Information and Communication Technology Law

Lecture 1

Title: Introduction to IT and Data Protection Law

Lecturer: Sharon Xuereb, Camilleri Preziosi

Date: 19.04.2023

Diploma in Law (Malta)

CAMILLERI PREZIOSI
ADVOCATES

What is ICT Law?

The law which governs information processing (and how this is undertaken by ‘computers’).

What topics are covered under ICT Law?

- Contracts to purchase computer hardware or software
- Intellectual property protection of IT products / services
- Data protection and confidentiality of data
- Computer crime
- Electronic commerce
- New (disruptive) technologies

Digitisation: What is it?

- The Information Economy

- Industrial Economic Model –19th/20th Centuries
  - Economic value within physical goods (*atoms*)
  - Economies of scale & Mechanisation

- Information Economy – present time
  - Economic value sited within information *(bits*)
  - Information collected, stored, processed.
  - Provision of services – banking, financial etc
  - Information society – encoding: *atoms to bits*

Digitisation: What is it?

- Atoms used in the physical world to construct everything.
- Digitization = Conversion from *atoms to bits* (0 or 1)
- Bits – building blocks of the information society.

- Digitisation:
  - cheaper to store and distribute goods/services
  - new models to market and deliver products/services
  - new avenues for communication, exchange of ideas
  - Non-rivalrous goods – intangibles, consumed by several consumers at the same time – "informational goods"
    - Versus rivalrous goods, "Atomic" – those whose consumption by one consumer prevents simultaneous consumption by other consumers.
  - Cross-border effects of information transfers on law – jurisdiction, identification of lawbreakers

Digitisation: What is it?

We have experienced a move from industrial based society to an information society

- Shift from ownership or control of things to ownership of or control over information
  - Information is important. e.g. a UK newspaper can be instantly printed anywhere in the world if the information (e.g. in a file) is available. No need to transport newspaper from country A to country B - disintermediation

- New and revolutionary models to market and deliver products/services
  - Example music or film streaming services e.g. SoundCloud, Netflix

Digitisation: Legal challenges of information society

- Traditional legal values based on:
  - Valuable goods being physical, tangible and rivalrous or intangible goods (protected by intellectual property rights) fixed to a tangible carrier (CDs, books etc)

- With digitisation - possible to replace all previous information storage forms/media with bits
  - Valuable content (non-rivalrous goods) separated from traditional carrier (which was rivalrous)
  - Undermines traditional legal models for enforcing intangible, intellectual property rights
  - Legal challenge to protect information that is instantly replicable, transmissible and infinitely scalable.

Digitisation: What are its drivers?

- Fall in cost of storing digital information (bits).
- Fall in cost and speed of transmitting bits across computer networks.
- Rise in consumer demand for greater storage capacity and multi-platform support in digital devices.

Digitisation: What are its drivers?

Information / data is:

- Easier to generate, manipulate, transmit and store information
- Lower cost of collecting, manipulating, transmitting data
- Nature of electronic information has developed an intrinsic value in itself
- Operation of IT systems and networks generate additional digital information (backup copies, cache copies etc)

Digitisation: Information disintermediation

- Traditional distribution: standard chain of manufacturer – carrier (middleman) – e.g. consumption from a shop

- Modern distribution: direct delivery from producer to consumer (*disintermediation*)
  - Direct downloading of products online
  - Middle man in supply chain cut off
  - Push media (websites) vs social networking tools

Digitisation: Convergence

The technological merger of several industries - computers, communications, consumer electronics, entertainment, and mass media - through various devices that exchange information in common electronic, or digital, formats.

ICT Regulation: What is Law?

- **Regulation** – creates, limits, or constrains a right; creates or limits a duty; or allocates a responsibility.
  - Many forms: laws, rules, obligations, social norms etc.

- **Law** – A set of rules that guides/govern our conduct in society and is enforceable through public bodies.

Why is Law important in the ICT sector?

- *Responsibility* (the liability for damages arising from breaches of the law).

