

# DATA PROTECTION OFFICERS GDPR COMPLIANCE

Alexia Valenzia

5 November 2024



CAMILLERI PREZIOSI  
ADVOCATES





## Overview of this session

- ✓ The role of controllers and processors and the relationship between them.
- ✓ Transferring personal data outside the EU and the mechanisms for compliance.





# The Role of Controllers and Processors:

## The Evolution of their Roles





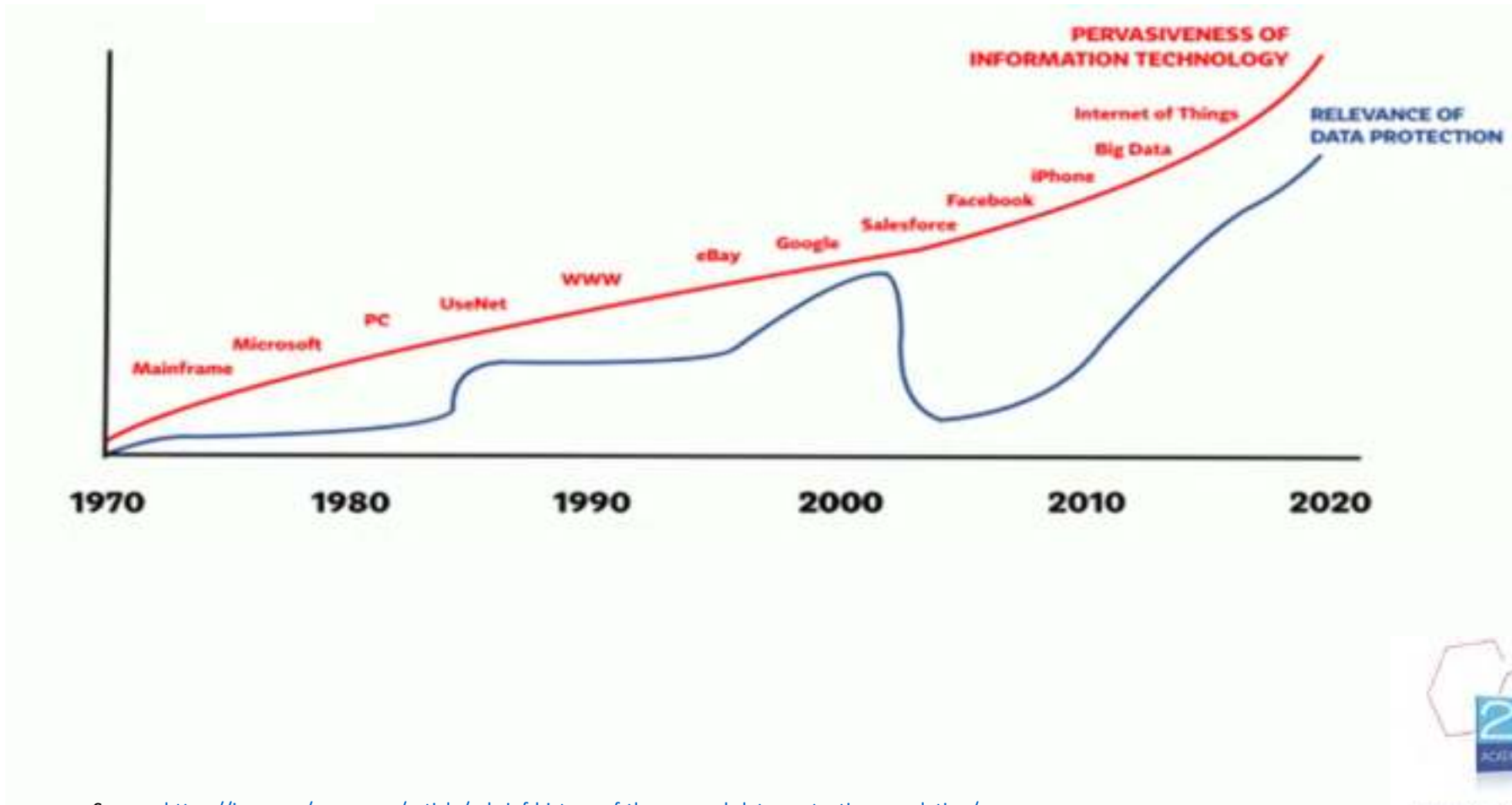
# Overview of DP Laws

- ✓ Privacy as a Fundamental Human Right
- ✓ Data Protection Act, Chapter 586 LOM (repealed former Chapter 440 - LOM)
- ✓ General Data Protection Regulation (EU) 2016/679 (repealed Directive 95/46/EC on protection of personal data)
- ✓ Directive (EU) 2016/680 on processing for law enforcement purposes (The Police and Criminal Justice Authorities)
- ✓ **E-Privacy Directive and Subsidiary Legislation 586.01**





# Legal Challenges: Tech Evolution v Legal Evolution



Source: <https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/>





# 1995 Directive - Definition

## **Controller:**

shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

## **Processor:**

shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;





# GDPR – Definition of Controller

## Directive Controller:

shall mean the natural or legal person, public authority, agency or any other body **which alone or jointly with others determines the purposes and means of the processing of personal data**; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

## GDPR Controller:

means the natural or legal person, public authority, agency or other body **which, alone or jointly with others, determines the purposes and means of the processing of personal data**; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law





# GDPR – Definition of Processor

## Directive Processor:

shall mean a natural or legal person, public authority, agency or any other body **which processes personal data on behalf of the controller;**

## GDPR Processor:

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

→ Both definitions are essentially the same, so what's changed?



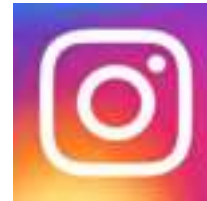




## Major Breaches Pre 2018



## Post 1995 Companies





# Liability

Article 23 of the Directive:

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive **is entitled to receive compensation from the controller for the damage suffered.**
2. **The controller** may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 82 of the GDPR:

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation **shall have the right to receive compensation from the controller or processor for the damage suffered.**
2. **Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.**





