Information & Communication Technology Law

Comparative analysis of common IT & data privacy laws within the EU

Lecturer: Veronica Campbell
Date: 23rd May 2024

Diploma in Law (Malta)

National Measures

- The following aspects of additional measures to the GDPR shall be analysed comparatively in various EU Member States:

1. Additional lawful bases for processing sensitive data;
2. Additional authorisations for processing criminal data;
3. Age of consent;
4. Exemptions for processing relating to big data;
5. Are data protection officers required under local law;
6. Processing relating to employment;
7. Additional sanctions;
8. Consultation with local supervisory authority.

France

- The French Data Protection Act provides that special categories of PD may be processed in the context of:
  - activities which comply with standards set by CNIL;
  - carried out by employers which involve biometric data if strictly necessary for access control to workplace devices and software;
  - public information contained in court decisions, if such processing activities do not aim to identify data subjects.
- Inclusion of further exemptions to the prohibition of processing PD relating to criminal offences:
  - entities collaborating in the public service of justice (such categories of entities to be defined by an implementing decree);
  - victims or defendants (whether natural or legal persons) for the purposes of enabling them to prepare, bring, and follow legal proceedings; and
  - users of public information available in court decisions.

France

- If the minor is less than 15 years old and the processing activity is based on consent, the lawfulness of the processing activity is subject to requirement of a double consent, the consent of the minor and that of the holder of parental rights.

- The DPA allows derogation from GDPR rights granted under Articles 15, 16, 18, 19, 20 and 21 where they render impossible or seriously impair processing of personal data by public archive services for archival purposes in the public interest in accordance with existing relevant French laws.

- No requirements for the appointment of a DPO, beyond GDPR provisions.

- The French DPA does not provide for special laws relating to employment, however, there is no legal basis for processing criminal record background checks.

France

- Additional sanctions include:
  - an injunction to bring processing operations into compliance with the provisions of the Data Protection Act or to answer to data subject requests for the exercise of their rights, accompanied by a fine that may not exceed EUR 100,000 for each day non-compliance is sustained beyond the deadline; and
  - in urgent cases, the possibility for the chairman of the CNIL to ask the restricted committee of the CNIL to take measures as per an emergency procedure that will be defined by a decree to be adopted.

- Prior consultation with the local supervisory authority is required when:
  - Processing of health data;
  - Processing is implemented on behalf of the State and is related to genetic or biometric data necessary for the authentication or control of individual's identity;
  - Processing of social security numbers.

Germany

- No additional lawful bases for processing of sensitive data are provided.

- There is no general additional authorisation under German law for processing of criminal data. Employee's personal data may be processed to detect crimes:
  - only if there is a documented reason to believe the data subject has committed a crime while employed;
  - the processing of such data is necessary to investigate the crime and is not outweighed by the data subject's legitimate interest in not processing the data;
  - The type and extent are not disproportionate to the reason.

Germany

- No changes to the age of consent.
- There are exemptions in relation to the processing of special types of data for research and statistical purposes, however, this must be anonymised as soon as possible, with identifying data stored separately.
- Data controllers and processors are required to designate a data protection officer if they employ at least ten people dealing with the automated processing of personal data.

Germany

- The BDSG permits the processing of personal data of employees for:
  - employment-related purposes;
  - hiring decisions;
  - carrying out termination of employment;
  - exercise or satisfy rights and obligations of employees' representation laid down by law.

The BDSG further stipulates an exemption from Article 9(1) GDPR for employment-related purposes shall be permitted if it is necessary to exercise rights or comply with legal obligations derived from labour law, social security, and social protection law, and there is no reason to believe that the data subject has an overriding legitimate interest in not processing the data.

Background checks with the help of third parties (authorities, former employers) are therefore only admissible if the reliability of the applicant is of particular relevance, for example, in finance and childcare, or where special information is essential for the employment relationship.

Germany

- The BDSG imposes the following additional sanctions:
  - Deliberately transferring or making data that is not publicly accessible or available to a large of people for commercial purposes shall be punishable with imprisonment of up to three years or a fine;
  - processing or fraudulently acquiring personal data of individuals with the intention of enriching oneself shall be punishable with imprisonment of up to two years or a fine.
  - intentionally or negligently failing to treat a request for information properly, or failing to inform a consumer or doing so incorrectly, incompletely or too late shall be deemed an administrative offence punishable by a fine of up to EUR 50,000.