- *Trust* (the commercial and personal trust necessary for electronic transactions). Examples of laws fostering trust:
  - The General Data Protection Regulation (EU Regulation 2016/679)

- *Ownership* (of intellectual property and information). Examples of laws ensuring ownership:
  - Trademarks Act, Chapter 597 of the Laws of Malta
  - Patents and Designs Act, Chapter 417 of the Laws of Malta
  - Copyrights Act, Chapter 415 of the Laws of Malta

Type of Laws

- Lex Specialis
- Lex Generalis

Lex Specialis

Examples:

- Computer Misuse
- Net Neutrality
- E-signature laws (EIDAS)
- VFA Framework
- EU AI Regulation

Computer Misuse: Legal Issues related to Computers

- Hacking
- Encryption
- Censorship
- Harassment and DOS Attacks
- Defamation
- Copyright & Trademark infringement
- Privacy & data protection
- Illegal Content
- Hate speech

Computer Misuse as a Crime

- A crime is an act that violates a political, religious, or moral command considered important in protecting the interests of the State or the welfare of its citizens or subjects.

Computer Misuse as a Crime

- A crime or criminal offence - violation of a criminal law

- Criminal law sets out types of behaviour that are forbidden within society and if the behaviour occurs, then punishment will follow

- The State prosecutes in a court of law, a person (defendant) who commits a crime

If found guilty a defendant is also punished by the State (e.g. imprisonment, fine (criminal) etc)

Computer Misuse as a Crime

- The prosecution must prove beyond reasonable doubt all elements of that offence
- The burden of proof is upon the prosecution
- The elements of an offence are:
  - The actus reus (the act)
  - The mens rea (mental state)

Computer Crime

- Crime involving computers and networks – *obtain, store, manipulate, transmit information*

- Illegal behavior committed by means of, or in relation to, a computer system or network

- The perpetrator uses special knowledge about computer technology
  - Includes *cybercrime* = use of special knowledge of cyberspace/internet/computer networks

Computer Crime: Types

- Computer-assisted crimes
  - Computer used to support old criminal activity, without them e.g. fraud, theft, child pornography, copyright infringement

- Computer-focused crimes
  - New crimes emerges as a result of computers e.g. hacking, viruses, denial of service attacks.

Computer Crime: Types

- **Classification of cybercrime (*Council of Europe Convention on Cybercrime 2001*) - the "Budapest Convention"**

1. Offences against the confidentiality, integrity and availability of computer data and systems.
2. Computer-related offences.
3. Content-related offences.
4. Copyright and trademark related offences.

(see ITU, 2012, p12)

Computer Crime: Types

1. Offences against the confidentiality, integrity and availability of computer data and systems.

- Illegal access (e.g., hacking, cracking)
- Illegal data acquisition (e.g., data espionage)
- Illegal interception (e.g., intercepting communications between users)
- Data interference (e.g., deletion of data by viruses)
- System interference (e.g., denial of service attacks)

(see ITU, 2012, p12)

Computer Crime: Types

2. Content-related offences

- Erotic or pornographic material (excluding child pornography) – *depends on a country's laws*
- Child pornography & extreme pornography
- Racism, hate speech, glorification of violence
- Religious offences
- Illegal gambling and online games
- Libel and false information
- Spam and related threats
- Other forms of illegal content

(see ITU, 2012, p12)

Computer Crime: Types

3. Copyright and trademark related offences

- Copyright-related offences e.g. copying of software
- Trademark-related offences e.g. Use of trademarks in criminal activities to mislead users.

(see ITU, 2012, p12)

Computer Crime: Types

4. Computer-related offences

- Fraud and computer-related fraud
- Computer-related forgery
- Identity theft
- Misuse of devices

(see ITU, 2012, p12)

Computer Crime: Types

Europol 2021: Internet organised crime threat assessment (IOCTA)

- Ransomware affiliate programs enable a larger group of criminals to attack big corporations and public institutions by threatening them with multi-layered extortion methods such as DDoS attacks.

- Mobile malware evolves with criminals trying to circumvent additional security measures such as two-factor authentication.

- Online shopping has led to a steep increase in online fraud.

- Explicit self-generated material is an increasing concern and is also distributed for profit.

