* DATA IS NOT OWNED; data pertain to your identity. They are not owned because they cannot be sold.

Information and technology law course

LECTURE 10 + 12 – 24 AND 31 OCTOBER 2024

FEDERICA CASAROSA – 2024/2025

Data protection = more connected with control over the flow of data. Control where data go, who can use

Privacy can be overlap or stay within the same bounds of data protection.

Privacy: non interference with data for different entities. Data prot. is about the ability to make data flow but control it.

There can be conflicts: ex: when you have logging of activities of a user
For the security perspective you might want to know what is going on in a system, but that might violate the privacy of a user.

Conflict between security and privacy

Values protected within cybersecurity

identification and implementation of measures and techniques for the protection of information from

- unauthorized access,
- unauthorized use,
- unauthorized modification,
- unauthorized destruction,
- unauthorized disclosure or disruption

You don't want problems w/ CIA, so you want to avoid (1)

Values protected within cybersecurity

Security

Privacy

Fairness

Accountability

Security is one of the aspects. There are other elements to be taken into account. Security is avoiding problems, but... If I'm adopting a measure to control who access the document, it is a way to protect privacy and security (only access to auth.). The measures aren't necessarily conflicting and that's the idea. Ex. nurse has access to only parts of data of a patient that are relevant for the moment needed.

Then, fairness: non-discrimination; want to make sure that the use of data doesn't discriminate others; for ex. In case of adoptions, mothers can leave children and decide to be anonymous. There's a balance of newborn childs and database of mothers who gotta birth. There's the possibility to stay anonymous (not for the state) but for kind (be 25 years) and other people. We are protecting the right to remain anonymous (secrecy) (We want to avoid influence to avoid discrimination). Or the fact that you are coming from a different country is not a discriminatory factor.

Accountability: being responsible for what you did. I need to know who choose the measures, why they did that exc. Ex: company is accountable for risk analysis.

Security

Security is the state of being free from danger or threat

- Safety / security
  - safety is protection against accidental or unintentional danger whereas security is protection against intended harm
- absence of danger or threat

Privacy

informational privacy is about what information about a person is (not) known to, or shared with, others

Distinction between

- confidentiality or secrecy of data and
- control over what data is shared with whom

Fairness

Cybersecurity threats and measures impact differently on people so you want equality and non discr.

Connected issues of equality, justice, non-discrimination and democracy

Accountability

Who does what, why and for what purpose

Connected issues of transparency, openness and explainability

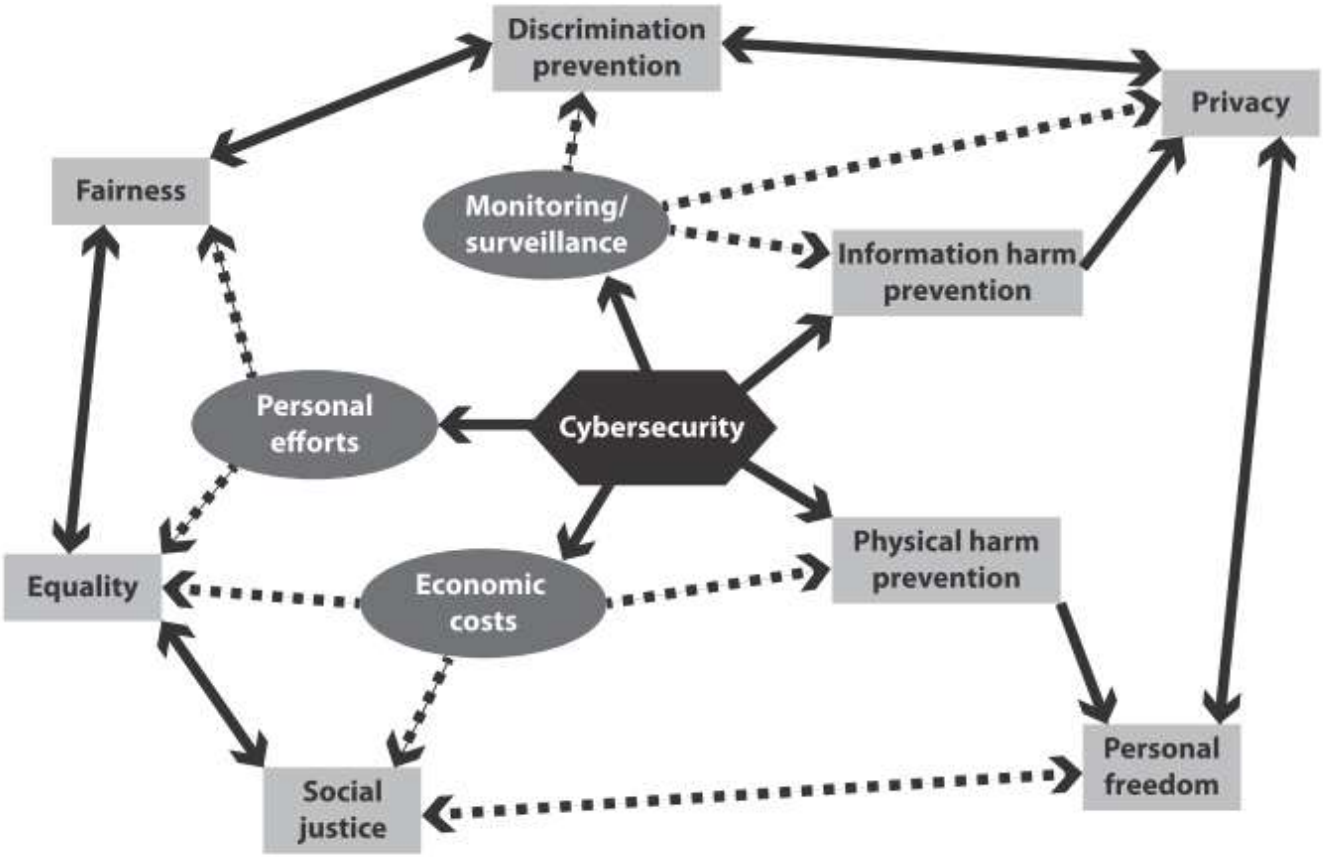
↳ doesn't mean clarifying the exact measure you are taking, it's a matter of security.

Two possible scenarios:

- situations in which someone (allegedly) harms someone else, or infringes on the rights of that person
- situations in which there is a power imbalance* between two agents and in which the more powerful is in the position to introduce rules or measures that may harm the less powerful ones

↳ need to make sure that someone doing something can justify the work.