- No prior consultation requirements.

Italy

1. No additional requirements, however the IDPA is entitled to set additional measures concerning the processing of genetic, biometric and health data.

2. Processing of criminal data is authorised in a number of cases:
   - for employment/HR purposes;
   - for the assessment, exercise or defence of a right in court;
   - for mediation aimed at reconciling civil or commercial disputes;
   - to fulfil legal obligations related to the prevention of anti-money laundering and terrorism using financial systems.

3. the IPDPC sets the age limit of 14 years for the purpose of expressing the valid consent for the processing of minors' personal data in relation to the direct offer of services of the information society.

Italy

4. the IDPA may authorise the reuse of data, including sensitive data, for scientific research or statistical purposes by third parties working in the field, when for any reason informing the data subjects proves to be impossible or involves a manifestly disproportionate effort or may seriously affect the objectives of the research, provided that adequate measures to protect data subjects are applied (including preventive minimisation and anonymization measures).

5. Italian law does not require appointment of data protection officers in any situations beyond what is required under the GDPR.

Italy

6. The IDPA is to issues specific guidelines for processing with regards to employment. These have not been issued to date.

7. the IPDPC introduces criminal sanctions in case of:
   - unlawful processing of personal data;
   - unlawful communication and dissemination of personal data processed on a large scale;
   - the fraudulent acquisition of personal data processed on a large scale;
   - falsity in the declarations to the IDPA and interruption of the execution of the tasks or exercise of the powers of the IDPA itself;
   - failure to comply with IDPA provisions; and
   - violation of provisions on remote controls and investigations on workers' opinions.

Italy

8. Prior to commencement of processing on the basis of the legitimate interest of the controller and using new technology or automated processing, shall give notice of such processing to the Data Protection Authority.

The notice shall disclose the object, the purposes and the context of processing. If the Data Protection Authority does not issue a response within 15 days, the controller may proceed with the processing.

If the Data Protection Authority determines that the processing threatens the rights and freedoms of data subjects, it may suspend the processing for 30 days in order to obtain further information and clarifications from the controller.

Notwithstanding the suspension period, if the Data Protection Authority still determines that the processing threatens the rights and freedoms of the data subjects, it has the power to issue an injunction order to stop the processing.

Netherlands

1. The prohibition on processing special categories of personal data will not apply where:
   - the processing is necessary to comply with an obligation under international public law;
   - the data is processed by the DDPA or an ombudsman and this is necessary, for reasons of a compelling public interest, for the performance of the functions entrusted to them by law, and safeguards have been put in place for the processing such that the data subject's privacy is not disproportionately compromised; or
   - processing is necessary in addition to the processing of criminal data for the purposes for which such data are processed.

Netherlands

2. Criminal personal data may be processed on the following grounds:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving its consent;
- processing relates to personal data which is manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity;
- processing is necessary to comply with an obligation under international public law or the data is processed by the DDPA or an ombudsman and this is necessary, for reasons of a compelling public interest, for the performance of the functions entrusted to them by law, and safeguards have been put in place for the processing, such that the data subject's privacy is not disproportionately compromised.

Netherlands

3. No additional changes to the age of consent.

4. In the event that personal data is processed by institutions or service providers for scientific research or statistics, and the required measures have been taken in order to ensure that the relevant personal data can only be used for the statistical or scientific purposes, then Articles 15, 16, and 18 GDPR do not apply to the controller.

5. Data protection officers are not required under local law, over and above the GDPR.

6. No specific rules regarding the processing of data relating to employment/HR.

Netherlands

7. No additional sanctions within national law.

8. No requirements for prior consultation with local supervisory authority.

E-Privacy Directive

- Passed in 2002 and amended in 2009, Directive 2009/136/EC, or the ePrivacy Directive (the "Directive") has become known as the "cookie law" since its most notable effect was the proliferation of cookie consent pop-ups after it was passed.

- From a material point of view, the ePrivacy Directive aims to regulate the processing of electronic communications data arising from the provision and use of electronic communications services.

- Electronic communications services include internet access services, interpersonal communications services and services that consist wholly or mainly in the transmission of signals.

E-Privacy Directive

- the ePrivacy Directive also contains provisions concerning:
  - Information on and about users‘ end devices (especially cookies),
  - the provision of publicly accessible directories of users of electronic communications services, and
  - the sending of direct marketing communications to end-users by means of electronic communications.

