

Information & Communication Technology Law

An Introduction to Data Protection Legislation & Freedom of Information

Lecturer: **Alexia Valenzia**

Date: **23rd May 2022**



Diploma in Law (Malta)



CAMILLERI PREZIOSI
ADVOCATES

MAMO TCV
ADVOCATES

Privacy or Data Protection?



Privacy

- Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties.
- The right to privacy or private life is enshrined in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (Article 8) and the European Charter of Fundamental Rights (Article 7).



Universal Declaration of Human Rights (Art 12)

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

European Charter of Fundamental Rights (Art 7)

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



The European Convention of Human Rights (Art 8)

Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.



Privacy

- In the EU, human dignity is recognised as an absolute fundamental right. In this notion of dignity, privacy or the right to a private life, to be autonomous, in control of information about yourself, to be let alone, plays a pivotal role. Privacy is not only an individual right but also a social value.
- Historically, in other parts of the world, such as the U.S.A., privacy has often been regarded as an element of liberty, the right to be free from intrusions by the state (ironically enough).
- This distinction between Europe and other parts of the world is relative since it is also an element of privacy in the EU.



Data Protection

- Data protection is about protecting any information relating to an identified or identifiable natural (living) person, including names, dates of birth, photographs, video footage, email addresses and telephone numbers. Other information such as IP addresses and communications content - related to or provided by end-users of communications services - are also considered personal data.
- The notion of data protection originates from the right to privacy and both are instrumental in preserving and promoting fundamental values and rights; and to exercise other rights and freedoms - such as free speech or the right to assembly.
- Data protection has precise aims to ensure the fair processing (collection, use, storage) of personal data by both the public and private sectors



Data Protection

- Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union provide that everyone has the right to the protection of personal data concerning him or her.
- The entry into force of the Lisbon Treaty in 2009, gave the Charter of Fundamental Rights the same legal value as the constitutional treaties of the EU. Thus the EU institutions and bodies and the Member States are bound by the Charter.



Art 8(1) of the Charter of Fundamental Rights of the EU

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.
3. Compliance with these rules shall be subject to control by an independent authority



Art 16(1) of the Treaty on the Functioning of the EU

Everyone has the right to the protection of personal data concerning them.



Key Differences

- The two rights differ in their formulation and scope. The right to respect for private life consists of a general prohibition on interference, subject to some public interest criteria that can justify interference in certain cases.
- The protection of personal data is viewed as a modern and active right, putting in place a system of checks and balances to protect individuals whenever their personal data are processed.
- The processing must comply with the essential components of personal data protection, namely independent supervision and the respect for the data subject's rights.



Key Differences

- The right to personal data protection comes into play whenever personal data are processed – it is thus broader than the right to respect for private life.
- Any processing operation of personal data is subject to appropriate protection. Data protection concerns all kinds of personal data and data processing, irrespective of the relationship and impact on privacy.
- Processing of personal data may also infringe on the right to private life, as shown in the examples below. However, it is not necessary to demonstrate an infringement on private life for data protection rules to be triggered.



Key Differences

- The right to privacy concerns situations where a private interest, or the “private life” of an individual, has been compromised.
- The concept of “private life” has been broadly interpreted in the case law, covering:
 - intimate situations;
 - sensitive or confidential information;
 - information that could prejudice the perception of the public against an individual;
 - aspects of one’s professional life and public behaviour.



A Brief History

- In 1970, the German state of Hesse enacted the world's first Data Protection Act. The other states soon followed, and on 1 January 1978, the first German Federal Data Protection Act (BDSG) entered into force.
- On 28 January 1981 the treaty regarding the protection of individuals with regard to automatic processing of personal data was signed as Council of Europe Convention 108 and went into effect on 1 October 1985.
- In 1983, the German Federal Constitutional Court held that the individual has a constitutional right to 'informational self-determination'.



