Cybersecurity and Privacy Preservation Techniques and Digital Security and Privacy

Luca Paoletti

September 2022

Contents

1 Lecture 1

Privacy and animals
An organism lays private claim to an area of land, water, or air and defends it against intrusion by members of its own species. These territorial patterns ensure propagation of species by regulating density to available resources.

Privacy and humans
The individual seeks privacy at some times and disclosure or companionship at other times. This basic process of interaction with others is usually discussed under the terms *social distance* and *avoidance rules.*

The modern idea of privacy
We switched from the idea to regulate mainly physical social distance, to the need to regulate the widespread of information about us. Privacy becomes a way to intend freedom.

Privacy and property
In very early times, the *right to life* served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually, the scope of these legal rights broadened and now the right to life has come to mean the right to enjoy life intangible, as well as tangible.

Privacy and strong powers
Instantaneous photographs and newspaper enterprise have invaded the sacred precints of private and domestic life. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery.

Privacy and surveillance by Authorities
Every humans being must have a protective shell between public and private life, in order to not be under control of those who knows his/her intimate beliefs.

The two different approach for regulating privacy in USA and EU
Privacy regulation i EU is described as *omnibus*, while privacy law in the USA is described as *sectoral.* In EU, one statute (Directive 95/46 first and Regulation 2016/679 now) typically regulates the processing of personal information in public and private sectors alike. In the absence of more specific regulation (Directive 2016/680 for the processing of personal data for judicial cooperation for example) the general privacy law in EU is able to set the terms for processing, storage and transfer of personal information. In EU, we have sectoral regulations in specific areas of data use, such as electronic communications (e-privacy). In USA, there are only sectoral laws (i.e., HIPAA, FERPA, ECPA). Other countries around the world are moving toward adopting comprehensive privacy legislation based on the European model.

CoE and EU
In Europe, privacy laws are shaped by the Council of Europe and European Union. It was Article 8 of the Council of Europe's Convention on Human Rights of 1950, which firmly established privacy protection as a critical human right claim in postwar Europe.

Nothing to hide
Data can be always interpreted. Privacy protects us from abuses by those in power, even if we're doing nothing wrong at the time of surveillance.

First definition of privacy

The claim of individuals to determine for themselves when, how, and to what extend information about them is communicated.
Privacy as an expression of the right to self-determination. The right to self-determination is a basis for democratic society.

German Constitutional Court

In the context of modern data processing, the general right of personality encompasses the protection of the individual against unlimited collection, storage, use and sharing of personal data. The fundamental right guarantees the authority conferred on the individual to, in principle, decide themselves on the disclosure and use of their personal data.

Public interest

Limitations of this right to 'informational self-determination' are only permissible if there is an overriding public interest. They require a statutory basis that must be constitutional itself and comply with the principle of legal clarity under the rule of law. The legislator must furthermore observe the principle of proportionality, It must also put in place organisational and procedural safeguards that counter the risk of violating the general right of personality.

privacy vs Data Protection

In EU, more than the idea of privacy, we use the expression of data protection. The two ideas are similar, but there are differences.

Charter of Fundamental Right of the European Union

Article 7 - Respect of private and family life. *Everyone has the right to respect for this or her private and family life, home and communications.*
Article 8 - Protection of personal data.

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 control by and independent authority*

EU's Lisbon Treaty

EU's Lisbon Treaty of 2007 explicitly recognized a right to data protection and also made the Charter of Fundamental Rights a legally enforceable document within the EU (European Court of Justice - Luxembourg).

TFEU

Acrticle 16 TFEU.

1. *Everyone has the right to the protection of personal data concerning them*
2. *The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.*
3. *The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.*

Article 12 of the Universal Declaration of Human Rights. *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

2 Lecture 2

The tech paradox
In general, you can only trust the biggest tech companies like Google, Facebook, Amazon, Microsoft and Apple to actually store your information securely. The technological landscape is very convergent to the big tech companies. On the other hand, they abuse it themselves within their surveillance capitalism.

EU data strategy
Data-driven innovation will bring enormous benefits for citizens, for example through improved personalised medicine, new mobility and through its contribution to the European Green Deal. In a society where individuals generate ever-increasing amounts of data, *the way in which the data are collected and used must place the interests of the individual first, in accordance with European values, fundamental rights and rules. Citizens will trust and embrace data-driven innovations only if they are confident that any personal data sharing in the EU will be subject to full compliance with the EU's strict data protection rules.* At the same time, the increasing volume of non-personal industrial data and public data in Europe , combined with technological change in how the data is stored and processed, will constitute a potential source of growth and innovation that should be tapped.

Regulation 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the EU. *Data value chains are built on different data activities: data creation and collection; data aggregation and organisation; data processing; data analysis, marketing and distribution; use and re-use of data. the effective and efficient functioning of data processing is a fundamental building block in any data value chain. However, the effective and efficient functioning of data processing, and the development of the data economy in the Union, are hampered, in particular, by two types of obstacles to data mobility and to the internal market: data localisation requirements put in place y Member States' authorities and vendor lock-in practice in the private sector.*

Non personal data?
The expanding Internet of Things, artificial intelligence and machine learning, represent major sources of non-personal data, for example as a result of their deployment in automated industrial production process. Specific examples of non-personal data include aggregate and anonymised datasets used for big data analytics, data on precision farming that can help monitor and optimise the use of pesticides and water, or data on maintenance need for industrial machines. If technological developments make it possible to turn anonymised data into personal data, such data are to be treated as personal data, and Regulation (EU) 2016/679 is to apply accordingly.

EU data strategy
Citizens should be empowered to make better decision based on insights gleaned from non-personal data. And that data should be available to all - whether public or private, big or small, start-up or giant. This will help society to get the most out of innovation and competition and ensure that everyone benefits from a digital dividend. This digital Europe should reflect the best of Europe - open, fair, diverse, democratic and confident. The EU can become a leading role model for a society empowered by data to make better decisions - in business and the public sector. To fulfil this ambition, the EU can build

on a strong legal framework - in terms of data protection, fundamental rights, safety and cyber-security - and its internal market with competitive companies of all sizes and varied industrial base. If the EU is to acquire a leading role in the data economy, it has to act now and tackle, in a concerted manner, issues ranging from connectivity to processing and storage of data, computing power and cybersecurity. Moreover, it will have to improve its governance structures for handling data and to increase its *pools of quality data* available for use and re-use.

The European data space will give businesses in the EU the possibility to build on the scale of the Single market. Common European rules and efficient enforcement mechanisms should ensure that:

- data can flow within the EU and across sectors;
- European rules and values, in particular personal data protection, consumer protection legislation and competition law, are fully respected.
- the rules for access to and use of data are fair, practical and clear, and there are clear and trustworthy data governance mechanisms in place; there is an open, but assertive approach to international data flows, based on European values.

The Commission's vision stems from European values and fundamental rights and the conviction that *the human being is and should remain at the centre.* The EU should create an attractive policy environment. The aim is to create a single European data space - a genuine single market for data, open to data from across the world - where personal as well as non-personal data, including sensitive business data, are secure and businesses quality also have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value, while minimising the human carbon and environmental footprint.

The action are based on four pillars:

1. cross-sectoral governance framework for data access and use: should create the necessary over-arching framework for the data-agile economy, thereby avoiding harmful fragmentation of the internal market through inconsistent actions between sectors and between the Member States.
2. Enablers: investments in data and strengthening Europe's capabilities and infrastructures for hosting, processing and using data, interoperability. Europe's data strategy relies on a thriving ecosystem of private actors to create economic and societal value from data. Start-ups and scale-ups will play a key role in developing and growing disruptive new business models that fully take advantage of the data revolution. Europe should offer an environment that supports data-driven innovation and stimulates demand for products and services that rely on data as an important factor of production.
3. Competences: empowering individuals, investing in skills and in SMEs: individuals should be further supported in enforcing their rights with regard to the use of the data they generate. They can be empowered to be in control of their data though tools and means to decide at a granular level about what is done with their data (*personal data spaces*)
4. Common European data spaces in strategic sectors and domains of public interest: in complement to the horizontal framework, as well as to the funding and the actions on skills and empowerment of individuals under 1, 2 and 3, the Commission will promote the development of common European data spaces in strategic economic sectors and domains of public interest. These sectors or domains are those where the use of data will have systemic impact on the entire ecosystem, but also on citizens.

3 Lecture 3

General Data Protection Regulation (GDPR)
Regulation (EU) 2016/679 if the European Parliament of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
GDPR has been approved by European Parliament in 14 April 2016. Entered into force on 25 May 2016 and applies to all the EU States from May 2018 → violation of GDPR's provisions is sanctioned since may 2018.

GDPR aims
Single set of rules for all EU nations in order to create a modern and harmonised data protection framework across the EU. Requires Data protection by design and by default and documented accountability. Gives back control to citizens over their personal data. Simplifies the regulatory environment for business and it applies to international organisations that offer goods or services or monitor EU citizens.

GDPR what has changed?
Increased fines. before GDPR according to jurisdictions there were fine up to 10.000.000 € or 2% of global annual turnover. Maximum fine up to 20.000.000 € or 4% of global annual turnover.
Before GDPR there were generally no obligations to report breaches. GDPR requires to report privacy breaches to the regulator within 72 hours and potentially to the Data subject.
Before GDPR: generally no requirements to appoint a Data Protection Officer (DPO). GDPR requires a DPO for:

- public authority or body
- organisations conducting processing on a large scale of special categories of data and personal data relating to criminal convictions and offences
- organisations conducting mass surveillance (processing operations which require regular and systematic monitoring of data subject on a large scale)

Before GDPR potential to rely on implicit consent, depending on jurisdiction. GDPR requires to gain explicit consent (not ambiguous).

Article 1 - Subject-matter and objectives

1. this Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data
2. this Regulation protects fundamental rights and freedoms of natural persons and in particular their *right to the protection of personal data*
3. the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data

GDPR should apply to natural persons, whatever their nationality or place of residence, in relation to eh processing of their personal data, but it does not cover the processing of personal data which concerns legal persons.

Article 2 - Material scope

1. this Regulation 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 a a filing system.
   Definition of *Filing system*: a filing system is one which categorises a set of personal data, making them accessible according to certain criteria.
2. this Regulation does not apply to the processing of personal data
   (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
   (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

Article 3 - Territorial scope
The GDPR applies to:

- the processing of personal data int eh 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
- the processing of personal data 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:
  - the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union
  - the monitoring of their behaviour as far as their behaviour takes place within the Union

Article 4(1) - Personal data
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*, from that data. in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factor specific to the physical , physiological, genetic, mental, economic, cultural or social identity of that natural person.

Categories of personal data
Data that allow a direct identification: name, surname, profile or biometric data. Data that allow an indirect identification: vat number, social security number, phone or mobile number, identification number or online identifier.

Personal data - Anonymisation
Accordin to recital 26: *to determine whether a natural person is identifiable, account should be take of all the means reasonably likely to be used, either by the controller or by another person to identify the natural person directly or indirectly.* The principle of data protection should therefore not apply to *anonymous information*, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

The process of anonymising data means that all elements are eliminated from a set of personal data so that the data subject is no longer identifiable. For data to be anonymised, no element may be left in the information which could, by exercising reasonable effort, serve to re-identify the person concerned. When data have been successfully anonymised, they are no longer personal data and data protection legislation no longer applies.

Special categories of personal data (ex sensitive data)
Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Genetic data: 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: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
Data concerning health: personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
Recital 35: *Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject.*

What is processing?
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, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Article 6 - Lawfulness of processing
Processing shall be lawful only if and to extent that at least one of the following applies;

1. consent
   Condition of consent. Implicit consent to processing is unacceptable. the controller should demonstrate by a statement or a clear affirmative action that the data subject has consented to processing of his or her personal data. freely given, specific, informed unambiguous. Consent must be obtained for every processing scenario and can be withdrawn at any time.

2. performance of a contract

3. compliance with a legal obligation

4. protect the vital interests of the data subject or of another natural person.
   It should in principle takes place only where the processing cannot be manifestly based on another legal basis.

5. performance of task carried out in the public interest

6. purposes of the legitimate interests

Performance of a contract
Article 6 provides the first basis for a lawful processing, namely *if it is necessary for the performance of a contract to which the data subject is party.* This basis applies when the data controller has a contract with a natural person and need to process personal data

under contract obligations. The contract should be between the data controller and the data subject. This provision also covers pre-contractual relationships (for instance, in cases where a party intends to enter into a contract, but has not yet done so, possibly because some checks remain to be completed). The data controller can rely on this basis if needs to process data subject's personal data:

1. to fulfil a contractual obligation to the data subject
2. because the data subject has asked the data controller to do anything prior to entering into a contract

The processing must be necessary: it must be a reasonable and proportionate bay of achieving the purpose.

Legal duties of the controller
Another ground for making data processing lawful is the *compliance with a legal obligation to which the data controller is subject.* This provision refers to controllers acting in both the private and public sector. Data controllers can rely on this lawful basis when they are obliged to process personal data in order to comply with a common law. It should be for the law to determine the purpose of processing, the type of personal data subject to processing, the data subject concerned, the entities to which the data can be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing.

Vital interests of the data subject or of another natural person
Data controller is likely to be able to rely on this legal basis if needs to process personal data to protect someone's life. This basis may only be invoked for processing personal data base on the vital interests of another natural person, if such processing *cannot be based on another legal basis.* Sometimes a type of processing may be based on the vital interests of the data subject or of another person. This is the case, for example, when monitoring epidemics and their development, or where there is a humanitarian emergency. Vital interests is most likely to be relevant in the context of health data - if so the data controller also need to identify a condition for processing special categories of personal data (art. 9 GDPR).

Public interest
Data controller can rely on this legal basis if personal data are processed *in the exercise of official authority* or to perform a specific tasks in the public interest that is set out in law. Official authority includes:

- public functions
- tasks in the public interest that are stipulated by the law

Legitimate interests pursued by the controller or by a third party
The existence of a legitimate interest must be assessed in each specific case. If the legitimate interests of the controller are identified, then a balancing exercise must be made between those interests and the interests of fundamental rights and freedoms of the data subject. The reasonable expectation of the data subject must be considered during such an assessment to understand whether the interests of the controller override the interests of the data subject. If the data subject's rights override the controller's legitimate interests, then the controller can take and implement measures to ensure that the impact on the data subject's rights is minimised (such as pseudonymising data), and invert the balance before being able to lawfully rely on this lawful basis for processing. In its Opinion on the notion of legitimate interests of the data controller, the Article 29 Working Party underlined the important role of *accountability* and *transparency*, and of the data subject's rights to object to the processing of his data, or to it being modified, deleted or transferred, when balancing the legitimate interests of the controller and the interests of

the data subject's fundamental rights. In the GDPR recitals, some examples are given as to what is a legitimate interest of data controller. For instance, the processing of personal data is allowed when such processing is *necessary for the purposes of preventing fraud.*

Article 9 - Special categories of personal data
GDPR requires special condition to be met for processing 'special categories of personal data'. *"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited".*
Paragraph 1 shall not apply if one of the following applies:

- explicit consent
- required to comply with employment, social security, or social protection legislation
- protect vital interests of individual
- in connection with legal proceedings and administration of justice
- necessary for medical reasons or public interest in relation to public health
- necessary for archiving purposes int eh public interest, scientific or historical research, or statistical purposes

4 Lecture 4

Article 4 (7) - Data controller
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.
The natural or legal person, public authority, agency or other body: there is no limitation to the type of entity that may assume the role of controller. The controller might be an organisation, and individual or a group of individuals. It is usually the organisation as such, and not an individual within the organisation (such as the CEO, an employee or a member of the board), that acts as a controller within the meaning of the GDPR.
Determines: the second building block of the controller concept refers to the controller's influence over the processing. A controller is a body that decides certain key elements about the processing. This controllership may be defined by law or may stem from an analysis of the factual elements or circumstances of the case.
Alone or jointly with others: article 4 (7) states that the 'purposes and means' of the processing might be determined by more than one actor. It states that controller is the actor who 'alone or jointly with others' determines the purposes and means of the processing → several different entities may act as controllers for the same processing.
Purposes and means: the data controller determines the purposes for which and the means by which personal data is processed. *Purpose* is an anticipated outcome that is intended or tat guides your planned actions. *Means* as how a result is obtained or an end is achieved. So, if a company / organisation decides why and how the personal data should be processed, it is the data controller.
Essential and non-essential means: essential means are linked to the propose and the scope of the processing and are traditionally reserved to the controller (e.g., type of personal data which are processed, the duration, the categories of recipients and the categories of data subjects). Non-essential means concern more practical aspects of implementation, such as the choice for a particular type of software or the detailed security measures which may be left to the processor to decide on (non-essential means can be determined by data processor, while essential means are to be determined by the

controller).