*EU has to justify their implementation of NIS, NIS 2


Discrimination prevention
Privacy
Fairness
Monitoring/ surveillance
Information harm prevention
Personal efforts
Cybersecurity
Physical harm prevention
Equality
Economic costs
Social justice
Personal freedom

Privacy v security

Sometimes security is attained at the cost of privacy

Sometimes security helps to achieve privacy

Privacy requires some degree of cybersecurity

Sometimes, privacy is attained at the cost of security

Sometimes, privacy contributes to security

GDPR – Data protection

GDPR's a regulation: document immediately applicable in the MS. DP was repealing a directive in '95. A little old directive, yeah?

Was looking more about privacy than data protection, not that much controlling the flow of data. Now we have reg. Problems: directive was not sufficiently harmonized MS. One was old and not efficient anymore.

Since 2010 there was a lot of discussion. Final doc was a compromise, because regulation is doing something but not that much. The regulation was trying to update the legislation and establish a common ground for data protection.

In the DIR was left to each member state to enforce measures and impose fines and sanctions.

In Italy directive was implemented with a law and other activities resulting in Codice...

What happened when the regulation arrived? We have a lot of debated parts of the document.

The reg. became enforceable in 2018.

The decreto (2) was a way to put patches needed to adapt to the regulation. This because there were also open clauses that would need a MS to adapt there legislation to it.

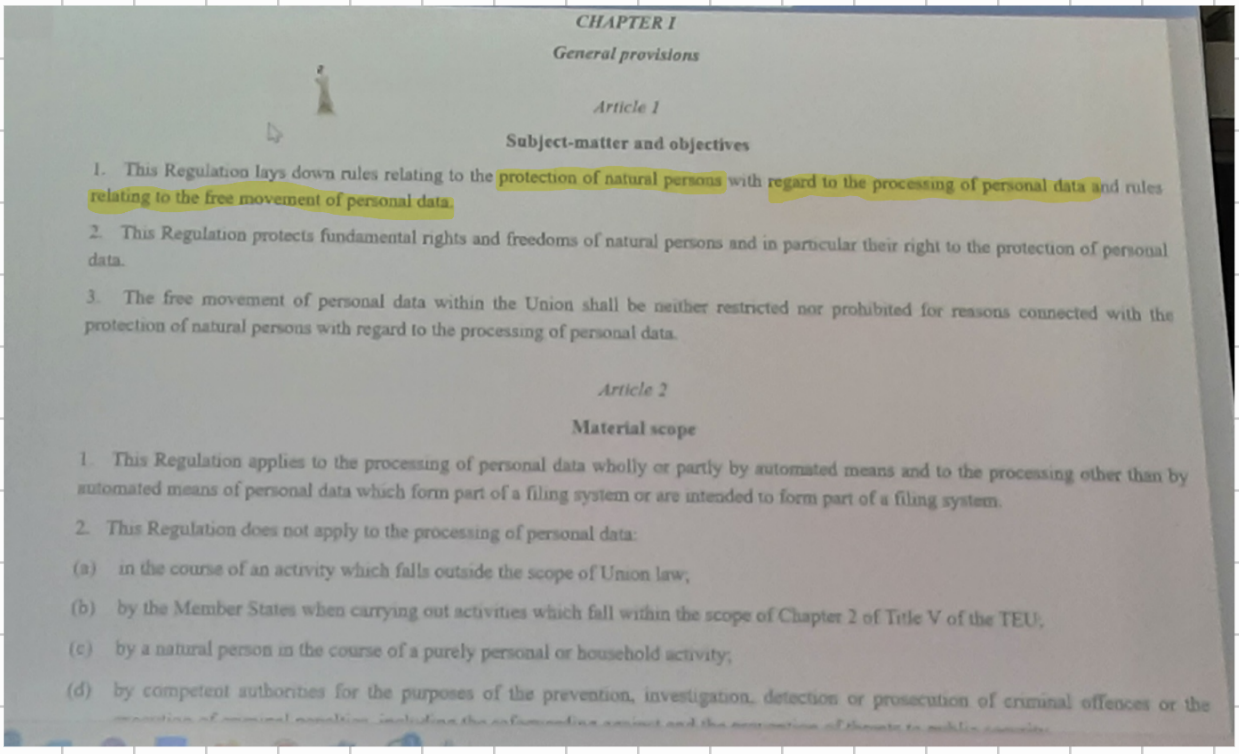
Legal sources

Regulation (EU) 2016/679 of the European Parliament and 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, OJ L 119, 04.05.2016, pp. 1-88.

Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196),

- Decreto legislativo 10 agosto 2018, n. 101.

Article 16 of TFEU is on personal data protection



CHAPTER I

General provisions

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.

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 of a filing system.

2. This Regulation does not apply to the processing of personal data:

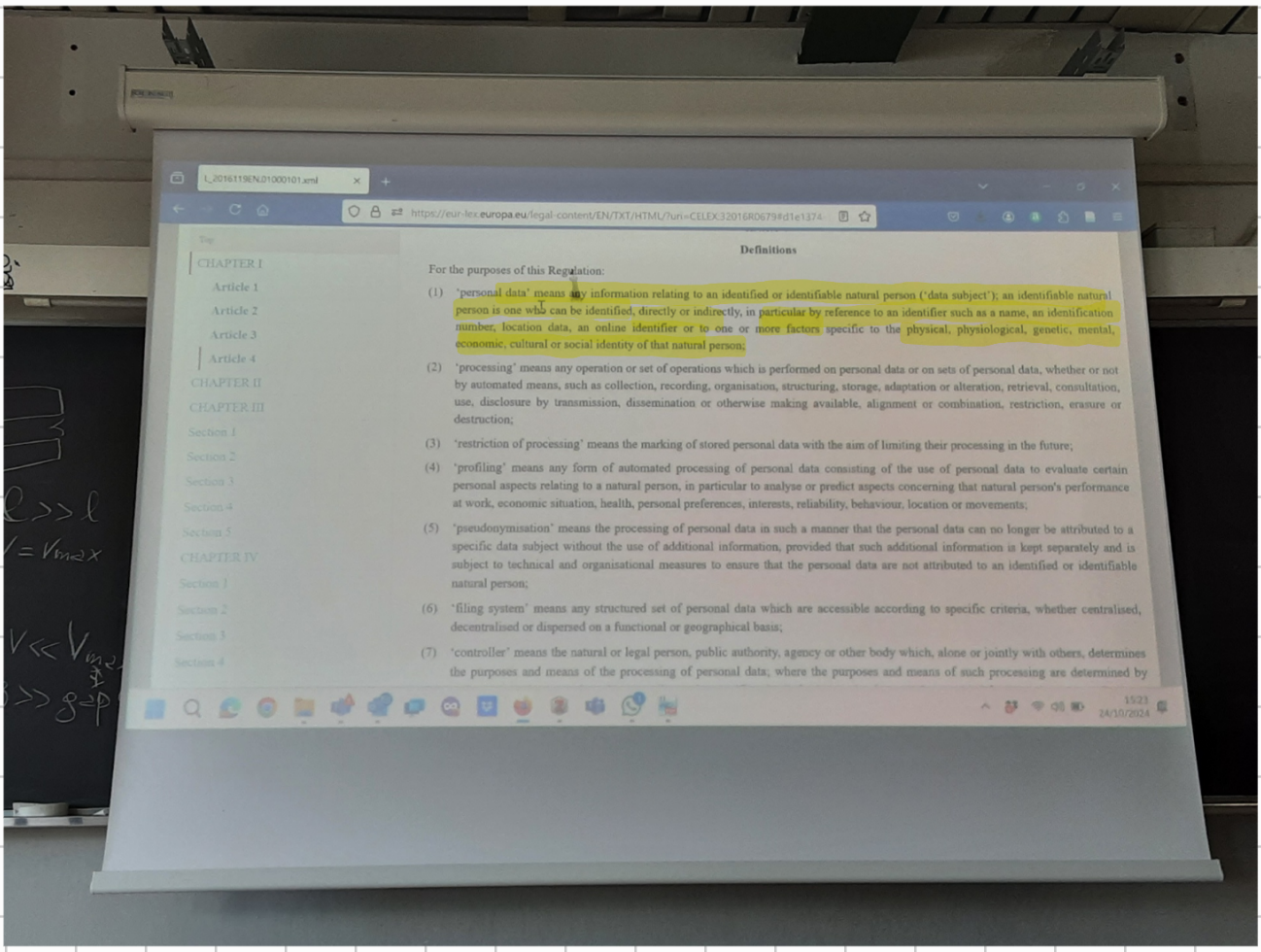
(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

