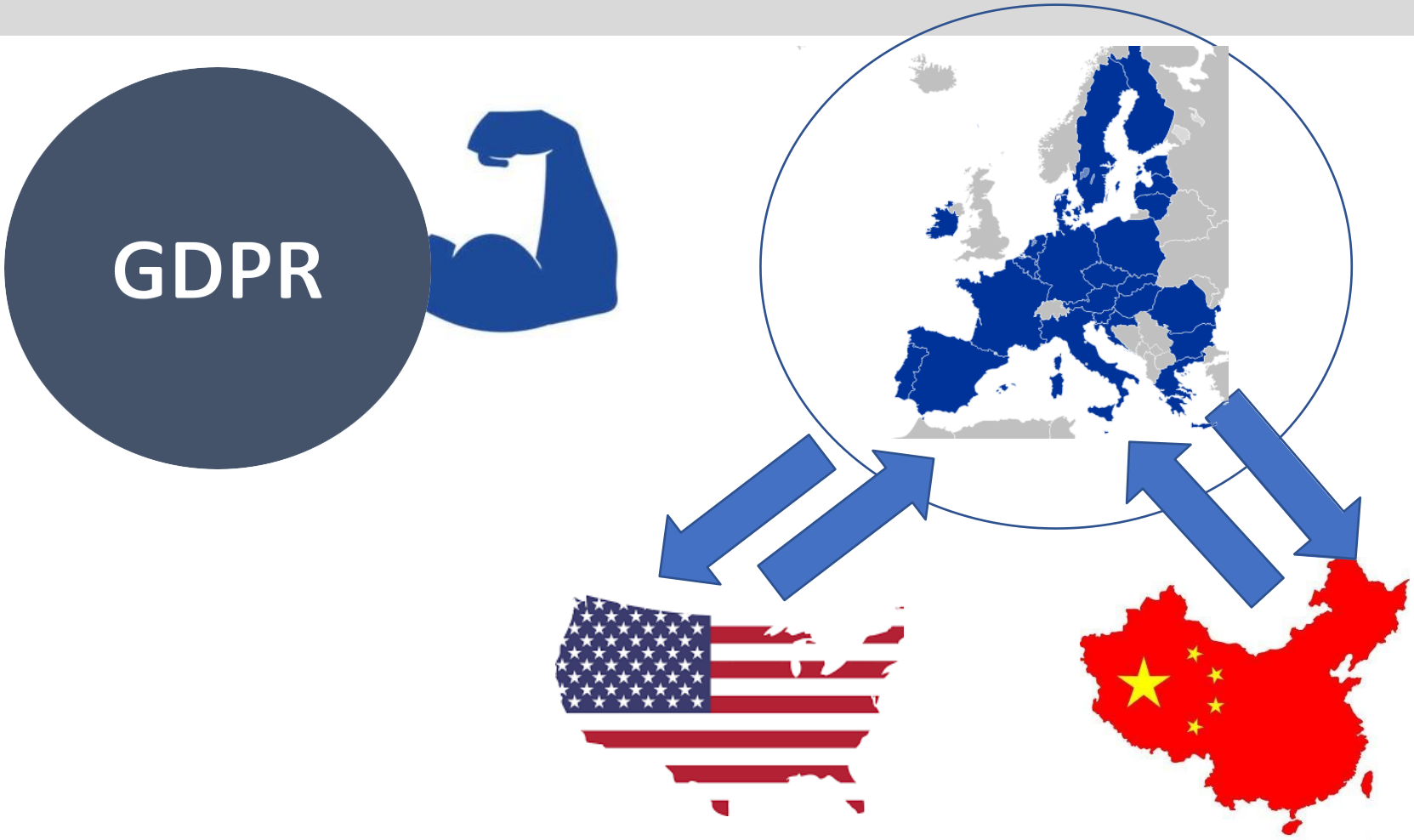
Applicability (2)

Processing of EU-Based Data Subjects
by controllers/processors
not established in the EU

(i) **offering services in the EU**
(even free of charge); **&**

(ii) **monitoring DS behaviour in the EU**
(e.g. profiling)

Background on the GDPR



Background on the GDPR

€20 million
Or
4% of global group turnover

Whichever is the higher

Background on the GDPR

REPUTATION

Background on the GDPR

CRIMINAL OFFENCE
Imprisonment/fines

Background on the GDPR

GDPR

Recital 13 – GDPR

The aim is:

*"To provide natural persons in all Member States with the **same level of legally enforceable rights and obligations** and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, **and equivalent sanctions in all Member States***

EQUIVALENCE

Background on the GDPR

1. HIGHER POTENTIAL FINES

Art. 29 W.P.: Authorities are encouraged to use a considered and balanced approach …

***BUT** "the point is not [to] qualify the fines as a last resort, nor to shy away from issuing fines"*

Background on the GDPR

The Right to Privacy

Background on the GDPR

The Right to Privacy

Article 8 of the **European** Convention on Human **Rights**.
(an international agreement between the 47 States of the Council of Europe)

the **right** to respect for one's "***private and family life, his home and his correspondence",*** *subject to certain restrictions that are "in accordance with law" and "necessary in a democratic society*".

