Jean Monnet Short Course

Co-funded by the
Erasmus+ Programme
of the European Union

Privacy and Data Protection – The GDPR

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Prof. Federico FERRETTI

Dipartimento di Sociologia e Diritto dell'Economia

The need for EU harmonisation

- Growth of information technology
- Free movement of personal data within the EU
- Goal of achieving the Internal Market whilst protecting fundamental rights and freedoms
- Directive 95/46/EC (legally, on Internal Market grounds

EU harmonisation

- Role of the Charter of Fundamental Rights (Art. 8)
- The Lisbon Treaty and the incorporation of the Charter (distinction between privacy and data protection)
- Art 16 TFEU elevates data protection provision of general application alongside other fundamental principles of the EU

Lisbon Treaty – Art 16 TFEU

- 1. Everyone has the right to the protection of personal data concerning them.
- 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.
- EU data protection reform

Art. 7 Charter

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

Art. 8 Charter

- 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. 41 Right to good administration

- 1. Every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions, bodies, offices and agencies of the Union.
- 2. This right includes:
- … (b) the right of every person to have access to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy;

The GDPR – Legal Form

- Its Articles describe the Members States' obligations without leaving them the same room for manoeuvre as it was the case under Directive 95/46/EC
- In contrast to a ‘Directive’, the use of the legal form of a ‘Regulation’ means that it has direct effect and does not need national implementation. This is designed to eliminate risks of national particularities and diversity of practices, which would frustrate the goal of using that precise EU legal instrument to achieve uniformity
- Through the use of the legal instrument of a ‘Regulation’, the move from a decentralised to a centralised system of governance shall ensure the uniform application and interpretation of norms in the Member States having direct effect from their EU origin

The GDPR - Structure

- The GDPR consists of 173 recitals, 11 chapters and 99 articles. It is formulated as a EU Regulation. It provides for the protection of personal data. However, such a right is not an absolute one but it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality, including the freedom to conduct a business.

The GDPR - Structure

- Recitals and Articles
- In distinction to the Articles the Recitals are very detailed, explaining the theories and assumptions behind the law, its drivers and motivations. They provide tremendous assistance with interpretation, providing an important evidential record of huge historical significance showing what was in the mind of the law maker

Key changes of the GDPR

- No revolution but evolution
- Increased territorial scope: the GDPR has extended jurisdiction. It applies to all legal persons processing the personal data of data subjects residing in the EU, regardless of the location of the Data Controller or Data Processors
- Consent: Consent is again a core tenet of the GDPR, which reinforces its concept providing for new stricter conditions
- Right to Be Forgotten
- Data Portability
- Data Protection by Design and Accountability
- Supervision, enforcement and penalties
- Breach Notification

The GDPR - Content

- The GDPR lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data [Article 1(1) GDPR]
- The right to the protection of personal data is accounted as a fundamental right and freedom of individuals [Article 1(2) GDPR]
- At the same time, the free movement of personal data within the EU shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data [Article 1(3) GDPR]
- This means that the circulation of personal data in the EU is allowed as long as the rules laid down in the GDPR are respected

The GDPR – Scope of Application

- The law applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system [Article 2(1) GDPR]
- By contrast, the GDPR does not apply for processing carried out by individuals purely for personal or household activity [Article 2(2)(c) GDPR]. This exemption also covers social networking and online activities undertaken as long as these are for social or domestic purposes (as per the extension of the CJEU case of *Bodil Lindqvist*)

Territorial Scope of the GDPR

- The territorial scope of the GDPR has been extended to include the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not [Art. 3(1)].

Territorial Scope of the GDPR

- For data controllers or processors outside the European Economic Area ('EEA'), the GDPR applies to the processing of personal data of data subjects who are in the Union anytime the processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; likewise, the GDPR applies to any processing activity relating to the monitoring of the behaviour of data subjects, as far as their behaviour takes place within the Union [Art. 3(2)]

Territorial Scope of the GDPR

- Where the controllers or processors are not established in the EU but they are caught within the territorial scope of the GDPR (see slide before), such controllers or processors must designate in writing a representative in the EU Member State where the data subjects, whose personal data are processed in relation to the offering of goods or services, or whose behaviour is monitored, are located, unless an exception applies
- An exception is a processing which is occasional, does not include processing of special categories of data listed in Article 9(1) (see infra) or processing of personal data relating to criminal convictions and offences on a large-scale, and is unlikely to result in a risk to the rights and freedoms of natural persons. Such an assessment should consider the nature, context, scope and purposes of the processing
- Another exception is data processed by public authorities and bodies

Key Definitions

- ‘Personal data’: any information relating to an identified or identifiable natural person (‘data subject’); an identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier (e.g. a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual) [Article 4(1) GDPR]

Key Definitions

- ‘Processing’ relates to any operation or set of operations performed on personal data or on sets of personal data. These operations are irrespective of the methods used, e.g. by automated means or else. They include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data

Key Definitions

- ‘Controller’: any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Therefore, a controller defines the scope and extent of activities involved in data processing for meeting its objectives and deriving benefits. Controllers are typically primary organizations and entities that have direct contact with consumers. Where two or more controllers jointly determine the purposes and means of processing, they are considered ‘joint controllers’. In this case, they have to determine in a transparent manner their respective responsibilities for compliance with the obligations under the GDPR, in particular as regards the obligations vis-à-vis data subjects.