- Criminals continue to abuse legitimate services such as VPNs, encrypted communication services and cryptocurrencies

Computer Misuse: Criminal Code

- Malta's Criminal Code (Chapter 9, Laws of Malta) regulates computer misuse through 337B-337H
- Based on the UK Computer Misuse Act and the Budapest Cybercrime Convention
- Drafted and defined broadly to account for 'all' scenarios

Unlawful access to, or use of, information – Art. 337C

A person who without authorisation does any of the following acts shall be guilty of an offence

a) **uses** a computer or any other device or equipment to access any data, software or supporting documentation held in that computer or on any other computer, or uses, copies or modifies any such data, software or supporting documentation;

b) **outputs** any data, software or supporting documentation from the computer in which it is held, whether by having it displayed or in any other manner whatsoever;

c) **copies** any data, software or supporting documentation to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

d) **prevents** or **hinders access** to any data, software or supporting documentation;

e) **impairs** the operation of any system, software or the integrity or reliability of any data.

Unlawful access to, or use of, information – Art. 337C

f) **takes possession** of or makes use of any data, software or supporting documentation;

g) **installs**, **moves**, **alters**, **erases**, **destroys**, varies or adds to any data, software or supporting documentation;

h) **discloses** a password or any other means of access, access code or other access information to any unauthorised person;

i) **uses another person's** access code, password, user name, electronic mail address or other means of access or identification information in a computer;

j) **discloses** any data, software or supporting documentation unless this is required in the course of his duties or by any other law.

Unlawful access to, or use of, information – Art. 337C

- Any person who performs any type of operation on a computer system or network, **without authorisation**, shall be guilty of an offence under the Criminal Code if convicted.

- Article 337c provides an exhaustive list of such operations. That said, Art. 337C was drafted in such a manner so as to include any **unauthorised** possession, alteration (not limited to impairment), use or distribution of the system of network.

- Therefore, one should note that the regulator's intention with this clause was to prevent any form of **unauthorized** activity to the computer system or network.

- This has broad implications, ranging from employee activity on their employer's system, intellectual property rights within software, and also criminal activity aimed at hindering such systems.

Pornographic Content Depicting Minors

- Article 204(c) and (d) of the Criminal Code imposes a term of imprisonment between **five** and **ten** years upon whosever:

(c) knowingly causes, for sexual purposes, a person underage to participate in real **or simulated** sexually explicit conduct or exhibition of sexual organs, **including through information and communication technologies**, or

(d) knowingly **attends a pornographic performance** involving the participation of a person under age.

Tech Governance: Net Neutrality

"The principle that data packets on the internet should move impartially without regard to content, destination or source." (Murray, 2013)

Net Neutrality: Advocates

Includes: Consumer groups, content providers, Internet founders

- The internet should be a free an open technology.
- Internet plurality – everyone has the right to free, open access
- Preserves fundamental internet standards
- Preserves end-to-end principle of the Internet
- A tiered system will favour large, well-established content providers who can afford to pay a premium.
- Tiered system will lead to Premium service vs degraded service
- Preferential treatment of certain internet traffic will affect competition and innovation (esp. new entrants).
- Discrimination against certain applications or data types.

Net Neutrality: Opponents

Includes: Many ISPs, Telecoms companies, network operators

- Rise of Internet traffic puts burden on infrastructure hence best to control data rates for different types of content
- Allow allocation of bandwidth for more urgent applications
- Have a tiered system that would prioritise certain types of traffic for those able to pay.
- Revenue gained by premium payers can be used to invest in better networks and improve bandwidth
- Make more efficient use of the network (a limited resource)

Net Neutrality: Regulation

- EU Regulation No. (EU) 2015/2120 of 27th Nov 2015
  - states the principle of open internet access or "net neutrality" for the first time under European law
  - clarifies the set of rights and obligations associated with this principle. Gives some exceptions from basic net neutrality premise. Came into force on 30th April 2016

Net Neutrality: Regulation

- **1.** Enshrines an **end-user's right** to be "free to access and distribute information and content, use and provide applications and services of their choice".
  - Specific provisions ensure that national authorities can enforce this new right.

- **2. ISPs are prohibited from blocking or slowing down of internet traffic**, except where necessary. Exceptions are limited to:
  - traffic management to comply with a legal order,
  - to ensure network integrity and security,
  - to manage exceptional or temporary network congestion, provided that equivalent categories of traffic are treated equally.