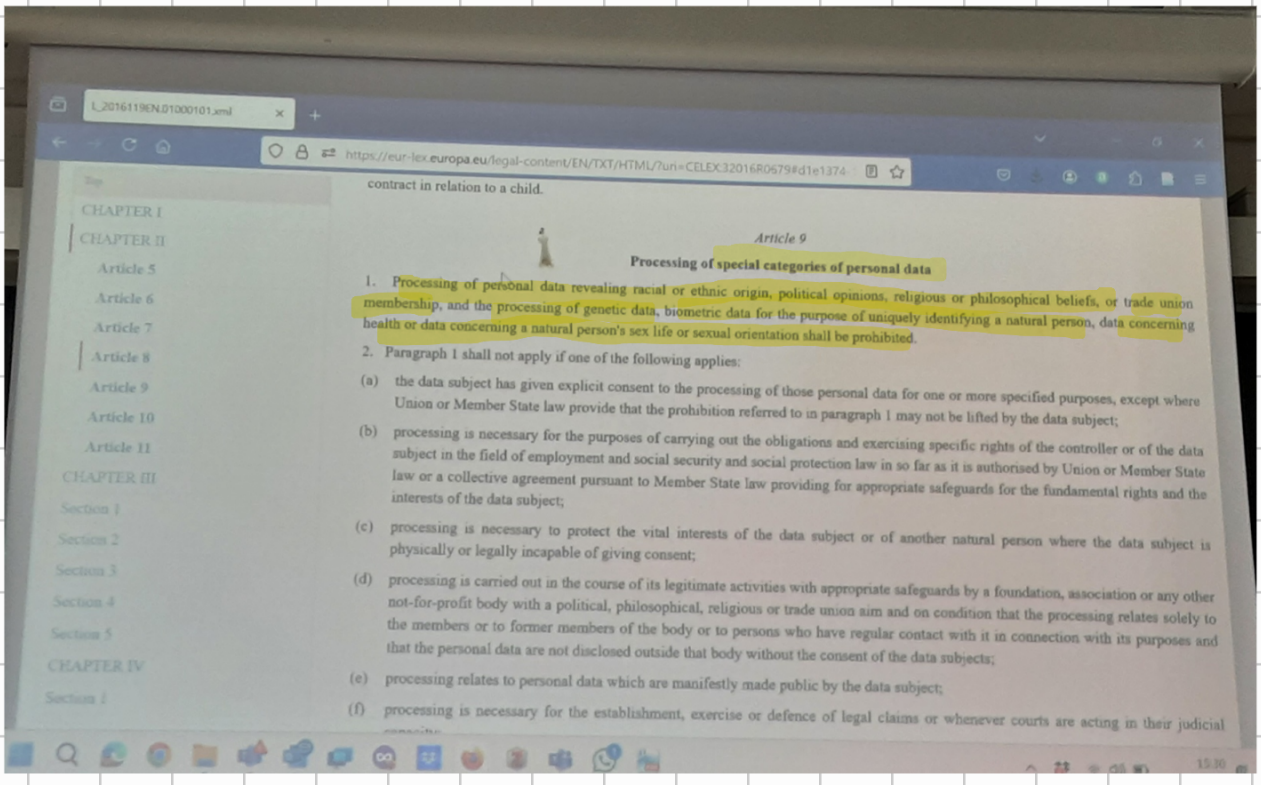
(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the

