Information & Communication Technology Law

Lecture Title: The Foundational Concepts of Data Protection Law

Lecturer: Alexia Valenzia

Date: 24 May 2023

Diploma in Law (Malta)

CAMILLERI PREZIOSI
ADVOCATES

Introduction

- **What is Personal Data?**

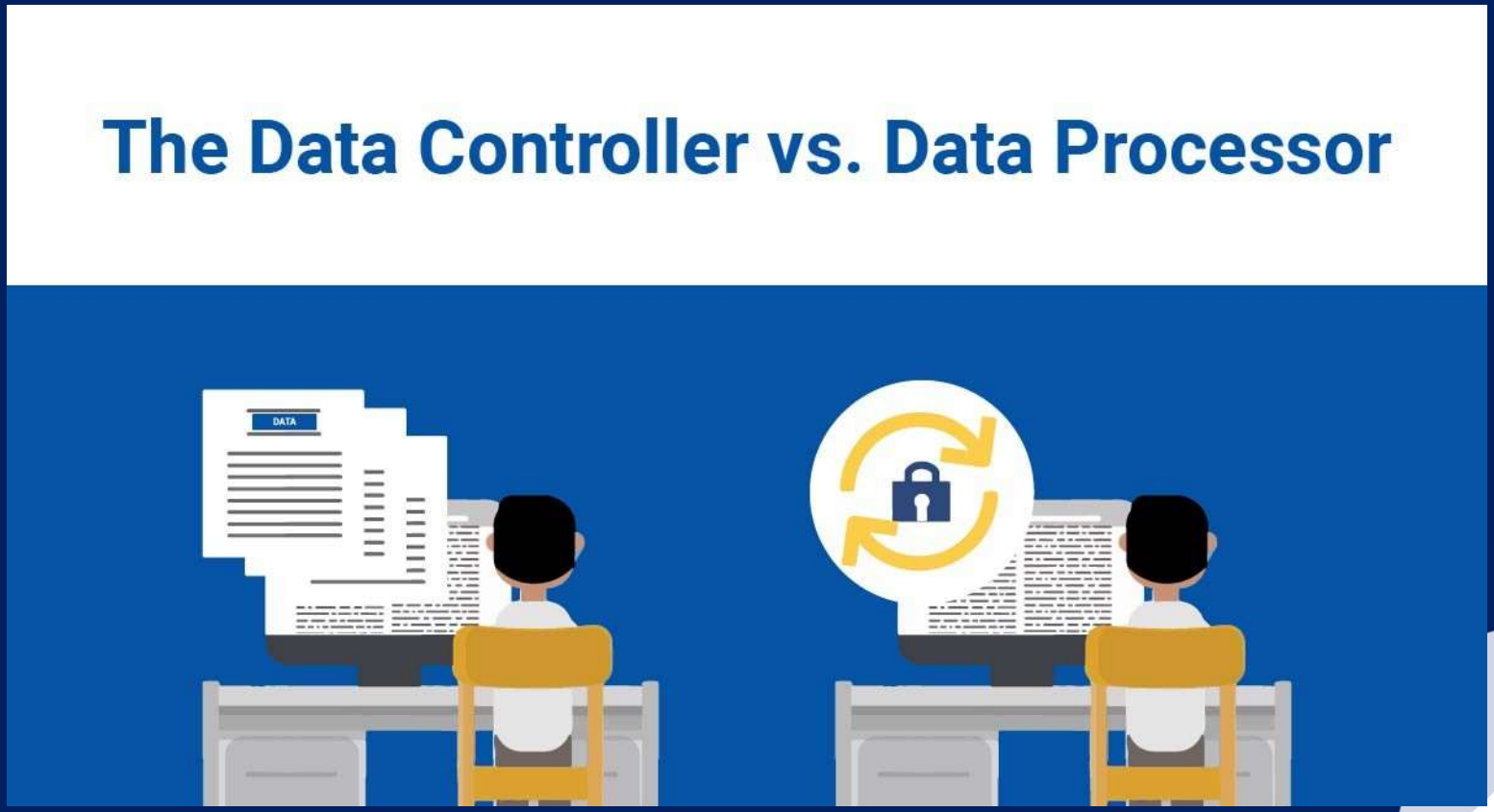
- Data relating to an individual which renders that individual identifiable, either directly or indirectly.
- E.g. Name, surname, email address, phone number, home address
- IP address, vehicle license plate number, ID card number