Net Neutrality: Regulation

- Internet access providers can implement **reasonable traffic management measures** to enable an efficient use of network resources and the optimization of overall transmission quality.

- '**reasonable**' means:
  - Must be transparent, non-discriminatory and proportionate,
  - Must not be based on commercial considerations but only on objectively different technical quality of service requirements.
  - Must not monitor the specific content of traffic.
  - Must not be maintained for longer than necessary.

Net Neutrality: Regulation

One of the exceptions to basic neutrality premise:

'**Specialised services**': providers of certain services will have access to special transmission quality if there is network capacity and there will not be an adverse effect on overall internet access. E.g. critical services such as remote surgery, driverless cars and preventing terrorist activities

Electronic Signatures

- **Electronic signature**: “data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign

- Very broad term and can take many different forms, including:
  - Typing a name into a contract or into an email containing contract terms
  - Clicking an “I accept” button on a website.
  - Pasting a signature (in the form of an image) into an electronic contract.
  - Using a web-based electronic signature platform to generate:
    - an electronic representation of a handwritten signature; or
    - a **digital signature** using public key encryption technology and backed by a digital certificate from the provider (or a trusted third party) verifying the identity of the signatory.

- After the 2016 EU eIDAS law, e-signatures can only be used by natural persons. Legal person (e.g. companies) use eSeals.

Electronic Signatures

- "Digital signatures" are a specific technology implementation of electronic signatures
  - Uses public key infrastructure (PKI) technology to associate a signer with a document & to protect the signed document.
  - It imprints 'time' into the signature stamp.
  - It is unique, Impossible to forgery, easy to authentication, impossibility of denial etc.
  - A "digital signature" offers both signer and document authentication.
    - Signer authentication is the capability to identify the person who digitally signed the document.
    - Document authentication ensures that the document or transaction (or the signature) cannot be easily altered.

eIDAS and Electronic Identification (eID)

- "*Regulation on electronic identification and trust services for electronic transactions in the internal market*" (commonly referred as "e-IDAS" Regulation) replaced the Directive on Electronic Signatures (1999/93/EC) on 01/July/2016

- eIDAS establishes a legal framework to support the **EU-wide recognition of electronic identification schemes (eIDs)** used by Member States

- Ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available

- Mainly targets the public sector

EIDAS: Trust Services

- **Electronic Signature** (eSignature) – used only by natural persons to sign documents in the online world.
- **Electronic seal** (eSeals) - can only be issued to and used by legal persons (companies) to ensure origin & integrity of data/documents. An eSeal is NOT an eSignature of the legal person.
- **Electronic Time Stamps** - electronic time stamps are issued to ensure the correctness of the time linked to data/documents.
- **Electronic registered delivery services** - a secure channel for the transmission of documents bringing evidence of (the time of) sending and receiving the message.
- **Electronic Website authentication** - certificates for website authentication are issued to ensure that users are reassured that behind the website there is a legal person on which trustworthy information is provided.

Virtual Financial Assets (VFAs) Framework

- A framework supporting innovation and new technologies for financial services in the area of crypto-assets.

- Chapter 590 of the Laws of Malta – Virtual Financial Assets Act definitions:

➢ "Distributed Ledger Technology" means "*a database system in which information is recorded, consensually shared, and synchronised across a network of multiple nodes as further described in the Act (chapter 590 of the Laws of Malta)*."

➢ "DLT asset" means *"(a) a virtual token; (b) a virtual financial asset; (c) electronic money; or(d) a financial instrument, that is intrinsically dependent on, or utilises, Distributed Ledger Technology*".

Virtual Financial Assets (VFAs) Framework

The legal framework:

- Introduction of a Financial Instrument Test with the objective to determine whether a DLT asset, based on its specific features, is encompassed under (i) the existing EU legislation and the corresponding national legislation, (ii) the Virtual Financial Assets Act or (iii) is otherwise exempt.
- The Test is applicable to (i) issuers offering DLT assets to the public or wishing to admit such DLT assets on a DLT exchange in or from within Malta; and (ii) persons providing any service and/or performing any activity, within the context of either the VFA Act or traditional financial services legislation, in relation to DLT assets whose classification has not been determined.