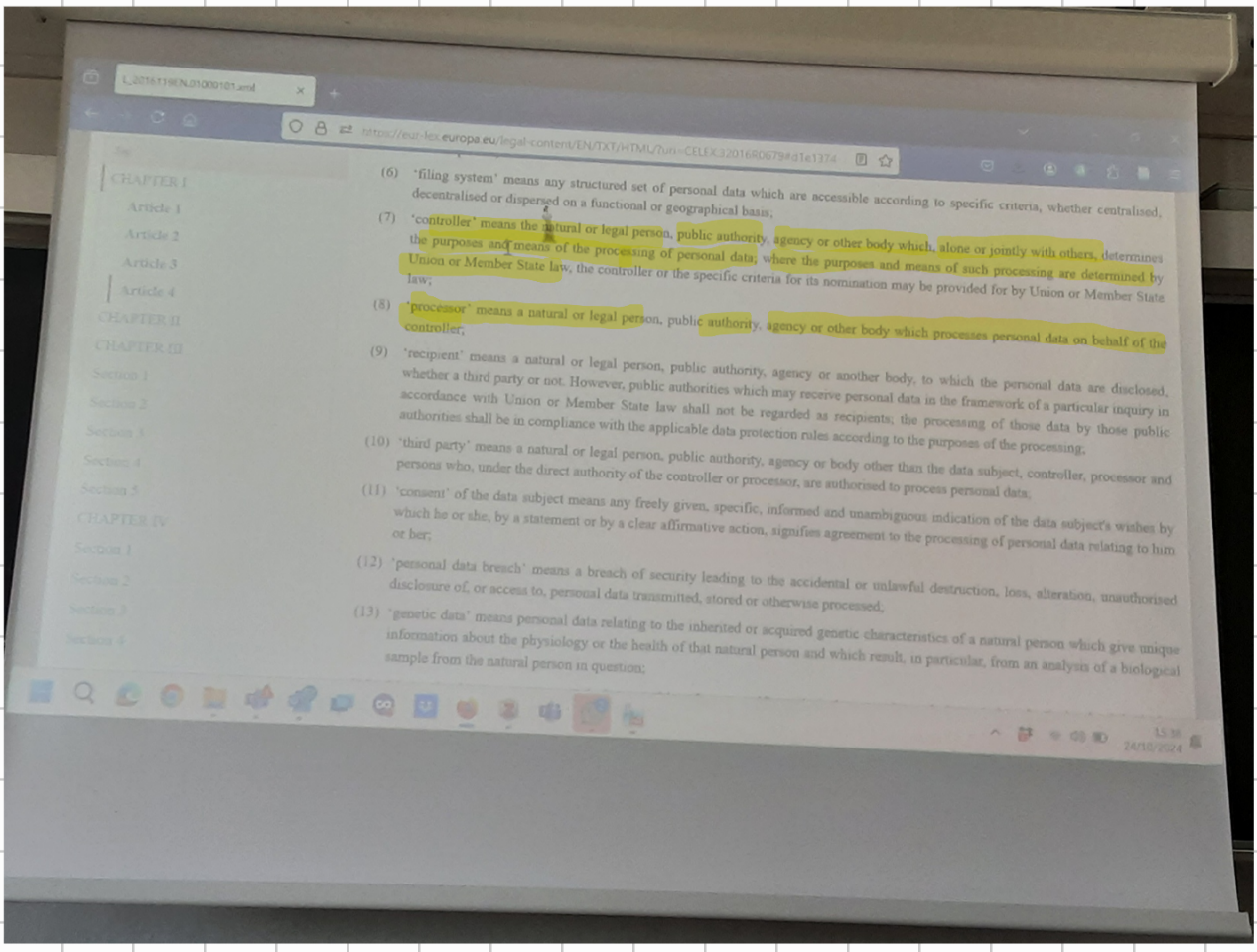
(1) Two aims: 1, I want to make sure that the natural person (personal data only refer to individual). Individual is POR. And, we want to make sure that the system allows personal data to flow safely.



(1) Whatever is related to you is personal data. Whatever your preferences etc. There are personal data a bit more problematic



Article 9 says: personal data is huge, but there's some data that is more critical. Almost impossible not to process them though. So there are exceptions:
General personal data VS SENSITIVE data (special categories of personal data)
They are special because can be used for discrimination. You have to be aware of continually to process them. Snap back: Who is the data controller?



As a data controller I am the one that decides which data I want, for what purpose exc. They are the ones that process data.
The purpose might be important. It has to be justifiable.
The controller decides which kind of info and how it has to be collected.
(2) The processor is the one that processes the data on behalf of the controller.
Contr. and Proc. work together. They can be the same or an employee or a part of the org.

'Data Subject', the one whose data will be collected.
JMP 1.5

Personal data – definition

Personal data are defined as information that identifies or makes identifiable, directly or indirectly, a natural person and that can provide information on their characteristics, habits, lifestyle, personal relationships, health status, economic situation, etc.

- Data allowing direct identification and data allowing indirect identification
- Sensitive data and judicial data
- New data?
  - Data relating to electronic communications, geolocation data

Actors – definitions

Data subject is the natural person to whom the personal data relate (Article 4(1)(1) GDPR)

Data Controller is the natural person, public authority, company, public or private body, association, etc., who takes the decisions on the purposes and means of processing (Article 4(1)(7) GDPR)

Data processor is the natural or legal person whom the controller requires to perform specific and defined tasks of management and control on its behalf of the processing of data (Article 4(1)(8), GDPR)

Scope of application of GDPR

Regulation (EU) 2016/679 governs the processing of personal data

(1) irrespective of whether or not it is carried out in the EU,

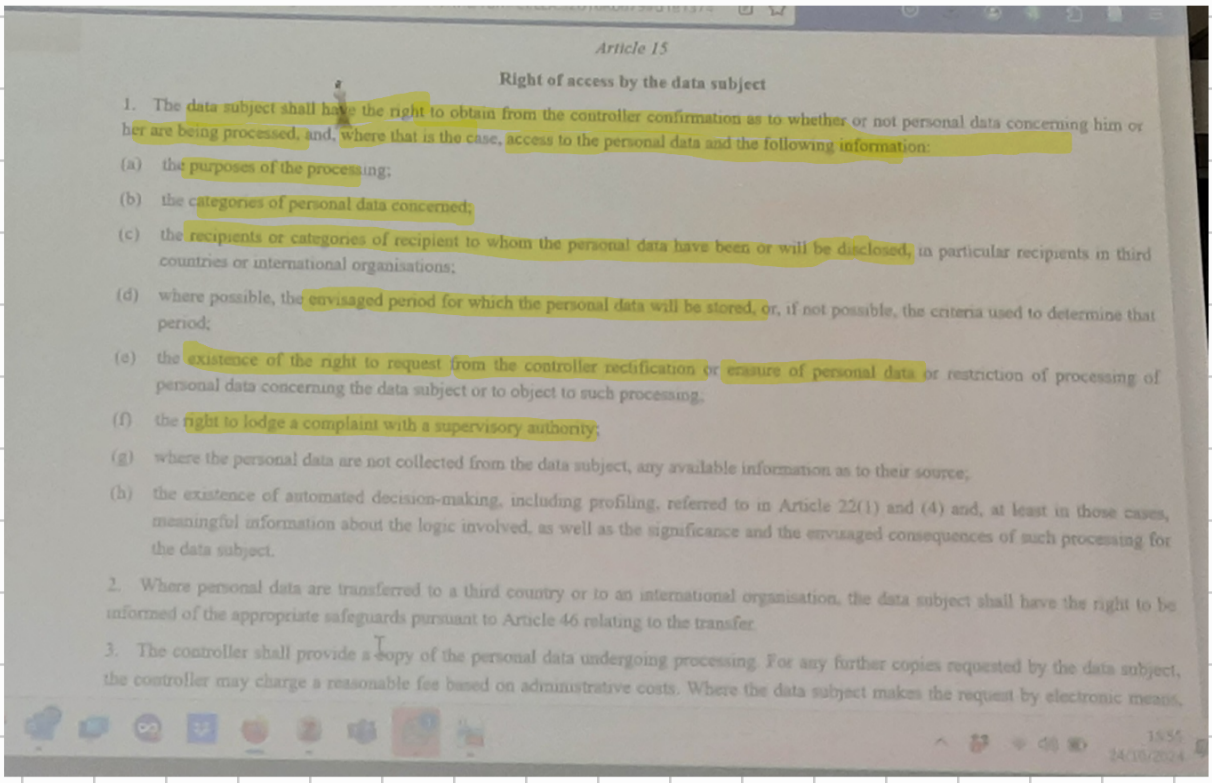
- either when carried out by data controllers or data processors established in the EU or in a place subject to the law of an EU Member State by virtue of public international law,
- or when the controller or processor is not established in the European Union but the processing activities concern
  - the offering of goods or the provision of services to the said data subjects in the European Union, irrespective of whether payment by the data subject is compulsory (2)
  - the monitoring of their behaviour to the extent that this behaviour takes place within the European Union.