## The Role of Controllers and Processors:

# What is a Data Controller and a Data Processor?





# Data Controller

*A 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*

## Data Controller



Personal Data

Data Subject





# Data Controller



Personal Data

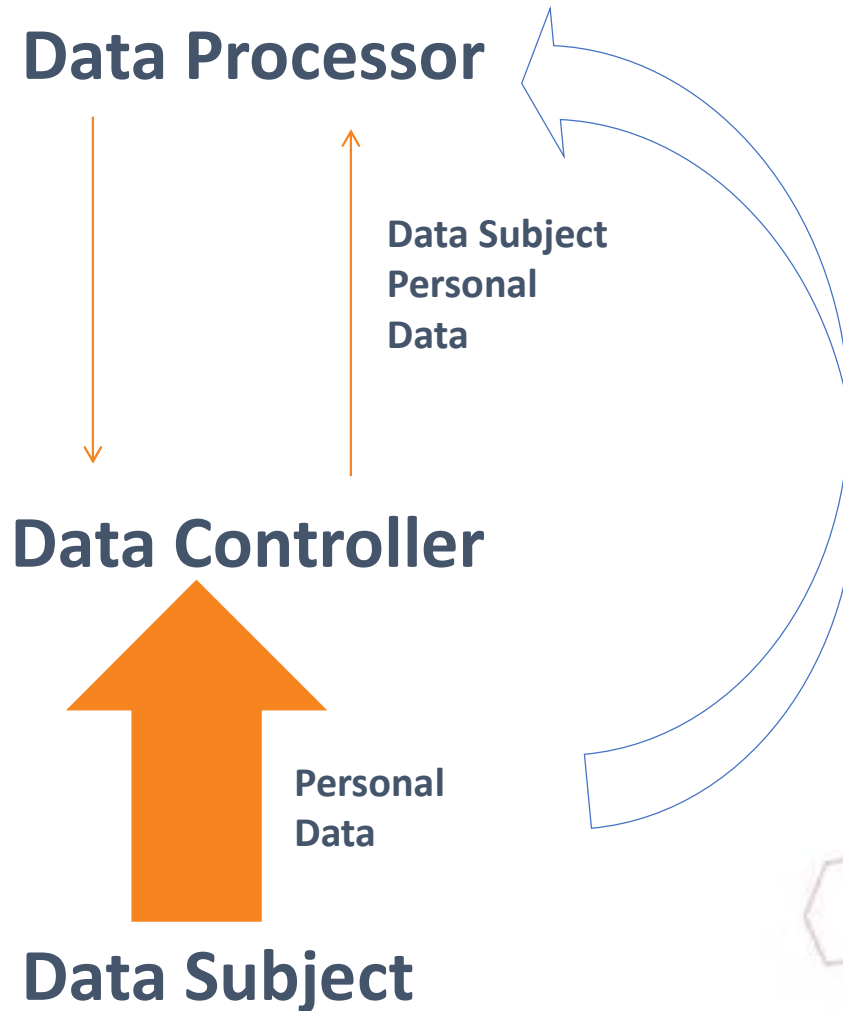
# Data Subject

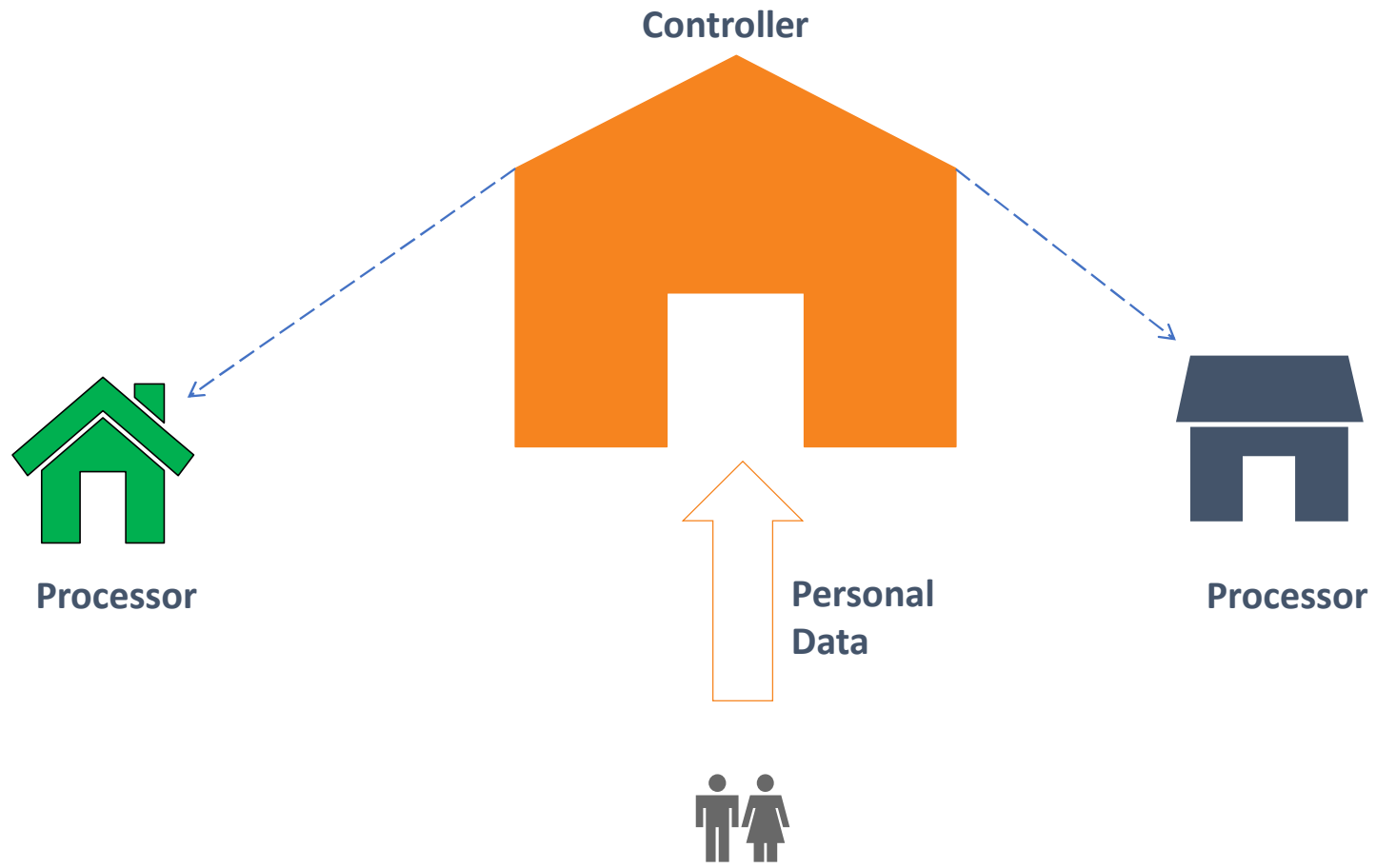
At the point of Personal Data collection, the Data Controller must provide the Data Subject with certain information that is stipulated in articles 13 and 14 of the GDPR