Virtual Financial Assets (VFAs) Framework

The VFA Framework establishes three types of authorisations, being (i) registration of VFA Agents, (ii) registration of Whitepapers, and (iii) applications of VFA Services Providers.

Proposed EU Law on Artificial Intelligence

- Proposed law: focuses on 2 areas: excellence in AI and trustworthy AI. The European approach to AI will ensure that any AI improvements are based on rules that safeguard the functioning of markets and the public sector, and people's safety and fundamental rights.

- Commission published its AI package in April 2021, proposing new rules and actions to turn Europe into the global hub for trustworthy AI. This package consists of:
  - a Communication on Fostering a European Approach to Artificial Intelligence;
  - the Coordinated Plan with Member States: 2021 update;
  - a proposal for an AI Regulation laying down harmonised rules for the EU (Artificial Intelligence Act).

Proposed EU Law on Artificial Intelligence

The AI Regulation:

- lays down harmonised rules for the EU (Artificial Intelligence Act)
- was announced by the Commission in April 2021
- addressed risks of specific uses of AI, categorising them into 4 different levels: unacceptable risk, high risk, limited risk, and minimal risk

Proposed EU Law on Artificial Intelligence

The AI Regulation:

- "artificial intelligence system" (AI system) means "*software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;*"

Proposed EU Law on Artificial Intelligence

Examples of prohibited AI practices in the law:

- the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm
- the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives
- the targeted search for specific potential victims of crime, including missing children

Proposed EU Law on Artificial Intelligence

What are considered as high risk AI Systems?

- AI systems shall be considered high-risk where both of the following conditions are fulfilled:
- (a)the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II; and,
- (b)the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II.

Proposed EU Law on Artificial Intelligence

Further compliance requirements for high risk AI Systems

- Examples:
- Risk management systems in place
- Data and data governance systems in place
- Technical documentation required
- Requirements for transparency and provision of information to users
- Human monitoring / oversight
- Further requirements for robust cybersecurity measures

Lex Generalis

Examples:

- Intellectual Property Laws
- Data Protection Laws

Intellectual Property Law

- **IP** - The results of intellectual activity in the industrial, scientific literary or artistic fields. Creations of the mind – e.g. inventions, artistic works, literary works, designs, images etc.

- **IP - intangible assets, different to physical property**
  - Non-rivalrous – consumption of asset by X does not affect consumption by Y.
  - Non-exclusive – X cannot prevent Y from consuming asset.

- **An IP right is a right :** (i) That can be treated as property (ii) To control particular uses and (iii) of a specified type of intangible asset.

- IP rights granted to creator(s) of work and enforced by both civil and criminal law.

Intellectual Property Law

- In Favour: *Granting of IP Rights*

  - To reward authors for their work
  - To prevent someone taking credit for the work of another
  - To encourage & facilitate innovation, creativity & individuality.

- Against

  - Creating monopoly situations in the market place
  - Inadequate supply to meet demand in the market.

Intellectual Property Law

Main Forms:

- Patents
- Copyright
- Database Right
- Trademarks
- Registered Designs
- Trade Secrets
- Breach of confidence
- Passing off

Intellectual Property Law: Copyrights

- Copyright Act, Chapter 415 Laws of Malta

- Copyright is a property right that exists in works that can be protected by copyrights. Examples:
  - (a) paintings, drawing, maps, plans, sculptures etc
  - (b) audiovisual works
  - (c) computer programs

- Copyright cannot be used to protect an 'idea'

- Copyright protection is available only once the idea/work exists in some tangible or permanent form (written or recorded) = fixation

Intellectual Property Law: Copyrights

The owner of the copyright in a work has the exclusive right to prevent others from doing the following (amongst others):

- copy the work
- issue copies of the work to the public
- rent or lend the work to the public
- perform, show or play the work in public

Intellectual Property Law: Copyrights

- Moral rights relate to the ability of authors to control the eventual fate of their works.
- They cannot be sold/transferred but can be waived.
- They must be asserted by the copyright owner.