Of the processing of personal data: the purpose and means determined by the controller must relate to the processing of personal data. Article 4 (2) GDPR defines the processing of personal data as *any operation or set of operations which is performed on personal data or on set of personal data.* As a result, the concept of a controller can be linked either to a single processing operation or to a set of operations.

Article 26 - Joint controllers
Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. An organisation is a *joint organisation* when together with one or more organisations it jointly determines why and how personal data should be processed. Joint controller must agree upon their responsibilities for complying with the GDPR rules. They shall determine their responsibilities, in particular as regards the exercising of the rights of the data subject and their duties to inform the data subject about the processing. Besides, the agreement may designate a contact point for data subjects.

Article 4 (8) - Data processor
Processor means a natural or legal, public authority, agency or other body which processes personal data on behalf of the controller.
The data processor processes personal data only on behalf of the controller and on instructions from the controller. Two basic conditions qualify a data processor:

1. it is a separate entity in relation to the controller
2. it processes personal data on the controller's behalf

Acting on behalf of also means that the processor may not carry out processing for its own purposes. As provided in Article 28 (10), a processor infringes the GDPR by going beyond the controller's instructions and starting to determine its own purposes and means of processing. The processor will be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions.
The data processor is usually a third party external to the organisation. A typical activity of data processor is offering IT solutions, including cloud storage or a payroll company.

Relationship between controller and processor
The controller has the duty to use *only processors providing sufficient guarantees to implement appropriate technical and organisational measures*, so that processing meets the requirements of the GDPR. The controller is therefore responsible for assessing the adequacy of the guarantees provided by the processor. The following elements should be taken into account by the controller in order to assess the adequacy of the guarantees:

1. the expert knowledge of the processor
2. the processor's resources
3. the reputation of the processor on the market may also be a relevant factor for controllers to consider.

Article 28 - Data processor
The duties of the processor towards the controller must be specified in a contract. The contract shall be in writing, including in electronic form. non-written agreements cannot be considered sufficient to meet the requirements laid down by Article 28. The contract between the controller and the processor is an essential element of their relationship and *is a legal requirement.*
the contract must include:

- the subject matter
- the nature and the purpose of the processing
- the duration of the processing
- the type of personal data
- the categories of data subjects

It should also stipulate the controller's and the processor's obligations and rights.the contract shall stipulate that the processor:

- processes the personal data only on *documented instructions* from the controller
- ensures that person authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- takes all appropriate technical and organisational measures
- respects the conditions referred for engaging another processor
- assists the controller or the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights
- at the choice of the controller, deletes or return all the personal data to the controller after the end of the provision of services relating to processing
- makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller

Definition of a contract
A written or spoken agreement, that is intended to be enforceable by law. The Italian Civil Code defines the contract as: *the agreement of two or more parties aimed at establishing, governing or terminating a legal relationship.* EDPB recommends to sign the contract to avoid any difficulties in demonstrating that the contract is actually in force!

Data processor
The processor must keep records of all categories of processing activities it carries out on behalf of the controller. These record must be made available to the *supervisory authority at its request*, as the controller and the processor must both cooperate with that authority in the performance of its tasks. The processor also has to appoint a DPO when necessary (Article 37).

Sub-processors
The data processor might want to delegate some tasks to *another processor*, the so called *sub-processor.* In this case the processor need a prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. Where a processor engages another processor for carrying out specific activities on behalf of the controller, the same data protection obligations as st out in the contract or other legal act between the controller and he processor shall be imposed on that other processor by way of a contract or other legal act. The GDPR stipulates that the initial processor remains fully liable to the controller where a sub-processor fails to fulfil its dtaa protection obligations.

Responsibilities and obligations of the data controller
To comply with GDPR, data controller must determine:

- the *legals basis*for collecting data
- which kind of personal data are collected
- the purpose or purposes the data is to be used for
- which individuals can collect personal data

- whether to disclose the data and, if so, to whom
- whether third parties could access to personal data
- how long to retain the data for

Data controller has to comply with Article 5 of GDPR that contains the six principles to processing of personal data

1. Personal data shall be
   (a) processed *lawfully, fairly* and in a *transparent* manner in relation to the data subject
      - Lawful - processing must meet one of the six legal tests
      - Fair - what is processed must match up with how it has been described
      - Transparent - tell the subject what data processing will be done

   (b) collected for *specified, explicit and legitimate purposes* and not further processed in a manner no in line with those purposes

   (c) *accurate* and, where necessary, *kept up to date*

   (d) kept in a form which allows identification of data subjects *for no longer than is necessary* for the purposes for which the personal data are processed

   (e) processed in a manner that *ensures appropriate security* of the personal data
2. The controller shall be responsible for and be able to *demonstrate compliance* with the above

Article 24 - Responsibility of the controller
Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller *shall implement appropriate technical and organizational measures* to *ensure* and to be able to demonstrate that processing is performed in accordance with this Regulation. those measures shall be reviewed and updated where necessary.
Where proportionate in relation to processing activities, the measures referred to before shall include the implementation of *appropriate data protection policies* by the controller.

Accountability
The accountability principle in Article 5 (2) requires data controller to ensure or to be able to demonstrate that processing is performed in accordance with GDPR provisions. The controller has to implement measures to promote and safeguard data protection in their processing activities. This means that data controller shall:

- implement appropriate technical and organisational measures that ensure and demonstrate that he complies with GDPR
- maintain relevant documentation on processing activities
- recording processing activities and making them available to the supervisory authority upon request
- in some situations, appoint a DPO who is involved in all issues relating to personal data protection
- implement measures that meet principle of privacy by design and by default
- implementing procedures for the exercies of the rights of the data subjects
- use *data protection impact assessment* where appropriate

GDPR includes provisions that promote accountability and governance. Data controller and data processors are expected to put into place comprehensive but proportionate governance measures. Good practice tools such as privacy impact assessments and privacy by design are now legally required in certain circumstances. Besides, these measures should minimize the risk of breaches and uphold the protection of personal data.

Data protection impact assessment (DPIA)
A DPIA is required when:

- using new technologies
- profiling
- surveiling
- processing of special categories of personal data
- processing is likely to result in risk to rights and freedoms of individuals

Any processing that results in a high risk to the right to privacy or the protection requires a DPIA. A DPIA is a process design to.

- describe the processing and purpose of the processing
- assess the necessity and proportionality of a processing
- help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data
- assess the risks and determine the measures to address them = risk assessment and detial of risk avoidance measures

5 Lecture 5

Cybersecurity - The 'mantras' of cybersecurity
Cybersecurity is not a product, but an asymptotic process. Total security is impossible. We are vulnerably by definition. Be paranoid. For cyber security, KISS rule is the best way to design a policy. Being too much confident is more dangerous than being insecure.

Cybersecurity - definition
The definition of Cybersecurity is provided by the Cybersecurity Act (EU Regulation 2019/881): *the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.*

Threat
Cyber threat: *any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.*

Network Security
The NIS Directive (Directive (EU) 2016/1148) does not use these two definitions, but that of: *network and information security* (Article 4(1)(2)): *the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or related services offered by, or accessible via, those network and information systems.*
The DPCM of 17 February 2017 describes cyber security as: *the condition whereby cyber space is protected by the adoption of appropriate physical, logical and procedural security measures against events, of a voluntary or accidental nature, consisting in the undue*

acquisition and transfer of data, their unlawful modification or destruction, or the undue control, damage, destruction or blocking of the regular functioning of networks and information systems or their constituent elements.

Regulatory provisions - European level
Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (ENISA);
EU Regulation 526/2013, concerning the European Union Network and information Security Agency (ENISA) and repealing Regulation (EC) No 460/2004.
NIS Directive (EU Directive 2016/1148 of the European Parliament and of the Council laying down measures for a common high level of security of networks and information systems in the Union).
Commission Implementing Regulation (EU) 2018/151 of 30 January 2018, (laying down detailed rules for the implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards the further specification of the elements to be taken into account by digital service providers for the purpose of managing risks posed to the security of networks and information systems and the parameters for determining the possible significant impact of an incident) (this is the *Implementing Regulation of the NIS Directive).*

Three aims
The The regulation aims to strengthen the resilience of the Union to cyber attacks, create a single market for cyber security in terms of products services and processes, and increase consumer confidence in digital technologies.

Provisions in other areas
EU Directive 2018/1972 (European Electronic Communications Code).
Directive 2002/58/EC (ePrivacy Directive) eventually replaced by a Regulation.
These are addressed to the telecommunications sector and public electronic communication services).
EU Regulation 910/2014 (eIDAS Regulation).
EU Directive 2015/2366 (PSD2) on payment services in the internal market.
EU Regulation 2017/745, on medical devices.
EU Regulation 2017/746, on in vitro diagnostic medical devices.
(These are addressed to the health sector).
EU Regulation 2016/679 (GDPR).

Standards
then there are the national and international (European level) standards, such as:

- *ISO/IEC 27001:2017* (implementation of an information security management system)
- *ISO 22301:2019* (business continuity management)

In addition, the European Commission has adopted:

- in 2013, a first *Cybersecurity Strategy*
- in 2015, a *Cybersecurity Agenda*

the Cybersecurity Strategy and Agenda together describe the policies and initiatives adopted at European level with regard to cybersecurity (including legislation, investment, etc.) and encourage cooperation between states. This led to the NIS Directive and the launch of ENISA's second mandate.

Open and secure cyberspace
The main aim of the strategy, as also indicated in its title, is to ensure an 'open and

secure' cyberspace, accessible to all and, at the same time, adequately equipped to ensure the confidentiality of the data and information ti contains. The task of the Union is to promote the application of principles, rules and values that are already valid in the physical dimension, also in the digital dimension. Fundamental rights, democracy and the rule of law should also be protected in cyberspace.

Principle
These principles are listed within the strategy:

1. protection of fundamental rights, freedom of expression, personal data and privacy
2. guaranteed network access for all
3. multi-stakeholder democratic and efficient governance
4. shared responsibility among all actors involved

New strategy
In 2017, the EU enacted a *Cybersecurity Strategy*. This strategy includes a broad package, aimed at strengthening cybersecurity in the EU, also in relation to the evolving technological landscape. included in this strategy are various recommendations, reports and studies but, above all, the proposal for a new regulation (*Cybersecurity Act*), as well as the proposal for a *European certification system for cybersecurity.*

Centre of action
The report Assessment of the EU 2013 Cyber Security Strategy highlighted the need to shift the centre if gravity of EU action from a purely economic-centric approach (focused on the old open, safe and secure cyberspace concept) towards a *proactive approach* based primarily on the *resilience, deterrence* and *cooperation* capabilities of the Member States and the Union itself.

Resilience
Resilience (understood both as the ability of Member State and the EU as a whole to build more robust and effective IT or IT-dependent infrastructures and the ability to produce secure technologies to bring to the European market)

Deterrence
Deterrence (i.e., the political, diplomatic and military ability to dissuade potential adversaries, state and non-state, from launching an attach against EU Member States and the operational ability to anticipate and/or react to attacks)

Cooperation
International cooperation in the cyber filed (whose main objective is to facilitate cooperation with the main stakeholders in cyberspace, be they private individuals, states outside the Union or international organisations, primarily UN, OSCE and NATO, in order to mitigate the risks of misunderstanding and escalation). Resilience is, according to the EU, the precondition for effective and efficient cyber security.

6 Lecture 6

Analysis of the European and Italian legislative framework on Cybersecurity
In the definition of the legal framework in the filed of cybersecurity, European legislation has played an undoubted role as a catalyst for the identification of key profiles and the promotion of a unified approach.

Preset strategy
In 2020, the European Commission presented the *Security Strategy 2020-2025.*

Security context

This strategy manifests the intention to create a security environment that is up-to-date, in particular by developing systems that are resilient. The EU, especially post-CoViD period, is well aware of the primary importance of cybersecurity, also in relation to the exponential increase in cyber-attacks.

Collaboration

To this end, a *Joint Cyber Unit* should be set up to act as a centre of coordination between the various actors in the cyber field at European level. There is also the intention to create common, mandatory standards to enable the secure exchange of information and ensure the security of digital infrastructure and systems in all institutions.

Italy

Law No. 124 of August 3, 2007 (Information System for the Security of the Republic and New Discipline on Secrecy) (more connected to National Security)
DPCM 24 January 2013 (Directive laying down guidelines for cyber protection and national cybersecurity); (it provided for the adoption of a national strategic framework and the elaboration of a national plan for the security of cybernetic space. Led to the adoption of the National Strategic Framework for Cyberspace Security, in December 2017).
DPCM 17 February 2017 (Directive laying down guidelines for national cyber protection and cybersecurity) (Led to the adoption of the National Plan for Cyber Protection and Cybersecurity, in Macrh 2017).
Directive of the President of the Council of Ministers 1August 2015 (Minimum ICT security measures for public administrations)
Legislative Decree No. 65 of 18 May 2018 (Implementation of Directive (EU) 2016/1148 of the European Parliament and for the Council of 6 July 2016 on measures for a common high level of security of networks and information systems in the Union).
Decree 105/2019 (National Cyber Security Perimeter).
DPCM No. 131 of 30 July 2020 (Regulations on the national cyber security perimeter).
Decree of the President of the Republic No. 54 of 5 February 2021 (Regulation implementing Article 1, paragraph 6, of Decree-Law No. 105 of September 21, 2019, converted, with amendments, by Law No. 133 of November 18, 2109).
DPCM No. 81 of April 2021 (Regulation on the notification of incidents affecting networks, information systems and computer services of public administrations, bodies and operators and private operators having an office in the national territory, included in the perimeter of national cybersecurity).
Legislative Decree No. 82 of 14 June 2021 (Urgent provisions on cybersecuirty, definition of the national cybersecurity architecture and establishment of the National Cybersecurity Agency).
DPCM of 15 June 2021 (Identification of categories of ICT goods, systems and services for use in the national cyber security perimeter).

USA

In the US there are:

- *Federal laws* (which are addressed to specific sectors). The federal laws enacted to date are: Health Insurance Portability ad Accountability Act (HIPAA) (1996); Gramm-Leach-Biley Act (1999); Homeland Security Act (2002), which includes the Federal Information Security Management Act (FISMA). These three pieces of legislation are directed at healthcare facilities, financial institutions, and federal agencies, respectively;

- *State laws*

China

China Cybersecurity Law (entered into force on 1 June 2017) - includes provisions on both privacy and cybersecurity. Very broad scope: the legislation is in fact aimed at ensuring cybersecurity, protection of sovereignty in cybersecurity, national security, protection of legitimate rights and interest of citizens, legal entities and other organizations, and promoting sound economic development. It applies to network operators and critical infrastructure.

China PIPL

On September 15, 2021 China has approved the final Personal Information Protection Law (PIPL), and it will come into effect on November 1, 2021. Based in part on the GDPR, and building on top of China's Cyber Security.

Similarities

Both the PIPL and the GDPR are extraterritorial.
The PIPL and GDPR define personal data as involving identified and identifiable natural persons.
The PIPL uses the GDPR's lawful basis approach to data processing. Many other Asian privacy laws use the consent-based approach or an approach akin to the US approach of notice-and-choice.
Both the PIPL and GDPR have special protections for sensitive data, but they differ on the types of data they recognize as sensitive.
Both the PIPL and GDPR have a data breach notification requirement.
The PIPL and GDPR recognize many of the same rights.
Both the PIPL and GDPR require workforce training.
Under certain circumstances, both the PIPL and GDPR require DPOs.
Both the PIPL and GDPR require data protection impact assessments (DPIAs) in certain situations.

Differences

The PIPL has no lawful basis of legitimate purposes, which the GDPR recognizes.
The PIPL uses some different terminology than the GDPR. GDPR 'data subjects' are called 'individuals' under the PIPL. GDPR 'data controllers' are called 'personal information handlers' under the PIPL. GDPR 'data processors' are referred to as 'entrusted parties' under the PIPL. The PIPL has a strong data localization requirement. The PIPL recognizes a sew different types of sensitive data than the GDPR. For example, financial data is sensitive under the PIPL but not under the GDPR.
The PIPL has a post-mortem right for personal data after death.
The PIPL requires a representative in China for foreign data handlers.
The PIPL has less stringent requirements for corss-border data transfer than the GDPR.
Under the PIPL, data breach notification must be 'immediate' without the GDPR's specific 72 hour deadline.
The PIPL has a prohibition on personnel responsible for violations from holding high-level management or DPO positions.
The PIPL has fines up to 5% of annual revenue. The GDPR has fines of 2% and 4% of annual revenue. The GDPR looks to worldwide annual revenue; the PIPL is unclear about whether the fine is based on annual revenue in China or worldwide annual revenue.