A Brief History

- On 24 October 1995, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data was created as an essential element of EU privacy and human rights law.
- The directive came into force on 13 December 1995 and required EU member states to implement the corresponding provisions in national law by 24 October 1998.
- On 1 December 2009 the Article 29 Working Party and the Working Party on Police and Justice released the “Future of Privacy” paper as a response to the invitation for consultation by the European Commission on the new challenges for personal data protection.



Modern Data Protection Laws

- On the 27 April 2016, the European Commission adopted the General Data Protection Regulation, which entered into force, 20 days after publication in the Official Journal of the EU. The GDPR has been applicable since the 25 May 2018, after which organisations were obliged to adhere to the principles found therein.
- The GDPR provides a high level of data protection and is directly applicable in all EU member states. Companies (outside the EU) may also be subject to the GDPR if the establishment of a company is collecting personal data of an EU Member State or is addressing the EU market even if this establishment is located outside of the EU.



Data Protection in the Digital Age

- Despite its multiple benefits, the digital age also poses challenges to privacy and data protection, as huge amounts of personal information are being collected and processed in increasingly complex and opaque ways.
- Technological progress has led to the development of massive data sets that can be easily cross-checked and further analysed to look for patterns, or for the adoption of decisions based on algorithms, which can provide unprecedented insight into human behaviour and private life.



Data Protection in the Digital Age

- State authorities undertaking mass surveillance activities that may make use of these technologies are an example of the significant impact these technologies can have on the rights of individuals.
- In 2013, Edward Snowden's revelations on the operation of large-scale internet and phone surveillance programmes by intelligence agencies in some states sparked significant concerns about the dangers surveillance activities entail for privacy, democratic governance and freedom of expression.
- Mass surveillance and technologies allowing for globalised storage and processing of personal information and bulk access to data may impinge on the very essence of the right to privacy.



Data Protection in the Digital Age

- In 2015, the European Data Protection Supervisor launched several initiatives aimed at assessing the impact of big data and the Internet of Things on ethics.
- Notably, it has set up an Ethics Advisory Group that aims to stimulate “an open and informed discussion on digital ethics, which allows the EU to realise the benefits of technology for society and the economy and at the same time reinforces the rights and freedoms of individuals, particularly their rights to privacy and data protection.”



Introduction to Big Data



Big Data

- The term “big data” commonly encompasses the growing technological ability to collect process and extract new and predictive knowledge from great volume, velocity, and variety of data. The concept of big data therefore covers both the data themselves and the data analytics.
- The sources of the data are of various types, and include people and their personal data, machines or sensors, climate information, satellite imagery etc. A great deal of such data, however, is personal data which ranges from anything from a name, photo, e-mail address, GPS data, social media posts etc.



Big Data

- Big data also refers to the processing, analysis and evaluation of the masses of data to gain useful information for the purposes of big data analysis.
- This means that the data and information collected can be used for purposes than those originally intended, e.g. statistical trends, or more tailored services such as advertising.
- Big data analysis brings about a new quantitative dimension of data, one which can be evaluated and used in real-time, for example, to deliver tailored services to consumers.



Profiling and Targeted Advertising

- Profiling based on big data involves looking for patterns that reflect “characteristics of a type of personality”. For example, when online shopping companies propose products “you may also like” based on information gathered from the products previously placed into a customer’s shopping cart.
- Modern psychography (the science of studying personalities) uses certain techniques, on the basis of which it determines the types of character dealt with. This information profiles the person in question, which is then complemented by supplementary information acquired for sources such as data brokers, social networks, music listened to online etc.



Positive Aspects of Big Data

- Big data analytics can reveal patterns between different sources and data sets, enabling useful insights in areas like science and medicine. This is the case, for example, in fields such as health, food security, intelligent transport systems, energy efficiency or urban planning.
- In research, new insights can be gained by combining large amounts of data and statistical evaluations, especially in disciplines in which a great deal of data have, until today, only been evaluated manually



Risks

- Risks may include the mishandling of big data by those with access to the mass of information through manipulation, discrimination or oppression of individuals or specific groups in society.
- Where masses of personal data or information about individual behaviour are collected, processed and evaluated, their exploitation can lead to significant violations of fundamental rights and freedoms going beyond the right to privacy.
- The GDPR includes provisions on the right not to be subject to automated decision-making, including profiling.



