UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

Teacher

- Prof. Marco Orofino
- email: marco.orofino@unimi.it
- homepage: https://www.unimi.it/it/ugov/person/marco-orofino
- Course web page: https://morofinodar.ariel.ctu.unimi.it/
- Teams: https://teams.microsoft.com/l/team/19%3a2a694ae3a5634ad4bd9ed3b64c05eee9%40thread.tacv2/conversations?groupId=b427b0c0-ef1d-4464-aa4c-ad0c4313eb45&tenantId=13b55eef-7018-4674-a3d7-cc0db06d545c
- Code: g8gzboq

Classes

- Tuesday – Friday 9:00 -10:30
- Everyday at 8:30, I will be online for specific questions and doubts

Reference text book and papers

- Handbook on European Data Protection Law (https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf)

- Slides will be made available, before each class, on Ariel platform

Exam

- The exam aims at verifying the knowledge and comprehension of the subject.
- The exam is oral. For attending student we evaluate also a written on line text during the course

Syllabus

22/9. Introduction
25/9. The European concept of data protection between EU and ECHR
29/9 The fundamental right to personal data protection in the
02/10 Data protection terminology
06/10 Territorial and material scope
09/10 General Principles of European Data Protection Law I
13/10 General Principles of European Data Protection Law II
16/10 The Legal Conditions relating to processing of personal data;
20/10 The rights of the data subject (I part)
23/10 The rights of the data subject (II part)
27/10 The obligations of the controller and of the processor (I part)
30/10 The obligations of the controller and of the processor (II part)
03/11 The DPO
06/11 The Member States' Independent Supervisory Authorities
10/11 The European Data Protection Board; Competence, tasks and powers
13/11Transfers of personal data to third countries (non-EU countries)
17/11. Specific Type of Data (I part)
20/11. Specific Type of Data (II part)
24/11. Remedies and penalties
27/11 IA and Data protection

A good news and a bad news

- The good news is that almost ninety-five per cent of us are concerned about privacy

- The bad news is that we do not know what we mean

The need for Privacy

- The need of privacy, understood restraint in revealing one's feelings and in showing one's physical intimacy is ancestral...

BUT

... The "boundaries" of this need depend on:
social structure (relations between the associates) and the technology available

The concept of privacy: from its foundation

- 1891, S.D. Warren L.D. Brandeis publish “The Right to privacy” in Harvard Law Rewiev.

Right to be let alone

- 1967, A. Westin, Privacy and Freedom

The claim of individuals and groups to determine when, how and what extent information about them is communicated to others

The double dimension of privacy

- Relational dimension.

It deals with the relation one has with other people

- Informational dimension

It is related to the collection, storing and processing of personal data

The functions of privacy

- Personal autonomy
- Emotional release
- Self evaluation and decision making
- Need for protected communication

The judicial foundation: from Olmstead to Kats

- *Olmstead v. United States*, 1928
- USA Constitution Does Not Protect Privacy
- Justice Brandeis Dissenting Opinion («Privacy was invaded and privacy is the most comphrensive of rights and the right most valued by civilized men»

Kats vs United States

- *Katz v. United States*, 389 U.S. 347 (1967)
- It extended Fourth Amendment protection beyond the traditional boundaries of citizen's home and property.
- Set the s.c. "Kats text" that inquires wheater a person has a reasonable expectation of privacy.
- The Kats text is based on a two part test with two requirements: 1. that a person have exhibited an actual (subjective) expectation of privacy 2. that the expectation be one that society is prepared to recognizes as reasonable

The limits…

- If the privacy is limited by the Government, is necessary to evaluate if the imposed restriction aims to protect a constitutional interest which could prevail on privacy such as the protection of national security.

Privacy Under Attack (perceived as under attack)

- (Past) attacks were done by persons with whom individuals have a close contact or by governmental agencies, industry or by the press

✓ Use of information, Trespass, Correspondence, Instantaneouse Photography, Wiretapping, Psycological Testing and Lie Detectors, Computers

- (Present) attacks done through Internet and other methods of surveillance

✓ Videosurveillance, Biometric Identification, Genetic Data, Identity Theft, Data Mining, Chip or Smart Card, GPS, Internet, RFID, Wireless Networking, App, Ambient Technology, Neurolinguistic,

Protection of Privacy: 4 Models

- Comprehensive Law and Regulatory Agents
- Sectoral Law
- Self-Regulation
- Technologies of privacy

The main features of the American privacy protection model

- Constitutional recognition after Kats vs United States
- Absence of administrative protection.
- Ex post judicial protection at the initiative of the person who complains of an injury.
- Fragmentary federal legislation limited to those matters over which the federation has jurisdiction.
- Preference for a sector-by-sector legislative discipline.
- **Relations between private parties** largely left to the autonomy of the parties.

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

From the Right to respect for private life to the right to personal data protection

- Every European State protects in its own Constitution the Right to respect for private life with regard to corrispondence, communications, domicile.
- The need to protect data arises with the development of the computer (see. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, il Mulino, 1973).
- The Right to personal data protection is a right which answers (meanwhile) to a technological development and to an historical fear.
- The right to respect for private life consists of a general prohibition on interference, subject to some public inter-est criteria that can justify interference in certain cases. The protection of personal data is viewed as a modern and active right, putting in place a system of checks and balances to protect individuals whenever their personal data are processed.

Relevant norms on data protection in Europe

The European model of data protection is shaped by different subjects

- Council of Europe
- European Union
- National States.

Council of Europe

- Under Article 8 of the ECHR, a person's right to protection with respect to the processing of personal data forms part of the right to respect for private and family life, home and correspondence (see
- CoE Convention 108 is the first and, to date, the only international legally binding instrument dealing with data protection. The Convention underwent a modernisation process, completed with the adoption of amending Protocol CETS No. 223.

European Union

- Under EU law, data protection has been acknowledged as a distinct fundamental right. It is affirmed in Article 16 of the Treaty of the Functioning of the EU, as well as in Article 8 of the EU Charter of Fundamental Rights.
- Under EU law, data protection was regulated for the first time by the Data Protection Directive in 1995.
- In view of rapid technological developments, the EU adopted new legislation in 2016 to adapt data protection rules to the digital age. The General Data Protection Regulation became applicable in May 2018, repealing the Data Protection Directive.
- Together with the General Data Protection Regulation, the EU adopted legislation on the processing of personal data by state authorities for law enforcement purposes. Directive (EU) 2017/680 establishes the data protection rules and principles that govern personal data processing for the purposes of preventing, investigating, detecting and prosecuting criminal offences or executing criminal penalties.

Art. 8 of European Union Charter of Fundamental Rights

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**.

Right holders

- «**Everyone**»… every natural person regardless of citizenship or other personal or social requirement.

- Recognition of the law is not limited to European citizens only.

Scope of Protected Right

- Art. 8 affirms the right to personal data protection and spells out the core values associated (fairness, for specified purposes, based on consent or other legitimate conditions).
- Right to access and right to rectification are ancillar rights to the right to personal data protection.
- Substantial scope still depends on notion of personal data as well as on notion of processing as set out by legislators

Limitations

- The EU legal order places conditions on limitations on the exercise of the fundamental rights protected by the Charter. Any limitation to any fundamental right, including to personal data protection, can be lawful only if it:

I. is in accordance with the law;

II. respects the essence of the right;

III. subject to the principle of proportionality, is necessary

IV. pursues an objective of general interest recognized by the EU, or the need to protect the rights of others.

The main features of the European privacy protection model

- "Constitutional "recognition in National Constitution as well as on EU primary law and ECHR
- Administrative protection.
- Judicial protection
- Unified legislation for EU Member States and Harmonized protection of the fundamental right under UCHR.
- Preference for ah horizontal legislative discipline with spaces for national legislation in specified sectors.
- **Relations between private parties** largely regulated

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

The interaction of data protection fundamental right with other rights and legitimate interests

The concept of interaction

- Absolute rights do not exist.
- The idea of the limit is inherent to the idea of law.
- There are situation where **the rights and the freedoms** are in tension because they attribute juridical positions in contrast with each other
- There are cases where rights conflict with a community's fundamental interests (an interest qualified as a fundamental one in a constitutional norm or in a fundamental norm (as primary law in the EU system)

How is the interaction or contrast resolved?

- When different rights or interest are at stake, a balancing exercise is needed.
- The task of carrying out balancing rests primarily with the legislators.
- When a conflict has arisen, the task of reconciling rights rests with the Courts.
- The ordinary judge is always the first person called to resolve a dispute
- If the conflict concerns constitutional rules and it is not possible to use an adequate interpretation, the competence belongs to the national Constitutional Courts or to the European Court of Justice

The interaction of the Data Protection Right

- The right to data protection interacts with other rights, such as freedom of expression, the right to receive and impart information, freedom of the arts and the sciences, protection of intellectual property,
- The right to data protection interacts with many interests qualified as fundamental such as national security or free circulation

The rules of balancing

- The EU legal order places conditions on limitations on the exercise of the fundamental rights protected by the Charter.
- Any limitation (any balancing) to fundamental rights, including to personal data protection, can be lawful only if it:

a) is provided for by law;

b) respects the essence of the right;

c) subject to the principle of proportionality, is necessary

d) pursues an objective of general interest recognized by the EU, or the need to protect the rights of others

Provided for by law

- This requirements implies that any balancing operation must be based on a legal basis
- The concept of legal basis is substantial rather than formal

a) This means that rules must be accessible, foreseeable and precise)

b) This means, also, that the legal basis must define the scope and the manner of the exercise of power bt competent authorities

Respect the essence of the rights

- Any balancing that requires a limitation must respect the essence of the rights involved.

a) This means that limitations must not be so extensive or intrusive to devoid a fundamental right of its basic content

b) This means that in case of a contrast between rights, freedoms and fundamental interests, the solution the solution of the balance cannot be the annihilation of one of the rights involved

Necessity and proportionality/1

- These concepts are related but also autonomous
- Necessary means first and fore most that the limitation is needed for a public interest objective
- Necessary means also, according with jurisprudence, that the measures adopted must be less intrusive compared to other options for achieving the same goal

Necessity and proportionality/2

- Proportionality means that the advantages resulting from the limitation should outweigh the disadvantages the latter causes on the exercise of the fundamental rights
- Limitation must contain appropriate safeguards

Objective of general interest or rights and freedoms

- Objective of general interest recognized by the European Union (see art. 3 of the TUE – promotion of peace and well-being, social justice and protection and the establishment of an area of freedom, security and justice, free movement of people)
- General interest must be specified in sufficient detail

EU General Data Protection Regulation (EU-GDPR) – Table of content

- Recitals
- CHAPTER I - General provisions
- CHAPTER III - Rights of the data subject
- CHAPTER IV - Controller and processor
- CHAPTER V - Transfers of personal data to third countries or international organizations
- CHAPTER VI - Independent supervisory authorities
- CHAPTER VII - Cooperation and consistency
- CHAPTER VIII - Remedies, liability and penalties
- CHAPTER IX - Provisions relating to specific processing situations
- CHAPTER X - Delegated acts and implementing acts
- CHAPTER XI - Final provisions

What are recitals?