Background on the GDPR

The Right to Privacy

European Convention Act (CAP 319)

Transposes the ECHR into Maltese Law

Background on the GDPR

The Right to Privacy

Article 32 of the **Constitution of Malta**

Every person in Malta is entitled to the fundamental rights and freedoms of the individual, that is to say, the right, whatever his race, place of origin, political opinions, colour, creed, sex, sexual orientation or gender identity, but subject to respect for the rights and freedoms of others and for the public interest, to each and all of the following, namely […] ***respect for his private and family life.***

Background on the GDPR

The Right to Privacy

EU Charter of Fundamental Human Rights

(applies to EU Institutions & its M-States when implementing EU law)

Article 7: <u>Respect for private and family life</u>

Everyone has the right to respect for his or her private and family life, home and communications.

Background on the GDPR

The Right to Privacy

EU Charter of Fundamental Human Rights

(applies to EU Institutions & its M-States when implementing EU law)

Article 8 : <u>Protection of Personal Data</u>

1.Everyone has the right to the protection of personal data concerning him or her.

2.Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

Background on the GDPR

The Right to Privacy & the GDPR

The 1st Paragraph of the GDPR:

"The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that ***everyone has the right to the protection of personal data concerning him or her****."*

Background on the GDPR

So if there already is a right to privacy, why have GDPR ?

Background on the GDPR

So if there already is a right to privacy, why have GDPR ?

- *GDPR is a tool used to implement and enforce the right to privacy.*
- *One is not a subset of the other – but they complement each other.*

Background on the GDPR

So if there already is a right to privacy, why have GDPR ?

- *GDPR RECITAL 11 : Effective protection of personal data throughout the Union requires the **strengthening and setting out in detail** of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.*

Background on the GDPR

So if there already is a right to privacy, why have GDPR ?

- *GDPR is having an impact on "the right to privacy"*

  Ref. **Bărbulescu v. Romania (Sept. 2017)**

Background on the GDPR

Ref. **Bărbulescu v. Romania (Sept. 2017)**

- **Employer had policies in place which precluded employees from using company equipment for personal use. Employees were informed of same via notices. The notice also informed employees that their work would be monitored and that misconduct would be monitored and punished.**

- **Mr Bărbulescu had been asked by his employer to set up a Yahoo Messenger account for work purposes. He also had a personal Yahoo Messenger account.**

- **Employee was informed that the company had monitored his Yahoo Messenger communications over the course of a week and that it considered he had been using it for personal purposes, contrary to its IT policy.**

Background on the GDPR

Ref. **Bărbulescu v. Romania (Sept. 2017)**

- **Mr Bărbulescu replied saying that he had only used Yahoo Messenger for work purposes.**

- **The same day, the employer presented Mr Bărbulescu with a 45 page transcript of his Yahoo Messenger communications, including the text of communications he had exchanged with his brother and his fiancée relating to personal matters, some of which were of an intimate nature. The majority of the messages had been sent on his work Yahoo Messenger account but a few had been sent on his personal account.**

- **Mr Bărbulescu was dismissed on 1 August.**

Background on the GDPR

Ref. **Bărbulescu v. Romania (Sept. 2017)**

- **He brought a claim in the Romanian courts challenging his dismissal. He was unsuccessful in his claim as the Romanian courts found that the employer was entitled to check his work and that he had been told about the company's position on personal use of IT equipment and monitoring of use of the equipment.**

Background on the GDPR

Ref. **Bărbulescu v. Romania (Sept. 2017)**

- **Having lost his claim in the Romanian courts, Mr Bărbulescu claimed in the ECtHR that his dismissal had been because of a breach of his Article 8 rights (i.e. right to respect for private life and correspondence) and, as such, the domestic courts had failed to protect his rights.**

- **The Grand Chamber overturned the decision of the lower Chamber of the ECtHR, finding that respect for private life and for the privacy of correspondence continues to exist at work, even if these may be restricted in so far as necessary.**

Background on the GDPR

Ref. **Bărbulescu v. Romania (Sept. 2017)**

- **Grand Chamber ECHR – "***While it was clear that the applicant had been informed of the ban on the use of company internet for personal purposes, it was less clear whether the applicant had been* ***informed prior to the monitoring*** *that such monitoring could take place. It considered that the applicant did not appear to have been informed "of the* ***extent and nature*** *of his employer's monitoring activities, or of the possibility that the employer might have access to the actual contents of his communications". While acknowledging that it was unclear to what extent the applicant could have a reasonable expectation of privacy under the employer's restrictive regulations, the Court concluded that Article 8 was applicable as* ***"employer's instructions cannot reduce private social life in the workplace to zero".***

Background on the GDPR

Ref. **Bărbulescu v. Romania (Sept. 2017)**

- *Domestic authorities did not afford adequate protection of the applicant's right to respect for his private life and correspondence and they consequently failed to strike a fair balance between the interests at stake*

The Court used this judgment to provide specific guidelines for employers, which conform with the relevant United Nations, Council of Europe standards and EU legislation, such as the General Data Protection Regulation, on how to monitor employees' communications at work.