The “Three Vs”

- Big data also carries risks, generally associated with its “three Vs” attributes: volume, velocity and variety of the data processed.
- The volume refers to the amount of data processed, variety to the number and diversity of types of data, while velocity refers to the speed of data processing.
- Specific considerations for data protection arise notably when big data analytics are used on large sets of data to extract new and predictive knowledge for decision-making purposes concerning individuals and/or groups.



Impact on Data Protection Principles

- The nature, analysis and use of big data described above challenge the application of some of the traditional, fundamental principles of European data protection law. Such challenges mainly relate to the principles of lawfulness, data minimisation, purpose limitation, and transparency.
- The principle of data minimisation requires personal data to be adequate, relevant and limited to what is necessary for the purposes for which they are processed. However, big data's business model may be the antithesis of data minimisation, as it requires more and more data, often for unspecified purposes.



Impact on Data Protection Principles

- The same applies to the principle of purpose limitation, which requires that data must be processed for specified aims, and cannot be used for purposes that are incompatible with the initial purpose of collection, unless such processing is based on a legal ground – such as consent of the data subject.
- Big data also challenges the principle of accuracy of data, as big data applications tend to collect data from a variety of sources without having the possibility to check and/or maintain the accuracy of the data collected.



Questions

- Differentiate between the right to privacy and the right to the protection of one's personal data.
- Name a few historic milestones regarding data protection legislation.
- Describe the main risks associated with 'Big Data' and how these effect data processing principles.



The Freedom of Information Act



Freedom of Information

- The Freedom of Information Act (Cap. 496) (the “FOIA”) gives the general public the right to request documents or information from public authorities. There are specific limitations to this right, while a number of obligations are imposed on public authorities.
- Eligible persons are entitled to submit Freedom of Information (“FOI”) requests to all established Public Authorities. In order to be eligible to submit FOI requests, a person has to be a resident in Malta and to have been so for a period of at least five years.



Freedom of Information

- When submitting a FOI Request, applicants will be required, apart from providing contact details, to give an indication of the document or information that they wish to obtain.
- Applicants will also need to indicate the format in which they wish to receive such document or information, namely as a hard copy/print-out, as an electronic copy, in the form of a summary or by on-site inspection of the document / information in question.



Formal Requirements

- Art. 6 of the FOIA provides for certain formalities in order for a request to be deemed valid. Any FOI requests shall:
 - Be delivered in writing (including post and e-mail) to an office of the public authority;
 - Contain information concerning the requested document to enable its identification;
 - Include a copy of the applicant's ID;
 - Specify the address at which the applicant shall receive notices;
 - Include any fees due.
- Applicants shall not be required to justify or give any reasons for their request.
- The public authority is obliged to take reasonable steps to assist the applicant, where the application does not comply with the above.



Fees

- The Authority may charge 'reasonable' fees for the applicant to access the requested document. Art. 9(2) regulates such fees, whereby they may not exceed the average cost of making the documents available.
- Applicants have the right to complain to the Commissioner if they feel that the fee imposed is excessive, depending on the nature of the requested document.
- If the Authority fails to meet the prescribed time period to respond, it shall not charge any fees for access to the documents.



Decisions and Exemptions

- Art. 10 of the FOIA requires that the Authority shall inform the applicant as to whether their request has been granted (or otherwise) within 20 working days.
- If a request is made to the wrong department, or if the requested document is held by another Authority, the request shall be transferred within 10 working days, which shall not effect the abovementioned period. The applicant must be informed of this transfer.
- The 20 day limit may be extended by up to 40 working days if the request is for a large number of documents which and meeting the original time limit would unreasonably interfere with the Authority's operations.
- The applicant must be informed of this extension, and that they have the right to lodge a complaint with the Commissioner.