The international framework

both the US and China are know or their use of cybersecurity 'in the name of fighting terrorism'. However as far as the US is concerned, Snowden's revelations have shown that, in reality, NSA activity also targeted *ordinary citizens*. Similarly, in China, the true motivations behind cybersecurity regulations are often unclear.

Differences between the two states

The differences between the two States stems from the different concept of the Internet which, according to the American approach, at an ideal level, should be a place open to everyone, safe and free. According to the different Chinese approach, instead, the national government wants to have full *control* and be completely *independent from* the other states (centralization of power). This desire for independence, in the eyes of the Chinese government, also justifies activities such as cyber breaches, cyber espionage, and the theft of company data.

Cyber espionage activities
China had already speculated about US cyber-espionage activity (activity that, indeed, was done), well before Datagate, but the US should be considered as 'benign hacking', while the activity of accessing systems and stealing corporate data (as China did) should be considered 'malicious hacking', even if such activity is intended to help companies and strengthen their competitiveness.

Tensions CHINA/US
In 2015, however, the two countries finally tried to resolve these tensions. In 2015, China's President, while visiting the US, signed a *cyber agreement* that prohibits both counties from knowingly supporting cyber theft of intellectual property for the economic benefit of domestic companies. China often sees itself more as a *victim* than an *attacker.* In any case, both countries have shown a willingness to cooperate.

Chinese Cybersecurity Law
2017: China's Cybersecurity Law comes into effect, covering many areas. As China's first omnibus privacy and cybersecurity regulation, CCSL increases data protection in many respects, but poses possible *compliance* challenges for the global community.

Protection of the nation
It is of particular concern for businesses with a 'significant online/digital presence', businesses that depend on a telecommunications network, or those that rely ion cross-border movement and sharing of business data. According to Chinese officials, it would specifically aim to protect the nation from *cyber attack by* other nations.

Regulatory uncertainties
As the first comprehensive cybersecurity law, the CCSL provisions are still very *general* and *vague.* Much, in fact, will depend on the implementing regulations and standards that will be issued by the State Council, the CAC, the Ministry of Public Security and the Ministry of Industry and Information Technology.
Some of the contents of the law repeat existing regulations adopted by China over the years and simply combine separate *regulations* into on. the previous existing rules were scattered in different regulations.

Sense of security
The EU supports an approach that gives civil societies the sens of *security* they need when dealing with cyber threats. Unlike the US and China, which approach issue of security i cybrspace through the logic *national security* and *cyber superiority*, the EU's approach is *legalistic* and *protective.*

Cyber security in the EU
The EU Cyber Security Concept focuses on fighting *cybercrime* and building resilience to ensure recovery from cyber attacks. EU capability development focuses on building capabilities to detect, respond to and protect against cyber attacks.

Types of computer security
We can therefore say that the legislator (especially European) has typified different frameworks of information security:

- cybersecurity as protection of the state, the EU and critical infrastructure

- cybersecurity in the sense of protection of the economic system and activities that rely no the reliability and resilience of electronic communication networks
- computer security as protection of the individual his data and his dignity

Common elements of European regulations
Risk-based approach.
Accountability of the owner of the information system.
Cooperation between agencies to ensure a safe environment.
Centralism of alert and controls (CSIRT and CNAIPIC).
Community-level strategy.

7 Lecture 7

Introduction to offensive and defensive security

Basic Security Requirements
The so-called *CIA Paradigm* for information security states three requirements:

- *Confidentiality*: information can be accessed only by authorized entities
- *Integrity*: information can be modified only by authorized entities, and only in the way such entities are entitled to modify it.
- *Availability*: information must be available to all the parties who have a right to access it, within specified time constraints.

A conflict with *C* and *I*: engineering problem.

Security as an Engineering Problem
We need some concepts to 'solve' it:

- Vulnerabilities
- Exploits
- Assets
- Threats
- Risks

Vulnerability vs Exploits
Vulnerability: something that allows to violate one of the constraints of the CIA paradigm.
Exploit: a specific way to use one or more vulnerabilities to accomplish a specific objective that violates the constraints.

Assets and Threats
Asset: identifies what is valuable for an organization (hardware software, data, reputation).
Threat: potential violation of CIA (denial of service, identify theft, data leak).

Attack and Threat Agents
Attack: is an intentional use of one or more exploits with the objective of compromising a system's CIA.
Threat Agent: whoever/whatever may cause an attack to occur (malicious software, thief).

Attackers, Hackers, ...
Mass media created false myths and controversies around these and other words.

Hacker: someone with an advanced understanding of computers and computer networks, and willingness to learn everything.
Black hast: malicious hackers.

Security as Risk Management
Risk: statistical and economical evaluation of the exposure to damage because of the presence of vulnerabilities and threats.

$$Risk = \underbrace{\text{Asset} \times \text{Vulnerabilities}}_{\text{controllable variables}} \times \underbrace{\text{Threats}}_{independent variable}$$

Security: balance the (reduction of vulnerabilities + damage containment) vs (cost).

Security vs Cost Balance
Direct costs

- management
- operational
- equipment

Indirect costs (more relevant)

- less usability
- slower performance
- less privacy
- reduced productivity

Trust and Assumptions
We must put boundaries. Part of the system will be assumed secure (can we trust the security officer? the can we trust the software we just install? can we trust our own code?...).

Software security fundamentals
Good software engineering: meet requirements:

- *functional*: requirements - software must do what it is designed for
- *non-functional*: requirements - usability, safety, security
- creating inherently secure applications is hard

Software has Vulnerabilities
Software should implement the specifications.
Unmet specification → *software bug.*
Unmet security specification → *vulnerability.*

The Untrustworthy Client
The golden rule of web application security is that the *client is never trustworthy.* We need to *filter* and check carefully anything that is sent to us. Web developers see client as a (cooperative) part of the application.

Filtering is hard
The sequence of validation:

1. *whitelisting*, only allowing through what we expect
2. *blacklisting*, on top of that discard known-bad stuff

3. *escaping*, transform special characters into something else which is less dangerous

Bad Things can Happen: XSS
Suppose now we have a simple blog app, lets anybody post a comment and the text displayed back to next visitors. If we do not apply any filter to what is inserted, an attacker cold type. Popup would appear on next visitors' screen,. This is called *Cross Site Scripting.*

The Notion of Same Origin Policy
Implemented by all web clients. *Same Origin Policy (SOP)* → all client-side code loaded from origin A should only be able to access data from origin A.

8 Lecture 8

Cybersecurity and protection of personal data according to GDPR

Two key messages from OECD
First, there is a focus on the economic and social objectives of public and private organisations and the need to adopt an approach grounded in risk management. Instead of being treated a s technical problem that calls for technical solutions, digital risk should be approached as an economic risk; it should therefore be an integral part of an organisation's overall risk management and decision making processes. The notion that digital security risk merits a response fundamentally different in nature from other categories of risk need to be countered. To that effect, the term cybersecurity and more generally the prefix cyber which helped convey this misleading sense of specificity do not appear in the 2015 Recommendation.
Second, there is recognition that through dynamic management, security risk can be reduced to a level deemed acceptable relative to the economic benefits expected from the activities at stake. In this respect, digital security measures should be designed in a way that takes into account the interests of others, is appropriate to and commensurate with the risks faced and does not undermine the economic and social activity they aim to protect.

Definition of information security
There is no universally accepted definition of Information Security. However, we can define it as *the science that studies how to protect electronically processed or transferred information from undesirable acts that may occur accidentally, or be that result of negligent or malicious actions.*

Security
Security is the study, development ad implementation of strategies, policies and operational plans aimed at preventing, coping with and overcoming events mainly of a malicious and/or culpable nature, which may damage the tangible, intangible and human resources that the company has and needs to ensure an adequate competitive capacity in the short, medium and long term.

Security in the processing of personal data
The issue of security in the processing of personal data has undergone several evolutionary moments, first alongside the text of the law (Presidential Decree 318/99), then ending up incorporated into the text of the law (Articles 31-36 and Annex B of Legislative Decree 196/03) and then become an element that permeates the entire text of the law, inspiring in the GDPR the action of the owner and the person responsible for processing.

Change of perspective

This change in perspective is also evident in the way in which the requirements for IT security have evolved: from sets of instructions to be adopted, sometimes inefficiently, to actual policies that the data controller and processor must put in place based on the specific analysis pf their structure and the characteristic of the processing.

Risk base approach

The representation of personal data processing from a risk perspective is a direct derivation of this conception. This is the typical approach of compliance regulations. It falls under what is known as preparedness.

The Deming cycle of security

Another feature of GDPR is that of a *cyclical* conception of security. The process never ends, but is always subject to revision and adjustment.

Safety requirement

Therefore, we can say that the GDPR establishes a real *security obligation* for those who process personal data.

This obligation follows every phase of the treatment: from the origin (Art. 25), to the assessment (Art. 32, paragraph 2 and Art. 35), to the implementation (Art.32, paragraph 1), to the management of the incident (Art. 33 and 34), up to the compensation of the damage (Art. 82) and the administrative sanction (Art. 83, paragraph 4).

Consequences

Consideration No. 85: *a personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.*

Security and Accountability

Art. 24 GDPR paragraphs 1 and 2. *1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

Consideration No. 85: *as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.*

Data Security

Art. 32 of the Regulations: *1. Taking into account the state of art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for he rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*

- *the pesudonymisation and encryption of personal data*

- *the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services*
- *the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*
- *a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing*

The suitable security measures in the Legislative Decree 196/03
Technical progress
Nature of the data
Specific features of the processing of personal data

The appropriate technical and organizational measures in Regulation 679/2016
They rely on Data Controller accountability. No more parameters to identify them but suggestions (rather generic).

Measure that allows the quality of personal data to be lost
Anonymization techniques applied on personal data. However, it is interesting to note that, as represented by the legislature in Regulation 1807/2018, anonymization could be invalidated by technology and cause non-personal data to regain the status of personal data. This might lead us to think hat, in the legislator's view, there is no such thing as absolute anonymity, but it is a relative quality of the data.

Pseudonymization
Art. 4 n. 5) of the GDPR: *the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject, without the use of additional information, provided that such additional information is stored separately and subject to technical and organizational measures designed to ensure that such personal data is not attributed to an identified or identifiable natural person.*

Distinguishing
GDPR's definition of pseudonymization differs profoundly from how the term has been used in other contexts. For example, the UK Anonymisation Network's Anonymisation Decision-Making Framework defines it as *a technique where direct identifiers are replaced with a dummy name or code that is unique to an individual but does not directly identify them.* Similarly, the ICO defines pseudonymization as *the process by which individuals are identified in a data set using a unique identifier that does not reveal their identity in the real world.*

Definition
One of the definitions given in the doctrine is the following: *pseudonymization consists in replacing an attribute, usually unique, of a data with another equally unique and usually not intelligible.* It is precisely on that *uniqueness* that the robustness of the pseudonymization system rests. In fact, the application of pseudonymization techniques on one piece of data rather than another could represent the weakest link in the security system.

Risks
Clearly, the less data that is pseudonymized or the smallest the degrees of separation, the easier it will be to overcome the security measure. One of the attacks that is used in large databases, for example, is the so-called record linkage attack, especially when the database is populated by multiple sources that increase certain recurrences.

Pseudonymization techniques
Linking the unique identifier to a hash (the more personal data is linked to the hash, the

greater the risk of identifying the content of the hash)
Linking the pseudo-identifier to the hash (security is related to the type of pseudo-identifier used and the randomization of the hash algorithm)
Hash encryption
The addition of a random value to the unique identifier at the beginning of the data before the hash algorithm is applied (so called 'salt')
The addition of 'noise' in the data before the hash algorithm is applied.

How to choose a pseudonymization technique or method
The choice of a pseudonymization technique and method depends on several factors, primarily the level of data protection and the functionality of the pseudonymization data set that the pseudonymization entity wishes to achieve. In terms or protection, RNG, Message Authentication Code, and encryption are more effective techniques for countering attacks operated through exhaustive searches, dictionary lookups, and guesswork. However, depending on the functionality requirement, the pseudonymization entity could opt for a combination of different techniques or variations of a given methodology. Similarly, with respect to pseudonymization methods, totally random pseudonymization offers the best level of protection, but prevents any comparison between databases.

Restoration
Since, by definition, the use of additional information is critical to pseudonymization, the pseudonymizing entity must implement a recovery mechanism. This may occur, for example, when the pseudonymizing entity detects an anomaly in its system and needs to contract the appropriate entity. The anomaly may consist, for example, of a data breach for which the pseudonymization entity, under the GDPR, must inform data subjects. Moreover, the remediation mechanism may be necessary in order to allow data subjects to exercise their rights under Articles 12-21 GDPR.

Pseudonymization secret protection
For pseudonymization to be effective, the pseudonymization entity must always protect the pseudonymization secret by appropriate technical and organizational measures.
First, the pseudonymization secret must be separated from the data set, so that the pseudonymization secret and the data set are never processed within the same file.
Second, the pseudonymization secret must be securely removed from any unsecured media.
Third, strict access control procedures must ensure that only authorized individuals have access to the secret. A secure logging system must keep track of all access requests made.
Finally, the pseudonymization secret, if stored on a computer, must be encrypted, resulting in the need to properly store and manage the encryption keys.

Pseudonymization vs Anonymization
Pseudonymization has a diametrically opposed result with respect to anonymization, because while pseudonymization does not change the biunivocal association between data and person, with the adoption of anonymization techniques the referability of data to the person becomes as likely a s a random attribution. Pseudonymous data therefore, retains the nature of personal data while anonymous data falls outside the scope of the GDPR.

Panta rei
The principle of data protection should therefore not apply to anonymous information, namely information which doe not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

Progressive anonymity?

Reading Recital 26 may lead us to consider pseudonymization as a step in a larger anonymization process. Unless the data is born anonymous or does not refer to a natural person, in fact, pseudonymization will always be the basis on which a data will be made more and more anonymous, until it becomes so even with respect to the subject closest to the personal data.

The elements that could lead to a re-identification
The attacker's motivation for the anonymization system. The potential consequences of re-identification. The possibility of a re-identification occurring without malicious intent. The governance, data security, and other infrastructures that oversee the release or sharing of data. Ancillary data that could be linked to the anonymous data. Divergences between the data being analyzed and other data, which could reveal intrinsic properties of the data.

Big Data and Anonymity
The cognitive investigation on Big Data promoted by the three Italian Supervisor Authorities has reaffirmed the importance of these techniques and the risks of re-identification that can drive from the calculation capacities, from the ability to interconnect different datasets and also to memorize different temporal states of the data, typical of Big Data. In fact, it is reiterated by industry experts that the value of Big Data lies not so much in the amount of data as in its quality.

Big data and non-personal data
The survey clearly showed that those who resort to profiling activities tend to use anonymized data, as they can still obtain the information they need in order to plan their market strategies, as well as not violating the legislation on the protection of personal data. Information about the personal identity of a user / customer, therefore, would seem to have less appeal, compared to knowledge about the characterizations of ideal type, although it has been empirically demonstrated that, under certain conditions, it is technically possible to discover a person's identity from generic data or metadata.

Anonymization as an escape from GDPR
Understandably a way out is sough i technological solutions, first and foremost in the effective anonymization of the data that should go to make up Big Data, to which, where necessary, organizational and/or contractual measures should be associated for the same purpose. However, as mentioned above, even this road must be traveled with caution, with case analysis, having long been the scientific community, as well as the data protection authorities highlighted the risks of re-identification of those concerned using additional datasets risk amplified by the growing mass of information freely available online.

Security
Notwithstanding these considerations, the analysis techniques based on the Big Data paradigm entail series of direct or indirect risks that must be faced with adequate, effective, state of the art security measures that are continually assessed and updated, both with a view to compliance with art. 25 of the RGPD (data protection by design / default) and with art. 32 of the RGPD (security of processing). In fact, it is clear that Big Data processing, even if based on anonymous datasets or considered anonymous, carries dangers of possible prejudice to the rights and freedoms of the interested parties to whom the data my be referred: as mentioned, even starting from anonymous data very often there is still the possibility that the output data produce effects of single-outing or re-identification, with consequences that are reflected on an individual or a group of individuals, even if not fully identified.