Background on the GDPR

Ref. **Bărbulescu v. Romania (Sept. 2017)**

Some action points and practical tips include:

- Carrying out an assessment of the degree of intrusion into the employees' privacy. Monitoring the flow of communications rather than the actual content of communications and limiting the number of people who have access to the data that is collected will make the monitoring less intrusive.
- Considering why the monitoring is being carried out, what the employer is hoping to achieve and whether the objectives can be met through less intrusive means.
- Notifying employees of the possibility that monitoring may be carried out. Revisit existing policies, update where necessary and make sure employees are made aware of them. Notification should be given in advance of any monitoring taking place.

Background on the GDPR

The Right to Privacy is not absolute

Background on the GDPR

The Right to Privacy is not absolute

ECHR: the right to respect for one's *private and family life, his home and his correspondence, is subject to certain restrictions that are "**in accordance with law**" and "**necessary in a democratic society**".*

Background on the GDPR

Ex. Uzun Vs Germany (E.C.H.R.)

- *Uzun was suspected of involvement in a terrorist attack*

- *He complained that surveillance via GPS and use of such data in criminal proceedings was in breach of his privacy*

- *Court held :-*

    1. *GPS surveillance and use of the data admittedly interfered with the applicant's right to respect for his private life;*
    2. *However there was a legitimate aim of protecting national security, public safety and the rights of the victims, and of preventing crime;*
    3. *Such surveillance came about after other methods were tested, and in any case was for only 3 months*

*Therefore there was **no violation of right to privacy**.*

Background on the GDPR

Ex. L.H. Vs Latvia (E.C.H.R.)

- *LH complained that a Government authority collected excessive health data relating to her over a period of 7 years;*

- *Latvian Law gave wide discretion to the authority to collect the data without limitation.*

ECHR held

1. Since the law did not contain restrictions to protect the privacy of the person, then ***there was a violation of the right to privacy****.*

Background on the GDPR

The Right to Privacy is not absolute

GDPR Recital 4 : *"The processing of personal data should be designed to serve mankind.* ***The right to the protection of personal data is not an absolute right****; it must be considered in relation to its function in society and be* ***balanced*** *against other fundamental rights, in accordance with the principle of proportionality"*

Background on the GDPR

Balance is KEY

Any Questions?

2. The Data Protection Officer (DPO)

2. The Data Protection Officer (DPO)

Where?

- GDPR Article 37-39
- Article 29 Working Party Guidance

2. The Data Protection Officer (DPO)

New Feature

- No DPO's under Directive 95/46
- DPR's were appointed as good practice
- DPO is not mandatory for everyone

2. The Data Protection Officer (DPO)

Who needs to have one?

2. The Data Protection Officer (DPO)

Article 37(1) GDPR

The controller and the processor shall designate a data protection officer in any case where:

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

(b) 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; or

(c) 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.

2. The Data Protection Officer (DPO)

(a) the processing is carried out by a <u>public authority or body,</u> except for courts acting in their judicial capacity;

What is a " public authority" under Maltese law?

2. The Data Protection Officer (DPO)

What is a " public authority" under Maltese law?

- No definition in the GDPR
- No definition in the New Data Protection Act
- Definition exists in some other laws…

2. The Data Protection Officer (DPO)

E.g. Freedom of Information Act – Chapter 496

"public authority" means:

(*a*) the Government, including any ministry or department thereof;

(*b*) a Government agency established in terms of the Public Administration Act or any other law; and

(*c*) any body established under any law, or any partnership or other body in which the Government of Malta, a Government agency or any such body as aforesaid has a controlling interest or over which it has effective control;

2. The Data Protection Officer (DPO)

“Public Authority or Body”

- All ministries and departments
- All Agencies – EUPA, ERA, REWS
- Possibly companies in which government stake e.g. Enemalta.

2. The Data Protection Officer (DPO)

(b) 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; or

What are “core activities” and “regular and systematic”?

2. The Data Protection Officer (DPO)

Core Activities - Article 29 WP Guidance/243

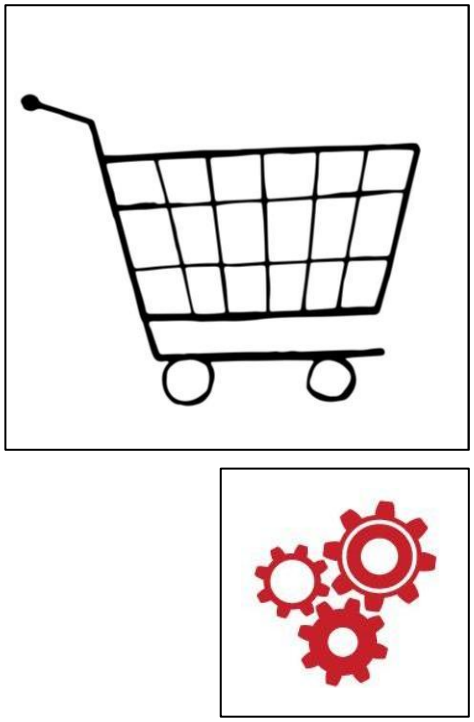
To determine whether 'core activities' involve processing of personal data you need to ask the question:

"Do I need to process personal data to achieve my key objectives?"