Introduction

- Processing:

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

Key Roles Within the GDPR



Data Controllers

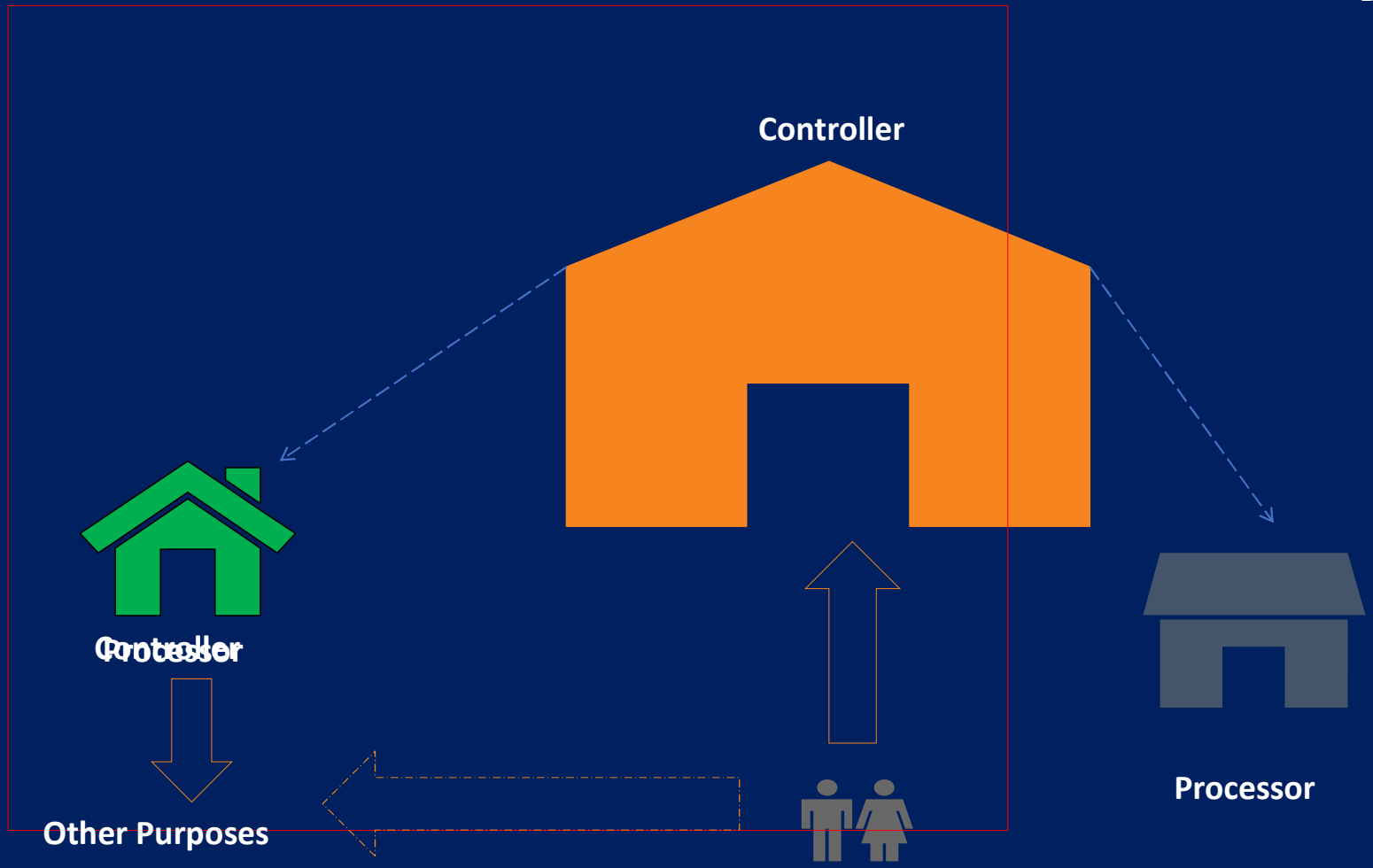
An entity which, alone or together with at least another entity, determines the purposes and means of the processing of personal data