Unintelligibility
From the Application Order of the Supervisory Authority of April 4, 2013: *the aforementioned communication is not due if the supplier is able to demonstrate to the supervisory*

Authority to have applied to the data-subject to the violation technological protection measures that have made them unintelligible to anyone who is not authorized to access them. In the opinion of the Authority, data is considered unintelligible if, for example:

- have been securely encrypted using a standardized algorithm, or using symmetrical or public key encryption schemes known ion the literature, provided that the decryption key is of adequate length, a policy for its safekeeping has been put in place by the owner and if it has not been compromised by security breaches and has been generated in such a away that it cannot be derived with the available technological tools by persons not authorized to access it
- have been replaced by a hash value calculated through a cryptographic key hashing function, provided that the key used to hashes the data is of adequate length, a policy for its safekeeping has been generated in a manner that does not allow it to be derived with available technological tools by persons not authorized to access it
- have been rendered anonymous with procedures such as not allow the re-identification of the interested parties to whom they refer by subjects not entitled to their treatment, including through the use of other information sources available at the owner or public

Robustness
The evaluation of the robustness of the anonymization technique adopted depends on three factors:

- detectability (singling out) (ability to isolate a person within a group based on the data)
- correlatability (ability to correlate two record regarding the same person)
- inference (ability to infer, with significant probability, unknown information about a person)

Anonymization and Pseudonymization
The concept of anonymization tends to be misunderstood and often confused with pseudonymization. While anonymization allows data to be used without restriction, pseudonymized data falls under the scope of the General Data Protection Regulation (GDPR). There are many options for achieving effective anonymization, but with one caveat. Data cannot be anonymized in isolation, which means that only entire sets of data or entire data sets are amenable to anonymization. In this sens, any intervention on an isolated piece of data or on the historical series of data referable to a single data subject can be considered, at best, a pseudonymization.

Transparency
Finally, given the complexity of the anonymization processes, it is strongly recommended that there be transparency regarding the anonymization methodology used.

Functional anonymity
Anonymization provides a mechanism to manage the conflict between safeguarding personal privacy and maximizing the utility of the data. Anonymization can never be absolute if any utility of the data is to be retained; therefore, it is important to avoid terms of success when describing anonymization as truly anonymous. Rather, the challenger is to understand an acceptable level of risk, and determining that level requires consideration of the downstream impact of any potential breach of confidentiality. The impact can be difficult to define, as it will depend not only on the data, but also on the release context and the resulting data situations that result from the use of the data and the data interacting with the data environment. In addition, the data environment is usually dynamic and complex depending on the constraints under which the data is shared and released. Although difficult to describe, in general the data environment can be described by referring to four parameters:

- agents - generally thought of as people, but increasingly may be artificial intelligence and machine learning systems
- other data within the local or global environment
- data governance that determines who can access data ad what usage restrictions are place on users
- security infrastructure

Everything is relative
Whether or not data is anonymized is a function of the relationship between that data and the specific data environment: the dame data set will have different risks under different circumstances. Thus, it can be argued that it is impossible to determine risk by considering the data alone: a framework is needed to develop an anonymization policy that conceptualizes, frames, and clarifies each individual data situation.

Anonymization Impact Assessment
Given the risk-based approach that permeates throughout the GDPR, the principle of accountability, and how the EDPB has expressed itself in relation to other complex situations, it may be useful to provide for an Anonymization Impact Assessment that can serve as a guide regarding the level of robustness of anonymization adopted or not. Elements to consider could be:

- nature of the data
- amount of data
- sample size
- criteria for access and who has access to it
- external data that can be linked to the data in the dataset

Policy
If Data Controller's needs require it, it may also be useful to consider drafting a policy for data anonymization and pseudonymization, such as the one shown as an example.

Security Policies
The GDPR requires security to fulfill three possible scenarios:

- *preventive* scenario, i.e., adopting those security measures that limit as much as possible the risk of actions aimed at illicitly knowing or damaging personal data (the risk-based approach, the principles of minimization and pseudonymization)
- *evaluation* scenario, i.e., having information on the nature and distribution of data within one's own structure, as well as the characteristics of the processing, so as to be able to quickly assess the risks associated with a possible security breach (e.g., data protection impact assessment)
- *reactive* and risk containment scenario, i.e., adopting those security measures that can contain the risk of unauthorized or improper processing of personal data and that can respond to the threat (e.g., notification of a personal data breach)

Policy as a component of a security methodology
If the definition of a security policy must take into account the technical, logistical, administrative, political and economic constraints imposed by the structure where the information system operates, it is necessary to identify a methodology for the design, implementation and maintenance of security which, by leveraging a correct policy, puts in place an effective security plan.

Instruct
Art. 32 paragraph 4 GDPR: *the controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has the access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.*

Design
The obligation to ensure on a permanent basis the requirements of integrity, confidentiality, availability and resilience means that it has become essential to design a security system that takes into account the parameters indicated by the legislator (state of the art, implementation costs, nature, object, context, purpose of processing and risk to the rights and freedoms of individuals).

Restore
It becomes essential to have backup and disaster recovery plans that can allow for the timely restoration of data availability and accessibility.

Check
The regulations also call for the adoption of audit procedures as they are useful for regularly testing, verifying and assessing the effectiveness of the technical and organizational employed.

Conclusions
Security is strictly related to the accountability of the Data Controller.
Security is something that the Regulation itself requires to be tailored to the individual owner or manager.
Security, being an obligation, is connected to the lawfulness of the treatment and is also functional with respect to the exercise of the rights of the interested party.
Security is necessarily a process, but one that must be monitored.
Safety requires continuous testing and improvement.
Security is not only an IT or technical aspect, but also organizational, logistical, procedural and regulatory.

9 Lecture 9

Lawful grounds for processing personal data
Article 5 GDPR - Principles relating to processing of personal data. Personal data should be processed lawfully, fairly and in a transparent way. ⇒ the processing must comply with one of the lawful grounds for making data processing lawful listed in article 6 and in article 9 GDPR.
Data controller must be able to demonstrate that a lawful basis has been applied in order to comply with the accountability principle (article 5 GDPR). → article 13 requires to include legal basis within the privacy notice that the data controller give to individuals.

Article 6 - Lawfulness of processing
Processing shall be lawful only if and to extent that at least one of the following conditions apply:

- consent
- performance of a contract
- compliance with legal obligation

Data protection by design and by default
Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and

severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of processing itself, *implement appropriate technical and organisation measures*, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Data protection by design
Maintain documentation and implement measures to demonstrate compliance with principles.
Internal audits, reviews, training.
Document processing activities to ensure transparency.
Employ data minimisation and pseudonymisation.
7 Principle - IPCO

1. preventative not remedial
2. privacy as the default
3. privacy embledded into design
4. full functionality
5. end to end security
6. visibility and transparency
7. respect for user privacy

Data protection impact assessment (DPIA)
Art. 35: *Where a type of processing in particular using new technologies, and taking into account eh nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.*

Data protection by default - art. 25, par. 2
The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
The principle of privacy by default requires that:

- the data controller implements appropriate measures to ensure that only personal data which are necessary for the purposes will be processed by default
- this obligation applies to the amount of personal data collected, the extent of the processing, the storage period and accessibility
- such a measure must ensure, for example, that not all the controllers' employees have access to the subjects' personal data

Such measures could consist of

- minimising the processing of personal data
- pseudonymising personal data asap

- transparency with regard to the functions and processing of personal data
- enabling the data subject to monitor the data processing
- enabling the controller to create and improve security features

Definition of consent - art. 4 GDPR, par. 11
Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Recital 32 GDPR
Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. Tick a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data should be an indication of a free consent. Silence, pre-ticked boxes or inactivity are not an indication of a free consent.
Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has many purposes, consent should be given for all of them. Is one lawful basis of the processing (art. 6 and 9 GDPR).

Article 7 GDPR - Conditions of consent
Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner that can be identified from the other matters, in an understandable and easily form, using clear and plain language.

Informed consent
The data subject must have sufficient information before exercising his or her choice. The data controller has to describe in a precise way the processing: the data subject needs full information of all relevant issues, such as the nature of the data processed, purposes of the processing and the rights of the data subject. For consent to be informed, individuals must also be aware of the consequences of not consenting to processing.

Withdraw of consent
The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be easy to withdraw as to give consent.

Conditions applicable to child's consent in relation to information society services - Art. 8 GDPR
In relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.
Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years. (IT has 14 years).

Right to be informed - article 12 GDPR

Data controller is obliged to inform the data subject at the time when personal data are collected about their intended processing. This obligation does not depend on a request from the data subject, rather the controller must comply with the obligation: the data subject does not need to show interest in the information or not. The transparency principle requires that any personal data processing should generally be transparent to individuals. The information must be concise, transparent, intelligible and accessible, using clear and plain language. It must be provided in written form, including electronically where appropriate, and it may even be provided orally at the data subject's request and if his or her identity is proven beyond doubt. The information shall be provided without excessive delay or expense: information must be free of charge, unless the data subject's requests are unfounded or excessive (i.e., of a repetitive nature). When providing information, the controller can use standardised icons to provide the information in an easily and intelligible manner. For example, an icon representing a lock may be used to prove that the data is safely collected. The fair processing principle requires that information be easily understandable to data subjects. The language used must be appropriate. The level and type of language used has to be different depending on whether the intended audience is, for example, a child, the general public or an academic expert.

Data subject has the right to receive privacy information such as how data are collected and processed, which data are collected, who will process their data, who it will be shared with, the risks relating to the processing, their rights regarding processing.

Rights of Data Subject

In order to mitigate power imbalances between data subjects and controllers, individuals have been given certain rights to exercise control over the processing of their personal information. In addition to providing individuals with rights, it is important to establish mechanisms or policies that enable data subjects to challenge violations of their rights and claim compensation. The rights of data subjects are: the right to be informed (art. 12, 13, 14), the right of access (art. 15), the right to rectification, the right to erasure (right to be forgotten), the right to restrict processing, the right to data portability, the right to object.

Right to be informed - article 12 GDPR

The privacy information supplied by the data controller must be:

- transparent, intelligible and accessible, provided without delay
- written in clear plain language, particularly if addressed to a child
- provided in written form, including electronically where appropriate, and it may even be provided orally at the data subject's request and if his or her identity if proven beyond doubt
- provided free of charge

Article 13 and 14 GDPR

Article 13 and Article 14 of the GDPR deal with the right of data subjects to be informed, either in situations where personal data were collected directly from them, or in situations where the data were not obtained from them. In this last case, where the personal data is not obtained from the data subject directly, the data controller must notify the individual about the origin of the personal data (Art. 14 GDPR). The GDPR distinguish between two scenarios and two points in time at which the data controller must provide information to the data subject:

1. where the personal data is obtained directly from the data subject, the controller must notify the data subject about all of his or her information and rights under the GDPR at the time the dare obtained

2. where the personal data has not been obtained from the data subject directly, the controller is obliged to provide the information about the processing to the data subject within a reasonable period after obtaining the personal data, but at the latest within one month

If the controller intends to further process the personal data of for a different purpose, the controller shall provide all the relevant information prior to the processing taking place.

Information to be provided where personal data are collected from the data subject
Where personal data relating to a data subject are collect from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

- the identity and the contact details of the controller and, where applicable, of the controller's representative
- the contact details of the data protection officer, where applicable
- the purposes of the processing for which the personal data are intended as well as the legals basis for the processing
- where the processing is based on point (f) of article 6 (1), the legitimate interests of the controller or by a third party
- the recipients or categories of recipients of the personal data, if any
- where applicable, the fact that the controller intends to transfer personal to a third country or international organisation

Article 13 - Privacy statement
In addition to the information referred in paragraph 1, the controller shall, at the time when personal data are collected, provide the following information:

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- where the processing is based on the consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- the right to lodge a complaint with a supervisory authority
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

10 Lecture 10

Article 37 GDPR - Designation of a data protection officer (DPO)
1. The controller and the processor shall designate a data protection officer in any case where:

- the processing is carried out by a public authority or body, except for courts acting in their juridical capacity
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and / or their purposes, require and systematic monitoring of data subjects on a large scale
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10

The appointment of the DPO, therefore, is always the responsibility of the owner and manager as part of their governance policies.

Public authority or public body
Art. 29 WP considers that this expression should be understood according to its meaning in national law. Take for example the definition of *public body* in national law: *pursuant to art. 3 paragraph 1 letter d) of Legislative Decree. 50/2016 and Table IV, the notion of a body governed by public law includes entities having legal personality which have been established for the specific purpose of meeting need in the general interest, not having an industrial or commercial character, and which are also subject to public influence, being financed for the most part by the State, regional authorities or other bodies governed by public law; or their management is subject to supervision by those authorities or bodies; or their administrative, managerial or supervisory body is made up of members more than half of whom are appointed by regional or local authorities or by other bodies governed by public law.*
The above requirements are not alternative but cumulative. It become very complex, in some cases, to determine whether or not a holder galls within the definition of *public body.*

The solution of Art. 29 WP
The Working Group recommends, in terms of good practice, that private bodies entrusted with public functions or exercising public authority appoint a DPO.

Main Activities
This expression can understood as 'those essential operations which are necessary for the achievement of the objectives pursued by the controller or processor'. However, according to Art. 29 WP there may be cases where the main activity of the controller necessarily involves the processing of personal data (e.g., hospital or private security firm). Other activities, such as the payment of wages and salaries to employees, constitute necessary treatment but cannot be counted as core activities.

Large scale
Quantitative criteria cannot be adopted, bu the WP suggests that these elements should be taken into account:

- the number of subjects affected by the treatment
- the volume of data and / or the different types of data being processed
- the duration of treatment
- the geographical scope of the processing activity

Examples of large-scale treatments: hospitals, insurance, banks, search engines (behavioural advertising). city public transport (location).
Examples of non large scale treatments: individual health professional, single lawyer.

Regular and systematic monitoring
This certainly includes all forms of tracking and profiling on the Internet for the purposes of behavioural advertising, but not only that.
Monitoring: in the text of the Regulation it is always found combined with the terms *behaviour* and *publicly accessible area*, so it could refer to both the profiling of users / customers and to the forms of surveillance and control of public areas.
Regular: that occurs continuously, recurrently or at defined intervals.
Systematic: predetermined, organized or methodical.
All this conditions must be met.
Examples: take care of the operation of the telecommunications network, providing telecommunications services, redirecting email messages, marketing based on the analysis of collected data and profiling.

Article 37 GDPR - Designation of a data protection officer (DPO)
2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.
3. Where the controller or the processor is a public authority or body, a single data protection officer may be designed for several such authorities or bodies, taking account of their organisational structure and size.
4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controller or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

Hamburg Commissioner for Data Protection and Freedom of Information
On December 2019, the Hamburg Commissioner for Data Protection and Freedom of Information imposed a fine of 51, 000 euros on the German branch of Facebook because it had failed to appoint a DPO. As its defense, Facebook has argued that its DPO was appointed in Ireland, and it would act as DPO for all European Facebook branches. On the other hand, the German DPA argued that Facebook did not notify about the referred nomination. Therefore, if one organization has managed to appoint its DPO to one supervisory authority, despite the consistency mechanism, it is highly recommended to notify other supervisory authorities wherever there are other branches of the organization.

Article 37 GDPR - Designation of a data protection officer
5. The DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.
6. The DPO may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.
7. The controller or the processor shall publish he contact details of the DPO and communicate them to the supervisory authority.

Professional qualities and personal skills
The network of DPOs of Community institutions and bodies identifies the following:

- knowledge of European regulations on privacy and data protection
- knowledge of IT and system security
- knowledge of how the institution operates and ability to interpret the relevant rules in the context of the context

- experience as DPO (between 3 and 7 years)
- capacity for initiative, organisation, perseverance and discretion
- integrity and confidentiality
- motivation
- communication, negotiation and conflict resolution skills

Ina any case, professional qualities must be assessed in the specific case in relation to the level of complexity.

How do you choose an in-house DPO?
the internal DPO must not have conflicts of interest, so it cannot be a person who 'involves the definition of the purposes or methods of the processing of personal data', such as: the managing director, the marketing director, the director of HR, the IT manager. You will need to have that 'specialized knowledge' required by law. You'll have to have time to be a DPO.