- Text at the start of an EU act that sets out the reasons for its operative provisions, while avoiding normative language and political argumentation.
- Recitals are introduced by the word "whereas" and are numbered, unless there is only one.
- Recitals to EU laws are not in themselves legally binding in the same way that the operative provisions are. However, where an EU law is ambiguous, the recitals can be important in interpreting the ambiguous provision.
- This is because the Court of Justice of the EU (CJEU) will take a "purposive" interpretation to EU law, rather than a strictly literal approach. In other words, if the text is not clear, the CJEU will interpret it to give effect to the aim or spirit of the legislation, taking into account its context and general objectives. However, recitals cannot overrule a relevant operative provision: if they are irredeemably inconsistent then the text of the operative provision will take precedence.
- Recitals are very important in a multilinguistic context, they help to avoid misunderstanding and incorrect interpretations.

Chapter I – General Provisions

Article 1 - Subject-matter and objectives

Article 2 - Material scope

Article 3 - Territorial scope

Article 4 - Definitions

Objective of the GDPR (art. 1)

- Protection of fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

- Free movement of personal data within the Union as tool to develop society (general interest)

- All GDPR must be read as the attempt to balance the fundamental right and the general interest

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

Data protection terminolgy

1. Personal Data

- GDPR art. 4, par 1, a) 'personal data' means **any information** relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, *in particular by reference to an identifier such as 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 natural person*;

Personal data

- Data are personal if they relate to an identified or identifiable person (basic concept)
- To determine wheather a person is identifiable is necessary to take into account all reasonable means (objective factors such as costs, time, technology that are likely to be used (recital 26)
- Personal data is **any information** that relates to an identified or identifiable **living** individual. (recital 27)

… data concerning the person (Opinion 4/2007)

- Data is concerning whether it concerns a person in the sense that there is a relationship of content, or purpose or result.

a) A relationship of content is classic, it relates to the content of the information itself (eg results of a medical test, filmed image)

b) A relationship of purpose exists when information pursues a purpose related to a person (for example, evaluation of a car).

c) A relationship of result occurs when information can have an impact, a consequence on a person. (evaluation of efficiency of taxi drivers group, evaluation of structure quality as a University department)

New problem: what about inferential data? Data created by the processing of personal data

… Any information

- Wide concept
- Objective information (eg. Personal Id, Name, Dna, Address, Weight, Colour of the eyes) and subjective information (opinion or evaluation eg. Marks, Judgments)
- Information is independent of content (it does not need to be true)
- Information is independent of characteristic (alphabetic, numerical, graphic, photographic, acoustic) or support (paper, videocassette, hard disk) --- eg. video surveillance, phone banking but also child's drawing

... Identified or identifiable

- "identified" is the natural person who, within a group, is "distinct" from all other members.
- identifiable "when, although it has not yet been identified, it is possible to identify it conducting further research

… directly or indirectly

- Depends on specific context (eg name)
- Phenomenon of "unique combinations", whether large or small. In cases where, at first glance, the available identifiers do not allow identifying a particular person, one can still consider that person to be "identifiable" because that information combined with others (whether or not kept by the controller) will make it possible to distinguish it from the other.
- Question of means that can reasonably be used by the controller or others to carry out identification

… living individuals

- GDPR just protects living natural person
- The protection of personal data of the deceased sees a space for national choices
- GDPR does not protect nor undertakings neither legal entities (just e-privacy directive protects the confidentiality of the communication and the interests of legal entities)

Special categories of personal data (art. 9 GDPR)

- Personal data revealing

a) racial or ethnic origin,
b) political opinions,
c) religious or philosophical beliefs, or trade union membership,
d) genetic data, biometric data for the purpose of uniquely identifying a natural person, (see also art. 4, par.1,, lett. 13,14)
e) data concerning health (see also art. 4, par. 1, lett. 15)
f) data concerning a natural person's sex life or sexual orientation

If a data is not a personal data...

- Anonymous data are not subject to GDPR rules
- Anonymous data might be anonymous in there essence (at first instance) or might be anonymized.
- The data is anonymized if it is no longer possible to refer to the data subject in any way.
- Pseudonymization is not anonymization

The concept of processing

- Art. 4, 1 lett. b) means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; (all-inclusive definition)

Key points

- Data processing concerns any operation performed on personal data
- The term processing covers both automated - and non-automated processing

3. Users of personal data

a) Controllers
b) Processors
c) Recipient and third parties

a) Controller

- means the **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*; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- A controller's decision why and how data shall be processed.
- If a controller is established outside of EU, that company need s to appoint a representative within Union

A1) Joint controller

- Where two or more controller determine jointly the purposes and the means of processing they are considered joint controller

b) Processor

- processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
- Close link with Controller but separate legal entity.
- As separate legal entity, the processor is operationally involved in processing, but **only on behalf and on instructions** of the controller.
- Instructions are compulsory

c) Third party and Recipient

- Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data
- Recipient means 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 someone who is different of the controller and the processor while a "recipient" may either be outside the controller or the processor or someone inside.
- The distinction is very important only because of the conditions for lawful disclosure of data

Examples

- A controller's employee who uses the data within his tasks is a recipent of data but not a third party

- If a controller provides to a training company data of its employers in order to tailor a training programm, the training company is a *Third Party*

4. Data subject

- The data subject is the person to whom the data being processed refers (the GDPR does not contain a definition)
- The data subject is the holder of many rights recognized by the GDPR
- The concept of *data subject* and *the concept of holder* of the data protection fundamental right are not completely overlapping
- The holder of the fundamental right is each individual while the holder of the rights recognized by the GDPR is each person to whom the data being processed

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

II. Scope

Material scope

- The legislation 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.
- **All processing** of personal data wholly or partly **by automated means**.
- **Processing of personal data by not automated means** which form part of **a filing system**

Processing out of the scope

a) in the course of an activity which falls outside the scope of Union law;

b) by the Member States when carrying out activities which fall within the scope of chapter 2 of Title V of the TEU; (Policies on border checks, asylum and immigration)

c) by a natural person in the course of a purely personal or household activity;

d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

e) For the processing of personal data by the Union institutions, bodies, offices and agencies (Regulation (EU) 2018/1725 applies).

Territorial scope

- Regulation applies to the processing of personal data:

a) 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.

b) of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

i. the offering of goods or services to individuals (data subject) in the Union;

ii. the monitoring of their behaviour as far as their behaviour takes place within the Union.

c) by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

III - Lawfulness of processing

Six conditions of lawfulness (art. 6 of the GDPR)

1. consent to the processing of his or her personal data for one or more specific purposes
2. processing is necessary for the performance of a contract
3. processing is necessary for compliance with a legal obligation to which the controller is subject
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person
5. 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
6. 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.

Conditions of consent

- Consent must freely given
- Consent constitutes an appropriate legitimate basis only if the interested party is offered control and effective choice.
- Consent guarantees data subject control over their data.
- If there is no possibility to choose or if there is no control, the consent is illusory. It is not a valid basis for processing.
- Controller must be able to prove that he has received consent

Processing is necessary for the performance of a contract

a) Necessary to conclude a contract.

b) Necessary to execute a contract (For example banking, insurance, telephone contracts)

- The principles of data processing always apply.
- To ask, always, to express the consent where it is not necessary, however, is wrong and misleading --- it can render the processing non-compliant.
- A different matter is the possible provision of a contractual addendum with information.

Processing is necessary for compliance with a legal obligation to which the controller is subject

- Legal obligation must comply with art. 52 Charter of Rights.
- Legal basis is in the law of the Union or in the law of the Member States (within the sphere of their respective competences).
- The Law of the Union or of the Member States that require the processing of personal data must also regulate purposes, type of data, recipients, limitation, conservation and other measures to make the treatment lawful and fair

Processing is necessary for the performance of a task carried out in the public interest

- Legal basis is in the law of the Union or in the law of the Member States (within the sphere of their respective competences).
- Law of the Union or of the Member States establishes treatments, aims, type of data, recipients, purpose limitation, conservation and other measures to render lawful and correct treatment.
- Right of the Union or of the States establishes whether the subject must be a public authority, a natural or legal person under public law or private law

Processing is necessary in order to protect the vital interests

- Notion of essential interest.
- This cause of legitimacy is residual. It is useful just if the processing cannot be manifestly based on another legal basis (inability to give consent) --- coexistence with relevant reasons of public interest
- Eg epidemics, humanitarian emergencies, natural and human catastrophes

Processing is necessary for the purposes of the legitimate interests

- Legitimate interest does not apply to public authorities.
- Legitimate interest is to process data for marketing purposes (ad hoc right to object to processing).
- It is legitimate to treat traffic data for network security and capacity.
- Legitimate interest is always to be concretely balanced with the rights and freedoms of the interested party (see Google vs. Costeja judgment).
- The interest of children shall always prevail

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

Key Principles

Lawfulness of processing

- Lawful processing requires the consent of the data subject or another legitimate ground provided in the data protection legislation (i.e. when processing personal data is necessary for the performance of a contract, for the performance of a task carried out in the exercise of public authority, for compliance with a legal obligation, for the purpose of the legitimate interests of the controller or third parties, or if necessary to protect the vital interests of the data subject.
- Legal obligations must always respect the Charter of Fundamental Right

Fairness of processing

- The principle of fair processing governs primarily the relationship between the controller and the data subject.
- Controllers should notify data subjects and the general public that they will process data in a lawful and transparent manner.
- Processing operations must not be performed in secret.
- Data subjects should be aware of potential risks

Transparency of processing

- EU data protection laws require personal data processing to be done "in a transparent manner in relation to the data subject".
- This principle establishes an obligation for the controller to take any appropriate measure in order to keep the data subjects informed about how their data are being used
- Transparency may refer to: a) the information given to the individual before the processing starts; b) the information that should be readily accessible to data subjects during the processing; c) the information given to data subjects following a request of access to their own data.