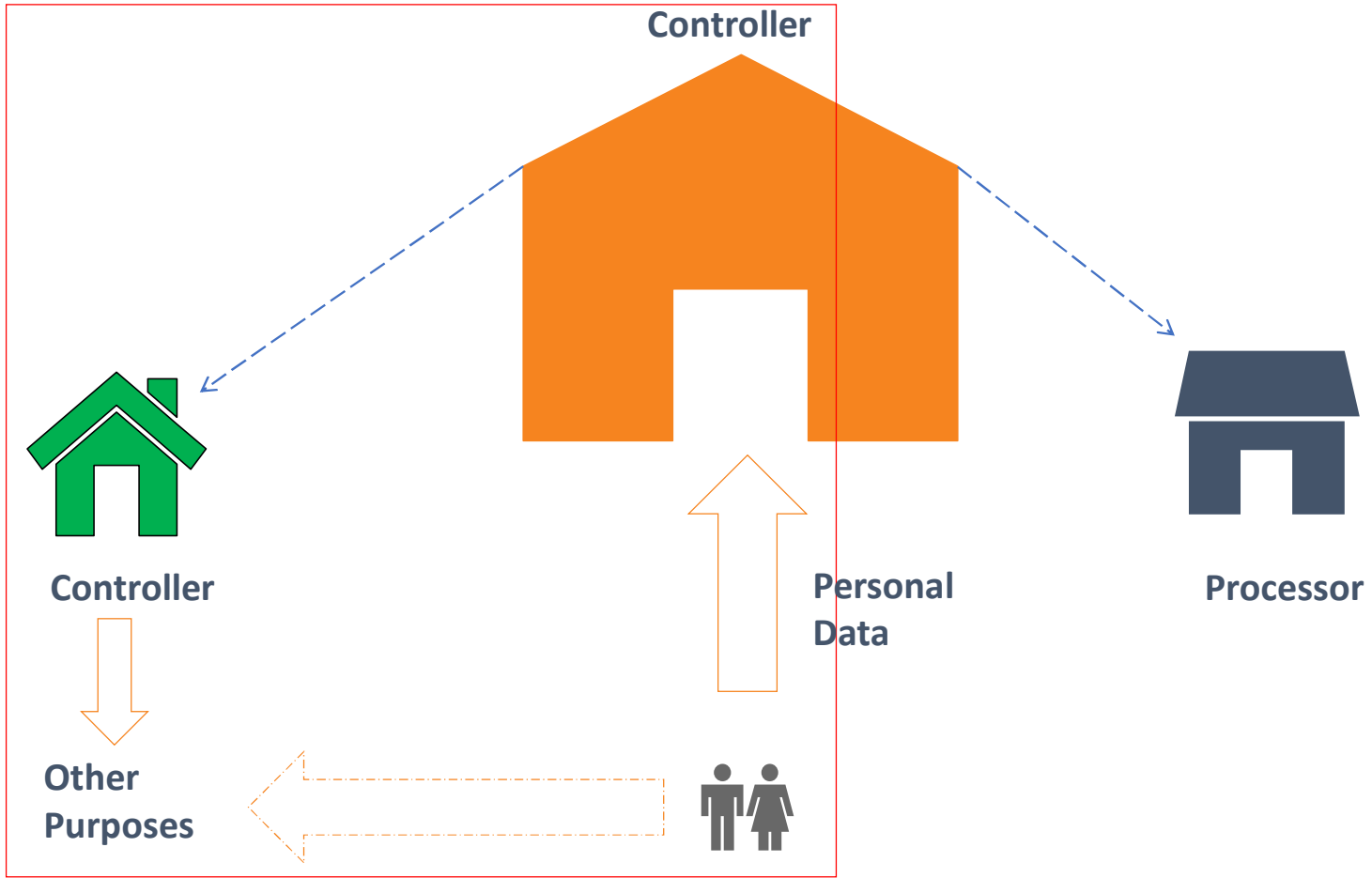


# Data Processor

*A natural or legal person, public authority, agency or other body (other than an employee) which processes personal data on behalf or on the instruction of the controller*











# Processing

Any operation or set of operations which is taken in regard to personal data, whether or not it occurs by automatic means:

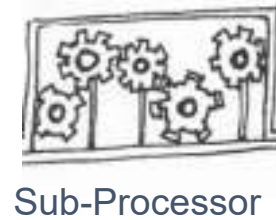
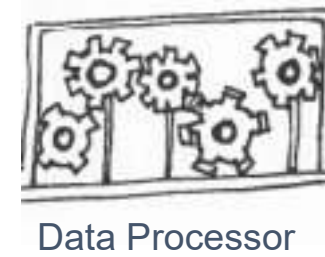
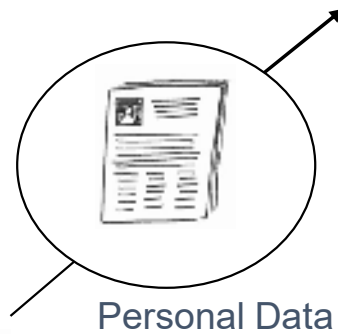
collection  
recording  
organization  
storage  
adaptation  
retrieval  
gathering  
erasure



use  
disclosure  
dissemination  
alignment  
alteration  
combination  
blocking  
destruction



# Key Players





## The Role of Controllers and Processors:

How can you determine who is a Controller and who is a Processor?

→ Can be tricky.





# Controller or Processor?

- ✓ Essential to determine whether an entity is a controller or processor
  - ✓ Different implications under the GDPR
  - ✓ Data breach responsibilities – notification to Supervisory Authorities
  - ✓ Rights of data subjects – Controllers responsibility to respect, Processor responsibility to assist
  - ✓ Liabilities and indemnities – both liable in terms of GDPR, unless proof can be provided that it is not in any way responsible for the event giving rise to the damage.





# Who is a Controller?

Data controller exercises overall control over the ‘what’, ‘why’ and the ‘how’ of a data processing activity.