GDPR's requirements for DPOs
Risk / IT. Recital 77 and Articles 39.2 and 35.2 requires DPOs to offer guidance on risk assessments, countermeasures and data protection impact assessments. DPOs must have significant experience in privacy and security risk assessment and best practice mitigation, including significant hands-on experience in privacy assessments, privacy certifications / seals, and information security standards certifications.
Legal expertise / independence. Recital 97 and Articles 37.1, 37.5, and 38.5 specify *a person with expert knowledge of data protection law and practises* to assist the controller or processor, to be *bound by secrecy or confidentiality*, and *perform their duties and tasks in an independent manner.* DPOs must know data protection law to a level of expertise based upon the type of processing carried out. In some cases, this was intended that DPOs should be a person with legal background knowledge of not only the GDPR and other relevant EU legislation but also privacy and related laws in all jurisdictions their organization does business or outsources operations.
Leadership. Article 38.2 requires, *the controller and processor shall support the DPO ... by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.* DPOs will need to have leadership and project management experience, to be able to request, marshal and lead the resources need to carry out their roles. They also must be able to critically assess themselves for knowledge gaps and request training in those areas.
Board-level. Article 38.3 requires, *the controller and processor shall ensure that the DPO does not receive any instructions regarding the exercise of those tasks ... the DPO shall directly report to the highest management level of the controller or the processor.* DPOs have to be self-starters, with the competence and skills to carry out the role without guidance and to know where to find necessary information. DPOs must also have board-level presence and be able to deal with experienced business people who will not know the intricacies of DPOs functions.
Teaching capabilities. Article 38.4 allows data subjects to contact the DPO *with regard to all issues related to processing of their personal data and to the exercise of their rights.* DPOs must be able to speak in the language of the average citizen, not in technical or legal jargon, to handle requests and complaints from data subjects. A common touch is helpful to DPOs in their role to protect data subjects' rights. DPOs must also have skills in both legal training and awareness raising, to ensure all data subjects are aware of their rights and responsibilities and to help train others to assist data subjects on specific requests.

The UNI 11697:2017 standard
The personal data processing and protection professional. *The professional working in*

the filed of the treatment and protection of personal data performs a wide range of activities that are often transversal in nature compared to other business processes, both with respect to the life cycle of the treatment - from design to termination - and with respect to the issues covered, technological, legal and other. The professional working in the filed of personal data processing and protection therefore contributes to the management or verification of a more or less extensive set of processes and information systems involved in the processing of personal data on behalf of individuals or legal entities such as, for example, bodies, institutions, associations, public or private entities.

The expected roles
Data protection officer. It is a profile corresponding to the professional profile regulated in the EU Regulation 2016/679, in particular in Article 39. The assignment to this profile of different and / or additional tasks included in other managerial level profiles is allowed in compliance with the principle of absence of conflict of interest.
Privacy Manager. It is a profile relevant to individuals with a very high level of knowledge, skills and competences in a specific organizational context (be it a functional area of the organization or the sector to which it belongs) to ensure the adoption of appropriate organizational measures in the processing of personal data.
Privacy specialist. This profile is relevant to individuals who support the DPO and / or Privacy Manager in developing appropriate technical and organizational measures of he processing of personal data.
Privacy Assessor. It is a profile relevant to independent individuals with knowledge and skills in the IT/technology and legal/organizational fields who conduct personal data processing and protections activities, and who may nevertheless use specialists in both fields to carry out audit activities.

Skills
Contribute to the strategy for processing and protection of personal data. Manage the application of applicable codes of conduct and certifications regarding the processing and protection of personal data. Ability to communicate. Analytical skills. Self-management and stress control. Capacity for self-development. Control capability. Ability to convince. Conflict management skills. Initiative and many others.

Knowledge
The principles of privacy and protection by design and by default. The rights of the interested parties provided for by current laws and regulations. The responsibilities related to the processing of personal data. Italian and European laws on the processing and protection of personal data and many other.

Definition of DPO
The DPO is the professional, internal or external to a given structure, who has the task of supervising all the process that relate to the processing of personal data carried out within the same, intervening with full independence and autonomy if it identifies problems that could lead to processing of data that presents risks of destruction or loss, even accidental, of the data, unauthorized access or treatment not allowed or not in accordance with the purposes of he collection that would undermine the rights and fundamental freedoms of he person concerned.

Data Controller, Data Processor and DPO
Neverthelesssm according to Opinion WP243 rev.01, the voluntary appointment of a DPO is a good practice for the owner because *this figure represents a fundamental element for the purposes of accountability.* It is not necessarily the case that if the owner appoints a DPO, the manager is also required to appoint one, but his *may also be good practice.*

The DPO and accountability
Recital 77: *guidance on the implementation of appropriate measures and on the demon-*

stration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the board or indications provided by a data protection officer.

Features
Professional: in order to be able to speak of DPO, it is necessary to refer to its professional qualities.
Internal or External: the DPO can be either an internal or an external subject to the structure.
Oversee: the DPO must have expertise across the various fields of knowledge affected by privacy rules, primarily law and information technology.
Intervening in full *independence* and *autonomy*: the DPO cannot be just a lightning rod but must have both authority of action and, to some extent, assets.

Delegations
The DPO must be appointed by the owner or controller, identified as their respective senior management. In the event that it is not the top management figure who appoints the DPO, any person in charge shall act in the presence of express delegation. A good *accountability* practice would be to briefly explain in the appointment resolution the reasons and the path that the owner has followed to decide to have a DPO within his organization.

The tasks
The minimum duties of the DPO are specified in Article 39 of the GDPR.

1. to inform and advise the controller or the processor as well as the employees carrying out the processing operations of their obligations pursuant to this Regulation and other Union or Member State data protection provisions

2. to monitor compliance with this Regulation, with other Union or Member State provisions on data protection and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness raising and training of staff involved in processing operations and related monitoring activities

3. to provide, where requested, an opinion on the data protection impact assessment and monitor its implementation in accordance with Article 35
   cooperate with the supervisory authority

4. to act as a contact point for the supervisory authority on matters related to the processing, including prior consultation referred to in Article 36, and to conduct, where appropriate, consultations on any other matters

In summary, its tasks are to *inform, monitor, advise, cooperate* with the MLCA and act as a*contact point.*

Minimum content according to IAPP
Parties: the controller's or processor's legal entity is one party, and the DPO firm or individual is the other party.
DPO's services: at a minimum, this should list the Article 39 tasks and then should add any other duties carried out by the DPO within the DPO role.
Controller's responsibilities: at a minimum, this should list the controller's/processor's obligations under Articles 37-38 and other obligations under local law.
Handling differences: outlines the procedure engaged if the DPO and the controller/processor do not agree upon an important issue related to GDPR compliance and whether external counsel must be provided for.

Compensation: whether a DPO is working on a fixed free or hourly basis and how additional hours are handled/approved.
Limitations of liability: the DPO should limit their potential liability to the controller or processor, perhaps to the amount of fees paid to the DPO for their services.
Indemnification: the DPO should be protected against any legal actions them initiated by third parties regarding the services, such as those impacted by a data breach.
Conflicts of interest: there should be a clear statement that there are no know conflicts from the services and any future conflicts will be notified to the parties and addressed at that time.
Confidentiality: that the DPO will comply with professional duties of confidentiality or secrecy.
Training: how the DPO will maintain their competence in data protection and related ares.
Term: it is important to set an appropriate duration for the agreement that allows the DPO sufficient time to assess and implement the necessary changes to bring about GDPR compliance.
Termination: which duties will continue upon termination of the contract and how personal data is returned/deleted.

How do a DPO perform his/her duties?
In the performance of his/her duties, the owner and the controller:

- ensure that the DPO is timely and properly involved in all matters concerning the protection of personal data
- support the DPO in the performance of the tasks referred to in Article 39 by providing him/her with the resources necessary to perform those tasks and to access personal data and processing operations and to maintain his/her expertise
- shall ensure that the DPO does not receive any instructions as regard the performance of those tasks, The data protection officer shall not be removed or penalised by the controller or processor for the performance of his/her tasks. The DPO shall report directly to the hierarchical superior of the controller or processor
- they shall ensure that other tasks and functions do not give rise to a conflict of interest

Resources
The WP provides this guidance:

- Active support of the DPO by senior management
- sufficient time to perform the tasks assigned to the DPO
- adequate support in terms of financial resources, infrastructure and, where appropriate, personnel
- official communication of the appointment of the DPO to all personnel
- guaranteed access to other company functions so that the DPO can have the support and information necessary to carry out his duties
- support for continuing education
- support for the establishment and remuneration of a team

Independence
The DPO does not have to be instructed to carry out his tasks but he cannot in any case overstep the bounds of Article 39. The DPO reports to senior management which is not obliged to follow his instructions. However, it is essential to keep a record of this dialogue between the owner or manager and the DPO. The DPO must have a contractually defined

timeframe for action that is compatible with the development of a data protection policy within the organization. The independence, borrowing what the jurisprudence and the doctrine have already provided for the Supervisory Board 231/01, can be declined in:

- independence form any interface by corporate bodies, in particular the Board of Directors
- independence from economic or personal constraints
- existence of possible conflicts of interest
- nonexistence of any elements of functional dependence on top management

Conflict of interest
The DPO may perform other functions as long as these do not give rise to a conflict of interest (Art. 38 para. 6 GDPR). In our legal system, a conflict of interest is generally recognised when there is a direct or indirect correlation between a personal interest of a person, or if his relatives or kin, and the interests of the body or entity he represents. It is sufficient for this interest to be divergent, since it need not be conflicting. The conflict of interest remains so even when the final decision taken is the most convenient or opportune one for the body or entity.

Art. 7 DPR 62/2013
The employee refrains from participating in the adoption of decision or activities that may involve his or her own interests, or those of his or here relatives, relatives by marriage up to the second degree of kinship, spouse or cohabitants, or persons with whom he or she has regular contact, or, subjects or organisations with which he or she or his or her spouse has a pending lawsuit or serious enmity or significant credit or debt relationships, or subjects or organisations of which he or she or guardian, curator, attorney or agent, or bodies, associations, including unrecognised ones, committees, companies or establishments of which he or she is director or manager or executive.

Art. 42 D.Lgs. 50/2016
2. A conflict of interest exists where staff of a contracting station or a service provider who, including on behalf of the contracting station, are involved in the conduct of the procurement and concession procedure or may influence, in any way, its outcome, have, directly or indirectly, a financial, economic or other personal interest that may be perceived as a threat to their impartiality and independence in the context of the procurement or concession procedure.

Conflict of interest in the GDPR
In the standard, the phrase *conflict of interest* is linked to *performing other duties and functions.* According to my personal interpretation, therefore, the conflict of interest applies ex nunc and not ex tunc. Those who perform functions that may give rise to conflicts of interest should ensure that these situations cease after being appointed as DPO (e.g., the entity's lawyer, when appointed as DPO, will no longer be able to defend cases in which data processing issues are discussed, such as employment cases).

DPO and DPIA
The WP recommends that the owner consult the DPO on these issues:

- whether or not to conduct a DPIA
- which methodology to adopt
- whether to conduct it with internal resources or outsource it
- which safeguards to apply in order to mitigate risks to the rights and interest of the persons concerned

- whether or not the DPIA has been properly conducted, and whether the conclusions reached are in compliance with the GDPR

If the owner disagrees with the DPO's guidance, the DPIA documentation must *specifically state in writing* the reasons for this non-compliance.

DPO Diligence
As far as diligence in performance is concerned, the second paragraph of article 1176 of the Civil Code can be recalled: *in fulfilling the obligation, the debtor must use the diligence of a good family man. In the performance of the obligations inherent in the exercise of a professional activity, the diligence must be assessed with regard to the nature of the activity exercised* → principle of teh so called *qualified diligence.*

Qualified Diligence
Cass. Civ. 10165/2016. *is expressed in the appropriate technical effort, with the use of energy and means normally and objectively necessary pr useful in relation to the nature of the activity carried out, aimed at the performance of the service due and the satisfaction of the interests of the creditor, as well as to avoid possible harmful events.*

Liability
General principle of the provision of intellectual work under article 2230 of the Civil Code, which provides for liability under article 2236. *If the service involves the solution of technical problems of special difficulty, the service provider shall not be liable for damages, except in the case of wilful misconduct or gross negligence.*

11 Lecture 11

What is the Council of Europe?
Established on 5 May 1949 (Treaty of London) by 10 states. Comprises 47 member states today. Based in Strasbourg (France). Intergovernmental political Organisation, founded on three main values: human rights, democracy and the rule of law.

Major achievements of CoE
More than 210 treaties, including on the following topics: abolition of death penalty, prevention of torture, social protection, protection of national minorities,, cybercrime, human trafficking, sexual exploitation of children, violence against women and domestic violence, madicrime.

Council of Europe vs European Union
Two separate organisations with complementary roles. A strategic partnership based on political dialogue and legal co-operation. Joint programs co-financed by the EU with the experience of the CoE in the fields of rule of law, democracy and human rights. Ratification of 16 conventions by the EU. Preparation for the accession of the Union to the European Convention on Human Rights. European Heritage Days: a common achievement.

Inter-relationship between cybersecurity and cybercrime
Cybersecurity and cybercrime can be distinguished in the context of law:

1. *cybersecurity* relates to the technical, administrative and procedural methods to ensure the confidentiality, integrity, availability and resilience of information systems
2. *cybercrime* relates to the criminal laws that punish crimes committed with a computer or where the information system is the target

Ransomware attack
Ransomware attack is a form of extortion that uses malware to encrypt documents stored

on the computer in order to deny the legitimate operator access to important documents. This type of ransomware is referred to as cryptoware. While the most prolific ransomware families currently fall under this category, there are other types of ransomware that do not encrypt data but e.g., block access to a computer, such as police ransomware. Once documents are encrypted, ransomware demands a ransom payment from the victim in order to release the information. The payment is usually done via an anonymous payment mechanism, such as Bitcoin.

The steps of a ransomware attack

1. prevention of or protection from a ransomware attack → Cybersecurity
2. identification, collection and analysis of digital evidence → Cybercrime
3. identification, prosecution and punishment of the attacker → Cybercrime

The recommendation of the Stockholm European Council
The Council will develop together with the Commission of comprehensive strategy for the security of electronic networks, including concrete implementation actions. This strategy should be presented in time for the Gothenburg European Council.

European bodies dealing with ICT security
Commision: Information Society Directorate
Council: working party on telecommunications and information society services
European Parliament: Parliamentary Committees
Funding: eEurope Action Plan

The Budapest Convention on Cybercrime
The Budapest Convention as opened for signature on 23 November 2001. It is not a self-executing treaty, but need to be implemented into domestic legislation. The Convention serves many other States as a guideline for domestic legislation. The Convention is backed up by the Cybercrime Programme Office for capacity building. The aim of the Budapest Convention is to provide an international framework to combat cybercrime through:

- common definition of the offences
- regulation of procedural tools
- foster international cooperation

Cybercrime and electronic evidence: Challenges for criminal justice
The scale and quantity of cybercrime, devices, users and victims, Technically challenges (VPN, anonymisers, encryption, VOIP, etc.). Cloud computing, territoriality and jurisdiction (cloud computing, unclear where data is stored and / or which legal regime applies, service provider under different layers of jurisdiction, unclear which provider for which services controls which data, is data stored or in transit?). The challenge of mutual legal assistance. No data → no evidence → do justice.

Problems
Differing national laws
Locus commissi delicti
Cross.border crimes
Interagency cooperation need
Common criteria for data retention

Advantages of Budapest Convention
The Budapest Convention requires States to ensure that the offences against and by

means of computers of Article 2 to 12 are criminalised in their domestic law, and that their criminal justice authorities have the powers prescribed in their procedural law not only to investigate cybercrime but any offence where evidence is in electronic form. Domestic legislation consistent with the Budapest Convention further facilitates international cooperation in that it helps meet the dual criminality requirement. Some of the domestic procedural powers of the Convention also have a corresponding provision in the chapter on international cooperation.

The 'computer system'
Article 1 of the Convention defines a *computer system* as *any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.* The term *computer data*, on the other hand, means *any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to a cause a computer system to perform a function.*

Other definitions
Service provider means *i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system*
ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.
Traffic data means *any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service.*

New criminal offences
Title I *Offences against the confidentiality, integrity and availability of data and IT systems.*
Art. 2 Illegal access: *each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.*

Art. 3 Illegal interceptions
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system. .

Art. 4 Data interference
1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Art. 5 System interference
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the

serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Art. 6 Offence of abuse of computer devices
Sanctioning the manufacture, sale, procurement for use, importation, distribution, or otherwise making available of a device (including a computer program, intended or used primarily for the propose of committing any offense) or even a computer password, access code, or similar information by which the entire computer system or any part thereof may be made accessible, with the intent to commit any offense.

The specific intent
2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offense established in accordance with Article 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

Art. 7 Forgery of electronic documents
If committed intentionally and without right. The input, alteration, deletion or suppression of computer data, resulting in inauthentic data with the intent that it be considered or used for legal purposes ass if it were authentic, regardless whether or not the data is directly readable or intelligible, is punishable.

Art. 8 Computer fraud
If committed intentionally and without any right, causing loss of property to another person by introducing, altering, deleting or suppressing computer data or by interfering with the operation of a computer system with the fraudulent or dishonest intention of procuring an unfair economic benefit for oneself or other, is punishable.

Art. 9 Child Pornography
Production of child pornography fot the purpose of its distribution through a computer system, the offering or making available of such pornography through a computer system, the distribution or transmission of such pornography trough a computer system, the procuring child pornography through a computer system for oneself or others, the possessing of such pornography by means of a computer system or a computer-data storage medium.