The principle of purpose limitation

- Keystone of the entire legislation (cross between the duty of the owner to inform interested parties on purpose of the processing and right of the data subject to express an informed consent or right to be informed is consent is not necessary necessary)

Consequences of the principle of purpose limitation (I)

- The purpose of processing data must be defined before processing is started.
- There can be no further processing of data in a way that is incompatible with the original purpose (exceptions to this rule for archiving purposes in the public interest, scientific or historical research purposes and statistical purposes.
- In essence, the principle of purpose limitation means that any processing of personal data must be done for a specific well-defined purpose and only for additional, specified, purposes that are compatible with the original one.
- Compatible purpose means that exists a margin of flexibility. (see recital 50)

Consequences of the principle of purpose limitation (II)

- Transfer abroad (outside EU) not provided for by original purpose provides always new legal basis
- Processing for undefined purposes is illegitimate.
- Processing for illegitimate purposes is illegitimate.
- Disclosure of data to third parties if not is part of the original purpose is not lawful.

Consequences of the principle of of purpose limitation (III)

- Problem of compatibility between the principle and the extraction of data from data and subsequent re-use of the data generated
- Problem of compatibility between the principle and the processing chains necessary to AI

The data minimisation principle

- Data processing must be limited to what is necessary to fulfil a legitimate purpose.
- The processing of personal data should only take place when the purpose of the processing cannot be reasonably fulfilled by other means.
- Data processing may not disproportionately interfere with the interests, rights and freedoms at stake.

The data accuracy principle

- The principle of data accuracy must be implemented by the controller in all processing operations.
- Inaccurate data must be erased or rectified without delay.
- Data may need to be checked regularly and kept up to date to secure accuracy

The storage limitation principle

- The principle of storage limitation means that personal data must be deleted or anonymised as soon as they are no longer needed for the purposes for which they were collected.

The data security principle

- The security and confidentiality of personal data are key to preventing adverse effects for the data subject.
- Security measures can be of a technical and/or organisational nature.
- Pseudonymisation is a process that can protect personal data.
- The appropriateness of security measures must be determined on a case-by-case basis and reviewed regularly.

The accountability principle

- Accountability requires controllers and processors to actively and continuously implement measures to promote and safeguard data protection in their processing activities.
- Controllers and processors are responsible for compliance of their processing operations with data protection law and their respective obligations.
- Controllers must be able to demonstrate compliance with data protection provisions to data subjects, the general public and supervisory authorities at any time. Processors must also comply with some obligations strictly linked to accountability (such as keeping a record of processing operations and appointing a Data Protection Officer).

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

Rights of the Data Subject/first part

The notion of data subject

- Neither Directive 95/46 nor Regulation 2016/679 contains a definition of interested parties. Both acts define "the person concerned" implicitly in the definition of personal data.
- National Code was more accurate. Ex, paragraph 1, art. 4 of the Code, it defined data subject as "the person concerned, the natural person, the legal entity, the body or association to which the personal data refer".
- Today data subject is just the natural person concerned

Right to get transparent information

- Distinction between person data obtained from the data subject (I) or not obtained from the data subject (II).
- Sub I. Information provided to the data subject at the time of the collection
- Sub II. Information provided within a reasonable time from the collection of personal data (within one month) or in the context of the first communication with data subject. Exceptions: a) data subject already has information, b) disproportionate effort; c) secrecy requirements

Right of access

- Right to obtain confirmation from the controller whether or not personal data are being processed
- Right of access to personal data and to information about the processing
- Right to obtain a copy

Content

- The purposes of the processing
- The categories of personal data
- Recipients or categories of recipients to whom data will be disclosed
- Period of conservation or the criteria to determine it
- The existence of the right to rectify, erasure, restrict or object to the processing .
- The right to lodge a complaint.
- Any information on the origin of the data (in case they are not collected by the controller)
- The existence of automated process and the logic involved.
- Transfer abroad and knowledge of adequate guarantees

Right to rectification

1. Right to modify inaccurate personal data.
2. Right to the integration of incomplete personal data.

Right of rectification is the data quality oversight (veracity, update, correct)

Right of the Data subject and obligation of the Controller

Right to erasure (right to be forgotten)

- Erasure and oblivion (right to be forgotten) are two very different concepts.
- The choice of the heading of the norm is not suitable.
- Data deletion is an objective activity that leads to "eliminating a certain data from a certain file".
- The notion of oblivion is, instead, linked to a subjective element, a balance between memory and forgetfulness.
- The erasure of data may favor oblivion but not assure it

Content of the right to erasure/1

- The right to obtain the cancellation of the personal data from the controller corresponds to the obligation of the controller to proceed without delay to the erasure
- Cases: 1. withdrawal of consent; 2. no longer necessary in relation to purposes; 3. opposition to processing; 4. unlawfulness of the processing; 5. legal cancellation obligation; 6. data relating to minors acquired for information society services.
- Obligation of the holder if he has made public such data to inform other holders of the request (technological limits, costs and reasonable measures)

Specific limitations

- Processing for the exercise of the right to freedom of information.
- Processing for compliance with a legal obligation or for the performance of a task carried out in the public interest
- Processing for reasons of public interest in the field of public health
- Processing for archiving purposes in the public interest, scientific and historical research
- Processing for the establishment, exerce or defence of legal claims

Rights to restriction of processing

- Residual and circumscribed case with respect to cancellation.
- Restriction of processing is heir to the freezing of processing

- Cases:

i. The accuracy of data is contested.
ii. The processing is illicit but the data subject opposes to cancellation and requests the restriction.
iii. The controller no longer needs the personal data but the data subject needs them to establish, exercise or defence of legal claims.
iv. Data subject objected the processing but the verification of the grounds is pending.

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

Rights of the Data Subject/second part

Right to data portability

- New Data Subject Right
- It deals with electronic data storage.
- Link with regulatory body on electronic communication (pro-competitive standard)
- Indispensable requirements of law:

a) Processing takes place in an automated manner

b) Processing is done with the consent for one or more specific purposes (also sensitive data) or in execution of a contract of which the interested party is a part.

Content of the right

a) Right to receive the personal data in a structured, commonly used and machine-readable format.

a) Right to transmit those data to another controller without impediment from the controller to which the personal data have been provided

Right to object

- Right of the data subject to object to processing of personal data on grounds relating his or her particular situation at any time
- Prerequisite:
  Processing is legitimate on very specific grounds (necessary for the performance of a task carried out in the public interest or necessary for purposes of the legitimate interests pursued by the controller that are not overridden by the interests or fundamental rights of tha data subject)
- The controller shall demonstrate compelling legitimate grounds or no longer process data.
- Where data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed.

Right not to be subject to an automated decision

- The data subject has the right not to be subject to a decision based solely on automated processing, which produces legal effects on him or significantly affects him.
- It is legitimate just in case this decision:

a) Is necessary to enter into a contract

b) Is authorised by law

c) Is based on an explicit consent

If the automated individual decision is lawful…

- The data subject has, at least, the right to:

a) Obtain human intervention

b) Express his or her point of view

c) Contest the decision

Not specified how?

- The controller has the obligation to implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests

Right to receive communication of a personal data breach

- In a nutshell:
- Assumption: data breach that presents an high risk for the rights and freedoms of the data subject.
- Description of the data breach in a clear language, supply of a contact name, and information about the consequences and the adopted measures in order to minimize the risks.
- Limitation clauses: a) adequate technical measures, b) adequate ex post measures; c) disproportionate efforts

Restrictions to data subject's rights

- The art. 23 of the Regulation refers literally to the clause of limitation of fundamental rights contained in art. 52 Charter of Fundamental Rights.
- The restraint is lawful if:

a) Provided by law

b) Respect the essential content of the rights

c) The restriction is necessary and proportionate in a democratic society

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

Controller and processor: duties and responsibilities/first part

The centrality of the Controller and Processor in the new European framework

- The Regulation dedicates to the discipline of the obligations of the controller and, separately, of those of the processor the entire Chapter IV.
- In the Regulations, controllers and processors assume a greater centrality than in the previous directives.

Definition of controller

- The definition of controller contains five main building blocks, which will be analysed separately. They are the following:
- "the natural or legal person, public authority, agency or other body"
- "determines"
- "alone or jointly with others"
- "the purposes and means"
- "of the processing of personal data".

The joint controllers

- The qualification as joint controllers may arise where more than one actor is involved in the processing. (art. 26 literally "[w]here two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers."
- Article 26 of the GDPR introduces specific rules for joint controllers and sets a framework to govern their relationship

Definition of processor

- A processor is defined in Article 4 (8) as a natural or legal person, public authority, agency or another body, which processes personal data on behalf of the controller.
- Similar to the definition of controller, the definition of processor envisages a broad range of actors - it can be "a natural or legal person, public authority, agency or other body".
- Two basic conditions for qualifying as processor are:

a) being a separate entity in relation to the controller and

b) processing personal data on the controller's behalf.