# Who is a Controller?

Decisions that can only be taken by controller include the purpose of processing and ‘essential means’:

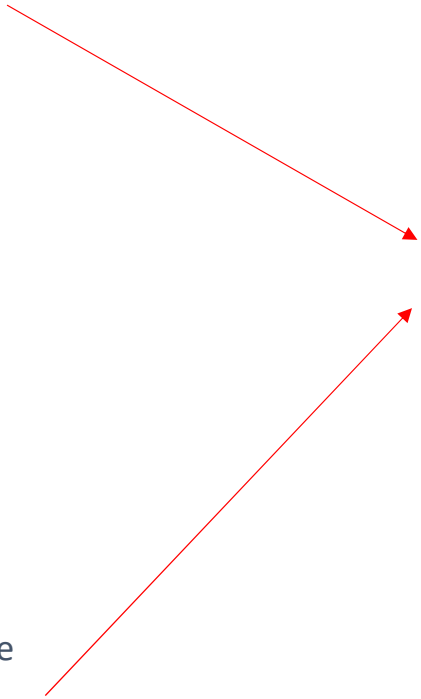
- ✓ collects the personal data in the first place;
- ✓ determines the legal bases of processing;
- ✓ determines purpose the data are to be used for;
- ✓ determines which items of personal data to collect;
- ✓ determines categories of data subjects;
- ✓ determines whether to disclose the data, and who to;
- ✓ determines whether data subject rights apply;
- ✓ determines how long to retain the data.





# Who is a Controller?

- ✓ collects the personal data in the first place;
- ✓ determines the legal bases of processing;
- ✓ determines purpose the data are to be used for;
- ✓ determines which items of personal data to collect;
- ✓ determines categories of data subjects;
- ✓ determines whether to disclose the data, and who to;
- ✓ determines whether data subject rights apply;
- ✓ determines how long to retain the data.



Privacy Notice





# Who is a Processor?

- ✓ Role limited to the more 'technical' aspects of an operation, such as data storage, retrieval or erasure.
- ✓ Acts as a service provider to the controller i.e. process data on the controller's behalf.
- ✓ Cannot take any of the over-arching decisions, e.g. what the personal data will be used for or what the content of the data is







# Who is a Processor?

A processor may decide the ‘non-essential means’:

- ✓ what IT systems or other methods to use to collect data;
- ✓ how to store the personal data;
- ✓ detail of the security surrounding the personal data;
- ✓ means used to transfer the personal data from one organisation to another;
- ✓ the means used to retrieve personal data about certain individuals;
- ✓ the method for ensuring a retention schedule is adhered to;
- ✓ the means used to delete or dispose of the data.





# Who is a Processor?

- ✓ IT admins
- ✓ An Internet Service Provider providing web hosting services which processes personal data published online by its customers, who use the ISP for their website hosting and maintenance
- ✓ Payment gateways (eg PayPal) that process payments
- ✓ Payroll companies. The payroll company stores the employee data in its IT systems and pays the wages at the instructions of the company which ultimately determines when they should be paid, at which amount and the information to be included in the pay slip
- ✓ Outsourced services





## Controller **and** a Processor?

A possibility!

Examples:

- The IT service provider is a processor to its clients and a controller to its employees
- A payment gateway services provider may be a processor to its clients and considered a controller for reporting money laundering





# Controller **and** a Processor?

Art.28(10) GDPR

If the processor makes its own decisions, rather than following controller's instructions, that processor **is treated as a controller in respect of that processing activity.**

May have implications on liability





## The Role of Controllers and Processors:

# Controller Responsibilities





## Controller Governance (1) – Privacy Notices

### Art.12 GDPR

The **controller** shall take appropriate measures to provide a Privacy Notice and any communication under Articles 15 to 22 and 34 relating to processing to the data subject





# Controller Governance (2) - Rights

## GDPR data subject rights

The infographic displays eight GDPR data subject rights arranged in two rows of four. Each right is represented by a white icon on a teal background, with the name of the right written below it.

			
Information	Access	Rectification	Erasure
			
Restrictions	Portability	Objection	Revision of automation



## Controller Governance (3) - Reporting

### Art.33 and 34 GDPR

It is the **controller's** responsibility to notify data protection authorities and/or data subjects as a result of a data breach, where applicable







# Controller Governance (4) – Record Keeping

## Art.30 GDPR

- (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- (b) the purposes of the processing;
- (c) a description of the categories of data subjects and of the categories of personal data;





# Controller Governance (4) – Record Keeping

- (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- (f) where possible, the envisaged time limits for erasure of the different categories of data;
- (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).





# Controller Governance (5) – DPAs

## Article 28 (1) GDPR

Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject





## The Role of Controllers and Processors:

# Processor Responsibilities





# Processor Governance

- ✓ Internal record keeping of processing activities
- ✓ Cooperation with supervisory authorities
- ✓ Data breach reporting to Controller
- ✓ Erasing, deleting or returning all the personal data processed to the controller at the end of the data processing services
- ✓ Appoint DPO
- ✓ Responsible for technical and organisational measures





# Processor Obligations





# The Role of Controllers and Processors:

# The Data Processing Agreement





# The Data Processing Agreement

- ✓ Must be a written legal instrument which must include:
  - Subject Matter of processing.
  - Duration of processing.
  - Nature of processing activity.
  - Type of personal data.
  - Categories of data subjects.
  - Obligations and rights of Controller
  
- ✓ Must contain certain provisions: the technical and organisational security measures put in place by the Data Processor, deletion of personal data at the request of the Data Controller
  
- ✓ Must Specify if personal data is going to be transferred to other entities
  
- ✓ Only applies to Controller – Processor (and Processor – SubProcessor) relationships
  
- ✓ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0915&from=EN>







# Article 28 (3)

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

- (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
- (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- (c) takes all measures required pursuant to Article 32;
- (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
- (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
- (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
- (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
- (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.





# Record Keeping Obligation: Processor

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:
  - (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
  - (b) the categories of processing carried out on behalf of each controller;
  - (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
  - (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).





The Role of Controllers and Processors:

What other relationships exist?





# Other Relationships

## ✓ Sub-Processors → flow down obligations

- Data Processing Agreement

## ✓ Joint Controllers

- Joint liability before Data Subjects and Authorities
- Publication of substance of the agreement

## ✓ Controller - Controller





# Joint Controllers

- ✓ A joint controller agreement must be entered into
- ✓ Must:
  - Cover compliance with the obligations under GDPR, in particular as regards the exercising of the rights of the data subject and the controllers' respective duties to provide the information referred to in Articles 13 and 14
  - designate a contact point for data subjects.
- ✓ The essence of the arrangement shall be made available to the data subject.
- ✓ Irrespective of the terms of the arrangement, the data subject may exercise his or her rights in respect of and against each of the controllers.





# Controller to Controller Situations

- ✓ Both parties act independently in the processing of PD
- ✓ Company X processes data of its employees for accounting purposes. Company X is obliged to send such data to the IRD for fiscal purposes. Both Company X and the IRD process the same data but lack shared purpose or means with regard to this data processing, and thus are two separate data controllers.
- ✓ An independent travel agent sends PD of its customers to an airline and a hotel in order to make reservations. The airline / hotel confirm booking. In this case, each of the 3 are separate data controllers.