Art. 10 Offences related to infringements of copyright and related rights
Any assault on intellectual property rights if such acts are committed deliberately, on a commercial scale, and through the use of a computer system. A Party may reserve the right not to impose criminal liability in certain circumstances (e.g., by providing civil remedies only), provided that other effective remedies are available and that such reservation does not derogate from that Party's international obligations under international instruments.

Art. 12 Corporate Liability
Legal persons can be held liable for a cybercrime committed on their behalf by a natural person acting either individually or as a member of an organ of the legal person, who exercises a power or direction within the legal person, based on: a power of representation of the legal person, authority to make decisions on behalf of the legal person, or authority to exercise control within the legal person. A legal entity may be held labile if the lack of supervision or control of a natural person has made possible the commission of computer crimes on behalf of the legal entity by a natural person acting under its authority.

The Italian law on computer crimes 'in a narrow sense'

Illegal access
Art. 615-ter c.p. *Anyone who illegally enters a computer or telecommunications system protected by security measures, or who remains there against the express or tacit will of those who have the right to exclude him/her, is punished with imprisonment of up to 3 years.*

Aggravating
The penalty is imprisonment for 1 to 5 years:

1. if the act is committed by a public official or a person in charge of a public service, with abuse of power or violation of the duties inherent in the function or service or by a person who also abusively exercises the profession of private investigator, or with abuse of the quality of system operator

2. if the culprit uses violence against property or persons to commit the act, or if he is obviously armed

3. if the fact results in the destruction of or damage to the system or the total or partial interruption of its operation, or the destruction of or damage to the data, information or programs contained therein.

Aggravating and procedural
If the facts referred to in the first and second paragraphs concern computer or telecommunications systems of military interest or relating to public order or public safety pr health or civil protection or in any case of public interest, the penalty is imprisonment for a period of between 1 and 5 years and between 3 and 8 years respectively. In the case envisaged in the first paragraph, the crime is punishable on complaint by the offended person; in other cases it is prosecuted ex officio.

The mailbox as a 'computer system'
Cass. Pen. , sez V, 28/10/2015 n. 13057. *The mail box is nothing else than a memory space of a computer system intended for the storage of messages, or information of other nature (images, video, etc.), of a subject identified by an account registered with a service provider. And the access to this memory space is, clearly, an access to the computer system, since the box is nothing else than a portion of the complex equipment - physical and abstract - destined to the memorization of the information. When this portion of memory is protected - as in this case, through the affixing of a password - in such a way as to reveal the clear will of the user to make it space reserved for himself, any unauthorized access to it constitutes the material element of the crime referred ton in art. 615/ter of the Italian penal code.*

the concept of 'computer domicile'
Cass. Pen. Sez. VI of December 14, 1999, n. 3067. *On the other hand, with the reference to the computer domicile, it seems that the legislator wanted to identify the physical place - as a site where the human personality can be expressed - in which the object of protection is contained (any kind of data and not data having as object particular contents), in order to safeguard it from any kind of intrusion (ius exludendi alios), regardless of the purpose that the author o the abuse proposes.*

The concept of security measure
Cass. Pen. Sez. V of December 6, 2000, no. 12732. *But it must be considered that, for the purposes of the configurability of the crime, any mechanism of selection of the subjects qualified to access the computer system is relevant, even when it is a matter of instruments external to the system and merely organisational, in that they are intended to regulate the entrance into the premises where the systems are kept.*

Overcoming security measure
Cass. Pen. Sec. V of February 15, 2007, no. 6459. *For the crime under Article 615-ter*

to exist, it is necessary that the computer of telematic system is protected by security measures that someone has neutralized.

Subjective element

Cass. Pen. Sez. Un. of February 7, 2012, n. 4694.
The criminal offence of abusive access to a protected computer or telematic system, provided for by art. 615-ter of the Italian Criminal Code, is constituted by the conduct of acces or maintenance in the system carried out by a subject who, although being authorized, violates the conditions and limits resulting from eh set of prescriptions given by the owner of the system in order to objectively limit the access. On the contrary, the purposes and aims that subjectively motivated the access to the system are not relevant for the configuration of the crime.

Locus commissi delicti

Cass. Pen. Sec. I, Sept. 8, 2015, No. 36338. *The abusive entry or introduction, then, are to be integrated in the place where the operator materially types the access password or performs the login procedure, which determines the overcoming of the security measures taken by the owner of the system, thus achieving access to the database. From this setting, the place of the committed crime is identified with that in which from the remote location the agent interfaces with the entire system, types the authentication credentials and presses the start key, thus putting in place the only material and voluntary action that puts him in a position to enter the domain of the information that is viewed directly within the peripheral location.*

Violations of limits imposed by the system owner

Cass. Pen. , sez. V, 29/09/2016 . 3818. *With regard to the alleged legitimacy of the access, the defense of the plaintiff puts forward a reading of the regulatory data that must now be understood to be superseded by the jurisprudence of the United Sections of this Court, according to which integrates the crime provided for by art. 615-ter cod. pen. anyone who, despite being authorized, accesses or remains in a protected computer or telecommunications system in violation of the conditions and limits resulting from the set of requirements remaining irrelevant, for the purposes of the existence of the crime, the purposes and aims that have subjectively motivated the entry into the system.*

Abusive access to a law firm

Cass. Pen., sec. V, 05/12/2016, no. 11994 (maximum). *The conduct of a collaborator of a law firm - entrusts exclusively with the management of a limited number of clients - who, although in possession of the access credentials, enters or remains within a protected system in violation of the conditions and limits imposed by the owner of the firm, copying and duplicating, transferring them to other computer media, the files concerning the entire clientele of the professional firm and, therefore, outside the competence assigned to him, constitutes the crime provided for by Article 615 ter of the Italian Criminal Code.*

Relationship between abusive access and unlawful data processing

Cass. Pen., sec. V, 05/1272016, no. 11994 (maximum). *There is no relationship within the scope of art. 15 of the Italian penal code between the offence referred to in art. 615 ter of the Italian penal code which punishes the abusive access to a computer system, and the one referred to in art. 167 Legislative Decree no. 169 of 2003, concerning the illegal processing of personal data, as they are different cases in terms of final conduct and material activities that exclude the existence of a relationship of homogeneity capable of leading them 'ad unum' in the figure of the special crime, pursuant to art. 15 of the Italian penal code.*

Aggravated access of the public official

Cass. Pen. Sez. V of 20/11/2020, n. 72. *On the subject of unauthorized access to a computer system, for the purposes of the configurability of the aggravating circumstances* *referred to in art. 615-ter, paragraph 2, n. 1, Criminal Code is not sufficient the mere qualification of public official or public service officer of the active subject, but it is necessary that the fact is committed with abuse of power or violation of the duties inherent in the function, so that the subjective quality of the agent has at least facilitated the realization of the crime.*

Knowledge of access credentials and abusiveness
Cass. Pen., sez. V, 06/06/2017, n. 52572. *In the case in point, the circumstance that the plaintiff was aware of the password for access to the computer system does not exclude the abusive nature of the accesses carried out by her, in view of the result obtained - clearly in contrast with the will of the owner of the electronic mailbox - to determine the challenge of the password with the setting of a new request for recovery and the insertion of the insulting phrase 'when you took in in your ***' It follows that the territorial court, in highlighting, moreover, as the abusive accesses have also temporarily excluded the A. from the use of the e-mail service, has concluded in the sense of considering fully proved the overcoming by the defendant of the intrinsic limits connected with the knowledge of the password.*

Unauthorized access and breach of correspondence
Cass. Pen. Sec. V of 25/03/2019, no. 18284. *Integrates the offence referred to in Article 615-ter of the Cp, the conduct of those who improperly access to other people's mailbox, being a memory space, protected by a custom password, a computer system designed to store messages, or information of another nature, the exclusive availability of its owner, identified by an account registered with the service provider. Nor, on he contrary, could the offensiveness of the conduct be resolved within the perimeter outlined by articles 616 and 635-bis of the Penal Code, which protect, respectively, the content of correspondence and the physical protection of computer equipment, sanctioning, however, conduct that is additional and subsequent to the abusive introduction into a protected computer system. Therefore, in case of abusive access to an email box protected by a password, the crime described in article 615-ter of the Italian Criminal Code is concurrent of the content of the emails stored in the archive, and with the crime of damaging computer data, in case the abusive modification of the access credentials results in the owner's inability to use the email box.*

Unauthorized possession and distribution of access codes
Article 615-quater. *Whoever, in order to procure a profit for himself/herself or for others or to case damage to others, illegally procures, reproduces, circulates, communicates or delivers codes, password or other means of access to a computer or telecommunications system protected by security measures, or in any case provides indications or instructions suitable for this purpose, is punished with imprisonment of up yo 1 year and a fine of up to 10 million lire. The penalty is imprisonment for a period of between 1 and 2 years and a fine of between 10 million and 20 million lire if any of the circumstances referred to in numbers 1) and 2) of the fourth paragraph of article 617-quater apply.*

Illegal interception, impeding or interrupting o computer or telematic communications
Article 617 - quater. *Whoever fraudulently intercept communications relating to a computer or telecommunications system or between several systems, or prevents or interrupts them, is punished with imprisonment from 6 months to 4 years. Unless the act constitutes a more serious offence, the same punishment applies to anyone who reveals, by any means of information the the public, in whole or in part, the contents of the communications referred to in the first paragraph.*

Aggravating
The offences referred to in the first and second paragraphs are punishable on complaint by the injured party. However, they are prosecuted ex officio and the penalty is imprisonment

for a period of between 1 and 5 years if the act is committed:

1. *to the detriment of a computer or telematic system used by the State or by another public body or by a company providing public services or services of public necessity*
2. *by a public official or a person in charge of public service, with abuse of power and violation of the duties inherent in the function or service, or with abuse of the quality of system operator*
3. *by those who also abusively practice the profession of private investigator*

Installation of equipment of designed to intercept, impede or interrupt computer or telematic communications
Article 617-quinquies. *Whoever, apart from the cases permitted by law, installs equipment designed to intercept, impede or interrupt communications relating to a computer or telecommunications system or between several systems, is punished with imprisonment from 1 to 4 years. The penalty is imprisonment from 1 to 5 years in the cases provided for in the fourth paragraph of Article 617-quarter.*

Falsification, alteration or suppression of the content of computer or telematic communications
Article 617-sexies. *Whoever, in order to procure for himself/herself or for others an advantage or to cause damage to others, falsely forms or alters or suppresses, in whole or in part, the content, even occasionally intercepted, of any of the communications relating to a computer or telecommunications system or between several systems, is punished, if he/she makes use of them or allows others to make use of them, with imprisonment of from 1 to 4 years. The penalty is imprisonment form 1 to 5 years in the cases provided for in the fourth paragraph of Article 617-quater.*

Art. 635-bis c.p.
Unless the act constitutes a more serious offence, anyone who destroys, deteriorates, deletes, alter or suppresses information , data or computer programs belonging to others shall be punished, on complaint by the injured party, by imprisonment from 6 month to 3 years.

The novelties introduced
The offence becomes subject to a lawsuit by the injured party, harmonizing with the provision of art. 635 of the Penal Code. The modalities of the conduct of damage are better specified and are no longer only *destruction* or *deterioration*, but also *cancellation, alteration* and *suppression.*

Art. 615-quinquies c.p.
Whoever, in order to illegally damage a computer or telecommunications system, the information, data or programs contained therein or pertaining to it, or to favour the total or partial interruption or alteration of its functioning, procured, produces, reproduces, imports, circulates, communicate, delivers or, in any case, makes available to others equipment, devices or computer programs, is punished with imprisonment of up to 2 years and a fine of up to 10.329 euros.

Advantages
However, Article 6 of the Convention is complies with by extending the material element of the conduct which now also includes *procuring, producing, reproducing, importing.* However, there have been those who have pointed out that there is a risk of excessively anticipating the threshold of criminal intervention. Finally, some conducts are overlapping.

Applicable facts
615-ter c.p. (illegal access)

615-quinquies penal code (distribution of computer programs designed to damage)
625-bis c.p. (damage to information, data and computer programs)
635-quater c.p. (damage to computer or telematic systems)
392 c.p. (violence on things)
629 c.p. (extortion)
610 c.p. (private violence).

12 Lecture 12

The challenge of deepfake-content removal

The deepfake phenomenon
Manipulated or synthetic audio or visual media that seem authentic, and which feature people that appear to say or do something they have never said or done, produced using artificial intelligence techniques, including machine learning and deep learning.

New AI techniques allow for generating new visual content or forge original visual content. 2 main technologies:

- *Autoencoders*
- *generative Adversarial Networks*

Five graphical deepfake techniques:

- *Facial expression manipulation*: these techniques can be used to modify a specific part of a target's face in an image or video, preserving the target's identity. For example, this can be achieved by transferring the expressions of an actor to the target. Similar techniques are used for *visual dubbing* proposes in which only the movement of the lips of a target are adjusted based on the modification of audio or by using text input. Any part of a person's can be targeted including adjusting the lighting or pose of the head.
- *Face morphing*: the goal of this technique is to create an image or video i which the faces of similar looking people are merged in such a way that the pictures seem to depict both. It is, for example, used to fraudulently obtain authentic identification documents, such as passports, that can be used by multiple persons.
- *Face replacement/swap*: with these techniques, the face of a target person is replaced by the face of the source video. Popular tools are Faceswap, DeepFaceLab and DFaker. Alternatively, a face can be replace with footage rendered based on a 3D model.
- *Face generation*: face generators synthesise partial or entirely new images of people that do no exist. The techniques makes use of GANs. Partial generators can be. for example, used t replace the VR goggles of a person by an image of their eyes.
- *Full body puppetry*: these techniques enable users to modify the pose of a part or entire body of a target in an image or video. An existing video could be used as a driver, or a sequence that was recorded using motion capture. This technology can, for example, make it appear as if anyone can dance like a professional.

Deep-fakes reddit user popularized the production of AI techniques to generate image of Princess Leia Organa. Reddit community face-swapped images of Emma Watson, Scarlett Johansson and Michelle Obama with graphic images of pornographic actresses. According to a 2019 September stat, 94% of 134.364.438 online deepfake video are pornographic.

Societal context:

- social media platform and growing importance of visual communication
- growing spread of misinformation / disinformation / malformation on social networking platforms
- proliferation of non-consensual deepfakes

Key drivers:

- availability of datasets and computing power
- accessibility of pre-trained models
- 5G
- 3D sensors
- cat-and-mouse game between producers and detectors

Trends:

- supply and demand of deepfake content
- commodification of deepfake tools
- deepfake-as-a-service companies (HourOne, X-Sidus, Rozy)
- live real-time deepfakes
- reduced input requirements

Benefits:

- audiographic production
- human-machine interactions
- video-conferencing
- satire
- personal and artistic creative expression
- medical research applications

Risks and impacts:

- Psychological harm: (s)extortion, defamation, intimidation, bullying, undermining trust
- Financial harm: extortion, identity theft, fraud, stock-price manipulation, brand damage, reputational damage
- Societal harm: news media manipulation, damage to economic stability, damage to the justice system, damage to the scientific system, erosion of trust, damage to democracy, manipulation of elections, damage to international relations, damage to national security

Regulatory landscape and gaps
The AI regulatory framework: creators are obliged to label deepfake content as such, in order for viewers to understand that is forged material (disclosure obligation) - Art. 52(3). This does not apply when *the use is authorized by law to detect, prevent, investigate and prosecute criminal offences or it is necessary for the exercise of the right to freedom of expression and the right to the freedom of the arts and sciences.* Art. 71 does not specify among the penalties non-compliance with art. 52(3). Deepfake technology is not categorized as high-risk as opposed to deepfake detection technology used by law

enforcement authorities.