Intellectual Property Law: Copyrights

Exceptions to Copyright : Fair Dealing example

- Reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the rightsholders receive fair compensation which take account of the application or non-application or technological measures to the work or subject-matter concerned.

Intellectual Property Law: Trademarks

- Trademarks Act, Chapter 597 of the Laws of Malta
- They allow consumers to distinguish between competing products and services in a market economy
- Distinctive - Goods marks / service marks
- Signs capable of being represented graphically which is capable of distinguishing goods or services of one undertaking from another. A trademark may, in particular, consist of words, slogans, designs, combined marks etc.
- Different methods of trademark protection: national, EU-wide, international

Intellectual Property Law: Trademarks

- Infringement: use of identical/similar mark in relation to identical/similar goods

Existing Trade Mark vs Proposed Mark	Goods/Services	Other Factor
Identical	Identical	N/A
Identical	Similar	Likelihood of Confusion
Similar	Identical or Similar	Likelihood of Confusion
Identical or Similar	Identical, Similar or Different	Reputation in & use for unfair advantage, detriment to reputation

Intellectual Property Law: Patents

An exclusive right to use and exploit an invention provided that that the essential elements for patentability exists where the invention:

- is new (Novelty)
- involves an inventive step going beyond state of the art
- is capable of industrial application

Exclusions – Non-patentable material :

- a discovery
- scientific theory
- mathematical method
- any aesthetic creation (e.g. artistic, musical work)
- any method of performing a mental act, playing a game or doing business
- the presentation of information

Intellectual Property Law: Domain Names

- ICANN (Internet Corporation for Assigned Names and Numbers) - passes responsibility to registrars.
  - Over 1500 accredited registrars worldwide each with own policies and procedures.
  - A registrant registers a domain name.
  - A registrar is an accredited company that takes your registration request and reserves your domain for you at the main registry (to which it is contracted).
  - A registry, operates the central database of a TLD
    - A Registry has a contract with ICANN to manage a TLD.
    - National registries: UK: Nominet; Malta: NIC Malta

Intellectual Property Law: Domain Names

- Domain names allocated on a first come first serve basis to genuine registrants.

- A domain name is an address to a server to identify an entity (person, company, organisation) online.

- When trademarks are used in domain names without the authority of the trademark owner then trademark law can be used to stop use of the offending domain name

Intellectual Property Law: Domain Names

- With regards to domain names there are several commonly accepted disputes that arise:
  - Domain name envy
  - Cyber squatting
  - Parasites
  - Typosquatting
  - Domain name hijacking
  - Reverse domain name hijacking
  - Parody
  - Sucks.com disputes

Intellectual Property Law: Domain Names

- Parasites - registering a domain name similar to a famous name.
- E.g: Court objected to the use of www.yahooindia.com as a domain name because of its similarity with www.yahoo.com.

- Typosquatting – registering domain names with common typos of major domain names to attempt to divert traffic to sites that benefit the registrant.
  - 1999 US case: *painewebber.com* took action against a site with the domain name wwwpainewebber.com,
  - E.g: *www.cmn.com* ; *www.mcdonolds.com; microsotf.com*

- Sucks.com disputes - Not an official company site but run by an individual to rubbish the company concerned. E.g. microsoftsucks.com

Data Protection

- Data Privacy vs. human rights law

What is Personal Data?

- Personal Data

Any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Key Definitions

- Special Categories of Personal Data

Personal Data that reveals race or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health or sex life