The Different Types of Relationships

1. Data Controller – Data Processor (- Sub Processor)

2. Data Controller – Data Controller

3. Joint Data Controllers - two or more controllers jointly determine the purposes and means of processing


Controller
Processor
Other Purposes

Data Controllers

- The GDPR defines a 'controller' as **natural** or **legal** person…which, alone or jointly, **determines** the **purposes** and (essential) **means** of processing.

- The controller determines the *why* and *how* of processing activities (cumulatively). Therefore, the controller does not need to access the personal data to be qualified as such.

- Certain practical aspects of implementation ("non-essential means") can be decided by the processor.

Responsibilities - Controller

- Art. 12 GDPR obliges controllers to make available their privacy notice to data subjects, which must include specific information such as *inter alia*:
  - Personal data being processed;
  - Intended purpose & Legal basis;
  - Retention period;
  - Data Subject's Rights;
  - Third-party recipients;

- Controllers are responsible to notify data subjects and the IDPC of any breaches if such merits notification under Arts. 33 & 34.

Liability

- Art. 82 of the GDPR provides that:
  - Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
  - Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation.
  - A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

Essential vs. Non-Essential Means

- "Essential means" are means that are closely linked to the purpose and the scope of the processing, such as the type of personal data which are processed, the duration, the recipients and the categories of data subjects.

- Together with the purpose of processing, the essential means are also closely linked to the question of whether the processing is lawful, necessary and proportionate.

- "Non-essential means" concern more practical aspects of implementation, such as the choice for a particular type of hard or software or the detailed security measures which may be left to the processor to decided on.

Essential Means

- Decisions that can only be taken by the controller include the purpose of processing and ‘essential means’, namely:
  - The legal bases of processing
  - The purpose the data are to be used for
  - Which items of personal data to collect
  - The categories of data subjects
  - Whether to disclose the data, and who to
  - Whether data subject rights apply
  - The retention period.
- Typically, though not always, the data controller is the entity that collects the personal data first.

Non-Essential Means

- A processor may decide the ‘non-essential means’, such as:
  - what IT systems or other methods to use to collect data;
  - how to store the personal data;
  - detail of the security surrounding the personal data;
  - means used to transfer the personal data from one organisation to another;
  - the means used to retrieve personal data about certain individuals;
  - the method for ensuring a retention schedule is adhered to;
  - the means used to delete or dispose of the data.

Data Processors

- The GDPR defines a ‘processor’ as a natural or legal person which processes personal data on behalf of the controller.
- Certain obligations directly applicable specifically to a processor, who can be held liable or fined in case of failure to comply with such obligations or in case it acts outside or contrary to the lawful instructions of the controller.
- Role limited to the more ‘technical’ aspects of an operation, such as data storage, retrieval or erasure and can be seen as a service provider to the controller.
- Cannot take any of the over-arching decisions, e.g. what the personal data will be used for or what the content of the data is.

Example – Cloud Service Provider

- A school has decided to use a cloud service provider for handling information in its education services. The cloud service provides messaging services, videoconferences, storage of documents, calendar management, word processing etc. and will entail processing of personal data about school children and teachers.

- The cloud service provider has offered a standardized service that is offered worldwide. The school however must make sure that the agreement in place complies with Article 28(3) of the GDPR, that the personal data of which it is controller are processed for the school's purposes only.

- It must also make sure that their specific instructions on storage periods, deletion of data etc. are respected by the cloud service provider regardless of what is generally offered in the standardized service.

Relationship Between Controllers & Processors

- The controller is obliged to only engage processors who provide sufficient guarantees to implement appropriate technical and organisational measures.