# Controller to Controller main issues

- ✓ Data transfer/sharing agreement
- ✓ Privacy Notice disclosures
- ✓ Handling of complaints/breaches
- ✓ Third party data
- ✓ Indemnities / liabilities
- ✓ Guarantees





# The Role of Controllers and Processors:

## Examples







# Example 1

- ✓ A bank hires an IT services firm to store archived data on its behalf. The bank will control how and why the data is used and determine its retention period. In reality the IT services firm will use a great deal of its own technical expertise and professional judgement to decide how best to store the data in a safe and accessible way.
- ✓ Is the IT services firm a controller or a processor?





# Example 1

Answer = Data Processor

- ✓ Despite the IT service provider's freedom to take technical decisions, the IT firm is still not a data controller in respect of the bank's data.
- ✓ It retains exclusive control over the purpose for which the data is processed and the content of the data, if not exclusively over the manner in which the processing takes place.
- ✓ Key consideration = who exercises control over the content of the personal data.





## Example 2

✓ A firm contracts a market research company to carry out some research. The firm's brief specifies its budget and that it requires a customer satisfaction survey of its main retail services. The firm leaves it to the research company to determine sample sizes, interview methods and presentation of results. The research company is processing personal data on the firm's behalf, but it is also determining which customers to contact, determining what to ask the firm's customers and the manner in which the survey will be carried out. It has the freedom to decide such matters as which customers to select for interview, what form the interview should take, what information to collect from customers and how to present the results.

✓ Is the market research company a controller or a processor?





## Example 2

Answer = Controller

- ✓ a data controller in its own right in respect of the processing of personal data done to carry out the survey
- ✓ even though the bank retains overall control of the data in terms of commissioning the research and determining the purpose the data will be used for, the 'how' and 'why' is determined by the marketing company when carrying out the research





## Example 3

A luxury car company teams up with a designer fashion brand to host a co-branded promotional event. The companies decide to run a prize draw at the event. They invite attendees to participate in the prize draw by entering their name and address into their prize draw system at the event. After the event, the companies post out the prizes to the winners. They do not use the personal data for any other purposes.

ICO <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/>





# Example 3

The companies will be joint controllers of the personal data processed in connection with the prize draw, because they both decided the purposes and means of the processing.

ICO <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/>





# Example 4

A gym engages a local printing company to produce invitations to a special event the gym is hosting. The gym gives the printing company the names and addresses of its members from its member database, which the printer uses to address the invitations and envelopes. The gym then sends out the invitations.

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/>





## Example 4

The gym is the controller of the personal data processed in connection with the invitations. The gym determines the purposes for which the personal data is being processed (to send individually addressed invitations to the event) and the means of the processing (mail merging the personal data using the data subjects' address details). The printing company is a processor processing the personal data only on the gym's instructions.

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/>







## Example 5

A firm uses an accountant to do its books. When acting for his client, the accountant is a controller in relation to the personal data in the accounts. This is because accountants and similar providers of professional services work under a range of professional obligations that oblige them to take responsibility for the personal data they process. For example, if the accountant detects malpractice while doing the firm's accounts he may, depending on its nature, be required under his monitoring obligations to report the malpractice to the police or other authorities. In doing so, an accountant would not be acting on the client's instructions but in line with his own professional obligations and therefore as a controller in his own right

If specialist service providers are processing data in line with their own professional obligations, they will always be acting as the controller. In this context, they cannot agree to hand over or share controller obligations with the client.

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/>





## Example 6

A GP surgery uses an automated system in its waiting room to notify patients when to proceed to a GP consulting room. The system consists of a digital screen that displays the waiting patient's name and the relevant consulting room number, and also a speaker for visually impaired patients that announces the same information.

The GP surgery will be the controller for the personal data processed in connection with the waiting room notification system because it is determining the purposes and means of the processing.

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/>





## Example 7

A property management company maintains student halls of residence for the landlord, the university. The company enters tenancy agreements with the students on the university's behalf and chases any rent arrears. It collects the rent and passes it to the university after taking a commission.

The company is a joint controller of the tenancy-related information, including regarding rental payments. It decides what information it needs from the residents to set up and manage the tenancies but will share this data with the university.

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/>





The Role of Controllers and Processors:

# Consequences of Non-Compliance





# Fines and Penalties

**10, 000, 000 EUR**

Or

**up to 2 % of the total  
worldwide annual turnover**





# Fines and Penalties

**20, 000, 000 EUR**

Or

**up to 4 % of the total  
worldwide annual turnover**



# Supervisory Authorities also have the power to ...

- ✓ order the controller and the processor, and, where applicable, the controller's or the processor's representative **to provide any information it requires for the performance of its tasks**;
- ✓ carry out **investigations** in the form of data protection audits;
- ✓ **notify** the controller or the processor of an alleged infringement of the GDPR;
- ✓ **obtain**, from the controller and the processor, **access to all personal data** and to all information necessary for the performance of its tasks;
- ✓ obtain **access to any premises** of the controller and the processor, including to any data processing equipment and means;
- ✓ **issue warnings** to a controller or processor that intended processing operations are likely to infringe provisions of the GDPR;
- ✓ **issue reprimands** to a controller or a processor where processing operations have infringed provisions of the GDPR;
- ✓ **order** the controller or the processor to **comply with the data subject's** requests to exercise his or her rights pursuant to the GDPR;



# The list goes on ...

- ✓ order the controller or processor to bring processing operations into compliance with the provisions of the GDPR, where appropriate, in a specified manner and within a specified period;
- ✓ order the controller to communicate a personal data breach to the data subject;
- ✓ impose a temporary or definitive limitation including a ban on processing;
- ✓ order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
- ✓ impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;
- ✓ order the suspension of data flows to a recipient in a third country or to an international organisation.