Even though we are living in the EU, we can impose external companies to comply. This is because of the extraterritorial application of GDPR.
Huge steps in the protection was: in article 3 :(1)
(2) My data should be treated according to the GDPR. It's a way to cover all the US companies exploiting EU citizens.
Look at Cambridge Analytics that collected data of users. No evidence of proof but allegedly this was used to push electors in one or the other direction for elections.

Rights of the data subject - 1

Right to access personal data

- The data subject has the right to ask the data controller
  - Whether his/her personal data have been processed, and if so
  - to obtain a copy of such data
  - to be informed about:
    - (a) the purposes of the processing; (b) the categories of personal data processed; (c) the recipients of the data; (d) the storage period of the personal data; (e) the origin of the personal data processed; (f) the identification details of the person processing the data (data controller, data processor, designated representative in the territory of the Italian State, recipients); (g) the existence of an automated decision-making process, including profiling; (h) the rights provided for by the Regulation



Article 15

Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

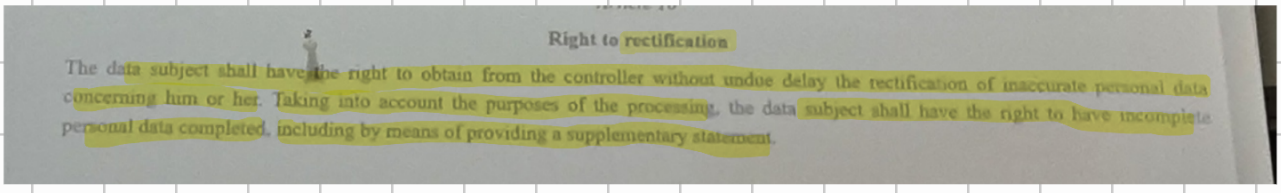
(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, 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.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means,

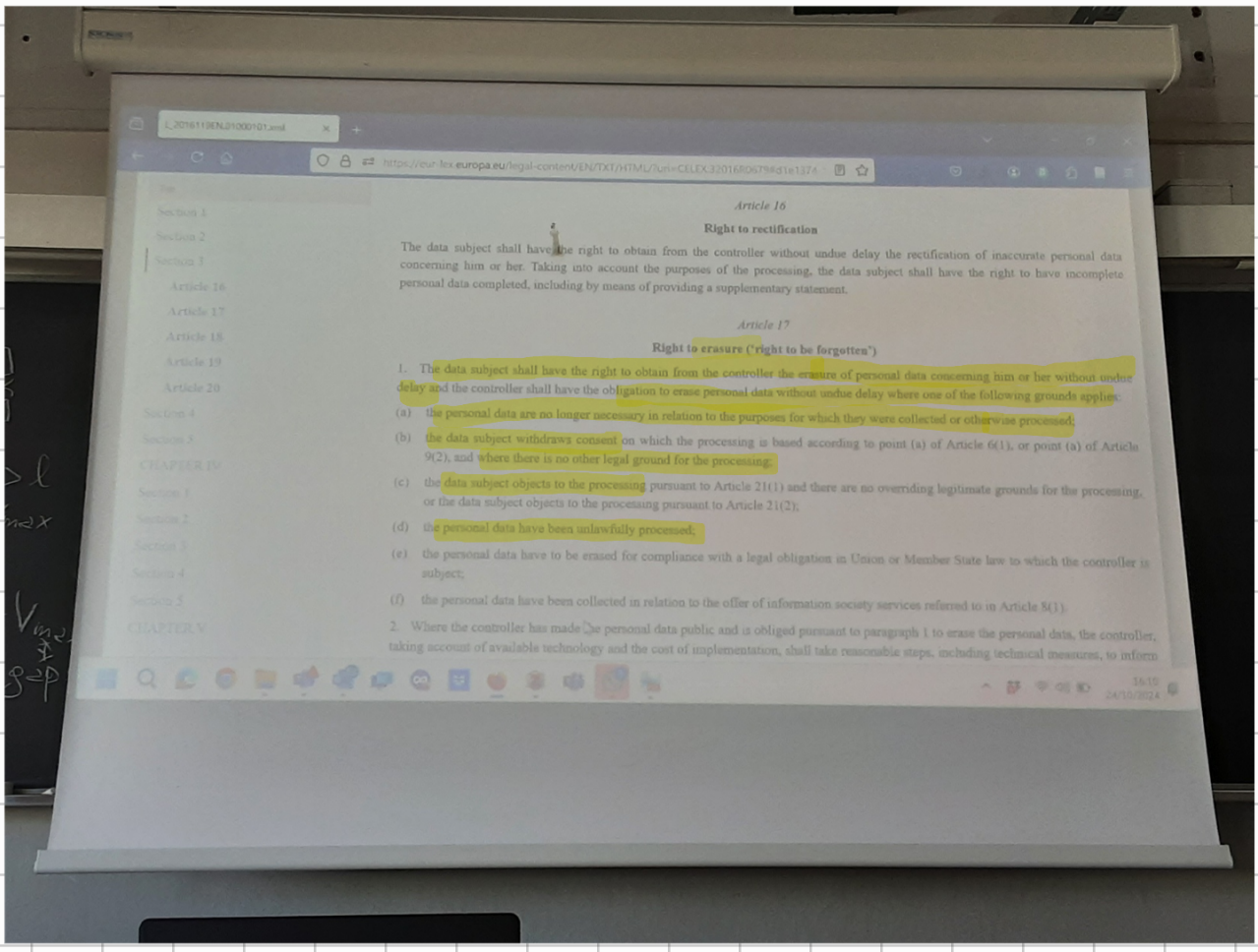
Data subject is the "owner" of the data, and has some rights regarding activity done by the data controller.
All of those you should have known in advance.



Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Either for mistakes or evolution of the personal data.
The decision of the Court of Justice for Google Costeja pushed toward the direction of right to be forgotten.