E-Commerce Directive: hosting service providers are not subject to any obligation to monitor the information flowing through their channels. Hosting service providers must remove content as soon as they are aware of the existence of illegal content. A clear definition of illegal content is lacking, notwithstanding further EU legal sources. The E-Commerce Directive harmonized the conditions for releasing providers from liability, but not the conditions to establish said liability.
Digital Services Act (DSA) - 2020 Proposal: it will replace the E-Commerce Directive jointly with the Digital Market Act (DMA). The DSA stipulates that intermediary providers which moderate user-generated content must make transparent

- which moderation rules apply
- which measures they implement to enforce these

Platforms using a notice-and-takedown-procedure must create a system to report illegal content. Platforms above a certain size must implement a procedure which those affected can appeal against any blocking. Platforms will be obliged to provide more transparency on blocking. Definition of illegal content still absent.
Copyright regime (national and harmonised EU law): works protected by the copyright regime can only be used when the author (and thus copyrighted owner) has given permission. Application scope photographic works and cinematographic works in particular. Copyrighter owners can make claims and object the use of their material in a deepfake video. A deepfake creator must in principle always have permission of the copyright owner of the original material, before using the work to create a deepfake. Restrictions as to what counts as a work that is protected under copyright law. The use of copyrighted material to generate deepfakes for scientific use, and purposes of caricature, parody or pastiche is widely permitted under exceptions.
Image rights: Art. 8 ECtHR. ECtHR ruling in 2009: one's image is *one of the essential components of personal development and presupposes the right to control the use of that image*, hence deserves legal protection. This is not an absolute right: balance with owner fundamental rights and freedoms (expression, speech, parody, political commentary, etc...).
The General Data Protection Regulation (GDPR): performance of DPIA (data protection impact assessment) for controllers. Information notice to data subjects if legitimate interest of the controller does not apply. Objection to data processing and right to ensure (right to be forgotten).
Audio Visual Media Directive (AVMD): A focus on the protection of the wellbeing of minors. Member States shall regulate video-sharing service to prevent impairment of the physical, mental or moral development of minors to offer effective parental controls. Pornography and violent content should be treated by the strictest measures, such as age-verification, pin-codes, clear labelling or automatic filtering. Video-sharing platforms shall detect the nature of the content shared and implement measures in the interest of the viewer, creator and general public. The AVMD thus contains provisions to respond to, for example, the distribution of non-consensual pornography deepfakes. Member States will have to balance the regulation of harmful content with applicable fundamental rights (freedom of expression and respect for private life).
Code of Practice of Disinformation: signed by Mozilla, Twitter, Facebook, Google and some other stakeholders in October 2018. Micorosoft and TikTok joined later in 2019 and 2020. Issue with published transparency reports: they lack meaningful information. Not really effective due to the self-regulation governance mechanism.

Removing deepfake content: challenges and issues
Tackling Illegal Content Online: towards and enhanced liability of online platforms. Towards a proactive definition of online platforms within the EU. European Commission suggested: enforcement of notice and take down mechanism. Cooperation with law enforcement agencies. trusted flaggers, automatic removal, automatic filtering out against

upload of harmful content.
May 2018 EU Parliament resolution on media pluralism. Additional proposals though not related to deepfakes, highly relevant to the discussion of deepfakes: full transparency in the use of algorithms, AI and automated decision-making with regard to the arbitrary blocking, filtering and removal of internet content (No 25). The importance of independent and impartial certified third-party fact-checking organisations (Nos 32 and 33). Obligations and instruments in relation to source verification (No 32). The enabling of users to report and flag potential disinformation (No 33). The displaying and labelling of disinformation revealed as such to stimulate public debate and prevent re-emergence of the content (No 33).
19 May 2021 EU Parliament resolution on AI in education, culture and the audiovisual sector. Forward looking proposal: raising awareness of the risks of deepfakes and improving literacy (No 90): addressing the increasing difficulty of detecting and labelling false and manipulated content by technological means (No 91); calling upon the Commission to introduce appropriate legal frameworks to govern the creation, production or distribution of deepfakes for malicious purpose (No 91); the promotion of the further development of detection capabilities (No 92); improving transparency with regard to what content is displayed to platform users and giving them greater freedom to decide whether and what information they want to receive (No 93).
Detection technology: facial recognition, facial feature analysis, temporal inconsistencies detection, visual artifacts detection, lack of authentic indicators.
Detection technology limits: unknown deepfake decrease the reliability of detector, quality and/or size compression/reduction, filters by default.
Technical prevention strategies: adversarial attacks n deepfake algorithms by exploiting vulnerabilities in computer vision algorithms; registering authentic content or (digitally) watermarking audio-visual materials - not really feasible; supporting detection initiatives.

13 Lecture 13

The Internet
Global network w/o central governing body. ICANN + standardization of core protocols. The origins of the Internet date back to research commissioned by the US Department of Defense 1960s to enable time sharing of computers. The WWW: allow access. Thousands of people and organizations own the internet. It consists of lots of different bits and pieces of ownership, The physical network of server, cables and routers that carry internet traffic between computer systems is referred to as the internet backbone. Arpanet originally backbone of the internet. whereas today large companies (ISPs) provide the Internet backbone (NTT, Verzon, AT&T, Comcast, etc.). In Italy: Telecom, Fastweb, Tiscali, Vodafone. Italian CSPs (local Data Center): Aruba, Amazon Web Services, BT, Fastweb, Tiscali, TIM.

The Cloud
Started evolving in the 1950s when companies like IBM implemented the concept of time sharing. Time sharing helped companies reduce costs by installing just one or two mainframe computers in their organizations and other terminals could gain access. User started to use infrastructure that was distant from them. Users felt sole users but instead they were sharing with others users. Virtualization of software, hardware, servers and storage evolved with the internet and use of the VPN (popular in 70s) and led to the development of the modern cloud computing.

How can we protect him or her?
European Convention on Human Rights and Fundamental Freedoms (1950)
Council of Europe Convention for the Protection of Individuals with regard to automatic processing of personal data n. 108 (1981)
Character of Fundamental Rights (2000)

Cybercrime Convention (2001)
Internet Charter (2015)
Let's never forget about the European fundamental rights when dealing with information technology.

Regulatory framework (basic)
EU Directive 95/46: abolished
e-Privacy Directive 2002/58/EC: concerning the processing of personal data and protection of privacy in the electronic communications sector applies to the processing of personal information relevant to the supply of electronic communication services available to the public and applies to the cloud service providers.
EU Regulation 2016/679: on the data protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46.
EU Regulation 2018/1807: relevant to the free circulation of non-personal data in EU.
EU Regulation 2016/1148 (so-called NIS Directive): concerning measures for a high common level of security of network and information systems across the Union and article 19 relevant to the designation by each Member State of a computer security incident response teams, Regulation 2019/881 representing the legal framework for ENISA (the European Union Agency for Cybersecurity) and on information communications technology cybersecurity certification. The regulation 2019/881 abolishes regulation 526/2013. Enisa Cloud Services Certification Scheme of December 2020; Agid Guidelines of September 12, 2020 effective as of 2021 for the document management of the PA. Proposals Digital Service Act (DSA) and Digital Market Act (DMA): new set of rules proposed by the EU Commission to regulate digital services. The DSA aims to set common but tailored obligations and accountability rules for providers of network infrastructure, hosting service providers, and in particular for online platform.

Children in the digital environment: the new OECD Recommendations
The OECD (Organisation for Economic Cooperation and Development) Recommendations were adopted in May 2021 with the aim inter alia to protect children aged 12-15 who own smartphones (50% more than in year 2011). An example of recommendation suggests to: *include separate guidelines for Digital Service Providers with four areas of action:*

1. *taking a child safety by design approach when designing or delivering services*
2. *ensuring effective information provision and transparency through clear, plain and age-appropriate language*
3. *establishing safeguards and taking precautions regarding children's privacy, data protection and the commercial use of such data*
4. *demonstrating governance and accountability*

The GDPR
Regualtion UE 2016/679 applies to the processing of personal data when a controller or a processor is established in the Union, regardless of whether the processing takes place in the Union. Furthermore, it applies to the processing of personal data of data subjects who are nio the Union by a controller of processor not established in the Union, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union
- the monitoring of their behaviour as far as such behaviour takes place within the Union.

Free floe of mixed data
Cloud Providers (CSP) process personal and non-personal information (mixed data). Regulation UE 2018/1807: aims to ensure the free flow of data, other than personal data, within the Union by laying down rules relating to data localisation requirements. The Regulation applies to the processing of electronic data:

- supplied as a service to users residing or having an establishment in the Union, regardless of whether the service provider is established in the Union
- carried out by a natural or legal person regarding or having an establishment in the Union for its own need

Where personal and non-personal data are inextricably linked the GDPR shall apply.

Cloud computing definition
The National Institute of Standards and Technology (NIST) of the US Department of Commerce. NIST promotes the US economy and public welfare by providing technical leadership of the nation's standard infrastructure. NIST is responsible for developing standards and guidelines for providing adequate information security for all agency operations and assets. Recommendations of the NIST are drafter for planners, program managers, technologists and providers of cloud service. Cloud computing is defined as *a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.* Cloud computing is made of technology that allows and makes it easier to use/or: Software, Hardware, process big data, store through Internet, Servers managed by third parties (CSP) by means of data centers located in various countries around the world. In Sum, an IT service model that provides resources by means of services provided by third parties that marks the legal transition from ownership to access.

Cloud Computing: service models
IaaS: describes a situation in which a provider leases a technological infrastructure. End users can rely on virtual remote servers that make it simple, effective and beneficial to replace the corporate IT systems at the company0s premises or to lease the infrastructure alongside the corporate system.
SaaS: a provider delivers, via the web, various application services and makes them available to the end users. These services are usually meant to replace conventional applications to be installed by users on their local systems, Users will outsource their data to the provider.
PaaS: a provider offers solutions for the advanced developing and hosting of applications. These services are usually addressed to market players' that use them to develop and host proprietary application to meet in-house requirements and/or provide services to third parties.

Cloud delivery models

1. *Private Cloud*: it is a model used by a single organization whereby resources and the tools are not shared between multiple users. The resources are delivered via a secure private network and not shared by any other channel. Data centers may be located on premise of offsite. The most important advantage of the private cloud is to be highly secure and customizable according to the unique business and security requirements of the organization that can purchase more and more resources according to its needs. The user does not share the services with others and can count on the support of the CSP by means of a private network. This model is the most expensive and mostly used in cases where sensitive data needs to be stored and the IT compliances are high. Usually, highly regulated industries like banks and public institutions, such as governments, use private clouds.

2. *Public Cloud*: here the infrastructure is owned by the CSPs and the IT services are delivered over the Internet. It is the most popular model of delivering cloud computing services because it is highly scalable and usually has lower costs. The CPS is responsible for developing, managing and maintaining the resources being shared between multiple users across the network. Public cloud is less secure and it should not be used for sensitive workloads. Users have minimum technical control and ensuring compliance can be an issues. The cost is low but can rise when the user reached certain levels. Lastly, the users transfer to the CPS not only the data bu also the relevant power to control such data.

3. *Hybrid Cloud*: is a mix of private and public cloud. It is getting more and more popular due to the growth of IoT over the past decade. I can be customized to include edge computing at scale. Edge computing brings computing closer to the IoT devices, which ensure that time and resources spent in communication with the data servers are decreased drastically. Hybrid solution is a choice based on multiple factors like: data security requirements, regulation ad compliance requirements, level of data control, applications used, business goals.

4. *Multi Cloud*: refers to a model in which several clouds of the same type (public or private) offered by different providers are used simultaneously to implement certain services or applications. unlike the Hybrid Cloud, which involves the creation of a single infrastructure that transparently uses different type of cloud, the Multi Cloud model is base on the use of different public or private cloud environments that are not interconnected. In the Hybrid Cloud is typically semi-automated and transparent to the user, whereas a Multi Cloud environment presents itself as a set of distinct computational resources that can potentially be integrated at application level.

the decision to select the appropriate cloud model should be taken o the basis of data security requirements, compliance requirements, business goals, applications used, etc.

Pros and Cons of cloud services
Benefits:

- Economic: purchase at marginal cost of sophisticated technologies (software and hardware), low maintenance and hardware management costs, reduction of human resources.
- Diversified solutions: storage of documents, outsourcing of electronic mail, increase memory capacity.
- Availability of data: at any time and location
- Security: updates and data savings (giving up periodic back-up), appropriate solutions for disaster and data recovery
- Space: for virtual processing systems

Disadvantages:

- loss of exclusive control over the data
- data transfer
- data subjects' rights
- vendor lock-in
- data portability

Cloud computing agreements

A Cloud Computing Agreement (CCA) is an agreement that sets out the main provision of cloud service between a Cloud Service Provider (CSP) and a cloud client (User). The CSPs provides the User with technology and online resources that enable the User process, store and transfer data. From a legal perspective, CCAs are not typical contracts having specific discipline in the Civil Code or in special laws. Italian scholars have categorized CCAs as agreements having mixed nature, embedding features of both licensing and outsourcing contracts. Generally speaking, the CCA falls within the outsourcing contractual framework with respect to: the scope of the contract, which provide for the outsourcing of services, i.e., the delegation of services to a third party provider, and the setting of specific standards of performance based on parameters capable of measuring the efficiency of the service provided and he reduction of costs. However, CCAs significantly depart from usual outsourcing agreements, insofar as: there is no consolidated relationship between the parties; services provided by the CSP are standardized and provided to a large number of users, soft negotiation of the relevant terms and conditions, short term and flexible termination rules, simplified fees based on frequency and duration of use.

The CCA is usually formed by the three different documents: general conditions of the service (service level agreement, SLA), policies governing the behavior of the parties, and GDPR. The general conditions set forth the main contractual terms of the CCA, e.g., duration, language, liability limitations, indemnities, applicable law and jurisdiction. The GDPR section takes care of the provisions on data flows connected with the cloud service, including category of, data protection and security, national and cross-border transfer of data, portability, etc. In particular, the GDPR provides for the protection of the personal data and defines, inter alia, the relationship between the parties (controller, processor, sub-processor) pursuant to article 28 of the GDPR and the regime applicable to data transfers.

Italian DPA framework for choosing the CSP

1. *Reliability*: users should establish how experienced, skilled ad reliable their provider is before moving the data to the cloud. Assess the legal safeguards afforded to ensure data confidentiality and to what extent the provider accepts to be liable for damages as set out in the terms of service especially i the case of security breaches and/or service breakdowns.

2. Enhanced data portability: preference should be given to services that rely on open format and standards to facilitate migration between cloud systems managed by different providers. This allows users to switch provider without incurring costs and, most importantly, reduce the risk that a provider may change the terms cloud service contract unilaterally to the client's detriment by taking advantage of his stronger negotiating power.

3. *Availability of data*: continuity safeguards and confidentiality may impact on both the cloud client and the data subjects in the case i which the cloud delivers services to third parties; for instance, in the health care and judicial processing, the loss and/or unavailability of such highly sensitive data will be harmful for both the data subjects and controllers.

4. *Identify the data to be moved*: information protected by industrial secrecy rules as well as sensitive data relating to health, ethnic origin, political opinions or membership of trade unions etc. - should be carefully transferred to the cloud, considering the risk of loss or unlawful access especially if a public cloud is involved in the choice of the model

5. *Keep control*: understand which entity is holding and controlling the data by knowing who does exactly what among the entities involve in providing the services.

6. *Know the location*: the location implies whether data will be moved to, and processed by, servers base in Italy, the EU, or in a non EU-country and this information is essential top determine the jurisdiction sand applicable law in case of disputes between users and service providers; above all, is necessary to heck the protection afforded to the data. Transferring data to countries where no adequate safeguards are in place in terms of security and confidentiality might make the processing of personal data unlawful and cause irreparable harm.
7. *Terms of service*: specific reference is made to the rights and duties applying to loss or unauthorized disclore of data kept on the cloud as well as for the mechanisms to withdraw from the service and shift to a new provider. Clear cut quality standards, penalties so that the provider is made liable for non-performance and in cases of data loss, unauthorized access, unavailability due to malfunctioning. Furthermore, it is necessary to assess whether third parties are involved in delivering cloud base services and/or data processing.
8. *Data retention*: all data on the cloud must kept in compliance with the purposes and arrangements agreed upfront. Deadlines for data cancellation should be provided in the contract if not provided by the law.
9. *Demand security measures*: performance should be given to providers that rely on secure data storage and transmission mechanisms based on encryption especially if highly sensitive information is processed
10. *Train staff*: training of client's and provider's staff is required to reduce risks of unauthorised access, data loss, and unlawful processing operations. Data protection may easily fail if staff make mistakes.
11. *Personal processing*: although the Italian Privacy Code does not apply to an individual who processes personal data for personal purposes, individuals are still expected to keep personal data with due care to prevent that any loss may harm other individuals. New mobile technology devices like smartphones and tablets have considerable memory capacity and often rely on unprotected cloud based services that are used both for private and professional purposes increasing therefore the risk of losing control over one's personal data.

Following the above listed rules will allow you to be accountable.