Key Definitions

- A ‘processor’ is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Processors are usually agents of controllers. They typically include service providers and such as software, servicers of information and records, etc.
- A ‘recipient’ of data is a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.
- A ‘third party’ is a natural or legal person, public authority, agency or body other than the data subject, controller, processor who, under the direct authority of the controller or processor, are authorised to process personal data (e.g. any third-party undertaking activities having an express or implied agreement with an organization for commercial purposes).

Key Definitions

- As regards a controller with establishments in more than one Member State, 'main establishment' is either the place of the central administration in the EU of a controller with establishments in more than one Member State
- This is so unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the EU and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment
- As regards a processor with establishments in more than one Member State, it is the place of the central administration of a processor with establishments in more than one Member State in the EU, or the establishment of the processor in the EU- in case the processor has no central administration in the Union - where the main processing activities take place

Key Definitions

- A ‘representative’ is a natural or legal person established in the EU who is designated in writing by the controller or processor when they are not established in the EU. The representative represents the controller or processor with regard to their respective obligations under the GDPR.

Principles: Art. 5 GDPR

- 'Lawfulness, fairness and transparency': personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject
- 'Purpose limitation': personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; any further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are not considered to be incompatible with the initial purposes
- 'Data minimisation': personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Principles: Art. 5 GDPR

- ‘Accuracy’: data must be accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay

- ‘Integrity and confidentiality’: data must be processed in a manner that ensures appropriate security and protection against accidental loss, destruction or damage; controllers must ensure that appropriate technical or organisational measures are in place

Principles: Art. 5 GDPR

- ‘Storage limitation’: data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed; longer periods of storage are allowed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures to safeguard the rights and freedoms of data subjects. The case of Google Spain under the Data Protection Directive has set an important precedent for EU data protection law in respect to the online world. The CJEU have granted the possibility to data subjects to request to search engines the delisting of links appearing in search results based on a person’s name when the information is no longer relevant. Commentators have labelled the case as introducing the right to be forgotten

Lawfulness of processing and further processing

- Article 6(1) GDPR sets out the conditions that must be satisfied for the processing of personal data to be lawful. The precise conditions are determined by the application of at least one of the following circumstances, which broadly replicate those in the Data Protection Directive

Article 6(1) GDPR

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

- (b) processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;

Article 6(1) GDPR

- (c) processing is necessary for compliance with a legal obligation to which the controller is subject. Member States may maintain or introduce more specific provisions to adapt the application of the rules of the GDPR with regard to processing for compliance with this point by determining more precisely specific requirements and measures for the processing. The basis for the processing must be laid down by union law or Member State law to which the controller is subject;

- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

Article 6(1) GDPR

- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Member States may maintain or introduce more specific provisions to adapt the application of the rules of the GDPR with regard to processing for compliance with this point by determining more precisely specific requirements and measures for the processing. The basis for the processing must be laid down by union law or Member State law to which the controller is subject

Article 6(1) GDPR

- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (this point does not apply to processing carried out by public authorities in the performance of their tasks).

Processing of special categories of data (sensitive data)

- Article 9 GDPR prohibits the processing of special categories of personal data
- The special categories of personal data are personal data revealing racial or ethnic origin, origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life
- The processing of these data is permitted only if the data subjects have given their ‘explicit consent’ [Article 9(2)(a) GDPR]

Sensitive Data

- Under Article 9 (2) (b-j) GDPR, the other grounds for legitimately processing such data are where:

  - the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by EU or national law, or a collective agreement pursuant to national law providing for appropriate safeguards;

  - the processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent;

Sensitive Data

- the processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim. This is on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes, and that the personal data are not disclosed outside that body without the (explicit) consent of the data subjects;

Sensitive Data

- the processing relates to personal data which are manifestly made public by the data subject;
- the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- the processing is necessary for reasons of substantial public interest, on the basis of EU or national law which must be proportionate to the aim pursued;
- the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or national law, or pursuant to contract with a health professional;

Sensitive Data

- the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or national law;
- the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Any processing of personal data relating to criminal convictions, offences, or related security measures must be carried out only under the control of official authority or when the processing is authorised by EU or national law. Any register of criminal convictions must be kept only under the control of official authority (Article 10 GDPR).