Article 16

Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 17

Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

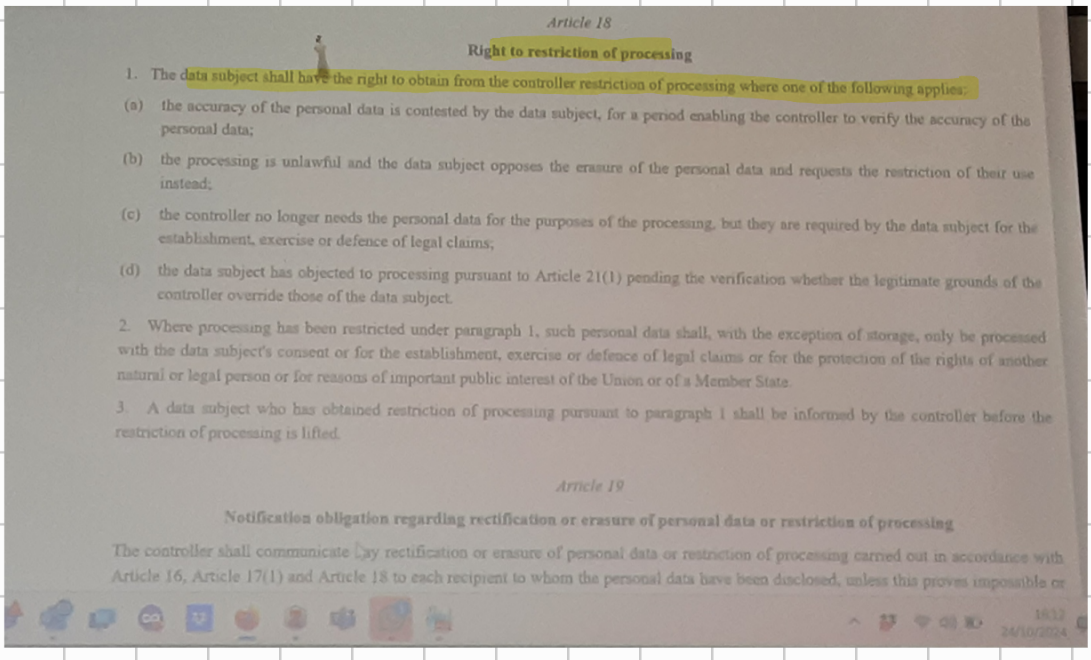
(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform

There is the possibility to erase the data.



Article 18

Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 19

Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or

Ability of the data subject to control what is happening (data security/protection)

For cookies, for example, I have information about "how much time I have spent on the websites etc."

Privacy policy: information per la privacy

Portability of data: I can transfer the data processed from a controller to another one, without losing control over them.

Rights of the data subject - 2

Right to rectification, erasure, restriction of processing, portability of personal data

- The data subject may request from the data controller that personal data be:
  - rectified (because they are inaccurate or not updated), possibly by supplementing incomplete information;
  - erased,
  - restricted in their processing
  - transferred to another data controller, if the processing is based on consent or on a contract concluded with the data subject and is carried out by automated means.

Right to be forgotten

right to erasure of one's personal data in an enhanced form:

Obligation for data controllers (if they have "made public" the personal data of the data subject) to inform other data controllers processing the deleted personal data of the erasure request, including "any link, copy or reproduction" (Art 17(2)).

If for ex. Google is asked to erase a specific info, google should inform other data controllers about the request for the erasure.

Rights of the data subject - 3

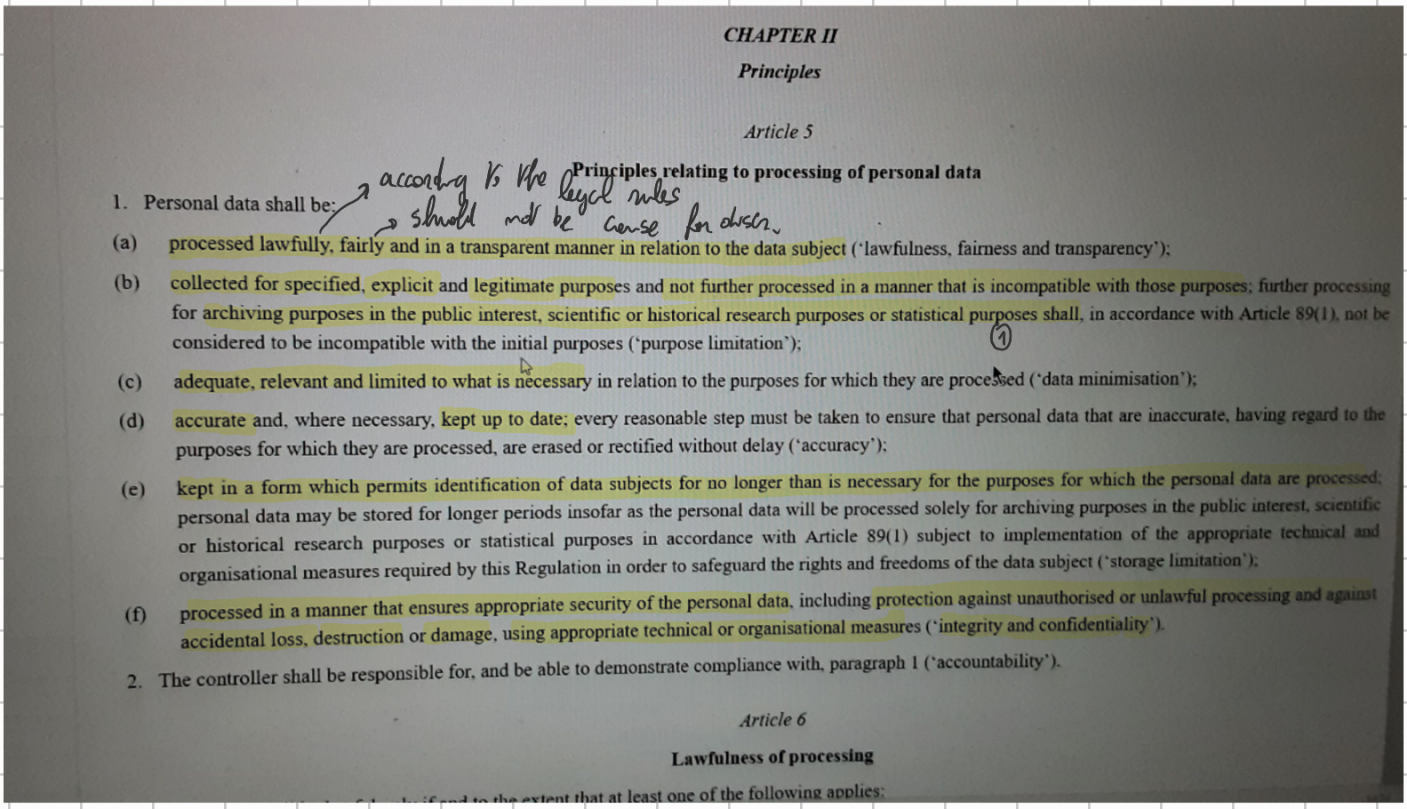
Right to object

- You may object to the processing of your personal data:
- for reasons related to the particular situation of the data subject, to be specified in the request;
- (without having to state the reasons for the objection) when the data are processed for direct marketing purposes.