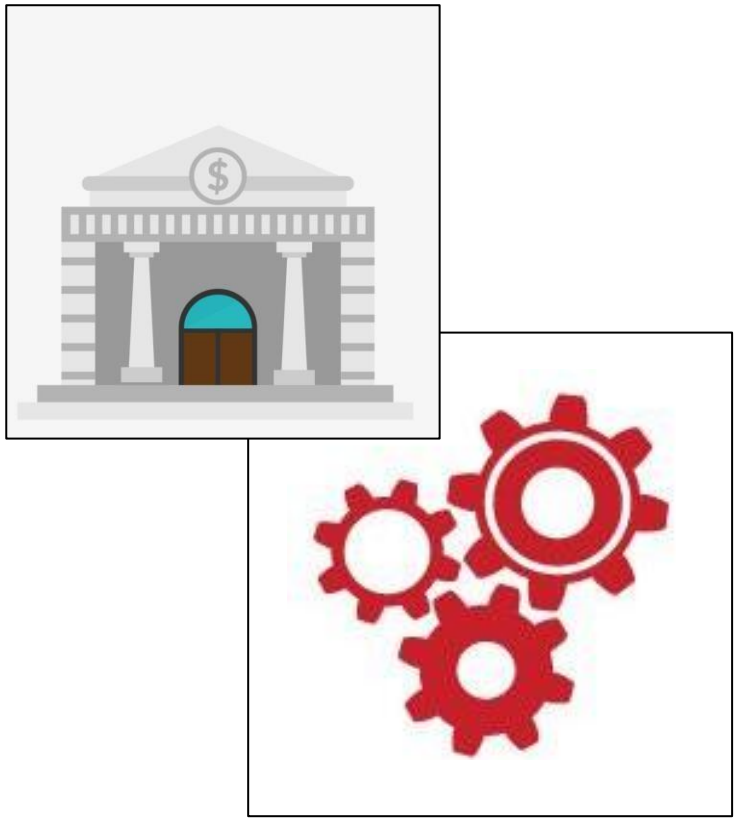
"Is my main line of business based on data processing?"

2. The Data Protection Officer (DPO)

Supermarket



Bank



2. The Data Protection Officer (DPO)

'**Regular and systematic**' monitoring of data subjects includes all forms of tracking and profiling, both online and offline. An example of this is for the purposes of behavioural advertising.

2. The Data Protection Officer (DPO)

'**Large Scale**' needs to factor in:

- the numbers of data subjects concerned;
- the volume of personal data being processed;
- the range of different data items being processed;
- the geographical extent of the activity;
- the duration or permanence of the processing activity.