Rights of data subjects - Transparency

- Controllers must provide information to individuals about the processing of their data in a concise, transparent, intelligible and easily accessible form, using clear and plain language
- The information must be provided in writing or electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means [Article 12(1) GDPR]
- The controller must act without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, considering the complexity and number of the requests. In such a case, the controller must inform the data subject of the extension within one month of receipt of the request, together with the reasons for the delay

Rights of data subjects - Transparency

- The information notice to data subjects must be provided free of charge
- Where requests from a data subject are manifestly unfounded or excessive the controller may charge a reasonable fee considering the administrative costs or s/he may refuse to act on the request
- However, the controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request

Rights of data subjects - Information notices

- At the time when personal data are collected from the data subject, the controller must provide the data subject with all of the following information [Article 13(1) GDPR], unless the individual already has this information [Article 13(4)]:
- (a) the identity and the contact details of the controller and, in case, of its representative;
- (b) the contact details of the data protection officer of the organisation;
- (c) the purposes of the processing of the personal data and the legal basis for the processing;
- (d) the legitimate interests pursued by the controller or by a third party, if this is the ground for processing the data;
- (e) the recipients or categories of recipients of the personal data, if any;
- (f) whether or not the controller intends to transfer personal data to a third country, together with the existence or absence of an adequacy decision by the Commission (see infra), or reference to the appropriate or suitable safeguards employed (see infra).

Rights of data subjects - Information notices

- In addition, the controller must provide data subjects with the following further information necessary to ensure fair and transparent processing:

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request access to and rectification or erasure of personal data, or to object to processing. Equally, the existence of the right to data portability (see infra);
- the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, and if the data subject is obliged to provide the personal data as well as the possible consequences of failure to provide such data;
- where applicable, the existence of automated decision-making, including profiling, and meaningful information about the logic involved, the significance, and the envisaged consequences of such processing.

Rights of data subjects - Information notices

- Any time the controller intends to further process the personal data for a purpose other than that for which they have been originally collected, the controller has the obligation to inform the data subject on that other purpose and any other relevant information [Article 13(3) GDPR].
- Under Article 14 GDPR, similar obligations exist for the data controller whenever the personal data have not been obtained directly from the data subject, unless the individual has already the information or the provision of said information involve a disproportionate effort. In this case, the data controller must act promptly, at least within one month after obtaining the personal data. If the personal data are to be used for communication with the data subject, the information notice must be given at the latest at the time of the first communication to that data subject or, if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed [Article 14(3) GDPR].

Rights of data subjects - Right of access

- Under Article 15 GDPR, data subjects have the right to know whether or not their personal data are being processed. They have the right of access to their personal data and the following information:

(a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed; (d) the envisaged period for which the personal data will be stored or the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data, or restriction of processing of personal data or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, as well as meaningful information about the logic involved, significance and consequences of such processing.

Rights of data subjects - Rectification and erasure

- According to Article 16 GDPR, data subjects have the right to obtain from the controller the rectification of inaccurate personal data without undue delay
- Equally, in case of incomplete data and depending on the purposes of the processing, data subjects have the right to obtain completion
- In turn, Article 17 provides for what has sometimes inappropriately been referred as the ‘right to be forgotten’.

Rights of data subjects – the Right to be Forgotten

- This right comes from the earlier jurisprudence of the CJEU in *Google Spain*
- Under the codified provision, data subjects have the right to obtain from the controller the erasure of personal data where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected; (b) the data subject withdraws consent and there is no other legal ground for the processing; (c) data subjects object to the processing and there are no overriding legitimate grounds for the processing; (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services offered to a child.

Rights of data subjects – the Right to be Forgotten

- The right to erasure does not apply when the processing is necessary for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority of the controller, for reasons of public health, for archiving or research purposes in the public interest, or for legal claims.

Rights of data subjects - Right to data portability

- Data subjects have the right to receive their personal data in a structured, commonly used and machine-readable format
- To this end, under Article 20 GDPR they have the right to transmit those data to another controller where the processing is based on consent or on a contract
- Equally, the right to data portability applies when the processing is carried out by automated means
- Data subjects have the right to have the personal data transmitted directly from one controller to another, where technically feasible

Automated decision-making and profiling

- Profiling is considered by the GDPR as “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements” [Article 4(4) GDPR]

Automated decision-making and profiling

- Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which may affect them significantly. Such significant automated processing can be used if it is:
  - necessary for enter into, or perform, a contract between data subjects and a controller;
  - authorised by EU or national law; or
  - based on the data subject's explicit consent.