- The controller is responsible for assessing the sufficiency of the guarantees provided by the processor and should be able to prove that it has taken all of the elements provided in the GDPR into consideration.

- The following elements should be taken into account by the controller in order to assess the sufficiency of the guarantees:
  - the processor's expert knowledge;
  - the processor's reliability;
  - the processor's resources.

The Data Processing Agreement.

- Any processing of personal data by a processor must be governed by a contract or other legal act between the controller and the processor, as required by Article 28(3) GDPR, which includes the following:
  - subject matter of processing;
  - duration of processing;
  - nature of processing activity;
  - type of personal data;
  - categories of data subjects;
  - obligations and rights of controller.

- Must contain certain provisions such as the technical and organisational security measures put in place by the processor, deletion of personal data at the request of the controller and specify if personal data is going to be transferred to third entities.

Joint Controllers

- The qualification as joint controllers may arise where more than one actor is involved in the processing. Art. 26 GDPR introduces specific rules for joint controllers and sets a framework to govern their relationship.

- The qualification of joint controllers will mainly have consequences in terms of allocation of obligations for compliance with data protection rules.

- In broad terms, joint controllership exists with regard to a specific processing activity when different parties determine jointly the purpose and means of this processing activity.

- Therefore, assessing the existence of joint controllers requires examining whether the determination of purposes and means that characterize a controller are decided by more than one party.

Example – Marketing Agency

- Companies A and B have launched a co-branded product C and wish to organise an event to promote this product.

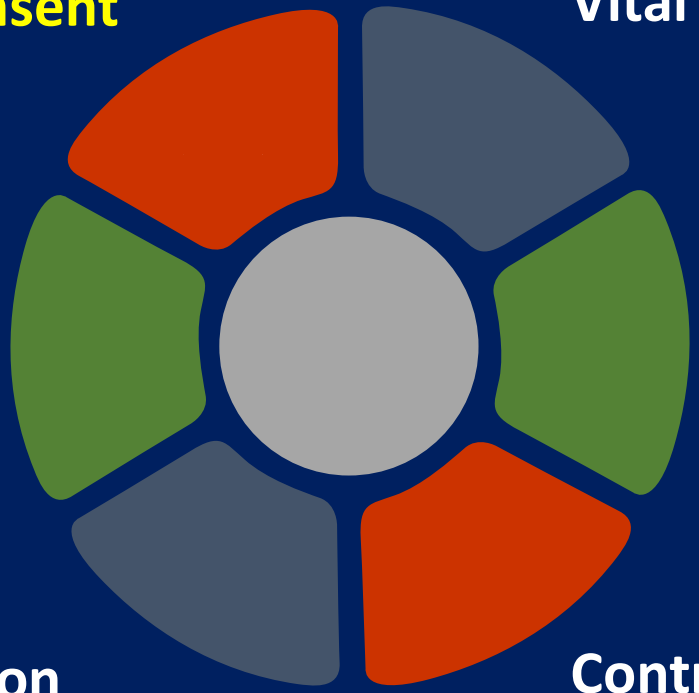
- They decide to share data from their respective clients and prospects database and decide on the list of invitees to the event on this basis. They also agree on the modalities for sending the invitations to the event, how to collect feedback during the event and follow-up marketing actions.

- Companies A and B can be considered as joint controllers for the processing of personal data related to the organisation of the promotional event as they decide together on the jointly defined purpose and essential means of the data processing in this context.

Questions

- What are the main differences between a controller and a processor?
- Distinguish between essential and non-essential means and who can determine these, respectively.
- What obligations do the different roles entail?
- When is a data processing agreement required? Mention some key considerations which must be included therein.
- What types of damages can data subjects claim if their rights have been breached?

The Lawful Bases



Consent

- Consent is one of the six lawful bases to process personal data under the GDPR and is defined as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them”.

- Generally, consent can only be an appropriate lawful basis if a data subject is a genuine choice to accept or decline the terms offered or declining them without detriment. When asking for consent, a controller has the duty to assess whether it will meet all the requirements to obtain valid consent.