General responsability of the controller

- Obligation to implement adequate technical and organizational measures to guarantee (and demonstrate) that the processing is carried out in accordance with the Regulation. Proactive role (privacy by design and privacy by default)
- Adequate technical and organizational measure **are not standard** Transition from the predetermined measures to the measures based on the **nature**, **scope**, **context** and **purposes** of the processing.
- Controller **must** take into account the risks for the rights and freedoms of natural persons (adequate policies)

The role and the responsabilities of the data processor

- Processor is the person (natural or legal person) who processes data on behalf of the controller.
- It mean that processors do not determine purposes and means of the processing.
- The controller in appointing a processor must:

a) Check that it provides sufficient guarantees.

b) Discipline processing through a contract or other legal act (written or electronic form).

Mandatory elements of the contract

- Indication that data processing takes place only on documented instructions from the controller.
- Guarantee that the persons authorized to process personal data are committed to confidentiality or have a legal obligation.
- Adoption of the necessary security measures (ex art. 32).
- Respect conditions for using a sub-processor
- Assistance to the controller for security measures
- Assistance to the controller to allow the exercise of the rights of the interested party.
- Obligation to cancel or return data at the end of the processing.
- Make available any information necessary to demonstrate compliance with contractual obligations and contribute to audit activities, including inspections, carried out by the controller
- Information obligation if, in his opinion, an instruction violates the Regulation

Sub-processor

- Using a sub-processor is legitimate only if the use is authorized in writing by the controller.
- Functions of the sub-processor must be defined by contract with the same mandatory elements.
- In case of omission of the sub-manager, the person in charge retains full responsibility towards the data controller.

How controller and processor comply with the general obligation?

- Adopting data protection by design and data protection by default measures
- Carrying out an assessment of the impact of the processing (Data protection impact assessment) – compulsory in specific cases.
- Appointing a DPO, where necessary
- Adhering to codes of conduct or acquiring certification (element to demonstrate compliance with obligations)

I. Data protection by design and data protection by default (art. 25 GDPR)

- Data protection by design means adopting technical and organizational appropriate measures in order to implement data protection principles and minimize risks for data subjects:
  a) Pseudo-anonymization
  b) Minimization
- Data protection by default means putting in place adequate technical and organizational measures to ensure that only the necessary data are processed, by pre-defined setting.
- Certification mechanism can be used to demonstrate compliance with these two obligations.

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

Controller and processor: duties and responsibilities/second part

The centrality of the Controller and Processor in the new European framework

- The Regulation dedicates to the discipline of the obligations of the controller and, separately, of those of the processor the entire Chapter IV.
- In the Regulations, controllers and processors assume a greater centrality than in the previous directives.

How controller and processor comply with the general obligation?

1. Adopting the adequate measures of data protection by design and data protection by default (art. 25 GDPR).
2. Appointing a representative for controllers not established in the Union
3. Assuring that any person processing data act under the authority of the data controller (Article 29)
4. Recording processing activities (Article 30)
5. Cooperating with Authorities and Data Protection Responsible (art. 31)
6. Implementing measure for the security of processing (art. 32-33-34)
7. Carrying out an assessment of the impact of the processing (Data protection impact assessment) – compulsory in specific cases. (35-36)
8. Appointing a DPO, where necessary (37-38-39)
9. Adhering to codes of conduct or acquiring certification (element to demonstrate compliance with obligations) (40-41-42)

2. Obligation to appoint a representative for controllers not established in the Union

- Representative designation must be in writing.
- The obligation to designate is not necessary in just two cases:

a) Occasional processing that is not on a large scale or includes sensitive data and data related to criminal convictions

b) Processing is carried out by public authorities or public bodies.

- The representative must be established in one of the Member States where the persons concerned are located.
- The representative has the obligation to speak (in addition or in replacement) with interested parties and with the Authority.
- Appointment of the representative is without prejudice to the legal actions that can be brought against the owner.

3. Processing under the authority of the data controller or under the authority of the data controller (art. 29)

- Processor or or any other person acting under its authority or under the responsibility of the Data Controller cannot process data unless instructed by the data controller.

4. Obligation to record processing activities (art. 30)

- Obligation lies on: a) controller or his representative b) processor.
- Compulsory information to be included in the register: a) name and contact details of the owner or manager (s); b) processing purposes; c) description of the categories of data subjects and categories of personal data; d) description of categories of recipients; e) transfers of personal data abroad; f) where possible, deadlines set for the deletion of data; g) general description of the security measures.
- Records are kept in writing, including electronic ones

5. Obligation to collaborate with Authorities and Data Protection Responsible (art. 31)

- Obligation on the controller, processor and (if existing) representative to cooperate on request with national control authority or European ones

6. Security obligation (art. 32)

- The controller and the processor must implement appropriate technical and organizational measures, taking into account the state of the art, the implementation costs and the nature, scope, context and purposes of processing.
- Security equally covers confidentiality, integrity and availability
- Security should be considered following a risk-based approach: the higher the risk the more rigorous the measures that the controller or the processor needs to take.
- Security of processing should be regarded within the overall GDPR accountability framework for data protection, which is also risk-based and impact-based and aims to fit into the specific operational context and practices of an organization.

Steps

- Definition of the processing operation and its context.
- Understanding and evaluation of impact.
- Definition of possible threats and evaluation of their likelihood (threat occurrence probability).
- Evaluation of risk (combining threat occurrence probability and impact).

Main Requirements

- Personal data should be pseudonymised and encrypted where possible.
- Ongoing confidentiality, integrity, availability and resilience of processing systems and services must be ensured..
- In case of a detrimental physical or technical incident, access to personal data must be able to be restored quickly.
- Organizations must implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures that are designed to ensure the security of processing.

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

Controller and processor. Third part

Data protection impact assessment (DPIA)

- Definition : The GDPR does not formally define the concept of a DPIA as such, but its minimal content is specified by Article 35(7) and by recital 84
- A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data4.
- DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation

Risk based approach and DPIA

- In line with the risk-based approach embodied by the GDPR, a DPIA is not mandatory for every processing operation. DPIA is only required when the processing is "likely to result in a high risk to the rights and freedoms of natural persons"

Nine criteria to identify processing that require DPIA

- Evaluation or scoring, including profiling and predicting
- Automated-decision making with legal or similar significant effect
- Systematic monitoring
- Sensitive data or data of a highly personal nature
- Data processed on a large scale
- Matching or combining datasets
- Data concerning vulnerable data subjects
- Innovative use or applying new technological or organisational solutions
- When the processing in itself "prevents data subjects from exercising a right or using a service or a contract

How to carry out a DPIA?

- The DPIA should be carried out "prior to the processing"
- The controller is responsible for ensuring that the DPIA is carried out (Article 35(2))
- The controller must also seek the advice of the Data Protection Officer (DPO)
- The controller must "seek the views of data subjects or their representatives" (Article 35(9)), "where appropriate"

The methodology *aka* the content of the evaluation

- A description of the envisaged processing operations and the purposes of the processing";

- An assessment of the necessity and proportionality of the processing";

- An assessment of the risks to the rights and freedoms of data subjects";

- The measures envisaged to:

- "address the risks";
- "demonstrate compliance with this Regulation".

Publishing

- Publishing a DPIA is not a legal requirement of the GDPR, it is the controller´s decision to do so.
- Controllers should consider publishing at least parts, such as a summary or a conclusion of their DPIA.

Prior consultation/1

- Controller must consult the supervisory authority if the processing "is likely to result in a high risk to the rights and freedoms of natural person".
- Whenever the data controller cannot find sufficient measures to reduce the risks to an acceptable level (i.e. the residual risks are still high), consultation with the supervisory authority is required
- Authority gives a written opinion
- Obligation to consult the Authority also by the States in the case of adoption of legislative measures relating to this

Prior consultation/2

- Authority gives a written opinion
- It should however be stated that regardless of whether or not consultation with the supervisory is required based on the level of residual risk then the obligations of retaining a record of the DPIA and updating the DPIA in due course remain

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

The Data Protection Officer (DPO)

DPO definition?

- An independent person with expert knowledge who monitors and facilitates compliance with the GDPR
- An instrument to promote (and demonstrate) compliance.

Principle of Accountability / Organisational measure

When is a DPO required?

When the processing:

1. is carried out by a **public authority**
2. requires **regular and systematic monitoring** on **a large scale**
3. consists of processing on a **large scale** of **special categories** or **criminal data**

\+ when Union or Member State law impose it.

DPO Identikit

- **Independent** and unbiased
- **Expert knowledge** in data protection law and practices
- **Easily accessible**
- Can be **one for many**
- **Able** to perform Art 39 tasks
- Can be an **employee or external**
- **Involved** properly and in a timely manner
- Reports **directly** to the highest management
- Bound by **secrecy** and **confidentiality**

Controller/Processor's obligations (1/2)

- **Appoint** a DPO when required
- **Involve** the DPO in a proper and timely manner
- Provide **resources** necessary to carry out art 39 tasks
- Provide **access** to personal data and processing operations
- Support the DPO in **maintaining their expert knowledge**

...

Controller/Processor's obligations (2/2)

- Ensure the DPO does **not** receive any **instructions**
- Ensure **direct line** between DPO and highest management
- **Not dismiss or penalise** the DPO for performing their tasks
- Protect the DPO from potential **conflict of interest**
- **Provide** the DPO's **contact details** to the public and the Authorities

What does the DPO do?

- ✓ **Informs and advises** the controller / processor
- ✓ Monitors compliance and performs **audits**
- ✓ Provides **training**, and raises awareness
- ✓ Advises and checks **DPIAs**
- ✓ Acts as **intermediary** between the controller/processor and regulators and individuals
- ✓ Monitors legal, regulatory and technical **developments**
- ✓ Regularly **updates** the highest management

What does not the DPO do?

- Acts on the basis of instructions
- Take decisions/lead product or service changes
- *Complete* Data Protection Impact Assessments
- Draft/negotiate contracts
- Draft/maintain policies, protocols, technical documentation etc.
- Liaise with vendors/partners to check *their* privacy compliance

Thank you!

Dott. Beatrice Cavicchioli
beatrice.cavicchioli

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

Independent supervision / Data Protection Authority

GDPR and national rules

- Independent supervision is an essential feature of Europena data protection law, according to art. 8 (3) of the Charter of Fundamental Rights
- GDPR (Chapter VI Regulation) requires, in this case, a national implementation through independent supervisory authority
- There remain discretionary space for national legislators.
- Implementation was to be completed by 25 May 2018.