Exceptions

- Art. 14 FOIA provides for several exceptions to the general right to information. These include:
 - That the document is exempt;
 - There is 'good reason' for withholding the document;
 - The Authority does not confirm nor deny the document's existence;
 - The document is publicly available or will be so within **3** months;
 - The resources required to locate/examine/copy the document would unreasonable divert the Authority's resources from its other operations;
 - The document is not held by the Authority;
 - The claim is frivolous or vexatious.



Exempt Documents

- The FOIA shall not apply to certain documents, such as those:
 - Held by a Local Council;
 - Subject to the Freedom of Access to Information on the Environment Regulations;
 - Transferred to the National Archives;
 - Accessible to the public;
 - Available for purchase;
 - Held by a commercial partnership in which the Government or another public authority has a **controlling interest**, in so far as the documents in question relate to the **commercial activities** of the commercial partnership;
- Documents which contain personal data are also exempt, provided that (where possible), the applicant should be provided a copy with any personal data redacted.



Exempt Documents

- Additionally, the FOIA shall not apply to documents held by:
 - The Electoral Commission;
 - The Employment Commission;
 - The Public Service Commission;
 - The Office of the Attorney General;
 - The National Audit Office;
 - The Security Service;
 - The Broadcasting Authority;
 - The Ombudsman



'Good Reasons' to not Disclose

- Documents containing certain sensitive information are also considered as being exempt documents. These include documents relating to (or which could effect):
 - National Security/Defence/International Relations;
 - Cabinet documents;
 - Enforcement of the law & public safety;
 - Documents subject to legal professional privilege;
 - Material obtained in confidence;
 - Business affairs, the economy and research.



The Objective Test

- Part VI FOIA provides additional reasons for withholding certain information. What is important here is the objective test imposed through Art. 35(2).
- Therein, a document may be withheld only if it contains matters in relation to which the public interest that is served by non-disclosure outweighs the public interest in its disclosure.
- Therefore, before relying on the following defences, the Authority must conduct a balancing test to determine (and justify) its decision to withhold information.



Additional Reasons for Withholding

- A document is an exempt document if its disclosure would disclose matters relating to:
 - Internal working documents for the deliberative process of the Government;
 - Financial or property interests of public authorities, the disclosure of which would have substantial adverse effects;
 - Certain operations of public authorities which would be prejudiced should they be disclosed such as negotiations.
- Note that the above are subject to the aforementioned test, and may not be relied upon as standalone reasons.



Frivolous or Vexatious Requests

- On a high-level basis, the five (5) main considerations employed by the Courts in determining whether a request is vexatious are as follows:
 - Can the request fairly be seen as obsessive?
 - Is the request harassing the authority or causing distress to staff?
 - Would complying with the request impose a significant burden in terms of expense and distraction.
 - Is the request designed to cause disruption or annoyance?
 - Does the request lack any serious purpose or value?



Frivolous or Vexatious Requests

- The main factor in determining whether a request is to be regarded as vexatious is whether or not such a request inflicts an **unjustified** (disproportionate) disruption or burden (irritation) on the Authority.
- The initial consideration in this regard should be whether there was a reasonable belief that the information sought would be of value to the requester, the public or any section of the public.
- If a relevant motive could be discerned with a sufficient degree of assurance, it might be evidence from which vexatiousness could be inferred. If a requester pursues his rights out of vengeance it might be said that his actions were improperly motivated but also that his request was without any reasonable foundation.



The Burden

- One must consider the history of the particular request as inextricably linked with the previous course of dealings. This should be considered in tandem with:
 - the number
 - breadth
 - pattern and
 - duration of the request.
- Depending on the amount of requests, one may argue that the requester is bombarding the Authority. A long history of requests is considered in determining the vexatious nature of a request.
- Volume alone is not a decisive factor. A single, wide-ranging may result in the request being considered vexatious.