- Obtaining consent does not negate the controller’s obligations to observe the principles of processing enshrined in the GDPR.

Elements of Consent

- From the previous definition, one may deduce 4 distinct elements in order for consent to be valid:
  1. Freely given;
  2. Specific;
  3. Informed; and
  4. Unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Freely Given

- The element “free” implies real choice and control for data subjects.
- If the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid.
- If consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given.
- Consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment. The notion of imbalance between the controller and the data subject is also taken into consideration by the GDPR.

Imbalance of Power

- It is unlikely that **public authorities or employers** can rely on consent for processing as there is often a clear imbalance of power in the relationship between the controller and the data subject.

- It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller.

- That said, there are certain exceptional circumstances where consent may be freely given and when it will have no adverse consequences at all whether or not such consent is provided.

Freely Given - Example

- A mobile app for photo editing asks its users to have their GPS localisation activated for the use of its services. The app also tells its users it will use the collected data for behavioural advertising purposes.

- Neither geolocalisation or online behavioural advertising are necessary for the provision of the photo editing service and go beyond the delivery of the core service provided.

- Since users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given.

Specific

- Consent must be given in relation to “one or more specific” purposes and that a data subject has a choice in relation to each of them. This aims to ensure a degree of user control and transparency for data subjects.

- To comply with the element of 'specific’, the controller must apply:
  - Purpose specification as a safeguard against function creep;
  - Granularity in consent requests; and
  - Clear separation of information related to obtaining consent for data processing activities from information about other matters.

Specific - Example

- A cable TV network collects subscribers' personal data, based on their consent, to present them with personal suggestions for new movies they might be interested in based on their viewing habits.

- After a while, the TV network decides it would like to enable third parties to send (or display) targeted advertising on the basis of the subscriber's viewing habits.

- Given this new purpose, new consent is needed.

Informed

- The requirement for transparency is one of the fundamental principles, closely related to the principles of fairness and lawfulness.
- Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent.
- If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing.

Informed - Requirements

- For consent to be informed, it is necessary to inform the data subject of certain elements that are crucial to make a choice. Therefore, the EDPB is of the opinion that at least the following information is required for obtaining valid consent:
  - the controller's identity;
  - the purpose of each of the processing operations for which consent is sought;
  - what data will be collected and used;
  - the existence of the right to withdraw consent;
  - information about the use of the data for automated decision-making;
  - on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards.

Unambiguous Indication of Wishes

- Consent requires a statement from the data subject or a clear affirmative act, which means that it must always be given through an active motion or declaration (such as a tick-box).

- It must be obvious that the data subject has consented to the particular processing. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice.

- When installing software, the application asks the data subject for consent to use non-anonymised crash reports to improve the software. A layered privacy notice providing the necessary information accompanies the request for consent.

- By actively ticking the optional box stating, “I consent”, the user is able to validly perform a ´clear affirmative act´ to consent to the processing”.

Explicit Consent

- Under the GDPR, explicit consent plays a role in processing of special categories of data, the provisions on data transfers to third countries or international organisations in the absence of adequate safeguards in and on automated individual decision-making, including profiling.

- The term explicit refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent.

- A data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature.

Additional Requirements

- The GDPR clearly outlines the explicit obligation of the controller to demonstrate a data subject's consent. The burden of proof will be on the controller.

- The controller must ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time. However, when consent is obtained via electronic means through only one mouse-click etc., data subjects must be able to withdraw that consent equally as easily.

- In cases where the data subject withdraws his/her consent and the controller wishes to continue to process the personal data on another lawful basis, they cannot silently migrate from consent (which is withdrawn) to this other lawful basis. Any change in the lawful basis for processing must be notified to a data subject.

Specific Areas

- In relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 13 years old, as per S.L 586.11.

- In the context of education, any student who has attained the age of 16 years shall be eligible to give their consent, as per S.L 586.07.

Questions

- List and describe the 4 facets of valid consent.
- When is ‘explicit’ consent required?
- Detail the meaning of ‘imbalance of power’ and its repercussions on the validity of consent.
- What is the age of consent under the GDPR? Does this differ in any specific scenarios?