General obligation

- Art. 51 – Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority'). .
- Obligation was already set by previous directives
- GDPR specifies the characteristics of the Authority, the status of the members conditions, tasks and powers.

Independence (art. 52)

- Internal independence (independence of its members in performing their activities – members can not receive prompts or soliciting them, they should prevent conflicts of interest and refrain any action incompatible with their duties)
- External independence (the Authority decisions must be taken independently, the law can not recognize to any Institution the power to revise Authority decisions')
- Substantial independence (Member States must provide with the necessary human, technical and financial resources and infrastructure – Authority must choose its own staff)

General conditions for the members of the supervisory authority (art. 53)

- Transparent procedure of appointment (GDPR requires States to choose between a parliamentary nomination, a government nomination, by the Head of State or by another independent body).
- Qualification of members (GDPR requires States to appoint member with solid experiences, skills and expertise in the field of personal data protection).
- Ceasing of the mandate (GDPR consents the ceasing of the mandate just in case of term expiry, of voluntary resignation or by office order (only in cases of gross negligence or if the member no longer meets the requirements)

Rules on the establishment of the supervisory authority

- GDPR refers to the law of the State for :

a) the establishment of each supervisory authority
b) the qualifications and eligibility conditions
c) the rules and procedures for the appointment
d) the duration of the term (no less than 4 years)
e) possible renewability and, if so, the number of mandates
f) Incompatibilities during and after the term of office and rules governing the cessation of employment.
g) duty of professional secrecy

Authority competence in terms of territorial scope

- Notion of territory of the State as a scope for performing assigned tasks.
- If processing takes place (under conditions of lawfulness) to fulfill a legal obligation to which the controller is subject (art. 6, par. Letter C) or for the execution of a task of public interest (art. 6, par. 1 lett. e) is competent theauthority of the country concerned.
- Authorities are not competent for processing carried out by jurisdictional authorities (judges).

Tasks (art. 57) (1)

1. monitor and enforce the application of this Regulation;
2. promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing
3. advise, in accordance with Member State law, the national parliament, the government, and other institutions.
4. promote the awareness of controllers and processors
5. provide information to any data subject concerning the exercise of their rights
6. handle complaints lodged by a data subject
7. cooperate with other supervisory authorities

Tasks (2)

8. monitor relevant developments,4
9. adopt standard contractual clauses
10. establish and maintain a list in relation to the requirement for data protection impact assessment
11. give advice on the processing operations
12. encourage the drawing up of codes of conduct
13. encourage the establishment of data protection certification mechanisms and carry out a periodic review of certifications

Tasks (3)

13. authorize contractual clauses
14. approve binding corporate rules pursuant to Article 47;
15. contribute to the activities of the Board;
16. keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and
17. fulfil any other tasks related to the protection of personal data.

Powers

a) Power of injunction
b) Investigative power (inspections)
c) Power of notification alleged violations
d) Power to obtain access to any personal data and any information and documents
e) Power of access to any premises of the controller and of the processor, including to any data processing equipment and means
f) Power to review certifications

Corrective powers towards the controllers and the processors

a) Warnings (where processing operations likely to infringe provisions)
b) Reprimands (where processing operations have infringed provision)
c) Orders (*to comply with the data subject's requests* and *to bring processing operations into compliance with the provisions* and *to communicate a personal data breach to the data subject*)
d) Order the rectification or erasure of personal data or restriction of processing and *order the suspension of data flows to a recipient in a third country*
e) Impose a temporary or definitive limitation including a ban on processing
f) Withdraw a certification
g) Impose an administrative fine

Sanctions (art. 83)

- Administrative pecuniary sanctions pursuant to art. 83
  a) Up to 10,000,000 euros.

  b) For companies, up to 2 percent of worldwide annual turnover if above previous threshold.
- Doubled thresholds if violation concerns basic principles of treatment, rights of data subjects, data transfers abroad, non-compliance with order, limitation or obligation placed by the Authority.
- GDPR admits States provide other sanctions (administrative and criminal penalties).

Identifying a lead supervisory authority: the key concepts

- Cross-border processing (within EU).
- 'Substantially affects'.
- Lead supervisory authority
- Main establishment

Competence of the lead supervisory authority

- Lead Supervisory Authority is the sole interlocutor of the data controller or data processor.
- Other Authorities may receive complaints if the object concerns only an establishment in its State (duties of information to the Lead Authority

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

European Institutions: the EDPB and the EDPS

Ms. Nerea Peris Brines – Legal Officer, EDPB

EDPB Tasks and Duties

PROVIDE **GENERAL GUIDANCE**

ADVISE THE EUROPEAN COMMISSION

ADOPT **CONSISTENCY FINDINGS** IN CROSS-BORDER CASES

PROMOTE **COOPERATION** BETWEEN NATIONAL SUPERVISORY AUTHORITIES.

ADOPT **BINDING DECISIONS** TOWARDS NATIONAL SUPERVISORY AUTHORITIES.

EDPB Membership and Participation

Members

- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- EDPS
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- UK*

Members with less rights

- Iceland
- Lichtenstein
- Norway

Other Participants

- European Commission
- Observers

EDPB Expert Subgroups

Borders, Travel & Law Enforcement

Compliance, e-Government and Health

Cooperation

Coordinators

Enforcement

Financial Matters

International Transfers

IT Users

Key Provisions

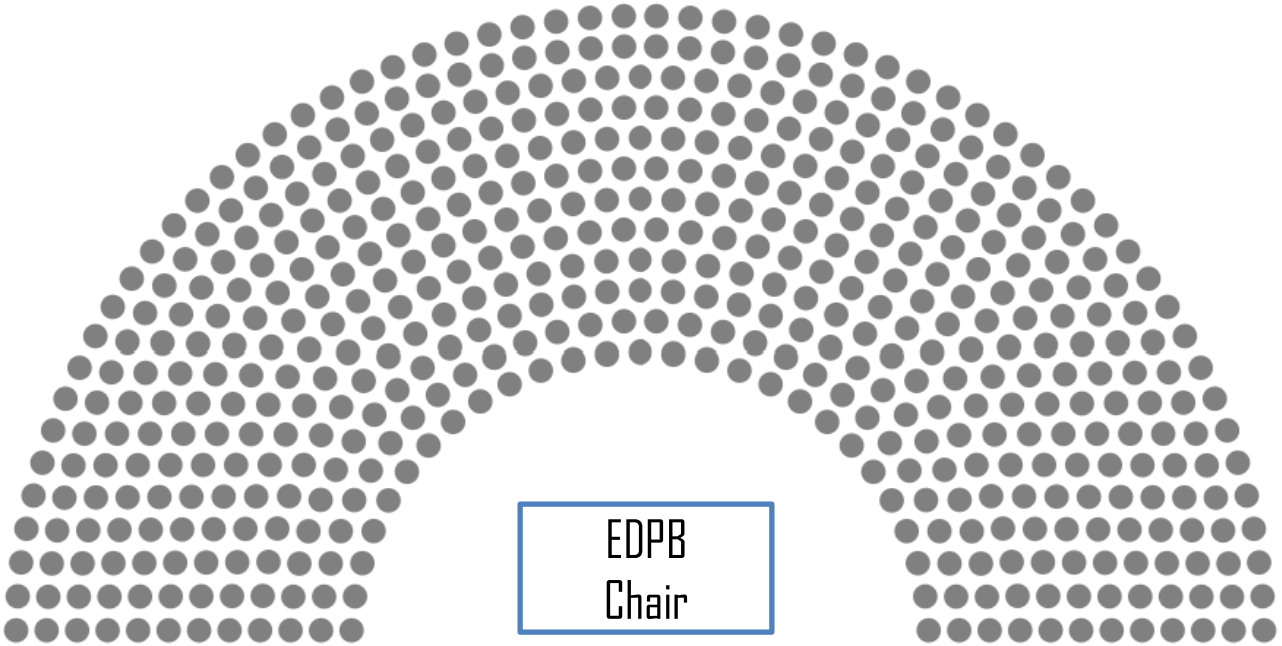
Social Media

Strategic Advisory

Taskforce on Administrative Fines

Technology

EDPB Plenary Meetings



Dott.ssa Beatrice Cavicchioli

Brief background on the EDPS

- Independent supervisory authority whose primary objective is to ensure that **EU institutions and bodies** respect the right to privacy and data protection when they process personal data and develop new policies.

- Established in 2001

- Now governed by **Reg. 2018/1725** (Not GDPR!)

- Shares many characteristics with National Data Protection Authorities

EDPS Tasks and Duties

SUPERVISE
EU INSTITUTIONS AND BODIES

ADVISE
EU INSTITUTIONS AND BODIES

COOPERATE WITH NATIONAL SA AND OTHER SUPERVISORY BODIES

MONITOR **NEW TECHNOLOGY**

INTERVENE BEFORE THE **CJEU**

EDPS Powers

Investigative powers

Obtain information, audit, notify alleged infringements, access to any premises, personal data, processing equipment and means.

Corrective powers

Issue warnings, reprimands, refer matters to the EU Parliament, Council and Commission, injunctions, administrative fines

Authorisation and advisory powers

Advise data subjects, EU institutions and bodies both in their role of controllers/processors and in their role of EU legislator, authorise administrative arrangements, intervene before the CJEU

Thank you!

edpb
European Data Protection Board

Ms. Nerea Peris Brines
Legal Officer

Dott.ssa Beatrice Cavicchioli
beatrice.cavicchioli

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

International Data Transfer and Flow of Personal Data

Introductory remarks/1

- The GDPR provides, as key objective, for the free flow of data **within** the European Union. Restrictions or prohibitions are forbidden. The area of free data flow has been extended by the EEA Agreement to Iceland, Liechtenstein and Norway
- The free flow of data is **necessary** to the development of the digital society and in particular to the adoption of artificial intelligence techniques. (international trade and cooperation)
- The free circulation of data outside European Union **increases risks for rights and freedoms** (the level of protection is not the same everywhere). Individuals risk losing the protection of the GDPR if their personal data is transferred outside of the EEA.