2. The Data Protection Officer (DPO)

(c) **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.**

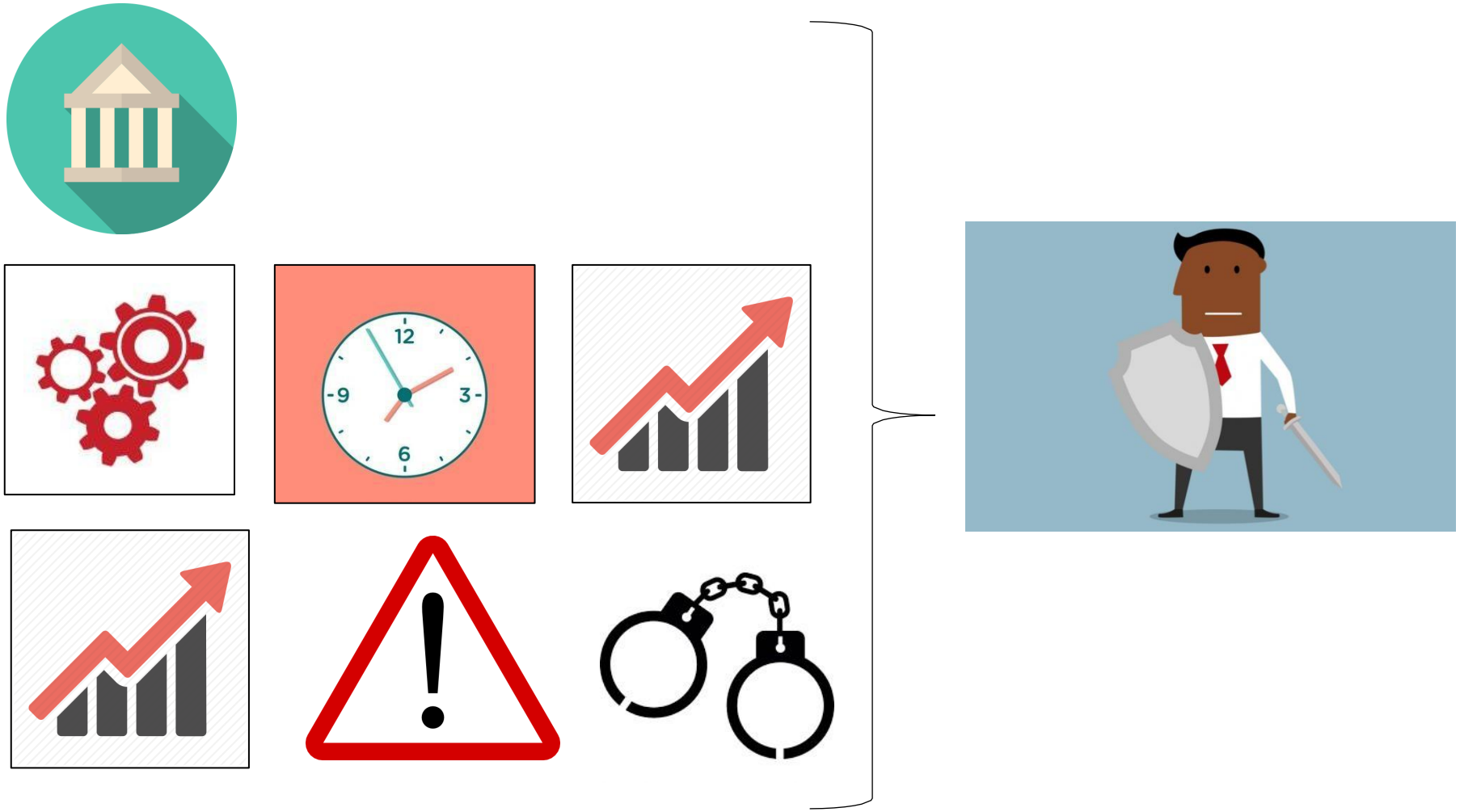
2. The Data Protection Officer (DPO)

- **Racial or ethnic origin**
- **Political opinions**
- **Religious or Philosophical beliefs**
- **Genetic Data**
- **Biometric Data**
- **Health Data**
- **Sex Life/Sexual Orientation**

2. The Data Protection Officer (DPO)

- Hospitals
- Insurance
- Clinics
- Trade Unions
- Schools
- Prisons
- Health Science Centres
- GU Clinic
- NSO
- Political Parties….

2. The Data Protection Officer (DPO)



2. The Data Protection Officer (DPO)

Optional but good practice

2. The Data Protection Officer (DPO)

How many?

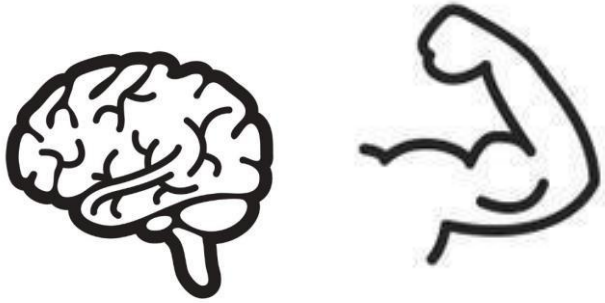
2. The Data Protection Officer (DPO)

How many?

- **Groups may appoint one DPO** – "*as long as the DPO is easily accessible from each establishment*"
- **Public Authorities or Bodies may have one DPO –** taking into account their organisational structure and size
- **Associations of processors or controllers may designate one DPO**

2. The Data Protection Officer (DPO)

2. The Data Protection Officer (DPO)



"The data protection officer shall be designated on the basis of **professional qualities** and, in particular, **expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39**."

May be staff or external

Once designated – DPO details must be published and communicated to IDPC

2. The Data Protection Officer (DPO)

"The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by **providing resources necessary** to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge"

2. The Data Protection Officer (DPO)

"The controller and the processor shall ensure that the data protection officer is **involved, properly and in a timely manner, in all issues which relate to the protection of personal data**."

2. The Data Protection Officer (DPO)

"The controller and processor shall ensure that the data protection officer **does not receive any instructions** regarding the exercise of those tasks.

He or she shall **not be dismissed or penalised** by the controller or the processor for performing his tasks.

The data protection officer shall directly report to the highest management level of the controller or the processor."

2. The Data Protection Officer (DPO)

"Data subjects may **contact the data protection officer with regard to all issues related to processing of their personal data** and to the exercise of their rights under this Regulation.

2. The Data Protection Officer (DPO)

"The data protection officer shall be **bound by secrecy or confidentiality** concerning the performance of his or her tasks, in accordance with Union or Member State law.