Data Breaches

Data Breaches

- A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

- This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

- Personal data breaches can include:
  - access by an unauthorised third party;
  - deliberate or accidental action (or inaction) by a controller or processor;
  - sending personal data to an incorrect recipient;
  - computing devices containing personal data being lost or stolen;
  - alteration of personal data without permission; and
  - loss of availability of personal data.

Data Breaches

- Most PDBs are caused by human error, such as sending out e-mails to the incorrect recipient.
- Controllers are obliged to notify PDBs within 72-hours of becoming aware of the breach, unless a delay is justifiable.
- Controllers are required to notify the IDPC where a risk to the data subject's rights and freedoms.
- Where the breach results in a high risk to the data subject's rights and freedoms, the data subjects are required to be notified, along with the IDPC

Notification Requirements

- The Notification should include:
  - Description of the nature of the PDB, the categories and approximate number of records concerned.
  - Name and contact details of the data protection;
  - Likely consequences of the PDB;
  - Measures taken or proposed to be taken by the controller to address the PDB, including mitigation measures.

- For the sake of practicality, the following should also be retained, in case of questioning by the Supvisory Authority:
  - Document a register of their processing activities;
  - Retain a copy of employee privacy policies (and any amendments in light of the breach);
  - Dates of employment training records on GDPR and the risks of human errors;
  - Internal technical and organisational measures aimed to prevent such breaches;
  - Any communications to upper management on mitigation measures and training;
  - Action plan going forward.

Managing Risk

- Robust private encryption prior to transmission, which conforms to state-of-the-art. Encryption key-length should reflect the sensitivity of the processed data. Keys are reliably generated, administered, stored and revoked.
- Physical/Virtual Access Control.
- Authentication & Authorisation Control.
- Transmission and Disclosure control.
- Change Management & Database Security.

Questions

- What is a personal data breach?
- Who is obliged to report any breaches (and in what timeframe)?
- Are all breaches notifiable?
- What should be included in this notification?
- Briefly describe the methodology to determine whether a breach is notifiable, or otherwise.
- Mention some risk-mitigating measures which one may implement to avoid or reduce the severity of a breach.

Jurisprudence

Data Transfers

- Personal data may be transferred to countries that have an adequate level of data protection (as determined by the EU Commission).
- Countries subject to an adequacy decision are:

Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom, and Uruguay.

- If not subject to an adequacy decision, transfer safeguards must be relied upon, such as the Standard Contractual Clauses (or SCCs).

What about the US?

- In July 2020, the European Court of Justice ("CJEU") issued its judgement on Case C-311/18 ("Schrems II"). The CJEU confirmed, in principle, that standard contractual clauses ("SCCs") can continue to be used to facilitate the transfer of personal data out of the EEA.

- At the same time, the CJEU imposed due diligence obligations on entities seeking to make such a transfer to assess whether SCCs alone offer sufficient protection in the recipient jurisdiction to comply with GDPR requirements.

- The GDPR contains strict rules on transferring data from the EU to third countries, and this case dealt with the compatibility of these rules with surveillance laws in other countries.

Schrems II – Key Aspects

- Whatever transfer mechanism is being used, the protection afforded to EU citizens' data must be "essentially equivalent" to that within the EU. This means that the standard of protection for EU citizen's data cannot be lowered when it is transferred under SCCs to a third country.

- Before using SCCs, a controller and recipient of personal data must verify that the level of protection required by EU law is respected in the third country concerned. This implies that some level of due diligence on the laws of the third country must be undertaken before transferring data under SCCs.

- The recipient is also under a duty to notify the controller where the law of the third country does not allow the recipient to ensure an adequate level of protection in that country.

Schrems II – Key Aspects

- Where the SCCs cannot ensure an adequate level of protection in the third country, the controller may adopt "supplementary measures" in addition to SCCs.

- If an adequate level of protection cannot be ensured in the third country through SCCs (or the adoption of supplementary measures), the controller is obliged to suspend or terminate the transfer of data under the SCCs.