Introductory remarks/2

- The GDPR restricts transfers of personal data outside the EEA, or the protection of the GDPR, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies.
- The flow of personal data for prevention of crimes, investigations, detections and prosecutions falls under the scope of directive 680/2016.

The concept of personal data transfer

- The concept of "transfer of personal data" covers the flows of personal data from a controller to a recipients.
- Transfer does not mean the same as transit.
- The concept of personal data transfer outside of the EU means that a controller is sending personal data, or making it accessible, to a receiver to which the GDPR does not apply. Usually because it is located in a country outside the EU.

General Principle

- Transfers may take place if the level of protection outside of the European Union is adequate. It means that the third country shows and adequate level of protection or if the recipient (controller or processor) provides appropriate measures in order to safeguard the rights of the data subjects.
- The reform of EU data protection legislation adopted in 2016 offers a diversified toolkit of mechanisms to transfer data to third countries: **adequacy decisions**, **standard contractual clauses**, **binding corporate rules**, so-called "derogations

Adequacy decision (art. 45)

- The European Commission has the power to determine, on the basis of article 45 of Regulation (EU) 2016/679 whether a country outside the EU offers an **adequate** level of data protection.
- «Adequate» means that the level of protection of personal data, regarding fundamental rights is «essentially equivalent» to the European Union level
- The adequacy decision has binding effects and Member States must respect it.
- European Commission may revise its decision at any time and periodically

The procedure

- The adoption of an adequacy decision involves:

a) a proposal from the European Commission

b) an opinion of the European Data Protection Board

c) an approval from representatives of EU countries

d) the adoption of the decision by the European Commission

- At any time, the European Parliament and the Council may request the European Commission to maintain, amend or withdraw the adequacy decision on the grounds that its act exceeds the implementing powers provided for in the regulation.

Grounds of the evaluation

a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral (data protection legislation).

b) the existence and effective functioning of one or more independent supervisory authorities.

c) the existence of international commitments that the third country has entered into or other obligations arising from legally binding conventions

What 'adequacy decisions' have there been?

- As at November 2020 the Commission has made a full finding of adequacy about the following countries and territories: Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.
- Adequacy talks are ongoing with South Korea.
- The Commission has made partial findings of adequacy about Japan, Canada and the USA.

❖ The adequacy finding for Japan only covers private sector organisations.

❖ The adequacy finding for Canada only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA. For more details please see the Commission's FAQs on the adequacy finding on the Canadian PIPEDA.

❖ The adequacy finding for the USA is only for personal data transfers covered by the EU-US Privacy Shield framework.

A critical example: the transfer from EU to USA

- ✓ The Commission adopted several general adequacy decisions (related to third countries).
- ✓ The adequacy of USA legislation has been always challenged.
- ✓ The Commission adopted an adequacy decision (Safe Harbour decision) but the ECJ declared it invalid in Schrems/Data Protection Commissioner because:

a) decision refers just to private companies which subscribe it and does not oblige public authorities. According to the USA legislation enforcement agencies may collect data stored by this companies.

b) does not provided any judicial or administrative redress No-US citizens against these agencies.

- ✓ Transfers for a while continued on the basis of Binding Corporate Rules decision or Contractual Clauses decision.
- ✓ A new decision was adopted in 2016 after the conclusion of the agreement on Privacy Shield

Transfers subject to appropriate safeguards (art. 46)

- Appropriate safeguards are:

✓ A legally binding instrument between public authorities.

✓ Binding corporate rules

✓ Standard data protection clause

✓ Codes of conduct

✓ Certificate mechanisms

Appropriate safeguards as tools for transfers between public bodies

- a legally binding and enforceable instrument, Article 46 (2) (a) GDPR or
- provisions to be inserted into administrative arrangements, Article 46 (3) (b) GDPR.

- These instruments and arrangements may be of bilateral or multilateral nature. Such instruments have to be legally binding and enforceable. Therefore, international treaties, public-law treaties or self-executing administrative agreements may be used under this provision.
- They should contain definitions of the basic personal data concepts and rights in line with the GDPR relevant to the agreement in question.
- Any legally binding and enforceable instrument should encompass the core set of data protection principles and data subject rights as required by the GDPR

Standard Contractual Clauses

- Contractual clauses between the data exporting controller and the recipient are a specific mean to safeguard a sufficient level of protection.
- European Commission develops (together with EDPB) standard contractual clauses. There are two sets of standard clauses available for controller to controller transfers and one for controller to processor transfers
- These standard clauses are certified as proof of adequate data protection.
- Controllers may formulate ad hoc clauses that must ensure the same level of protection

Binding Corporate Rule

- The Binding corporate rules take place within the same group of enterprises or undertakings that are part of a joint economic activity.
- BCR's must be approved by the competent supervisory authority.
- Conditions:

1. Legally binding
2. Confer enforceable rights
3. Describe data transfers and how data protection principles will be applied.

Derogations

- Explicit consent for the data transfer.
- Contractual relationship where the transfer of data abroad is necessary.
- Important reason of public interest
- Establish, exercise or defend legal claims.
- Protect a vital interest.
- For the transfer of data from public register

Transfer based on international agreements

- EU may conclude international agreements with third country regulating the transfer of personal data for specific purposes.
- These agreements must assure specific safeguards to ensure protection of personal data.
- Main agreements:

✓PNR

✓Messaging data

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

Special categories of data

Special categories of data

- Under EU law there are **special categories** of data that need an enhanced protection because the processing of these data may pose an higher risk to the data subject
- The GDPR defines partly different rules for sensitive data (art. 9) and for personal data relating to criminal convictions and offences (art. 10).
- In order to lawfully process special category data, you must identify both a lawful basis under Article 6 of the GDPR and a separate condition for processing under Article 9. These do not have to be linked.

Sensitive data

- Personal data revealing racial or ethnic origin
- Personal data revealing political opinions
- Personal data revealing religious or other beliefs
- Personal data revealing trade union membership
- Personal data concerning health
- Personal data concerning sexual life or sexual orientation
- Genetic data and biometric data

➢ Special category data includes personal data **revealing or concerning** the above types of data. Therefore, if you have inferred or guessed details about someone which fall into one of the above categories, this data may count as special category data. It depends on how certain that inference is, and whether you are deliberately drawing that inference.

Genetic data and biometric data

- 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question
- Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person"

Prohibition and derogation

- Par. 1, Art. 9 GDPR: The processing of personal data revealing … shall be prohibited

- Par. 2 Art. 9 GDPR: Paragraph 1 does not apply if it applies one of the following conditions:
- (a) Explicit consent
- (b) Employment, social security and social protection (if authorised by law)
- (c) Vital interests
- (d) Not-for-profit bodies
- (e) Made public by the data subject
- (f) Legal claims or judicial acts
- (g) Reasons of substantial public interest (with a basis in law)
- (h) Health or social care (with a basis in law)
- (i) Public health (with a basis in law)
- (j) Archiving, research and statistics (with a basis in law)

Conditions of legitimacy aka conditions which allows to superpose the prohibition/1

- Explicit consent to the processing for one or more specified purposes
- Union or Member States law can provide that the prohibition may not be lifted
- Processing is necessary to protect the vital interest of the data subject

Conditions of legitimacy aka conditions which allows to superpose the prohibition/2

- Processing is necessary for the purposes of carrying out the obligation and exercising specific rights in the field of social security, employment, social protection
- These cases must be provided for Union or Member States legislation or for by collective agreement
- Laws and collective agreements must provide appropriate safeguards

Conditions of legitimacy aka conditions which allows to superpose the prohibition/3

- Processing is necessary to protect the vital interest of the data subject or of another person where the data subject is incapable of giving consent

Conditions of legitimacy aka conditions which allows to superpose the prohibition/4

- Processing is carried out by a foundation, association or another no-profit body **with** a political, philosophical, religious and trade union aim.
- The processing **must solely relates** to the members or former members ot to persons that have a regular contact.
- The processing can not consist **in a disclosing outside that body** without the consent

Conditions of legitimacy aka conditions which allows to superpose the prohibition/5

- Processing relates to personal data that are manifestly made public by the data subject.

Conditions of legitimacy aka conditions which allows to superpose the prohibition/6

- Processing is necessary for the establishment, exercise or defense of a legal claim or whenever courts are acting in their judicial capacity.

Conditions of legitimacy aka conditions which allows to superpose the prohibition/7

- Processing is necessary for reason of substantial public interest
- Law is requested (Union law or Member States law) and must be proportioned to the aim pursued and respect the essence of the right.
- The law must also provide for specific measures to safeguard the rights and the interests of the data subject

Examples of substantial public interests

- Statutory and government purposes
- Administration of justice and parliamentary purposes
- Equality of opportunity or treatment
- Preventing or detecting unlawful acts
- Protecting the public
- Regulatory requirements
- Journalism, academia, art and literature
- Preventing fraud (to be continued)

Conditions of legitimacy aka conditions which allows to superpose the prohibition/8

- Processing is necessary for the purposes

a) of preventive or occupational medicine

b) of the assessment of the working capacity

c) medical diagnosis

d) of the provision of health or social care, or treatment or the management of health and social care system

- Processing is legitimate pursuant a law (EU or Member State) or pursuant a contract with a health professional (hold to the professional secret)

Conditions of legitimacy aka conditions which allows to superpose the prohibition/9

- Processing is necessary for reasons of public interest in the area of public health such as protecting against serious cross border threats to health (pandemia) or to ensure high standards of quality and safety of health care and of medicinal products or medical devices.
- Processing needs a law (EU or Member State)
- Law must provide specific measures to safeguard rights and freedoms and in particular professional secrecy.