# GDPR Enforcement Tracker

<https://www.enforcementtracker.com/>

ETId	Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type	Source
ETId-1469	ITALY	2022-09-15	2,000	Thiene municipality	Art. 5 (1) a), d) GDPR, Art. 6 GDPR, Art. 2-ter Codice della privacy	Insufficient legal basis for data processing	GD
ETId-1468	SPAIN	2022-10-24	6,000	ADSL HOUSE S.L.	Art. 48 (1) b) LGT, Art. 21 GDPR, Art. 23 (4) LOPDGD00	Insufficient fulfillment of data subjects rights	GD
ETId-1467	SPAIN	2022-10-24	400	Private individual	Art. 5 (1) d) GDPR	Non-compliance with general data processing principles	GD
ETId-1466	SPAIN	2022-10-24	240	Company	Art. 5 (1) d) GDPR	Non-compliance with general data processing principles	GD
ETId-1465	ITALY	2022-07-21	20,000	Acqua Nuova VCO S.p.a.	Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 28 GDPR, Art. 2-ter Codice della privacy	Insufficient legal basis for data processing	GD
ETId-1464	ITALY	2022-07-21	5,000	Grossa municipality	Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 28 GDPR, Art. 2-ter Codice della privacy	Insufficient legal basis for data processing	GD
ETId-1463	ITALY	2022-07-21	10,000	Clia S.r.l.	Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 30 (2) GDPR, Art. 2-ter Codice della privacy	Insufficient legal basis for data processing	GD
ETId-1462	ITALY	2022-10-08	15,000	Servizi Idrosc Integre S.p.a.	Art. 5 (1) b) GDPR, Art. 32 GDPR	Insufficient technical and organizational measures to ensure information security	GD
ETId-1461	UNITED KINGDOM	2022-10-19	5,033,000	Interserve Group Limited	Art. 5 (1) b) GDPR, Art. 32 GDPR	Insufficient technical and organizational measures to ensure information security	GD, GD
ETId-1460	ITALY	2022-09-15	10,000	Bper Banca S.p.A.	Art. 12 GDPR	Insufficient fulfillment of data subjects rights	GD



# Malta – IDPC Annual Report – 2022

**595**  
**COMPLAINTS**

**59**  
**DATA BREACH  
NOTIFICATIONS**

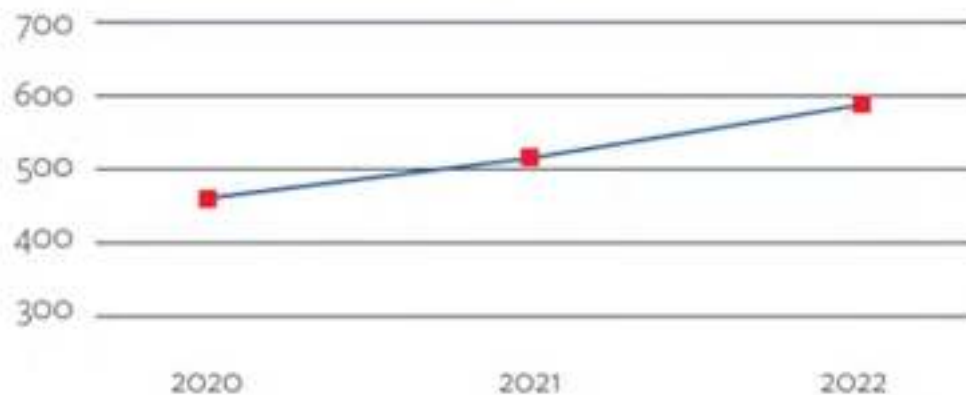


# Malta – IDPC Annual Report – 2022

## 5.1 Local Data Protection Complaints

In 2022, the IDPC experienced a significant increase in local cases compared to previous years, with a total of five hundred and ninety-five (595) cases received, marking a notable rise from five hundred and nine (509) cases in 2021 and four hundred and seventy (470) cases in 2020.

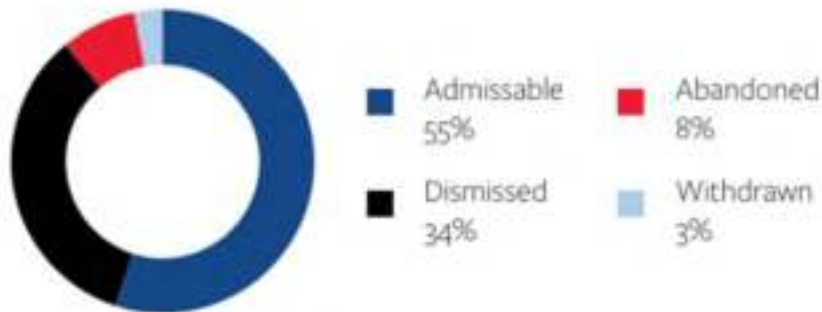
Complaint comparison by year





# Malta – IDPC Annual Report – 2022

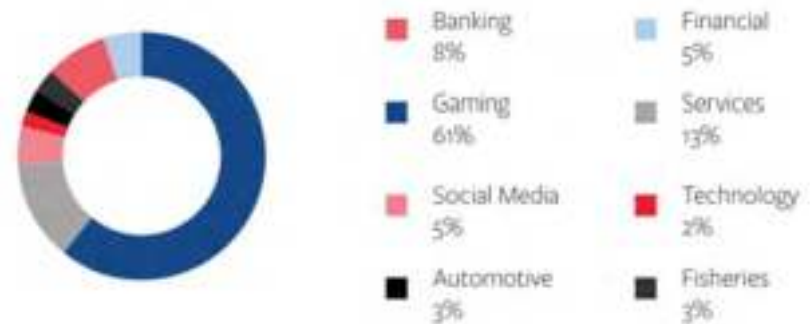
Complaints investigated during 2022



Sector of the Controller

Banking	3
Financial	2
Gaming	24
Services	5
Social Media	3
Technology	1
Automotive	1
Fisheries	1
<b>Total</b>	<b>39</b>

Sector of the Controller





2022	Data Protection Complaint	The controller failed to respect the timeframe prescribed by article 12(3) GDPR to respond the complainant's access request	Infringement of Article 12(3) GDPR	Reprimand and orders, in terms of Article 58.2 GDPR
2022	Data Protection Complaint	The controller infringed the GDPR for having processed the complainant's personal data included in her identity card without a valid legal basis	Infringement of Article 6(1) GDPR	Reprimand and orders, in terms of Article 58.2 GDPR
2022	Data Protection Complaint	The controller failed to inform the complainant that the call between the controller's employee and the complainant was being recorded	Infringement of Article 13 GDPR	Reprimand, in terms of Article 58.2 GDPR
2022	Personal Data Breach	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	Administrative fine of €250,000 in terms of Article 58.2 GDPR

<https://idpc.org.mt/decisions/>



# Liabilities

## Debate:

No exclusion of liability vis-à-vis:

1. the data subjects;
2. the supervisory authority imposing a penalty

But

- Either party may exclude their liability if “it is not in any way responsible for the event giving rise to the damage”
- Burden sharing for payment of compensation





## Re - Cap

- ✓ The data controller determines the purposes for which and the means by which personal data is processed.
- ✓ The data processor processes personal data only on behalf of the controller.
- ✓ Distinct yet linked controller vs processor obligations
- ✓ Distinguish between controller to controller, controller to processor, processor to sub-processor, joint controllers