- The Privacy Shield decision was invalidated as US surveillance is not sufficiently circumscribed in US legislation and because EU citizens do not have an effective and enforceable means of asserting their rights before the US courts.

Meta's record €1.2 billion fine

- Issued by the Irish Data Protection Authority against Meta in relation to transfers of personal data from the EU to the US and the safeguards
- The authority said that changes introduced by Meta Ireland in response to a 2020 ruling by the European Court of Justice "did not address the risks to the fundamental rights and freedoms" of such transfers — even though the transfers largely took place on the basis of contractual clauses endorsed by the European Commission.
- The DPC has now given Facebook's EU operation five months to "suspend any future transfer of personal data to the US". It has also laid down a deadline of six months for the group to cease the processing — including storage — of any European citizen's personal information in the US previously transferred in violation of the bloc's General Data Protection Regulation.

Google Analytics

- Following a series of complaints filed by the non-profit organization noyb in 2020 against 101 EEA websites using Google Analytics or Facebook Connect, EEA data protection authorities have started issuing rulings against the websites, declaring their use of Google Analytics as noncompliant with the GDPR.

- The Austrian Data Protection authority issued a decision, which relied on the manner in which Google Analytics has been implemented. This is important because Google Analytics can be implemented in several different ways, which has an impact on its assessment under the GDPR.

Google Analytics

- An implementation was chosen as a target by noyb.eu that did not use various features available for data protection compliance. The fact that the authority found the implementation non-compliant does not mean that other implementations of Google Analytics are also non-compliant.

- The Authority based its decision of certain factors, including:
  - Google Analytics was used without the user having consented to it;
  - The website operator was the controller, and Google the processor;
  - The website operator had a contract directly with Google LLC (US);
  - The transfer was safeguarded by the old EU Standard Contractual Clauses;
  - The feature for IP anonymization had not been implemented correctly;
  - The transfer occurred without a prior assessment of the risk of prohibited foreign lawful access;

Google Analytics

- Every time the website was accessed this caused it to send Google two unique IDs which permitted Google to track users across different websites.
- The data sent to Google is not considered pseudonymized, because individuals can be singled-out.
- Google has possession, custody and control of Google Analytics data in clear text, because it is technically able to access the data in that form.
- US intelligence authorities are able to track at least some users based on their unique IDs or IP addresses collected through Google Analytics when surfing on the Internet, based on pre-existing information they may have.

European Essential Guarantees for Surveillance Mechanisms

A. Processing should be based on clear, precise and accessible rules.
   - Any limitations on the exercise of data subjects' recognised rights and freedoms must be provided for by law;
   - Any justifiable interferences must be in accordance with applicable legislation.

B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated.
   - The applicable law must indicate in what circumstances, and under which conditions a measure providing for the processing of such data may be adopted;
   - There must be objective criterion which determine the limits in which public authorities may access personal data. Laws which allow general surveillance are to be regarded as compromising individuals' fundamental rights.

European Essential Guarantees for Surveillance Mechanisms

C. An independent oversight mechanism should exist.
- Any interference with the right to privacy should be subject to an effective, independent and impartial oversight mechanism;
- The aim of this review is to verify that a situation justifying surveillance measures exists and the conditions and safeguards that must be laid down are observed.

D. Effective remedies need to be available to the individual.
- The third country legislation must provide for legal remedies to individuals which are effective and not arbitrary.
- This means that third country legislation should provide legal avenues through which individuals in order to have access their personal data, or to obtain the rectification or erasure of such data;
- The notion of 'effectiveness' is interlinked to the notification of surveillance measures to the individual concerned, though lack of notification in justified circumstances is not the deciding factor.