- As a special law, the Directive takes precedence over the GDPR. Its provisions supplement and clarify the GDPR with more specific regulations.

E-Privacy Directive

- The Directive is based on the principle of confidentiality of electronic communications data.

- Therefore, any interference (e.g. listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance and processing) with communications data by a person other than the end user is prohibited.

- There are certain exceptions provided for in the Directive (so-called prohibition with reservation of permission).

War on Cookies

What are Cookies?

- Cookies are small text files that websites place on your device as you are browsing. They are processed and stored by your web browser. In and of themselves, cookies are harmless and serve crucial functions for websites. Cookies can also generally be easily viewed and deleted.

- However, cookies can store a wealth of data, enough to potentially identify data subjects without their consent. Cookies are the primary tool that advertisers use to track your online activity so that they can target you with highly specific ads.

- Given the amount of data that cookies can contain, they can be considered personal data in certain circumstances and may be subject to the GDPR.

First-Party vs Third-Party Cookies

- Cookies may be classified by the identity of the entity or website dropping the cookie on the user's device.

- **First-party cookies** are those created and placed on the user's device by the website being visited. They allow the website to personalise the user's website experience by remembering things like: a user's language or location preferences, usernames or passwords to keep users logged in; payment details; or items in a shopping cart; or to manage the performance of the website

- **Third-party cookies** are, as the name suggests, placed on a user's device by a third party (that is, not the owner of the website being visited). The third party supply content (such as images or advertisements), plug-ins or services (such as analytics) to the website being visited.

Cookies Classed by Duration

- Cookies may be temporary and last only as long as a single browsing session on a website, known as "session cookies" - or they may remain on a user's device after the browsing session is closed known as "persistent cookies".

- Persistent cookies send information back to the browser with subsequent sessions across the website or different websites until they expire at the time set by their creator, or are manually deleted by the user (for example, by the user clearing cookies in their browser).

Cookies Classed by Purpose

- Cookies can also be classified as those that are essential, which are sometimes referred to as strictly necessary, and those that are not. “Strictly necessary cookies” or “essential cookies” are those without which a website and its features cannot function.

- For example, cookies that allow websites to remember during a browsing session that a user is logged in, or to remember items in a user’s shopping cart, are strictly necessary so that the website does not require the user to continually log in to access content or so the website knows which items the user is looking to purchase. Strictly necessary cookies are generally first-party cookies.

Cookies Classed by Purpose

- Not all cookies (including first-party cookies) are essential or strictly necessary. Examples of “non-essential cookies” include:

  - preference (or functionality) cookies, which allow websites to remember user preferences, such as for language or location;

  - performance (or analytics or statistics) cookies, which allow website owners to understand how users interact with websites (the pages visited, links clicked on etc.) and thereby improve website functionality. These types of cookies may be first-party or third-party (where provided by third-party analytics services); and

  - marketing / advertising cookies, which are generally a type of persistent third-party cookie that track a user’s online activity, often across networks of websites, to allow advertisers to increase the relevance of advertising presented to users through the creation of an algorithmic profile for the user (see online behavioural advertising).

Processing of Personal Data (Electronic Communications Sector)

- S.L 586.01 transposes Art. 5(3) of the ePrivacy Directive which provides that "[t]he storing of information or the gaining of access to information stored in the terminal equipment of a subscriber or user shall only be allowed on condition that the subscriber or user concerned has given his consent, having been provided by the controller with clear and comprehensive information".

- The exception to this is when the cookie in question is "strictly necessary in order for the service provider to provide an information society service explicitly requested by the subscriber or user to provide the service".

Non-compliant Practices

- The following practices are considered to be non-compliant, and should not be implemented by organisations:

1. Cookie Walls;
2. Pre-ticked boxes;
3. Scrolling;

Cookie Walls

- A “cookie wall” is a banner linked with a website or a mobile app which only allows users to access the latter after the user grants consent to the use of all cookies and to the purposes for which they are processed. In these cases, access to the website or mobile app is not possible through any other means.

- The indiscriminate collection of personal data through this approach, which essentially presents the user with no genuine choice, falls foul of the consent requirements as set out in the applicable laws and it is considered to be an unlawful practice.

- If access to the service is subordinate to the provision of consent, this makes such consent not “freely given”. For consent to be freely given, access to services and functionalities should not be made conditional upon the user’s consent for storing information, or gaining access to information already stored, in the terminal equipment.