Cloud checklist - accountability
Analyize your organization (vision of the management)
Evaluate the actual data governance
Idneitfy the level of compliance and the level of reputation desired by the organization
Consider and identify the budget
Map and identify the data to be inserted in the cloud (categories of data, scope, storage)
Evaluate if the transfer of the data is necessary
Evaluate the segregation and encryption of the data
Identify the cloud model to be implemented (private, public, hybrid, multi) and the model of service (IAAS, PAAS, SAAS)
Identify a trusted cloud provider considering inter alia, the offer or the provider with respect to the portability, business continuity, security measures, reputation, data storage, contractual clauses, warranties, localisation of the EU and non-EU service providers
Define the contractual relationship with the provider (processor and sub-processor)

International aspects of the cloud

1. Transfer of personal data to third countries

(a) *the adequacy requirement*: entering the cloud environment is likely to imply the transfer of data to data centers located elsewhere. Therefore, using an international cloud infrastructure requires to assess if data will be transferred to a third country and where, unless the cloud provider clearly states in its terms of service that the data will not be processed outside of the EU. Pursuant to Article 45, paragraph 3, of the GDPR, data transfers towards countries outside of the EU or towards an international organization may take place only if the Commission has decided that the third country ensures an adequate level of protection. When assessing the adequacy, the Commission shall take account of inter alia:

    - the respect of the *human rights* and *fundamental freedoms*, to general and sectoral legislation, public security, defence, criminal law and the access of public authorities to personal data, *data protection rules*, including rules for the onward transfer of personal data to another third country or international organization, case law, *data subjects' rights and remedies.*
    - the existence of a *supervisory authorities* in the third country
    - the *international commitments* the third country or international organization has entered into

    the adequacy of the level of protection shall be re-assessed by the Commission through a periodic mechanism of review, at least every *four years* and shall take into account all relevant developments in the third country or international organization that could affect the functioning of decisions it has adopted. If *an adequate level of protection is no longer ensured the Commission shall repeal, amend or suspend the decision.* The Commission shall publish in the *Official Journal of the EU* and on its *website* a list of the third countries, territories and specified sectors within a third country and international organization for which it has decided that an adequate level of protection is or is no longer ensured.

(b) *transfers subject to appropriate safeguards (article 46 of the GDPR)*: in the absence of a decision pursuant to Art. 45 (3), a controller or processor may transfer personal data to a third country or an international organization in presence of:

    - a legally binding and enforceable instrument between public authorities or bodies
    - *binding corporate rules* in accordance with Art. 47
    - *standard data protection clauses* adopted by the *Commission* in accordance with the examination procedure referred to in Art. 93 (2)
    - *standard data protection clauses* adopted by a *supervisory authority* and approved by the *Commission* pursuant to the examination procedure referred to in Art. 93 (2)
    - and approved *code of conduct and appropriate safeguards* including *data subjects' rights*
    - an approved *certification mechanism* pursuant to Art. 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including data subjects' rights

    Please note that subjects to the authorisation from the competent supervisory authority, the appropriate safeguards may also be provided by:

    - *contractual clauses* between the *controller or processor and the controller, processor* or the recipient of the personal data in the third country or international organization
    - provisions to be inserted into *administrative arrangements* between *public authorities* or bodies which include enforceable and effective data subjects rights

(c) *Safe Harbour, Privacy Shield, SCCs: decisions of ECJ*: in 2015 the Schrems judgment of the Court of Justice of the EU declared invalid the European Commission's decision on a *Safe Harbour* for EU-US data transfers. The European Commission negotiated a new arrangement for EU-US data transfer, known as *Privacy Shield* that was adopted in 2016. In 2020, the Court of Justice of the EU issued its judgment known as the Schrems II case the ECJ invalidated the Privacy Shield *adequacy decision.* In the Schrems Case, *Facebook Ireland* transferred data to the US parent company, namely to servers of *Facebook Inc*, located in the US, on the basis of SCCs. According to the ECJ, the law of the US do not satisfy the adequacy set forth by Art. 45 of the GDPR. US surveillance programs interfere with fundamental rights to privacy provided by Art. 7, 8, 47 of the Charter of Fundamental Rights of the EU. US surveillance programs are not limited to what is *strictly necessary* and do not sufficiently limit the powers conferred upon US authorities and lack actionable rights for EU data subjects against US authorities. Data controllers that seek to transfer data based on SCCs, must ensure that the data subject is afforded a level of protection *essentially equivalent* to that guaranteed by the GDPR, if necessary, with *additional measures* that compensate the lack of protection afforded by the third country legal system.

(d) *EDPB recommendations on measures that supplement transfer tools*: the EDPB has adopted a set of recommendations that supplement transfer tools to ensure compliance with the EU level of protection of personal data such as:

- *know your transfer (this is for the data exporter/controller to know)*: mapping transfers of personal data is the first step to fulfill accountability obligations. It may be a complex exercise to map all transfers especially where there are multiple, regular transfers with third countries using a series of processors and sub-processors. Verify whether the transfer is complaint with the principle of data minimisation pursuant to Art. 5 (1) of the GDPR: the data to be transferred must be adequate, relevant and limited to what is necessary in relation the purposes for which it is transferred to an processed in the third country. Inform data subjects about the transfer pursuant to Art 13, 14 of the GDPR.
- *identify the data transfer tools and verify whether*: the destination, the level of protection and the existence of a valid adequacy decision; the adequacy decision is/are still valid and have not been revoked or invalidated; adequacy decisions may cover a country as a whole or be limited to a part of it; adequacy decisions may cover all data transfers to a country or be limited to some types of transfers; an adequacy decision allows data to flow from the EU to a third country without any Art. 46 GDPR transfer tool being necessary. The essentially equivalent requirements are present in all places where the data will be processed; remote access from a third party country and/or storage in a cloud situated outside the EU, is also a transfer of data. Therefore, if you are using an international cloud infrastructure you must assess if your data will be transferred to third countries and where, unless the cloud provider clearly states in its contract that the data will not be processed at all in the their countries
- *verify if the domestic legislation* of the country which data is transferred may have an impact on the effectiveness of the appropriate safeguards of the transfer tools chosen
- *adopt supplementary measures* necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence; suspend or interrupt the transfer if no measure can ensure an essentially equivalent level of protection
- *consult the DPA* if necessary to obtain clarifications on any procedural steps to undertake

- *continuous monitoring* on the adequacy of the measures adopted

Supplementary measures shall be determined on a case-by-case basis. If no measure will be identified the transfer of the data shall be suspended. The assessment activities by the controller must be recorded according to the principle of accountability.

(e) *Standard contractual clauses for data transfers*: pursuant to the GDPR, contractual clauses ensuring appropriate data protection safeguards can be used as a ground for data transfers from the EU to third countries. This includes model contract clauses, the so-called standard contractual clauses (SCCs), that have been pre-approved by the European Commission. On 4 June 2001, the Commission issued modernised standard contractual clauses under the GDPR for data transfers from controllers to processor sin the Eu to controllers or processors established outside the EU. These modernised SCCs replace the 3 sets of SCCs that were adopted under the previous Data Protection Directive 95/46. Since September 27, 2021, it is no longer possible to conclude contracts incorporating these earlier sets of SCCs. Until December 27, 2022 controllers and processors can continue to rely on those earlier SCCs for contracts that were concluded before September 27, 2001 provided that the processing operations that are the subject matter of the contract remain unchanged.

The controller or processor transferring data to a third country (data exporter) and the controller or processor receiving personal data (data importer) can include the SCCs in a wider contract provided that they do not contradict the SCCs or prejudice the fundamental rights of data subjects. The data importer should notify the data exporter if, after agreeing to the SCCs it has reasons to believe that it is not able to comply with the SCCs. The data exporter that receives such notification should identify appropriate safeguards measures such as technical and organisational measures to ensure security and confidentiality. The data exporter should suspend the transfer if it considers that no appropriate safeguards can be ensured or if so instructed by the competent supervisory authority.

2. *Issues relevant to foreign intelligence, surveillance and security and the requests by public authorities.*

Foreign intelligence, surveillance and security bring us back to the fundamental rights of individuals. In the US, pursuant to section 702 of the Foreign Intelligence Surveillance Act (FISA) and of the Executive Order (EO), *CSPs are required to provide public authorities (NSA, FBI, CIA) with personal information transferred to the US of identified individuals made part of a security program.* Public authorities have full discretion and no remedies are afforded to foreign data subjects. However, massive surveillance is unlawful pursuant to the Charter of Fundamental Rights and to the GDPR. In this respect, the EDPB states *as regards to possible interference with fundamental rights under EU law, the obligation imposed on providers of electronic communications service to withhold traffic data for the purpose of making it available, if necessary, to the competent national authorities, raises issues relating to the compatibility with Art. 7, 8 after Charter. Moreover, access to the data by a public authority constitutes a further interference, according to settled case-law. In order to find an interference, it does not matter whether the information in question relating to private life is sensitive or whether the person concerned have been inconvenienced in any way on account of that interference.* Some CSP providers take responsibility to forward any request of access directly to the user, refuse to respond to illegitimate request etc. Data centers located in the EU controlled by US corporations could be a solution further clarifications are issued.

(a) *the Microsoft case and the relevant EU, UK, US scholars*: Microsoft Ireland vs US Supreme Court. Stored Communications Act (1986), Cloud Act (2018).

If servers are located in the EU and providers are established in the EU, US government may request and obtain personal data of EU Cloud Users from CSPs (such as Google, Microsoft, Amazon) because the latter are subject to the US jurisdiction; same for EU providers with subsidiaries in the US. Clarifications are necessary in order to explain, inter alia: (i) the territorial scope of the Cloud Act to European providers operating in the US, and (ii) the meaning of control of US subsidiaries established in the EU.

(b) *the European Essential Guarantees and the relevant case law (CJEU, ECHR)*: the EDPB adopted the so called *European essential guarantees* relevant to the surveillance measures. The European essential guarantees are based on the jurisprudence of the Court of Justice of the European Union (CJEU) related to art. 7, 8, 47 of the Charter of Fundamental Rights of the EU and on the jurisprudence of the European Convention on Human Rights (ECHR) related to art. 8. The EDPB found that the *judicial requirements to justify limitations* to the protection of personal data and to the respect of the private life recognised by the Charter of fundamental rights can be summarized in *four* essential guarantees:

   i. processing should be based on clear, precise and accessible rules
   ii. necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated
   iii. an independent oversight mechanism should exist
   iv. effective remedies need to be available to the individual

   The jurisprudence of the CJEU and ECHR.

(c) *Transfers or disclosures not authorised by Union law*: is the extraterritoriality of the Cloud Act compliant with article 48 of the GDPR?
   Art. 48 of the GDPR: *any judgement of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be enforceable if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.*
   Consideranda 115 of the GDPR: *the extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may prevent the attainment of the protection of natural persons ensured in the Union by the GDPR.*

(d) *Derogation for specific situations*: pursuant to art. 49 of the GDPR, in the absence of an adequate pursuant to Art. 45(3), or of appropriate safeguards pursuant to Art. 46, transfer of personal data shall take place only in presence of specific conditions i.e., consent of the data subject or when the transfer is necessary for the performance of a contract between the data subject and the controller, a vital interest of the subject, etc.
   International cooperation mechanism ex art. 50 of the GDPR facilitate the effective enforcement of legislation for the protection of personal data by means of mutual assistance though information exchange.

14 Lecture 14

The technical, legal and operational management of a data breach

Characteristics of a data breach
Silent
Extended
Difficult to evaluate
Hard to control the damage

Difficult to calculate economic impact

Definition
Article 4 of the European Data Protection Regulation defines data breaches as a *personal data breach, i.e., a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*

Possible consequences
Recital 85: *A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.*

Obligations related to data breaches
Duty to notify the Supervisory Authority within 72 hours under Art. 33 of the GDPR. Duty to notify the data subjects when the personal data breach is likely to present a high risk to the rights and freedoms of natural persons.

When does the time limit or notification begin?
Art. 29 WP considers that the time for making the notification starts from when the data controller has a reasonable level of certainty that the security incident that occurred has compromised personal data. While recognizing that each data breach may have unique characteristics, the WP stresses the importance of having a procedure in place to investigate incidents and determine whether personal data have been accessed or modified or damaged.

Content of the notification
Nature of the personal data breach, including the categories and number of data subjects and the type and number of record involved. Contact details of the data protection officer. Description of the likely consequences of the violation. Description of the measures taken or to be taken to remedy the breach and counteract its negative affects.

When to notify the personal data concerned?
Art. 34 (Notification of a personal data breach to the data subject).

1. *When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.*

2. *The communication to the data subject referred to in paragraph 1 of this Art. shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Art. 33(3).*

3. *The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:*

   (a) *the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;*

   (b) *the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;*

(c) *it would involve disproportionate effort. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.*

4. *If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.*

High risk
When assessing the risk to individuals from a breach, the controller should consider the specific circumstances, including the severity of the potential impact and the likelihood f it occurring. In making this assessment, the WP29 recommends considering the following criteria: type of violation, nature, sensitivity and volume of personal data, ease of identification of individual, severity of consequences for individuals, special characteristics of the person concerned, special characteristic of the data controller, number of individuals involved.

When notification to the person concerned is not required
When the holder has implemented appropriate technical and organisational measures. Where the holder has subsequently taken measures to prevent the occurrence of high risks to the rights and freedoms of data subjects. Where such communication would require disproportionate effort, it may be replaced by a public communication.

Detection
Establish an obligation to notify suspicious behaviour to authorising officers and controllers. Equip yourself with alert systems for security components (antivirus, firewall, etc.). Program the signaling of anomalies related to network traffic, the use of server memory or the sudden saturation of hard disk space. Evaluate the adoption of an Intrusion Detection System (IDS). Evaluate the adoption of a Data Loss Prevention (DLP) system. Equip yourself with a log analysis tool.

Identification
At the identification stage, you must qualify the security breach as a generic breach, which may not have affected personal data, or a breach that did affect personal data. From this point of view, identifying contact persons who can ensure the continuation of the investigation and establishing a rule of cooperation with respect to the investigation team can be a good policy.

Classification
Art. 29 WP, in its Opinion 3/2014, identified different types of data breaches:

- *Confidentiality breach*: where there is an unauthorized or accidental disclosure of or access to personal data
- *Availability breach*: where there is an unauthorized or accidental loss or destruction of personal data
- *Integrity breach*: in the case of unauthorized or accidental modification of personal data

how to measure the impact of a cyber incident for operators of essential service
Art. 14 paragraph 4 of the NIS Directive.
Number of users affected by the computer incident.
Duration.
Geographical extension.

Accountability
Art. 33(5). *The controller shall document any personal data breach, compromising the facts relating to the personal data breaches, its effects and the remedial action taken. Such documentation shall enable the supervisory authority to verify compliance with this Article.*

Data breach response plan in 8 steps:

1. *Building an internal crisis unit*: Data controller
   DPO
   IT
   Legal
   Compliance
   Communication
   Customer service
   Management
   Data Processor

2. *Assessing the breach*: have a repository with all relevant and up-to-date documents in it. It is important to have a history of data breaches in order to evaluate decisions made under similar conditions. IT support is essential.

3. *Be collaborative*: data breaches 'break the news'. Depending on how the data breach occurred, a lawsuit may also be helpful in breaking the causal link. Having an already known vendor for any possible digital forensics activity can be very helpful. Decision should no be taken 'on an emergency basis' or under the pressure of inspection activity.

4. *Periodically test your data breach plan*
   Verify the soundness of your data breach management plan against an evolving crisis scenario. Check at the end each phase of the scenario the problems that emerged and possible solutions

5. *Provide additional training*: based on the result of step 4, study an additional training activity for the team

6. *Being accountable also in prevention*: document any activities that have been done to prepare for a possible data breach. Remember that a data breach is only a matter of 'when' and not 'if'

7. *Provide a budget chapter for data breach prevention and management*: incorporating the data breach into an owner's economic planning is, on the one hand, an element of accountability and, on the other hand, allows for an action that is compatible with the timeframe indicated by the GDPR.

DPO and data breach
To act as a point of contact for data subjects on any issues related to the processing of their data;
Act as a point of contact with the Supervisor;
Strucutre a data breach management plan within the organization;
The DPO may have relationships with the Chief Information Security Officer (CISO) members of the Incident Response Team (IRT), ICT Manager, legal department, communication experts, top management, audit compliance risk management functions, OdV 231, business owners.

Consequences for breach of Art. 33 and 44
Monetary administrative sanction of up to 10, 000, 000 euro or up to 2% of a company's total annual global turnover;
Imposition of a pecuniary administrative sanction, in association with a remedy pursuant

to Art 58(2) GDPR.

Common mistakes on the Data Controller side
Slow decision making. lack of clear contractual arrangements to get the information from the manager. Search for 'lighting rod'. Tendency to minimise in order to avoid notification.

Common mistakes on the Data Processor side
Slowness in providing information to the holder. Unprepared o handle a data breach. Tendency to protect one's own activity and business. Lack of personnel specialized in data protection.

Common mistakes on the DPO side
Failure to respect the obligation of confidentiality. Remember that you must give an opinion, not manage the data breach. Focus only on filling out the form and not on remediation. Tendency not to instruct 'post mortem' audit and verification activities.