Conditions of legitimacy aka conditions which allows to superpose the prohibition/10

- Processing is necessary for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes.
- Reference to art. 89, par. 1
- Need of a law (EU or Member States)

Further conditions or limitations

- Member States may introduce with regard to the processing of genetic data, biometric data or data concerning health
- There is room for national legislation

Personal data relating to criminal convictions and offences

- Processing is legitimate under the control of official authorities or when authorized by Union or Member State law.
- Need of appropriate measures, safeguards
- Comprehnsive register of criminal conviction must remain under the control of official authority

Consequences for the controller processing sensitive data/1

- There are additional limitations in case of automated individual decision-making.
- Controllers and processors located outside the EU which fall under the scope of the GDPR lose any exemption possibility with respect to the appointment of a representative in the EU if they process sensitive data on a large scale.
- Controllers and processors lose any exemption possibility with respect to the records of processing activities if they process sensitive data on a large scale.

Consequences for the controller processing sensitive data/2

- The processing of sensitive data on a large scale triggers the obligation to conduct a data protection impact assessment.
- If the core activity of the controller or processor consists of processing sensitive data on a large scale, then the controller or processor has the obligation to designate a data protection officer.
- The controller or processor must assure an higher level of security protection in order to avoid data breaches

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

Minors and data protection

Fundamental principles related to children

1) – Best interest of the child
2) – Protection and care necessary for the wellbeing of children
3) – Right to privacy
4) – Representation
5) – Competing interests: privacy and the best interest of the child
6) – Adapting to the degree of maturity of the child
7) – Right to participate

Introductory remarks

- The directive 95/46 does not contain any provision related to children. Despite that it applies to all individuals, adult or not. Differences were established at national level by Member States.
- The GDPR provides many opportunities to protect children, empower them and let them participate in all kinds of processes relating to them.

Who is actually considered 'a child'?

- According to the UN Convention on the Rights of the Child (UNCRC), a child is a person under 18.
- GDPR does not give any definition of child. So we have to refer to international legal text

The protection of minors under in the GDPR

1. The GDPR offers a few provisions that refer to children, either explicitly (e.g. articles 8, 12, 40 GDPR). See also Recitals (38) and (58) of the GDPR
2. or implicitly (by referring to the mechanism of article 8 GDPR, e.g. article 17 GDPR)
3. Despite the fact that some important provisions do not mention children, they are nevertheless considered particularly relevant for children (e.g. article 25, 35 GDPR) because the minor as "weak subject" must be considered by controllers when they project their data processing

Explicit Provision

Art. 8

- Article 8 GDPR specifically deals with the issue of providing consent and children. It affects one of the legitimacy condition set by the GDPR. As You remember, according to Article 6(1)(a) of the GDPR, the processing of personal data is considered lawful if data subjects provide their consent to this processing for one or more specific purposes.
- The general rule provides for a **parental consent** requirement for **all youth under 16 years old** (or lowered age) in situations where information society services are offered directly to them, and consent is the lawful ground on the basis of which the data is processed-
- Over 16 years old (or the lower age decided by Member States), children may give their own consent without the intervention of parents.
- These requirements do not affect the general contract law of EU Member States such as the rules on the validity, formation or effect of a contract in relation to children.

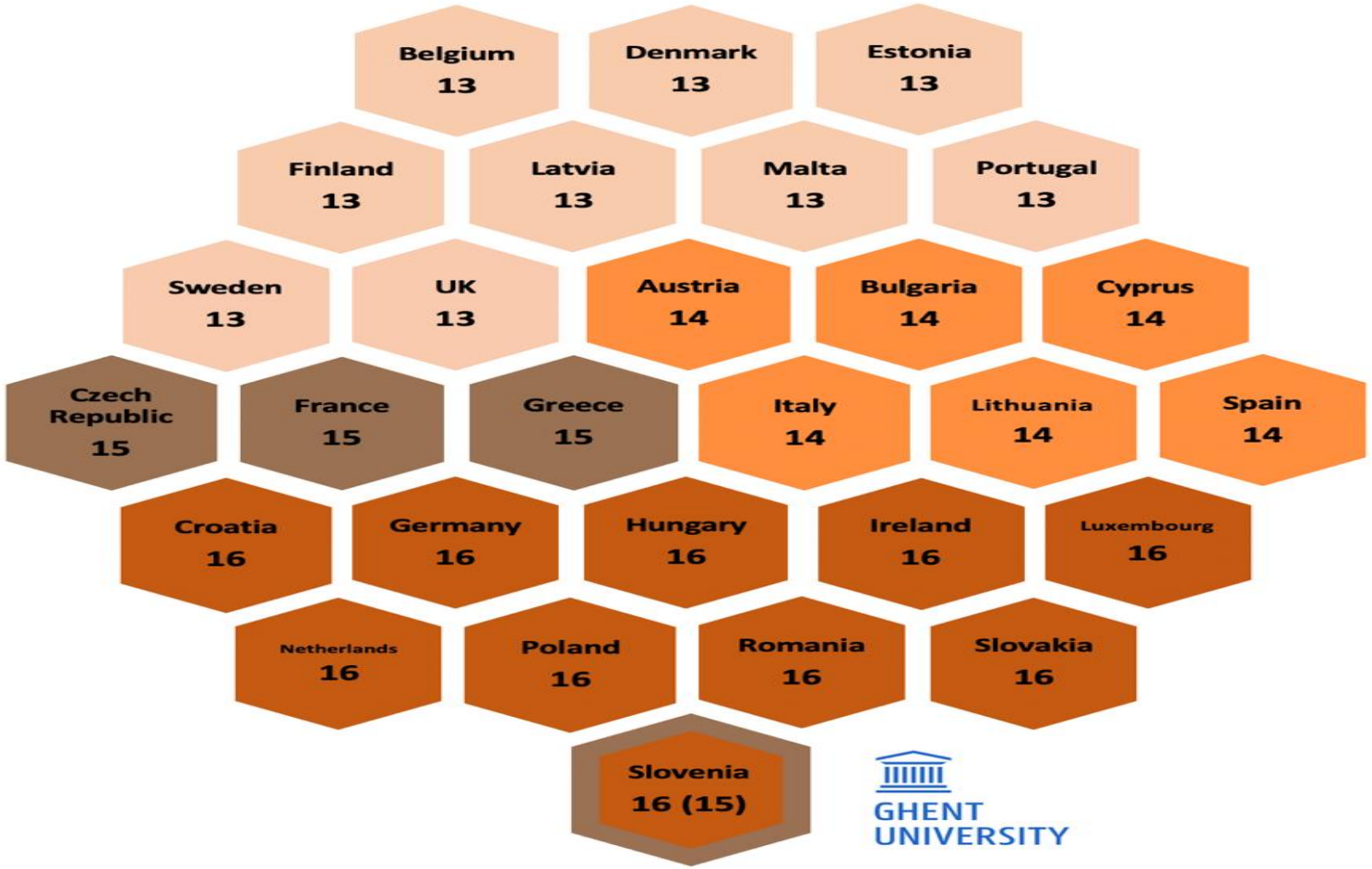
The parental control

- Art. 8 gives two options for the parental control:

1. collect such consent directly from the data subject's parents, or
2. the parents "authorize" the data subject's consent.

- No processing of personal data may be performed, before one of these two options has been played out.

EU Member States



Material Scope of Article 8

- It applies only to services provided online ("information society services").
- It only applies if the offer of information society services is expressly, solely or mainly, intended for children.
- It only applies in case the legal basis for processing personal data is consent
- "Minors" for the purposes of art. 8 GDPR are children below 16 years of age. The GDPR, however, allows member states to lower this minimum age to 13. For instance, Austria and Italy have lowered the threshold age to 14 years.

Article 12 GDPR and Recital 58

- Article 12 GDPR requires the provision of information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.
- Recital 58 GDPR provides that, given that children merit specific protection, data controllers need to provide transparent privacy notices.

Art. 40 GDPR

- Il deals with the Codes of conduct.
- The codes of conduct are, under the GDPR, an important instrument to contribute to the proper application of the Regulation
- They take account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.
- They help controllers (micro, small and medium-sized enterprises) to decide how to organize the processing in order to respect all obligation set by the GDPR.
- The adhesion to a code of conduct is a proof to demonstrate the effort to be complained wirh the GDPR

Codes of conduct and minors

- According with par. 2, let. G) codes shall contain provisions about the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained.

Implicit provisions

Art. 17 GDPR

- Article 17 GDPR provides for the right to erasure ('the right to be forgotten'). It puts more emphasis on what this right can mean for children (see also recital 65)
- That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet.
- The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.

Art. 22 GDPR

- Article 22 GDPR, regulating automated individual decision-making, including profiling, does not mention children. It does confer the right upon a data subject not to be subject to profiling, which produces a legal or a similarly significant effect.
- Recital 38 GDPR mentions profiling as one of the activities for which children merit specific protection.
- Recital 71 GDPR provides that 'such a measure' (profiling) should not concern a child. Although it has been argued that this means that profiling of children is prohibited, a close reading of the article shows that this is only the case if a decision is made that has a legal or similarly significant effect

Minors as weak subjects

General principles

- The general principles provided for in GDPR must naturally be adequately adapted when applied to children. Some examples:

a) The duty to process personal data in accordance with the principle of fairness must be interpreted strictly when it concerns a child.

b) Minimization principle requires that only adequate, relevant and non-excessive data can be collected and processed. Controllers should pay special attention to the situation of the child, as they must respect their best interests at all times.