Pre-ticked boxes

- Recital 32 of the GDPR states that “silence, pre-ticked boxes or inactivity should **not** […] constitute consent”. Consequently, pre-ticked boxes are not a valid tool to obtain consent under the GDPR specifically regarding cookies.

- Therefore, approach of using pre-ticked boxes is considered to be an unlawful practice. This has also been upheld by the Court of Justice of the European Union in Case C-673/17 wherein it was held that:

  - “consent referred to in those provisions is not validly constituted if, in the form of cookies, the storage of information or access to information already stored in a website user’s terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent”.

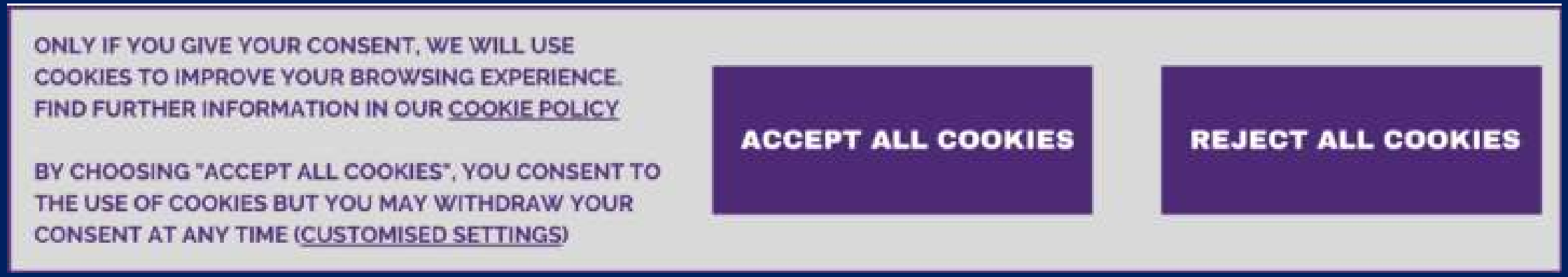
Scrolling

- The practice used to obtain consent by means of a user's action, such as scrolling or swiping through a webpage, does not constitute a "clear and affirmative" act in terms of the requirements of article 7 of the GDPR and as further elaborated in recital 32. Consequently, this approach does not satisfy one of the core requirements of valid consent.

- Organisations must be able to demonstrate that consent was obtained by means of an explicit and unambiguous positive action. Given the impractical nature of separating the precise action, by means of which the user would have given his or her consent from the other user's interactions, such mechanism does not enable the stakeholder to effectively demonstrate that explicit and unambiguous consent has been obtained.

- This practice makes it extremely difficult to grant the user with his right to withdraw the previously given consent, as easily as consent was initially obtained

Good Practice



The banner by means of which consent is sought should be configured to ensure that cookies that classify as non-exempt shall **not** be in use as soon as the user lands on the webpage, but are installed only **after** the user interacts with the banner and duly consents to the use of such cookies.

NOYB – Additional Malpractices

- On 31 May 2020, Max Schrems' organization, NOYB, launched a new campaign aimed at ending what they refer to as the “cookie banner terror”. The campaign was spearheaded by sending over 560 draft complaints to companies who, in their view, use “unlawful” cookie banners.

- NOYB has created a software that automatically identifies what they call "violation types." It notes that this system has the capability of generating up to 10,000 complaints over the course of 2021, and has indicated it will be focusing their attention on the most visited websites in Europe

Deceptive Link Design

- NOYB challenges the use of a hyperlink, instead of a button, in terms of the functionality for rejecting cookies. In its view, users are likely to perceive this hyperlink as not being an actual option and, therefore, only being able to accept all cookies.

- In other words, NOYB considers that users have no genuine choice and are essentially forced into clicking "accept all," and, therefore, that they are misled in giving their consent.

Deceptive Link Design

- Whilst NOYB raises an interesting point on whether links can "nudge" users towards accepting cookies, whether the design of such a link results in a breach of the GDPR is questionable.

- On one level, the GDPR does not provide a format of how consent should be obtained, or how and when the option to refuse should be offered. Companies are free to choose the appropriate format and design for and provision of a link, and for some users this may be a way to allow them to effectively give control over which cookies and processing activities they wish to accept or refuse.