2. The Data Protection Officer (DPO)

"The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties **do not result in a conflict of interests."**

2. The Data Protection Officer (DPO)

Job Description

"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;"

2. The Data Protection Officer (DPO)

Job Description

"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**;"

2. The Data Protection Officer (DPO)

Job Description

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

2. The Data Protection Officer (DPO)

Job Description

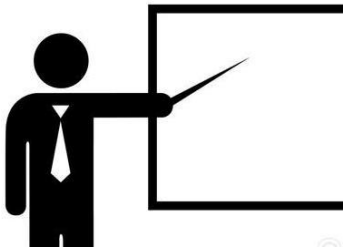
"to **cooperate** with the supervisory authority;"

2. The Data Protection Officer (DPO)

Job Description

""to act as the **contact point for the supervisory authority on issues relating to processing**, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter."

4. The Data Protection Officer (DPO)



- Know the ins-out
- Organisation is key
- Awareness and Training
- Compliance/Record-Keeping
- Pro-active NOT reactive
- Good Cop/Bad Cop

Any Questions?

3. What constitutes personal data ?

3. What constitutes personal data ?

personal data means **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);

3. What constitutes personal data ?

Anonymised Data VS Pseudonymised Data

- ✓ Personal data that has been pseudonymised – eg key-coded – typically falls within the scope of the GDPR.
- ✓ Fully anonymised data is not personal data

3. What constitutes personal data ?

Anonymised Data VS Pseudonymised Data

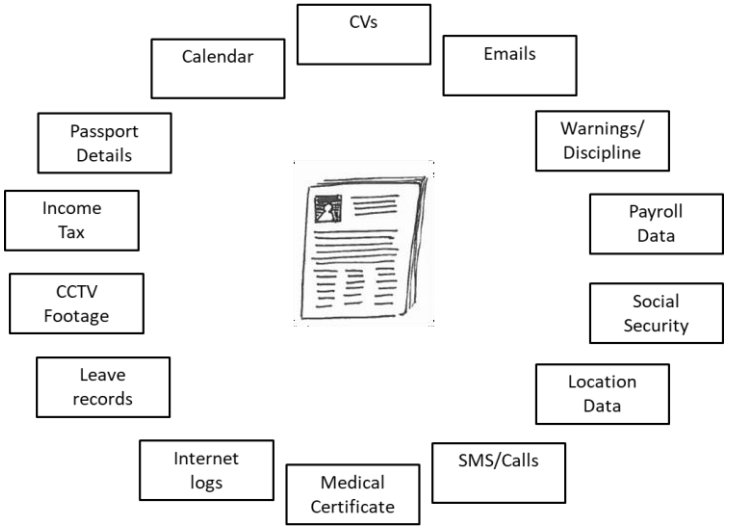
Think of the Employment Relationship…
What personal data is stored in that context?

3. What constitutes personal data ?

Anonymised Data VS Pseudonymised Data

Think of the Employment Relationship…

What personal data is stored in that context?

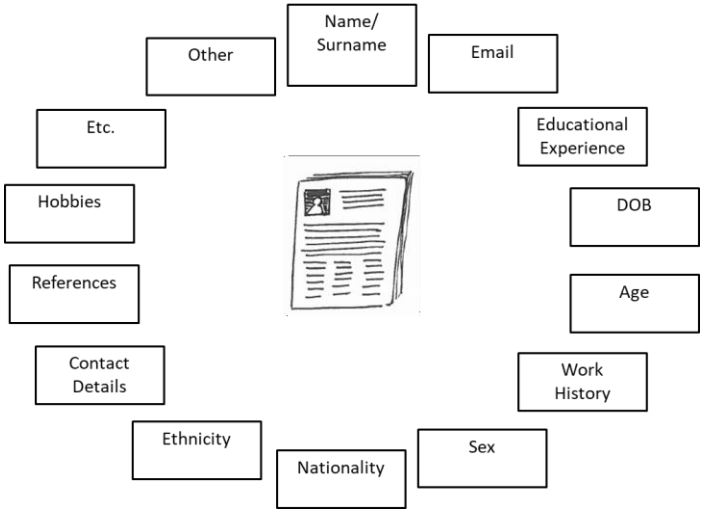


3. What constitutes personal data ?

Anonymised Data VS Pseudonymised Data

Think of the CV …

What personal data is stored in a CV?