Privacy by design and by default obligation

- The provisions on privacy by design and by default (article 25 GDPR) are particularly useful mechanisms for children because they require children to be considered as weak subject since the design of the processing.
- Products aimed at children, such as connected toys, integrate important principles, such as data minimization, in the design of the products.
- Data minimisation could, in any case, mean something different when personal data of children are concerned

Article 35 GDPR (DPIAs)

- It requires a prior assessment when a high risk to the rights of a data subject exists.
- The recitals on what may constitute a high risk do not mention children but they do mention profiling (recital 91 GDPR).
- It could be a good practice to carry out DPIAs every time personal data of children are being processed

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

Corrective measures and sanctions

Introduction

- Art. 24 of Directive 95/46 / EC left the Member States with the task of take appropriate measures to ensure full application of the provisions of the directive itself.
- Art. 58 and art. 83 of the GDPR define a system of corrective measures to guarantee the compliance with the new regulatory framework
- In the context of the new GDPR, the administrative sanction is part of a remedial process whose objective is essentially to restore the correctness of processing

Art. 58

- Art. 58 of the GDPR provides for both corrective measures ex ante, which therefore precede a violation and corrective measures ex post.
- Among the ex ante measures we can place **the warnings** to the data controller in cases where the processing may likely violate the Regulation.
- Among those ex post there are **warnings, injuctions, orders** (to limit the processing - including prohibition, rectification, cancellation and limitation or suspension of flows to a third country.
- The decision to add the pecuniary administrative sanction to the corrective measure is, therefore, left to the discretion of the Authority ex art. 83

Art. 83

- Article 83 is dedicated to administrative sanctions.
- For violations art. 83 provides for a maximum penalty equal to ten million euros or, for companies alone, equal to two per cent of worldwide turnover of the year preceding the violation.
- For the most serious violations, the fine is doubled (a maximum penalty equal to twenty million euros or, for companies alone, equal to four per cent of worldwide turnover of the year preceding the violation).
- There is a maximum ceiling but not a minimum ceiling. The sanction is not mandatory

I. Principles

1. Infringement of the Regulation should lead to the imposition of "equivalent sanctions".
2. Like all corrective measures chosen by the supervisory authorities, administrative fines should be "effective, proportionate and dissuasive".
3. The competent supervisory authority will make an assessment "in each individual case".
4. A harmonized approach to administrative fines in the field of data protection requires active participation and information exchange among Supervisory Authorities

II. Assessment criteria in article 83 / 1

a) the nature, gravity and duration of the infringement.

b) the intentional or negligent character of the infringement

c) any action taken by the controller or processor to mitigate the damage suffered by data subjects.

d) the degree of responsibility of the controller or processor taking into account technical and organizational measures implemented by them pursuant to Articles 25 (privacy by design and by default) and 32 (security).

II. Assessment criteria in article 83 / 2

e) any relevant previous infringements by the controller or processor;

f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

g) the categories of the personal data affected by the infringement.

h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

II. Assessment criteria in article 83 / 3

i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures.

j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42.

k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement

Penal sanctions

- Art. 84 of the GDPR allows Member States to establish «Other sanctions for violations of this regulation, in particular for violations not subject to administrative pecuniary sanctions "
- It authorizes Member states to adopt or maintain penal sanctions.
- Penal sanctions provided for at national level must respect the principle of *ne bis in idem*. It means they can not be based on the same legal cases

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI, GIURIDICI E STORICO-POLITICI

Unit of Data Protection Law

Prof. Marco Orofino

Modern challenges in personal data protection

General remarks

- Digital age is characterized by the widespread use of computers, internet and digital technologies.
- Collection and processing of data is global and cross-boarder flows are increasing everyday.
- Such processing bring benefits in everyday life and, as well many risks
- Legislations on data protection must be re-interpreted for new phenomena such as processing of big data, artificial intelligence techniques and robotics

Big data

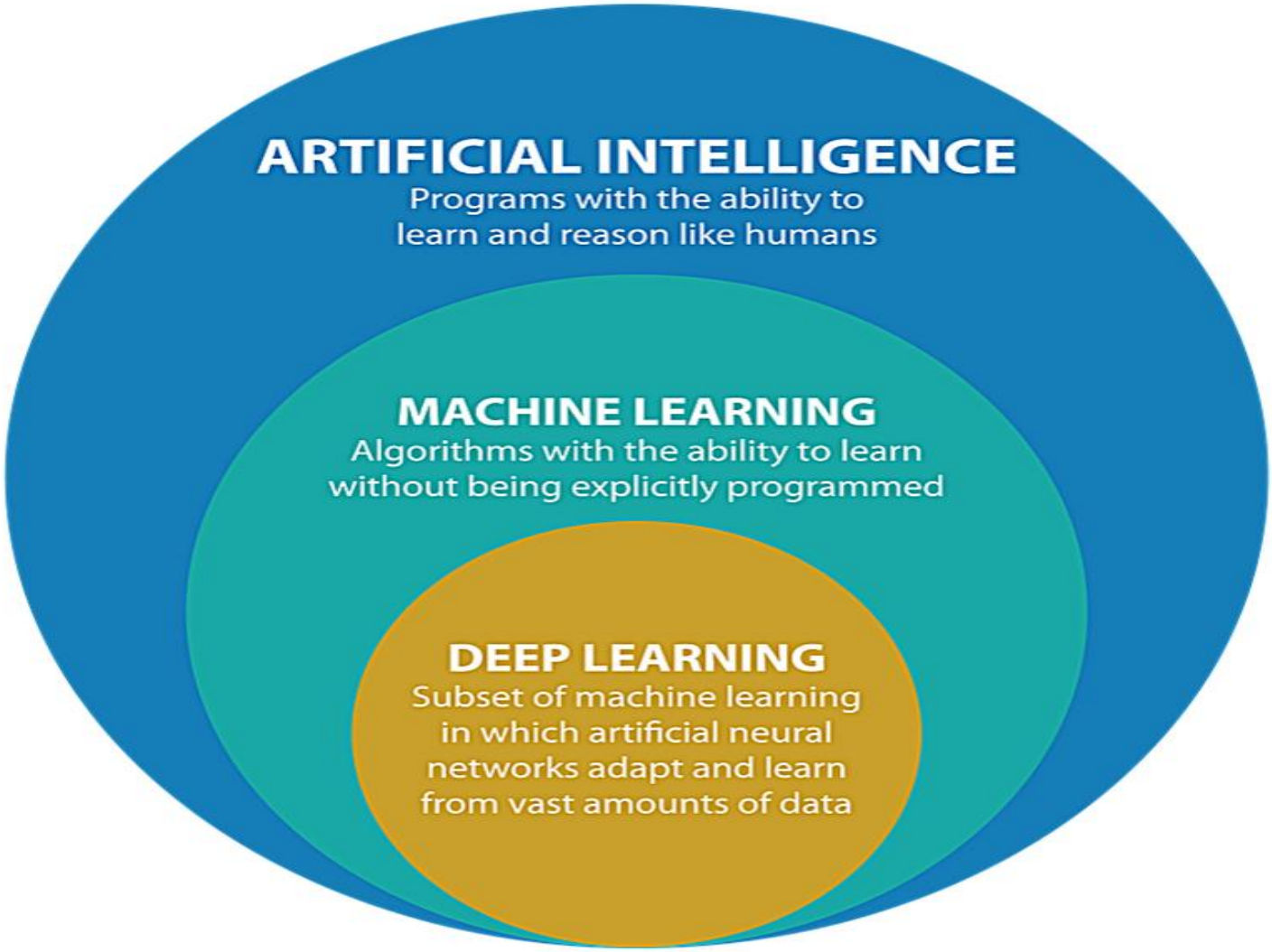
- Big data is a buzz word that it is commonly used to explain the "growing technical ability to collect process and extract new and predictive knowledge from great volume, velocity and variety of data".
- Sources of data are various: people and their smartphone, machines, sensors, climate information, digital pictures and video. A great part of these data are personal, often very sensitive
- Big data also refers to the processing, analysis and evaluation to gain useful information.
- Data processing techniques may impact on democratic processes to influence electors or on competition to influence consumers.
- Big data impact on people behaviors, on their self-determination (on their free will) and may produce conformism (which is very dangerous for the progress of the societies)

Algorithms and artificial intelligence

- An algorithm is a step by step procedure for calculation
- Artificial intelligence refers to the intelligence of machines acting as "intelligent agents" that is to sat that a machine mimics "cognitive functions".
- Computational possibility of AI is going to overpass the capacity of human brains.
- Algorithms drive machines action

Artificial Intelligence Machines

- Artificial Intelligence machines programs with the ability to learn and reason like humans
- Machine learning and deep learning are two subsets of artificial intelligence which have garnered a lot of attention over the past two years.


ARTIFICIAL INTELLIGENCE
Programs with the ability to learn and reason like humans
MACHINE LEARNING
Algorithms with the ability to learn without being explicitly programmed
DEEP LEARNING
Subset of machine learning in which artificial neural networks adapt and learn from vast amounts of data

Machine learning

- Machine learning algorithms almost always require structured data and are built to "learn" to do things by understanding labeled data, then use it to produce further outputs with more sets of data.
- The algorithms reproduces processes and set coordinates in order to get a specific result

Deep learning machines

- A subset of machine learning where algorithms are created and function similar to those in machine learning, but there are numerous layers of these algorithms- each providing a different interpretation to the data it feeds on.
- Such a network of algorithms are called artificial neural networks, being named so as their functioning is an inspiration or an attempt at imitating the function of the human neural networks present in the brain.
- Deep learning machines accept structured data and unstructured data

Have a look at the image

How a machine learning works?

- To help a machine learning algorithm You simply label the pictures of dogs and cats in a way which will define specific features of both the animals.
- This data will be enough for the machine learning algorithm to learn, and then it will continue working based on the labels that it understood, and classify millions of other pictures of both animals as per the features it learned through the said labels.

How a deep learning machine works

- Deep learning networks would take a different approach to solve this problem. The main advantage of deep learning networks is that they do not necessarily need structured/labeled data of the pictures to classify the two animals.
- The artificial neural networks using deep learning send the input (the data of images) through different layers of the network, with each network hierarchically defining specific features of images.
- This is, more or less similar to how our human brain works. The only difference is that Deep Learning needs million of pictures while for a baby is enough to see a cat or a dog twice.

Deep learning and data analytics

- Deep learning machine may be used in order to discover new patterns (data analytics).
- New patterns may be used to improve the systems implemented.
- New patterns may be used to discover new outputs in research.
- Just imagine what it means for health, intelligent transport systems, energy efficiency, urban planning, welfare

Data protection related issues I

- Identification of the controller/processor (liability)
- Impact on principle of purpose limitation and principle of data minimization.
- Impact on the information right (transparency)
- Impact on rights to access, rectify and erase

Data protection related issues II

- Interest of the controller as condition of legitimacy
- Profiling and automated decision
- Data portability
- **Security and privacy**