# Data Transfers





# When can personal data be transferred outside the EU?





# Cross-Border Transfers Limitation

Principle:

*No transfer of data to countries outside the EU that do not offer an “adequate level of protection”*

Rec.101-116; Art.44, 45: Cross-Border Data Transfers may only take place if:

- the transfer is made to an Adequate Jurisdiction;
- the data exporter has implemented a lawful data transfer mechanism; or
- or an exemption or derogation applies





## Cross-Border Transfers of Data

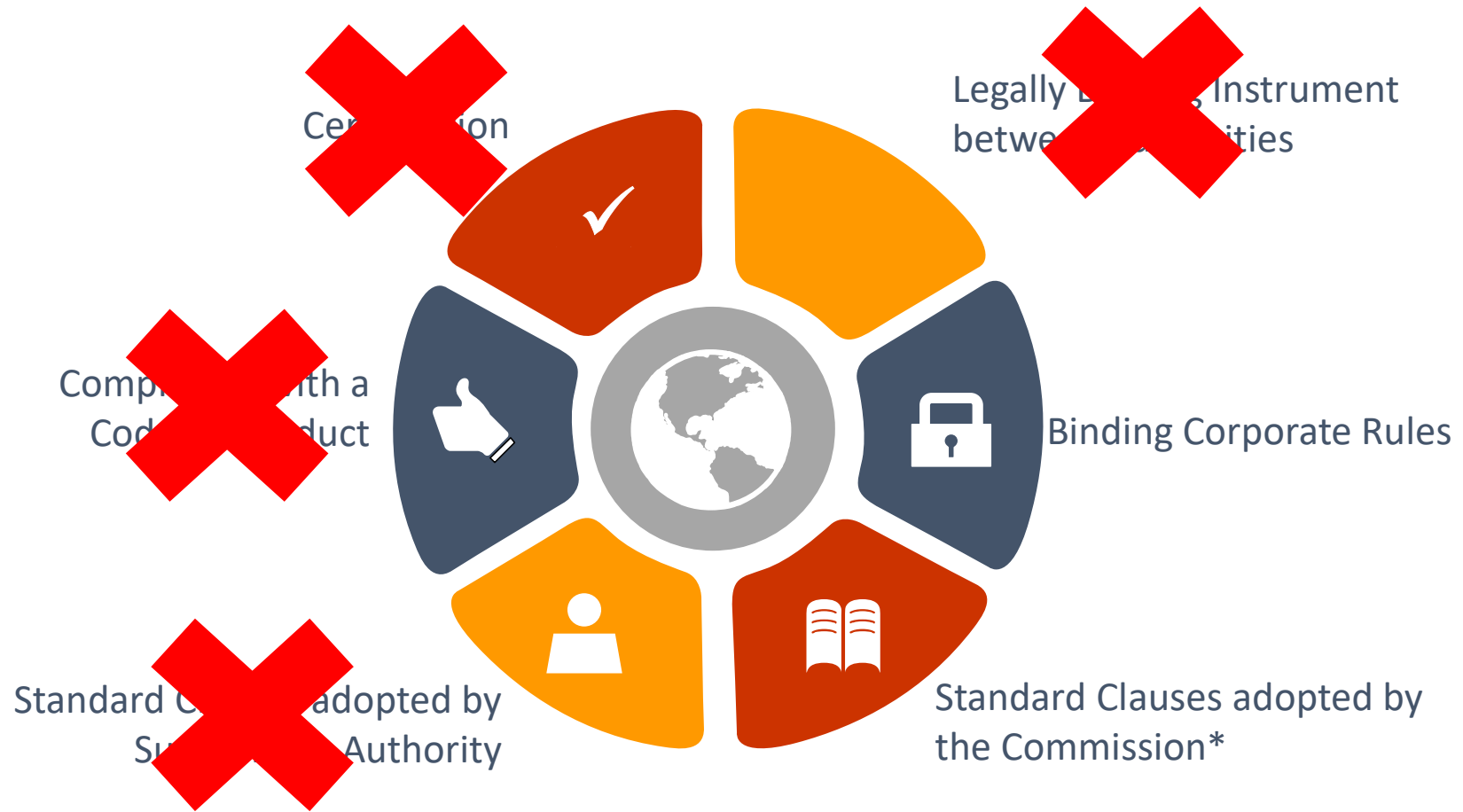
Current list of 'Adequate Jurisdictions':

Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom under the GDPR and the LED, the United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay





# Transfers subject to appropriate safeguards



# Standard Contractual Clauses/Model Clauses

**On 12 November 2020** - the European Commission released draft updated standard contractual clauses (SCCs) for consultation

**On 4 June 2021** - the Commission issued modernised SCCs under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR):

These modernised SCCs replace the 3 sets of SCCs that were adopted under the previous Data Protection Directive 95/46.





# Standard Contractual Clauses/Model Clauses

**Old SCCs:** only controller – controller or controller – processor

**Current SCCs:** controller – controller, controller – processor, processor to processor, and processor –controller – Module system

Contracts concluded before 27 September 2021 on the basis of the old SCCs shall be deemed to provide appropriate safeguards until 27 December 2022, provided the processing operations that are the subject matter of the contract remain unchanged and that reliance on those clauses ensures that the transfer of personal data is subject to appropriate safeguards.

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN>





# Derogations

- ✓ individual's informed consent;
- ✓ necessary for the performance of a contract;
- ✓ necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- ✓ necessary for important reasons of public interest;
- ✓ necessary for the establishment, exercise or defence of legal claims;
- ✓ necessary to protect the vital interests of the data subject; or
- ✓ made from a register which under national or EU law is intended to provide information to the public.