3. What constitutes personal data ?

The GDPR applies to both

- **automated personal data**

and to

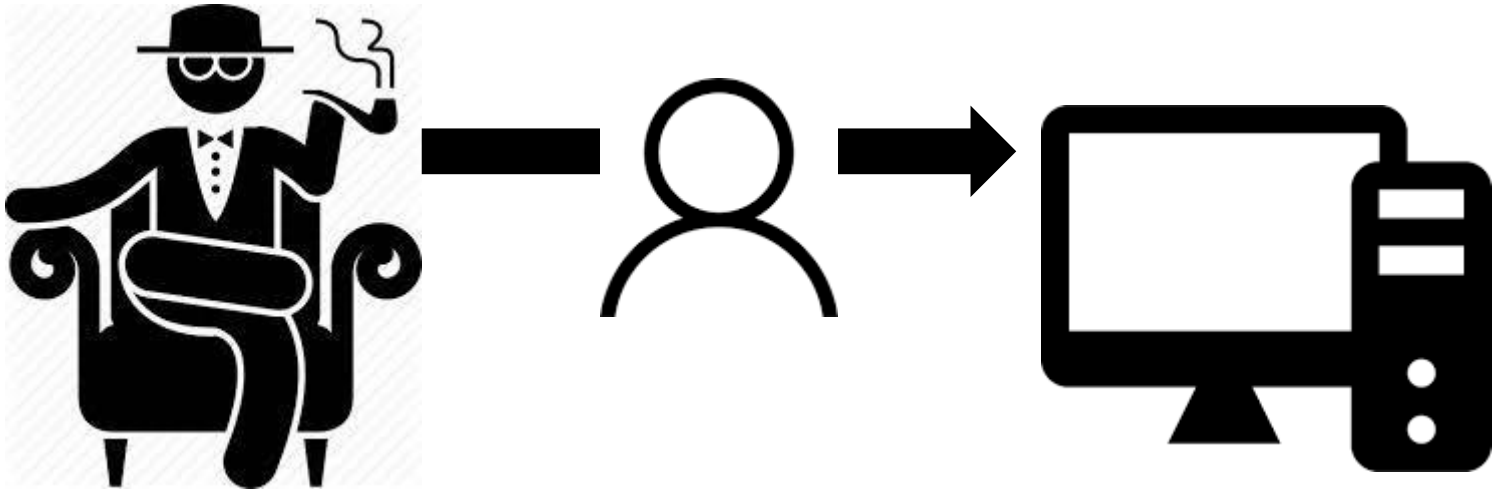
- **manual filing systems where personal data are accessible according to specific criteria**. This could include chronologically ordered sets of manual records containing personal data.

3. What constitutes personal data ?

The person who is directly or indirectly identified is **= the DATA SUBJECT**

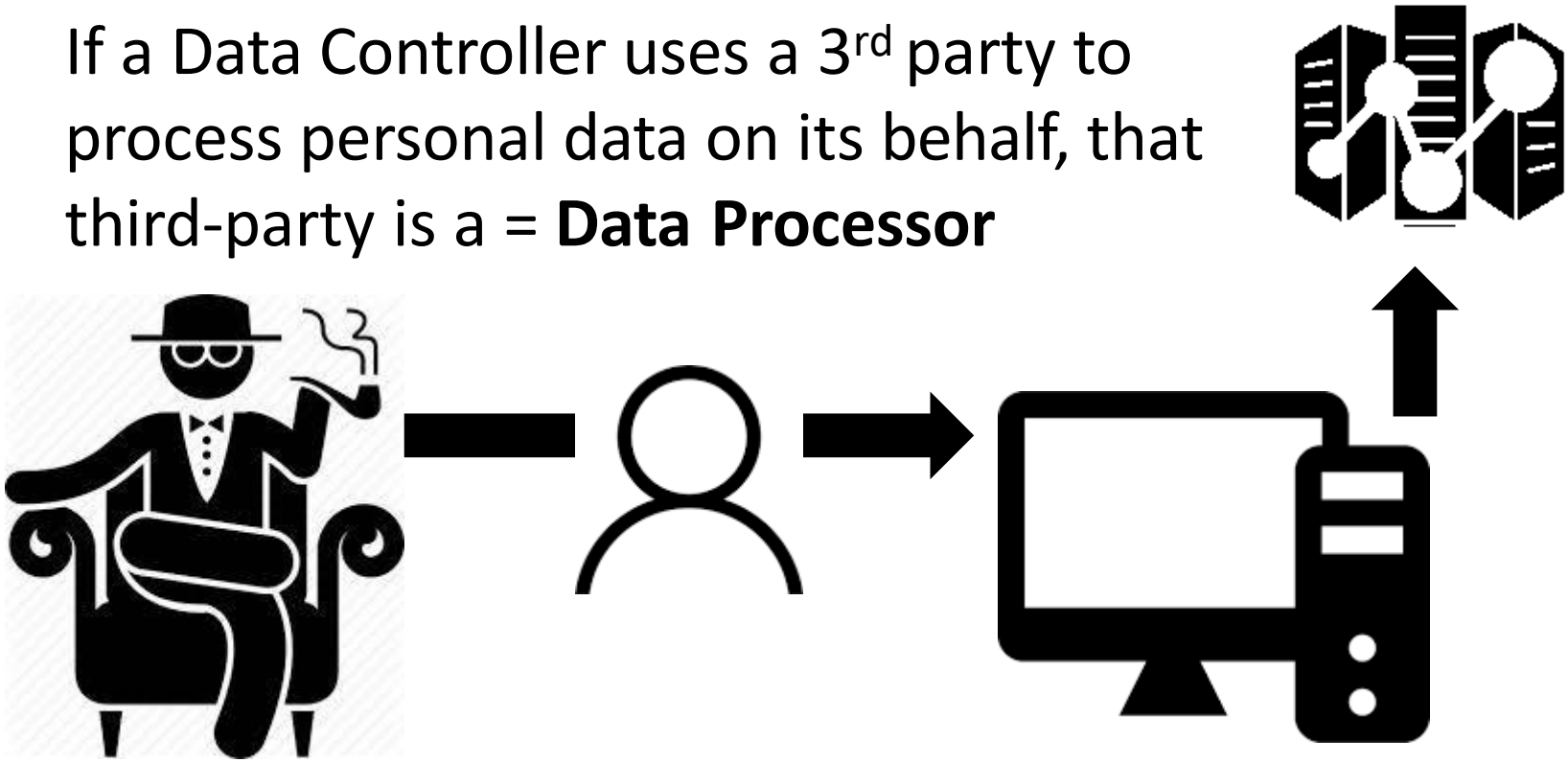
3. What constitutes personal data ?