The Motive

- The motive of the requestor is a significant factor in determining whether a request is vexatious. A request of this nature should not side-step the question of the underlying rationale or justification.
- Vexatiousness may be found where an entirely reasonable request leads on to a series of further requests on allied topics, where such subsequent requests become increasingly distant from the starting point.
- This should be considered together with the applicant's relationship with the Authority and any other requests made, which could imply that the applicant is abusing their right to information.



The Motive

- Note that the presiding judge has the discretion to decide whether ultimately, the FOI request should be deemed as frivolous or vexatious (albeit the aforementioned parameters will assist this consideration).
- Notably, Art. 6(2) of the Act provides that an applicant is free to submit a request with no justification required and that “any beliefs of public authorities as to what are the applicant’s reasons for seeking access shall not affect that request”.
- The generic nature of the final statement entails a degree of uncertainty. It is unclear whether the prohibit pertains to the ability of the applicant to submit an application, or whether its scope encompasses the applicant’s underlying intent as a consideration (when deliberating whether the claim was frivolous or otherwise).



The Value

- The inherent value of the request is another factor which will be considered by the Court. It should also be noted that the weighting of such value may diminish over-time.
- Therefore, Authorities may argue that the request *per se* has no value in terms of the objective public interest. The value of the request is inter-linked with the motive, and should be treated as an extension thereof.
- The weighting of such value may also diminish over time, depending on the context in which the request was made.



Serious Harm or Distress

- While harm or distress is not a prerequisite of vexatiousness, such may also be evidenced by obsessive conduct which harasses or distresses staff, notably if the request is extremely broad.
- This should be considered in tandem with the broader scope of the request, rather than as a standalone. While a request may not cause harm *per se*, one may argue that a multitude of requests induces a level of distress which is disproportionate to the individual rights produced by the FOIA.
- In answering the above, one must remember that the weighting of a particular answer is also taken into consideration. For example, if the 'significant burden' imposed is so great as to inhibit the Authority from functioning properly (to be balanced against its obligations of good governance and sound administration), this would be a sound argument in proving vexatiousness.



Questions

- Are there any formalities attached to applicants' requests?
- Can any fees be charged for such requests? May the applicant seek redress if fees are excessive?
- Detail certain exemptions to the general right to information under the FOIA.
- What does the 'Objective Test' seek to deduce?
- Explain the concept of vexatiousness and include some considerations which the Courts will use.



Liability for Illegal Content Online

- What is “illegal content” is determined by specific legislation at EU level as well as by national law.
- It includes material such as incitement to terrorism, illegal hate speech, child sexual abuse material and infringement of intellectual property rights.
- Certain national laws, such as those regarding online defamation, have been amended in the recent years, providing protection in the online environment.



Exclusion of Liability

- The main form of exclusion or limitation of liability that is proactively used in the online context are contractual solutions.
- One example is when users are requested to accept being bound by online terms and conditions or similar texts, which, to the extent permitted by Maltese law, exclude or limit liability.
- Intermediary service providers of information society services may benefit from the safe harbour protection afforded by the E-commerce Act to conduits, caching and hosting service providers.



Exclusion of Liability

- For instance, where a mere conduit service is provided (a service which consist in the transmission of information provided by the recipient of the service, or the provision of access to a network) the provider may claim a defence from liability in regard to the information transmitted where it does not:
 1. initiate the transmission;
 2. select the receiver of the transmission; and
 3. select or modify the information contained in the transmission
- That said, contingent liability can be extended to ISPs if they fail to act in a way that permits them to claim the defences available under the E-commerce Act. For example, if in providing hosting services the ISP obtains knowledge of the illegal activity and fails to act expeditiously to remove or disable such content.



Content Takedowns





- The E-commerce Act regulates content takedowns in Malta in the safe-harbour defence provisions. There appears to be a widespread practice of taking down content, both at the ISP's own initiative through moderation or similar techniques, and upon receiving a complaint.
- As a general rule, the E-commerce Act provides that no requirement should restrict the freedom to provide unrestricted information society services, and that nothing in the Act should be interpreted as imposing an obligation on information society service providers to monitor the information that they transmit or store or to seek actively facts or circumstances indicating illegal conduct in connection with the activities.