- In addition, the notion here of encouraging users to accept cookies is a subjective one, and leaves room for a wide degree of interpretation by the courts. The accompanying language in the banner is also a factor that should be considered as part of any assessment made, and may help to mitigate against any potential risks of nudging

Deceptive Button Colours and Button Contrast

- NOYB claims that contrasts between button colours on cookie banners results in invalid consent and a violation of the principles of fairness and transparency, as website users may be encouraged to give consent if the "Accept" button has, for example, been clearly highlighted in a certain colour over the other options.

- Design features, such as use of colour and colour contrast, are debated more and more in light of nudging techniques which lead or encourage users to choose certain options. It remains to be seen whether the use of colour and colour contrast in and of itself results in a violation of the GDPR.

- Not all users will experience a website or app, including user interfaces and coloured buttons or banners, in the same way or be (significantly) influenced by colour or contrast use. In any event, as mentioned above, the principle of nudging users is subjective and leaves scope for a variety of viewpoints

Legitimate Interest Claimed

- Another key violation raised by NOYB concerns legitimate interests in the context of cookies. NOYB indicates that any option in which users can opt to rely on legitimate interests should be removed from the cookie banner.

- Under the ePrivacy Directive, consent (as opposed to legitimate interests) is required for the storage of/access to non-essential cookies, and as such reference should not be made to legitimate interests in the banner.

- NOYB does not, however, appear to have addressed subsequent processing of data gained via cookies, including the most appropriate lawful grounds to rely on in this context. Crucially, such rules are separate from the ePrivacy Directive, and seem to fall outside of NOYB's scope of review.

Inaccurate Classification of Cookies

- NOYB seems to argue that some companies have incorrectly classified cookies, and points out that, for example, cookies relating to statistics/advertising are not "strictly necessary" as defined under the ePrivacy Directive.

- NOYB rightly notes that non-essential cookies should be correctly categorized as such, although the broader question relates to the level of granularity required with respect to how non-essential cookies are classified.

- Moreover, supervisory authorities across the EU adopt somewhat diverging views on what constitutes "essential cookies," with some adopting a broader interpretation of what can be deemed "essential" (which may, for example, in certain cases include non-personalized analytics cookies).

E-Privacy Regulation

- The ePrivacy Regulation was first proposed in 2017, but issues over law enforcement access and retention with digital communications data stalled negotiations
- The point of contention between the European Parliament and Council, the EU co-legislators, concerns the capacity of law enforcement agencies to access and retain data from private electronic communications.

Standard Contractual Clauses

New Standard Contractual Clauses

- On 4 June 2021 the European Commission issued its eagerly awaited decision publishing the new Standard Contractual Clauses, ("**New SCCs**") for the GDPR-compliant transfer of personal data to third countries.

- The New SCCs clarify what data exporters and data importers need to assess, and what further steps they need to take, to ensure that protection equivalent to that afforded to personal data in the EU is ensured in the importing country.

The Effect of Schrems II

- The use of SCCs as a means of transferring personal data to third countries has become a critical focus for privacy professionals following the decision of the Court of Justice of the European Union ("**CJEU**") in Schrems II.

- The decision struck down Privacy Shield, which was a key mechanism that allowed for the exchange of personal data between the EU/EEA and the US specifically.

- As a result, many organisations sending personal data to the US could only transfer personal data by means of employing SCCs.

The Effect of Schrems II

- The Schrems II decision cast significant uncertainty just how to legally transfer personal data outside of the EEA, notwithstanding that the SCCs were upheld.

- The New SCCs seek to extend the protections for personal data set out in the GDPR to third countries (who have not secured an 'adequacy' decision from the European Commission) when those third countries process EU citizens' personal data.

Key Obligations

- Clause 8 sets out many of the fundamental protections to which EU personal data is entitled and applies them to data importers. This clause also includes a warranty from the data exporter that it has used reasonable efforts to determine that the data importer can, through technical and organizational measures, meet its obligations under this Clause.

- These New SCCs also incorporate the requirements of Article 28 of the GDPR, and so can also be used as the 'data processing agreement' required to be entered into between controllers and processors.

- Clause 9 deals with any transfers to sub-processors by a processor and is also in line with Art. 28

Key Obligations

- Clause 10 sets out data subjects' rights, which are equivalent to those contained within the GDPR and reflect the obligations imposed upon controllers/processors.