The Transfer Impact Assessment

1. Create a data map of all transfers;
   - The scope is for the exporter to know what personal data is being transferred;
   - Awareness obligations are imposed on exporters to ensure that transfers are afforded an essentially equivalent level of protection wherever it is processed;
   - Exporters must also verify that any data transferred is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

2. Verify the transfer tool relied upon;

3. Assess the effectiveness of such tools;
   - Review of any third country laws or practices which may reduce the effectiveness of the abovementioned transfer tools. The data importer may include to assist in this review;
   - The data importer's legislation should be the first consideration;

4. Identify and adopt supplementary measures (if required);

5. Ensure ongoing re-evaluation of the transfer tools.

Supplementary Measures - Technical

- Robust private encryption prior to transmission, which conforms to state-of-the-art;
- Encryption key-length should reflect the sensitivity of the processed data;
- Keys are reliably generated, administered, stored and revoked;
- Keys are retained solely under the data exporter's control, within a jurisdiction that provides a level of protection essentially equivalent to the EU;
- Public-key certification agreed upon by both parties;
- Pseudonymisation of personal data, prior to this being transferred to the third country;
- Access control for outwards transfers which prevent disclosure or unauthorised use of the pseudonymised data.

Supplementary Measures - Organisational

- Internal policies imposed upon the data importer;
- Internal policies which clearly allocate responsibilities for data transfers, reporting channels;
- Operating procedures for formal or informal requests from public authorities;
- Training procedures for personnel managing access requests;
- Document and record access requests from public authorities, the response and legal basis for such response;
- Regular audits alongside strict disciplinary measures if data processing principles (such as lawfulness, transparency, accuracy, data minimisation, security);
- Procedure for review of internal policies to assess the suitability thereof.

Supplementary Measures - Contractual

- Imposing specific technical measures;
- Transparency obligations;
- Specify any laws which apply to the data importer which could entail access by public authorities;
- Indicate any measures which prevent access to transferred data;
- Obligation to provide detailed information on all access requests by public authorities;
- Specify whether and to what extent the importer is legally prohibited to provide information regarding access requests;
- Importer certifies that it has not purposefully created back-doors or similar programming tools;
- Audit clauses or inspections of importer's facilities;
- Obligation on the importer to review the legality of any disclosure orders within their jurisdiction.
- Commitments from the importer to not engage in any onward data transfers within the same or other third countries which do not provide the same level of protection as within the EU.

Questions

- What was the main outcome of Schrems II and why was this fundamental for organisations?
- Is the use of Google Analytics cookies illegal?
- What are the European Essential Guarantees and what do they aim to achieve?
- Briefly describe the Transfer Impact Assessment and its role in cross-border data transfers.
- What are the 3 forms of supplementary measures? Mention a few examples of each.

The IDPC

- The Office of the Information and Data Protection Commissioner ("IDPC") is the national supervisory authority responsible for monitoring and enforcing the provisions of the GDPR and the Data Protection Act.

- The Office is also responsible to enforce the provisions of the Freedom of Information Act and ensure that public authorities observe the requirements thereof.

Objectives

- Introduce a culture where safeguarding data protection rights is not seen as a legal burden but a natural process that forms an integral part of organisations' operations.
- Increase the level of trust for the general public to be confident that their personal data is used in accordance with the requirements deriving from data protection law.
- Be a relevant and an effective regulatory body particularly in the enforcement of data protection rules by taking the appropriate corrective action against controllers who infringe the provisions of the GDPR.
- Assist micro and small enterprises in complying with the GDPR.

Objectives

- Strive to take initiatives to raise data protection awareness and use dedicated EU funds to achieve this objective.
- Contribute to the consistent application of the GDPR by cooperating with his European Counterparts through the consistency mechanism.
- Ensure that every public authority upholds acceptable standards to ensure transparency and good governance in the conduct of their operations.

Fines

- The IDPC is also responsible for issuing administrative fines on organisations who breach the provisions of the GDPR.
- Some notable fines issued recently include:

  - €250,000 for failing to implement appropriate security measures
  - €65,000 for infringing security principles regarding special categories of PD;
  - €5,000 for the unauthorised disclosure of the complainant's personal data;
  - €2,500 for the disclosure of personal email addresses to all recipients of the email.

21 ACADEMY

Diploma in Law (Malta)

21 LAW

CAMILLERI PREZIOSI
ADVOCATES