Media and Defamation

**NEW
MEDIA AND
DEFAMATION BILL
IN #MALTA**

KEY POINTS

- ENDS CRIMINAL LIBEL 
- ENCOURAGES MEDIATION IN DEFAMATION CASES 
- WIDENS DEFINITION OF FREEDOM TO EXPRESSION 
- JOURNALISTS CAN NO LONGER BE VICTIM OF MULTIPLE LIBEL ACTIONS FOR SAME ARTICLE 

@MaltaGov



Media and Defamation

- The Media and Defamation Act (Cap. 579) was enacted on the 24th April 2018, repealing the Press Act and establishing a new legal framework for media law, libel, defamation, slander under Maltese law.
- Legislators included a number of definitions of terms which were already present under the old law, including defamation, libel and slander.
- While the old law made reference to 'printed matter', the new law makes use of the term 'written media', which introduces a more technology-neutral approach to Maltese media law.



Media and Defamation

- Art. 3(1) provides that defamatory words in written media shall be deemed to be published and to constitute libel. In the case of actions brought for allegedly defamatory statements, the plaintiff must bring proof of serious harm or a likelihood of serious harm. Art. 9 of the new Act makes it possible for the Court to award, in addition to actual damages, moral damages capped at €11,640, while in cases concerning slander, the cap is set at €5000.
- Art. 12 allows for an action for defamation to be brought against the editor of a website in respect of a statement posted on the website. It is a defence in mitigation of damages for the editor to show that it was not the operator or person who posted the statement on the website.
- That said, defences to the above include;
 - where it was not possible for the plaintiff to identify the person who posted the statement;
 - where the plaintiff gave the editor a notice of complaint in relation to the statement, and
 - where the editor failed to respond to the notice of complaint or did not act in accordance with any provision contained in regulations about such notice



Calculation of Damages

- The Act sets the basis for the calculation of damages by the Court in defamation actions.
- This includes the gravity and extent of the defamation or the extent of the likelihood of injury to the plaintiff's reputation, whether the defendant exercised due diligence before publishing the matter complained of and whether the defendant made or offered to make an apology.
- Where the defendant made an apology and published an unreserved correction before the institution of proceedings, the Court shall not award moral damages in excess of €5,000.



Single Publication

- Art. 13 of the Act introduces the single publication rule which tackles the issue of subsequent publications to the public.
- This precludes the plaintiff from instituting defamation actions for subsequent publications, unless the manner of that subsequent publication is materially different from the manner of the first publication.
- The question of whether the manner of the subsequent publication is materially different or not is left up to the Court to determine, taking into account the level of prominence given to the statement, the extent and likely circulation of the subsequent publication and the method of publication.



Right of Reply

- Art. 15 clarifies certain matters relating to the right of reply and details how it is to be published in newspapers, broadcasts, website and where multiple rights of reply are received.
- The right of reply may be availed of by any person whose actions or intentions have been misrepresented or who has been the victim of defamation or who has had his private life intruded into through a publication.
- It must be availed of by the person aggrieved within 1 month from publication and where it is availed of and an action is still instituted subsequent to the publication of the right of reply, the Court shall take this fact into account in its judgment and any award made therein



Deceased Persons & Criminal Libel

- Art. 17, makes it possible for the parents, siblings, children and heirs of a deceased person to file an action for defamation of a deceased person.
- That said, such persons must still prove that their own reputation was in fact harmed by the statement.
- The Act also abolishes criminal libel from Maltese media law and criminal law. Additionally, pending criminal proceedings are to be discontinued.



Questions

- Are information society services liable for illegal content hosted on their servers?
- How is liability excluded or limited in practice?
- What defences are available to website owners within the Media and Defamation Act?
- What factors are considered when quantifying damages for defamation cases?





Diploma in Law (Malta)



CAMILLERI PREZIOSI
ADVOCATES

MAMO TCV
ADVOCATES