Whosoever decides the means & purposes of processing of personal data of that Data Subject **= the DATA CONTROLLER**



3. What constitutes personal data ?

If a Data Controller uses a 3rd party to process personal data on its behalf, that third-party is a = **Data Processor**



3. What constitutes personal data ?

Controller VS Joint Controller

Processor VS Sub-Processor

Authorised Persons

3. What constitutes personal data ?

The GDPR does not apply to :

- Certain activities including processing covered by the Law Enforcement Directive;
- processing for national security purposes;
- processing carried out by individuals purely for personal/household activities;
- processing about deceased persons*;

* *Recital 27 of the GDPR sets out "This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons."*

3. What constitutes personal data ?

So what do we mean by processing ?

3. What constitutes personal data ?

So what do we mean by processing ?

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;*

3. What constitutes personal data ?

Note 1 : Special Categories of Personal Data

3. What constitutes personal data ?

Note 1 : Special Categories of Personal Data

Personal Data revealing :

- **Racial / ethnic origin**
- **Religious / philosophic beliefs**
- **Trade union membership & Political Opinion**
- **Genetic data**
- **Biometric data (when processed to uniquely identify a person)**
- **Data concerning Health**
- **Sex life / sexual orientation**

3. What constitutes personal data ?

Note 2 : Criminal Convictions

Personal data relating to criminal convictions and offences are special categories of data, but extra safeguards apply to its processing.

4. The Data Protection Principles

There are 6 Principles

4. The Data Protection Principles

Article 5(2) GDPR

“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

4. The Data Protection Principles

Each of the 6 principles must be satisfied cumulatively

4. The Data Protection Principles

NB There is a difference between the

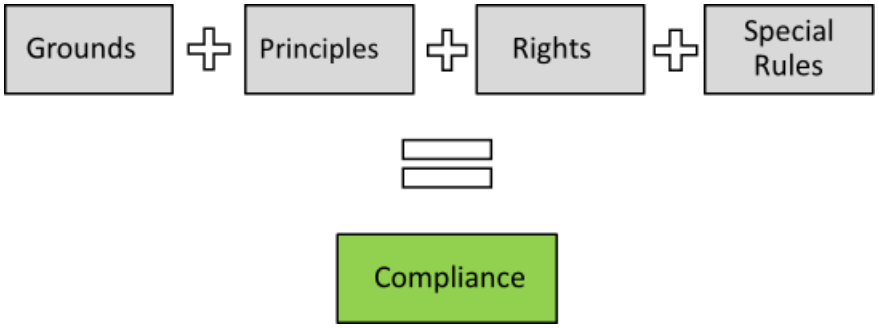
Principles **Grounds**

4. The Data Protection Principles

NB There is a difference between the

Principle	Grounds
HOW	WHY

4. The Data Protection Principles



4. The Data Protection Principles

Principle No. 1 : Lawfulness + Transparency

Personal Data must be
processed **lawfully**, fairly and in a **transparent** manner in relation to individuals;

4. The Data Protection Principles

Principle No. 2 : Purpose Limitation

Personal Data must be

collected for **specified, explicit and legitimate purposes** + not further processed in a manner that is **incompatible** with those purposes;

further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

4. The Data Protection Principles

Principle No. 3 : Data Minimisation

Personal Data must be

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. The Data Protection Principles

Principle No. 4 : Accuracy

Personal Data must be

accurate and, where necessary, **kept up to date;** every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

4. The Data Protection Principles

Principle No. 5 : Storage Limitation

Personal Data must be

kept in a form which permits identification of data subjects **for no longer than is necessary for the purposes for which the personal data are processed**;

personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

4. The Data Protection Principles

Principle No. 6 : Integrity & Confidentiality

Personal Data must be

processed in a manner that ensures **appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

FENECH + FENECH
ADVOCATES

www.21Academy.education

The slides do not constitute legal advice. Legal advice ought to be sought on a case-by-case basis