Automated decision-making and profiling

- In the case of automated decisions based on explicit consent or contractual fulfilment, controllers must have in place suitable measures to safeguard data subjects
- At a minimum, these must include a right for data subjects to obtain human intervention, express their point of view and contest decisions
- In any event, automated decisions cannot be based on the sensitive data of Article 9(1) GDPR, unless there is explicit consent and there are suitable measures to safeguard data subjects
- Differently from the Data Protection Directive, the GDPR no longer states that the above data subjects' rights are not necessary if the effect of the decision is to grant the individual's request

Data governance obligations

- The GDPR places accountability obligations on controllers and processors to demonstrate compliance with the GDPR
- Some elements that must be demonstrated are explicit but others are implied, e.g. the implementation of appropriate governance models so that data protection receives the due level of attention by controllers
- Considering the nature, scope, context, purposes and risks of processing controllers have the obligation to implement appropriate technical and organisational measures, to be reviewed and kept up-to-date, to demonstrate that processing complies with the GDPR
- E.g. these measures include the implementation of appropriate data protection policies or adherence to approved codes of conduct ex Article 40 GDPR or approved certification mechanisms ex Article 42 GDPR

Specific data governance obligations
Data protection by design and by default

- Controllers have to adopt internal policies and implement technical and organisational measures for ensuring the respect of the GDPR principles by design or by default. These include:
  - pseudonymisation, systems designed to implement data minimisation, the use of cryptographic procedures for the protection against unauthorised or unlawful external or internal processing;
  - measures which provide that only personal data which is necessary for each specific purpose of the processing is processed (in particular in relation to the amount of data collected, the extent of its processing, the period of its storage and its accessibility);
  - measures to prevent accessibility to more individuals than necessary for the purpose, using applications or processes which allow them to implement such controls and, where available, have been certified by a body accredited by a Supervisory Authority under Article 42 GDPR.

Specific data governance obligations
Data Protection Impact Assessments (DPIA)

- A DPIA is an assessment to identify and minimise the risks of non-compliance formalised in Article 35 GDPR.
- Controllers must undertake DPIA where there is a high-risk processing, in particular using new technologies.
- The GDPR gives some examples of where a DPIAs is required (e.g. in the event of a systematic monitoring of a publicly accessible area, in the context of profiling on which decisions affect individuals, or processing on a large scale of sensitive data).

Specific data governance obligations
Data Protection Impact Assessments (DPIA)

- The essential elements that a DPIA must contain are:

  (a) a systematic description of the envisaged processing operations and the purposes of the processing, including the legitimate interest pursued by the controller (if any);

  (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

  (c) an assessment of the risks for data subjects; and

  (d) the measures envisaged to address the identified risks.

- If a DPIA indicates that processing results in a high level of risk, in the absence of measures taken to mitigate the risk controllers must consult the Supervisory Authority prior to the processing

Personal data breaches and notification

- A personal data breach is an incident defined by Article 4(12) GDPR as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
- Under Article 33 GDPR, all personal data breaches have to be reported
- The law prescribes that processors must notify controllers without undue delay after becoming aware of a personal data breach
- In turn, controllers have to report not later than 72 hours after having become aware of it, the personal data breach to the competent Supervisory Authority, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. In case the notification of a breach to the Supervisory Authority is not made within 72 hours, it has to be accompanied by reasons for the delay

Personal data breaches and notification

- The notification to the competent Supervisory Authority must contain at least the following elements:

  - a description of the nature of the personal data breach, as well as the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

  - a communication of the name and contact details of the DPO or other contact point where more information can be obtained;

  - a description of the likely consequences of the personal data breach;

  - a description of the measures taken by the controller to address the personal data breach, including measures to mitigate its possible adverse effects; if such measures have not been taken at the time of the notification, the controller must indicate the proposed to be taken.

Personal data breaches and notification

- If controllers have not yet done so, they are under the obligation to communicate in clear and plain language the personal data breach to the data subjects involved (Article 34 GDPR). This must occur without undue delay
- By contrast, the communication to data subjects is not required if:

  - the concerned controller had implemented the appropriate technical and organisational protection measures (in particular, those that render the personal data unintelligible, such as encryption);
  - the concerned controller has taken subsequent measures which ensure that risks are no longer likely to materialise;
  - it would involve disproportionate efforts. In this event, the concerned controller has to issue a public communication or similar measure informing data subjects in an equally effective manner

Personal data breaches and notification

- Finally, the GDPR imposes stringent documentation requirements on the affected controllers: they must document all breaches, comprising the facts relating to the breach, its effects and the remedial action taken in order to enable Supervisory Authorities to verify compliance with their obligations above
- Failure to meet the above requirements exposes controllers to an administrative fine of up to 10 000 000 EUR, or in the case of an undertaking of up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher [Article 83(4) GDPR]

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Prof. Federico FERRETTI

Dipartimento di Sociologia e Diritto dell'Economia

f.ferretti@unibo.it