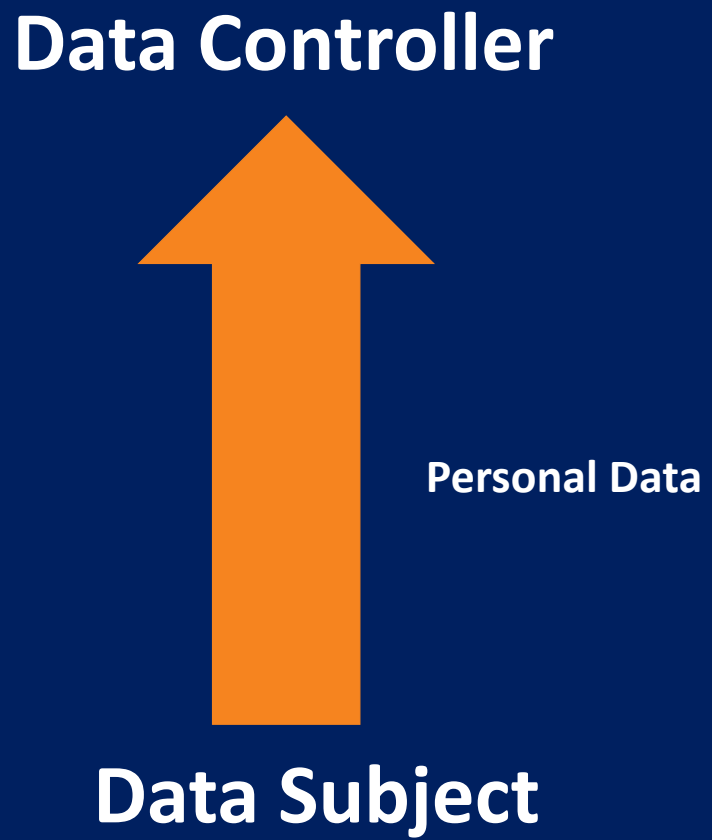
Processing

Use	Blocking	Retrieval	Destruction
Recording	Erasure	Storage	Gathering
Dissemination	Combination	Disclosure	Collection
Alignment	Adaptation	Organisation	Alteration

Data Controller

A natural or legal person, public authority, agency or other body

which, alone or jointly with other, determines the purposes and means of the processing of personal data



Principles of Accountability – Art 5 GDPR

1. **Fair** and **lawful** processing
2. Data collected for **specific, explicitly stated, and legitimate purposes**
3. Data not processed for any purpose that is **incompatible** with the reason for collection
4. Processing **adequate** and **relevant** for the purposes of processing
5. No more data is processed **than is necessary** and is **not kept for a period longer than necessary**
6. **Correct** and **up-to-date**
7. All reasonable measures are taken to **complete**, **correct**, **block** or **erase** data to the extent that such data is incomplete or incorrect
8. processed in a manner that **ensures appropriate security** of the personal data

Lawfulness of Processing – Art 6 GDPR

Six available lawful bases for processing:

- Data Subject Consent

or

- Processing 'necessary' for:
  - The performance of a contract;
  - Compliance with a legal obligation at law on DC;
  - Vital interests of the DS;
  - Performance of a task carried out in the public interest;
  - Legitimate interest of the data controller or a third party

Data Subject Rights

- ✓ Right to Information (Privacy Notices)
- ✓ Right to Access (DSARs)
- ✓ Right to Rectification
- ✓ Right to Withdraw Consent
- ✓ Right to Erasure (to be Forgotten)
- ✓ Right to Portability
- ✓ Right to know about Profiling
- ✓ Right to Object

Security and Data Breaches

- A Data Breach

a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

- Notification to the IDPC

(72 hours from awareness)

- Notification to Data Subjects

High risk

Policies

- Backup policy
- Call recordings policy
- CCTV/ANRP monitoring and recording procedure
- Clear screen and clean desk policy
- Complaint submission form
- Complaints register
- Data breach procedure
- Data breach register
- Data portability request procedure
- Data protection policy
- Data subject access request procedure and form

Policies

- DPIA policy
- DPIA register
- Employee policy
- GDPR training policy
- IT security policy
- Joiners, movers and leavers procedure
- Retention policy
- Vehicle tracking policy
- Website privacy policy, terms of use and cookies
- Collection of consent, recording and withdrawal

Auditing – why is it necessary?

Before you can do anything you must establish:

1. Exactly what data you are dealing with;

2. Whether you are a data controller or processor; and

3. Why you've come to those conclusions.

Cross-Border Transfers Limitation

Principle:

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

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, and Uruguay as providing adequate protection.

Transfers subject to appropriate safeguards

Certification

Legally Binding Instrument between authorities

Compliance with a Code of Conduct

Binding Corporate Rules

Standard Clauses adopted by Supervisory Authority

Standard Clauses adopted by the Commission

Any Questions?

Diploma in Law (Malta)

CAMILLERI PREZIOSI

ADVOCATES