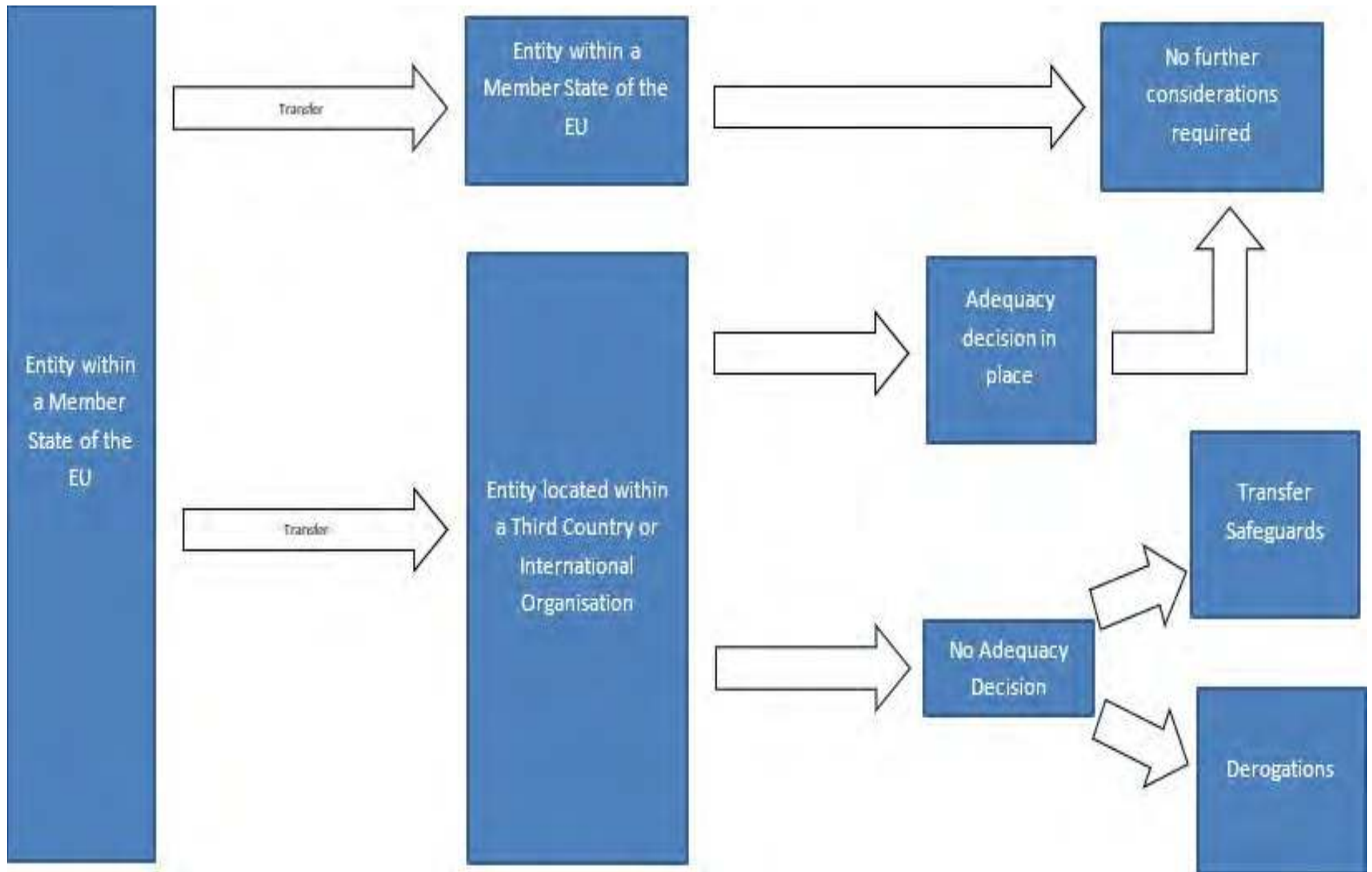
# Derogations Application

Where no safeguards are in place and where none of the derogations apply, a transfer to a third country or an international organisation may take place only if:

- ✓ the transfer is not repetitive
- ✓ the transfer concerns only a limited number of data subjects
- ✓ the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject; and
- ✓ the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.
- ✓ The controller shall inform the supervisory authority of the transfer.









# Brexit

The EU adopted two adequacy decision for the UK, whereby personal data can be transferred between the EU and the UK without restrictions.

## UK GDPR:

- ✓ affects EU-based entities that process personal data either (i) pertaining to UK citizens and/or (ii) with UK based entities

<https://ico.org.uk/for-organisations/data-protection-and-brexit/>



www.21Academy.education

# The Schrems II Judgement



- ✓ Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems (16 July 2020)
- ✓ CJEU ruled that the EU-US Privacy Shield was invalid and threw the use of standard contractual clauses (SCCs) into question
- ✓ In addition, the European Data Protection Board clarified that entities must carry out a review of the law in each country to which they export personal data if those transfers are pursuant to SCCs
- ✓ The new 2021 SCCs introduced the burdensome requirement of a Transfer Impact Assessment to be carried out by controllers and processors – this is an analysis of the laws of the third country to which personal data will be transferred, in order to ensure that the data will be adequately protected in said country





# The Schrems II Judgement

- Following the invalidation of the Privacy Shield, the European Commission and the US Government have started negotiations on a successor arrangement
- In March 2022, it was announced that the EC and the US have agreed in principle on a new Trans-Atlantic Data Privacy Framework
- The European Commission is now expected to prepare a draft adequacy decision and then launch its adoption procedure





# Transfers to the US

- ✓ Safe harbour and Privacy Shield
- ✓ Post Schrems II, Privacy Shield no longer offers a default adequate level of protection
- ✓ Businesses must prove and specify such protective measures over and above SCC to provide adequate level of protection.
- ✓ 'Adequate' has been construed to mean 'essentially equivalent to'.
- ✓ The above would need to be assessed on a case-by-case basis.





# Transfers to the US

- ✓ Schrems II judgement left businesses with legal uncertainty over their data processing with US entities
- ✓ A risk-based approach must be implemented, even when relying on SCCs.
- ✓ Problem arises that there is now a positive obligation on the data exporter to conduct a Transfer Impact Assessment, which in practical cases could prove unfeasible.
- ✓ Trans-Atlantic Data Privacy Framework

# Risk Mitigation – Administrative and Technical Safeguards to Consider



- ✓ Data Minimisation.
- ✓ Obfuscation/Encryption in certain use cases.
- ✓ Ensure all DPAs include all requisites under Art. 28 **and** Specify Technical and Organisational measures in place.
- ✓ Ensure Notice Obligations.
- ✓ Ensure Termination Clauses.
- ✓ Ensure Security of Return/Deletion of Data.
- ✓ Liability/Indemnity Considerations





## Re - Cap

- ✓ The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.
- ✓ These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.
- ✓ The GDPR provides derogations from the general prohibition on transfers of personal data outside the EU for certain specific situations.



CAMILLERI PREZIOSI ADVOCATES



**Alexia Valenzia**

[alexia.valenzia@camilleripreziosi.com](mailto:alexia.valenzia@camilleripreziosi.com)

(+356) 2123 8989

Camilleri Preziosi


Level 3, Valletta Buildings

South Street

Valletta, VLT 1103

Malta





THANK YOU

Technical Excellence, Practical Solutions



CAMILLERI PREZIOSI  
ASSOCIATES

INTERLAW.