- Clause 11 requires data importers to provide data subjects with an easily accessible contact who is authorised to handle complaint related to the New SCCs. The data importer may also allow data subjects lodge complaints to an independent dispute resolution body.

- If the data subject invokes third party beneficiary rights and files a complaint, the data importers must agree to accept a binding decision under EU or Member State law.

Modular & Docking Clauses

- The New SCCs introduce a ‘modular’ approach, which provide one set of SCCs with various modules, depending on the particular relationship between the data exporter and importer. This shift is a welcome approach, as the previous SCCs did not cater for the complexities of modern data processing chains.

- The optional ‘docking’ clause in Clause 7 enables third-parties to accede to the agreement at any time, provided the existing parties all agree. Previously, parties would need to enter into a new or additional agreement to achieve this.

Access Requests

- The New SCCs include detailed requirements regarding the actions that a data importer must take in the event that it receives a request from a government authority for access to personal data transferred using the New SCCs.

- Clause 14 goes on to require that parties consider:
  - the nature of personal data transferred and purpose for processing;
  - the law and practice of the third country; and
  - any relevant contractual, technical or organisational to supplementary measures implemented.

Ongoing Obligations

- The requirements set out in Clause 14 are ongoing. Hence, if at any point the data importer discovers that adequate protection will not be possible, they must notify the data exporter.

- The data exporter can then either adopt supplementary measures to ensure adequate protection or suspend the transfer if such measures cannot be applied.

Right to be Forgotten - Judgements

- The ‘Right to be Forgotten’ was enshrined in EU law in 2014. If requested, this law dictates that search engines and other directories (such as court judgements) must delete any links to information on an individual, as long as it is ‘inaccurate, inadequate, irrelevant or excessive.’ This ‘delisting’ prevents material from being found through search engines like Google.

- Legal Notice 456 of 2021, referred to also as the “Online Publication of Court Judgments (Data Protection) Conferment of Functions Regulations, 2021” was implemented into the Code of Organization and Civil Procedure (Cap. 12) earlier in 2021. The importance of the legal notice lies in the protection of personal data when on judgment is published online.

Online Publication of Judgements

- In order to be in a full compliance with the Data Protection Act, the Director General (Courts) shall have the function and the power to assess if one person has good reasons to exercise his right of erasure of personal data with respect to the content of a court judgement published online on the website of the Court Services Agency.

- The right of erasure of personal data, which forms part of a court judgment published on the website of the Court Services Agency, entitles its holder to have either the judgement or any part thereof anonymised or the judgment removed from the said website. The Director General (Courts) has the full power to determine if the application for the exercise of right of erasure of personal data can be actually exercised.

Guidelines

- The criteria and considerations to be used in assessing whether the removal, in whole or in part, or the anonymisation of a judgment from the online system is justified are the following:
  1. The reason for the request, which should be explained by the applicant;
  2. The necessity for the judgement to remain on the website for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;
  3. Whether the removal, in whole or in part, or the anonymisation of a judgment from the online system will have a negative impact on other individuals;
  4. The rules of GDPR (Art. 17);
  5. Decisions of International Courts in particular those of the Court of Justice of the European Union (CJEU) and of the European Court of Human Rights (ECHR) regarding the processing of personal data.

Guidelines

- As a rule, the following requirements must be met before approving the removal, in whole or in part, or the anonymisation of a judgment from the online system:
  1. Three years have elapsed from the date of the judgment;
  2. If the convicted person has been sentenced to pay a fine, the fine must be paid;
  3. If an appeal has been lodged from the judgment, the appeal must first be decided and the three years must commence from the date of the judgment of the court of appeal;
  4. In cases where the judgment is a preliminary judgement or subject to other ongoing proceedings, those proceedings must be terminated;
  5. In the event of a conviction for a suspended prison sentence, the operative period must have elapsed;
  6. If the applicant is acquitted, the judgement shall, except on grounds of public interest, be removed shortly after the request is made.

Notification

- The decision shall be communicated in writing to the person making request within thirty (30) days of receipt of the request by the Chief Executive of the Court Services Agency.

- The person making the request shall also be informed that there is a right of appeal from the decision of the Chief Executive Officer of the Court Services Agency to the Commissioner for Information and Data Protection in case the request is rejected.

21 ACADEMY

Diploma in Law (Malta)

21 LAW

CAMILLERI PREZIOSI
ADVOCATES