Data processing

Any processing of personal data must comply with the following principles

- Lawfulness, correctness and transparency of the processing, with regard to the person concerned
- purpose limitation of processing, including the obligation to ensure that any further processing is not incompatible with the purposes of data collection;
- data minimization: i.e., data must be adequate relevant and limited to what is necessary in relation to the purposes of the processing;
- accuracy and updating of data, including the timely deletion of data that are inaccurate in relation to the purposes of processing;
- storage limitation: i.e., data must be kept for no longer than is necessary for the purposes for which they are processed;
- integrity and confidentiality: it is necessary to ensure the adequate security of personal data being processed



CHAPTER II

Principles

Article 5

Principles relating 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 ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6

Lawfulness of processing

according to the legal rules
→ should not be cause for abuse.

We want data processing to be carried out in respect to certain criteria.

(b) We need to make sure that there is a purpose to be achieved.
Purpose should be explained and not general. The purpose needs to be clearly identified (tick the boxes: each purpose requires a data processing). Will be explicit, clearly identified and legitimate.

① There are exceptions. Something done further on for other purposes, including statistical, scientific, historical ...

© "What kind of data do I need for this achievement?". The minimum requirements.

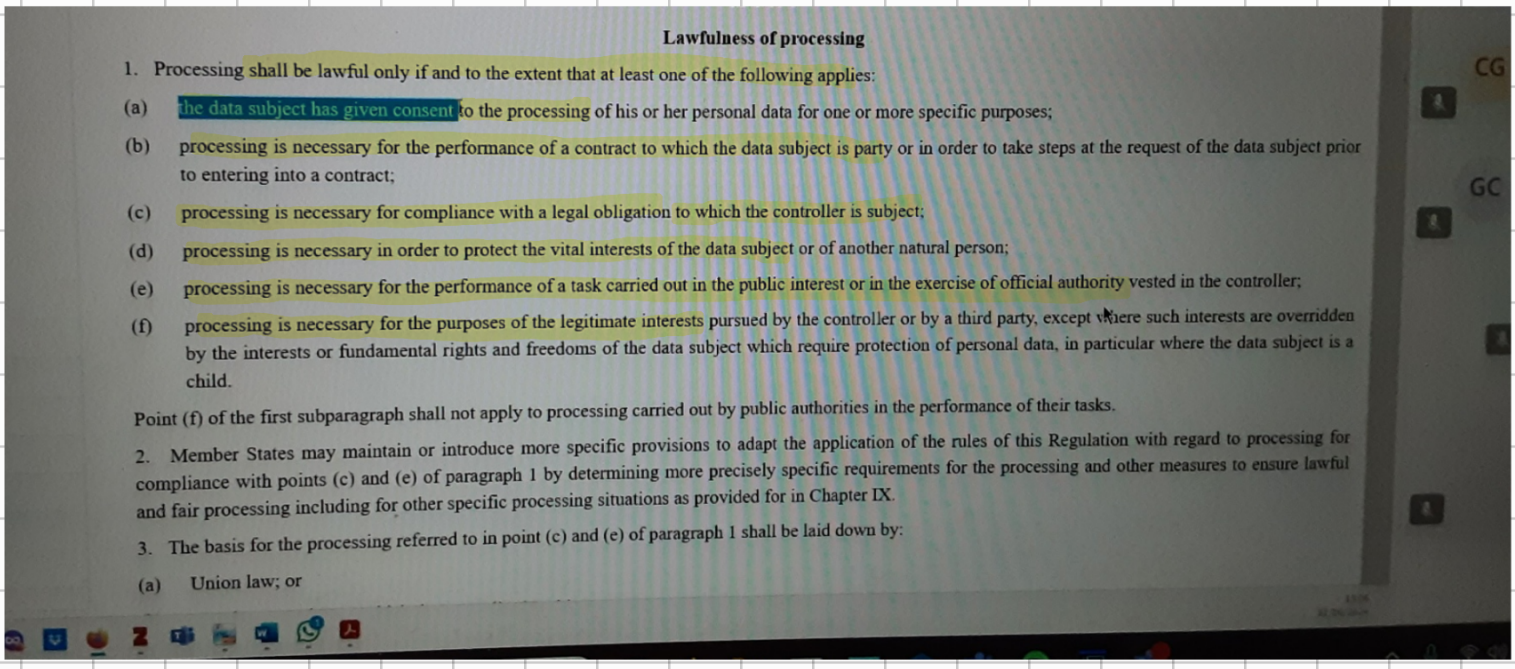
(d) If the data is incorrect, this will have impact on the data subject.

(e) This is the STORAGE LIMITATION PRINCIPLE

(f) Aiming to adopt security measures.

Those are the principles that apply to any data processing.

Art. 6 = lawfulness:



Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

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

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

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

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

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

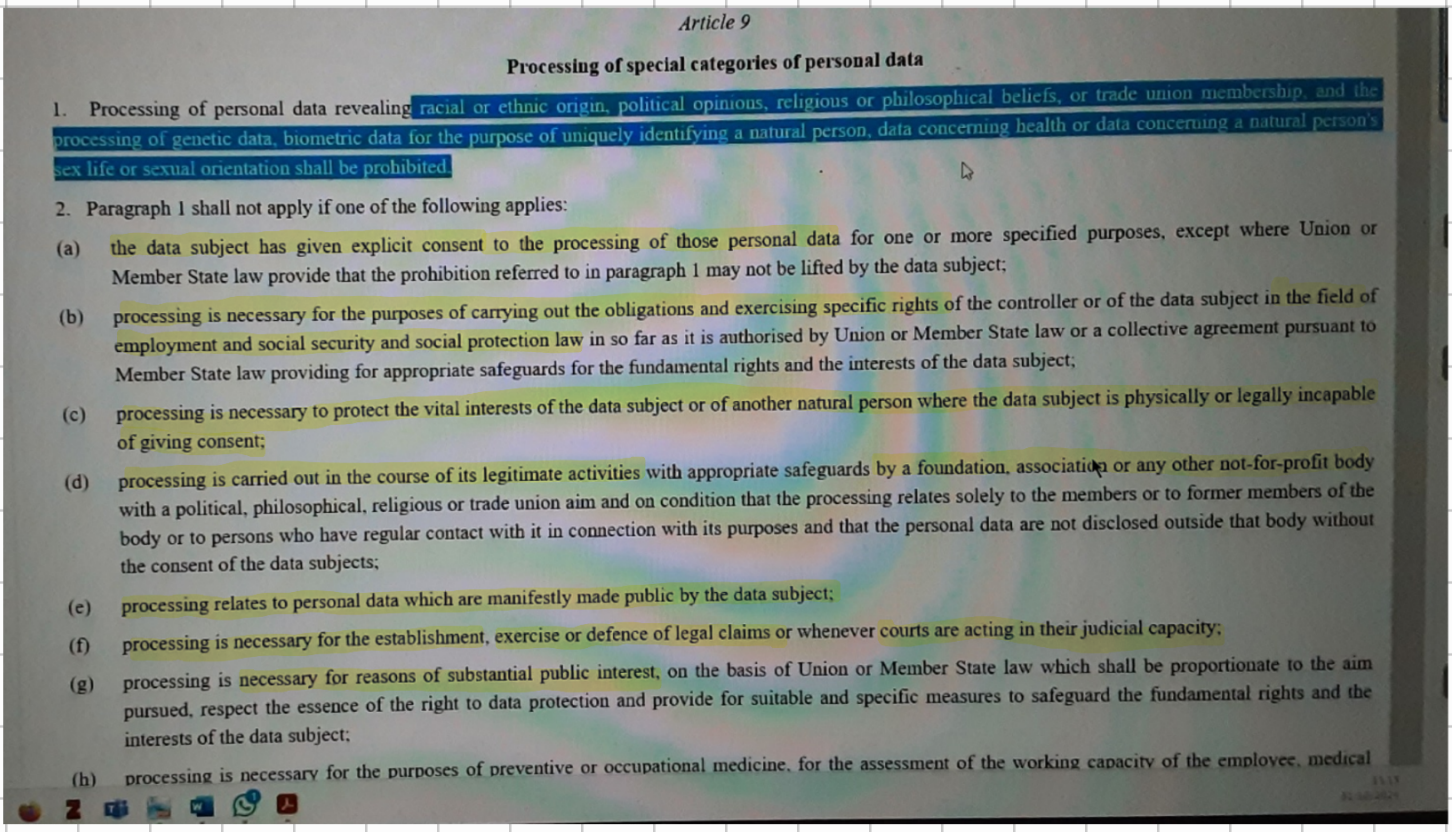
Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(a) Consent should be preliminary to the data processing,
• But can be possible that I consent later as soon as I know that the processing has started. (a) This is most used.
(b) Example: you give your personal data to Amazon. The processing is lawful because it is necessary for the performance of a contract.
(c) EX. Police officers can ask your personal data because they have a legal obligation.
(d) Protection of vital interest is of more importance.
(f) Example of cookies: legitimate interest (already set on on): they won't be able to achieve their activities without the processing of data. Economic activities can only be carried out through data processing.
Meta has a legitimate interest because it couldn't exist without the data it processes, but what should be the limit (purpose is only for the carrying out of activities).



Article 9

Processing of special categories of personal data

1. 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.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

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

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

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical

Rule: the processing of those special categories is prohibited, UNLESS:

1. Explicit consent is the easiest way to process.

(b) You need to find out if someone is in a trade union to give out extra free hours to carry out special activities.

(d) LGBT associations: they can get info about the pers involved in the assoc.

(e) If you publish info for ex. about your sexual orientation, that data can be processed.

(g) Case in pandemic, interventions included processing of over 80s vaccinated.

diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Lawful data processing – legal basis

- Consent
- fulfilment of contractual obligations
- vital interests of the data subject or of third parties,
- legal obligations to which the holder is subject,
- public interest or exercise of public authority,
- overriding legitimate interests of the data controller or of third parties to whom the data are disclosed.

In the case of special categories of personal data, processing is prohibited, subject to specific conditions.

Consent

Validity of consent:

- the data subject has been informed about the processing of personal data (Articles 13 or 14 of the Regulation);
- has been expressed by the data subject freely, unambiguously and, if the processing pursues several purposes, specifically with regard to each of them.

The request is distinct from others addressed to the data subject

Consent need not be "documented in writing", nor is "written form" required: you can "consent" through your behaviour

① If you want to use social media platforms you can't unlock the privacy policy box, which might lead to not receiving the service.

Information about data processing

It must be provided to the data subject before processing, i.e. before the data are collected.

The content is provided for in Articles 13 (1) and 14 (1)

- Identity of the data controller
- purpose of processing
- rights of the data subject
- contact details of the DPO
- legitimate interest
- Possible transfer to third countries
- period of data retention
- Right to lodge a complaint with the supervisory authority.
- Possible automated decision-making process

The information is in principle given in writing and preferably in electronic format

It must be comprehensible and transparent to the data subject, through the use of clear and plain language.

Section 2

Information and access to personal data

Article 13

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected 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:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) 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;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) 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;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) 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;

(f) 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.

3. 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.

Data transfer to third countries

The transfer of personal data to countries outside the European Union is prohibited, except in the following cases:

- adequacy of the third country recognised by a decision of the European Commission; that allows the processing (if data protection laws are similar)
- in the absence of a Commission adequacy decision, appropriate contractual or contractual safeguards (the contract allows safeguards)
- in the absence of any other prerequisite, use of exceptions to the prohibition of transfer applicable in specific situations

GDPR has an extraterritorial scope: applies to outsiders too.
Third parties can have access to data and do not have the same GDPR obligation.

Privacy shield = agreement between US and EU, agreement to have EU personal data to be transferred

Who should check the compliance?

Data protection Supervisory Authorities

- the Article 29 Working Party has become the European Board of Supervisors (EDPB)
- National supervisory authorities exist at member state level
  - The Italian Data Protection Authority (Garante Privacy)
- One stop shop mechanism

Euro data protection board provides instructions and guidelines to DPA. These work is not binding but can have influence.

Data protection in Ireland checks conformity for Meta. What happens if Meta processes data across all Europe? Who should be in charge in case of claims?
The irish
The first one decides and then the next ones follow. One stop shop mechanism.
Supports harmonization at EU level.

The **one-stop-shop (OSS) mechanism** in the GDPR is designed to streamline data protection oversight across EU member states, making things easier for organizations that operate in multiple countries. Essentially, it allows companies that process data across several EU countries to deal primarily with a single data protection authority (DPA) instead of facing each country's regulator individually.

Here's how it works: if a company has cross-border processing activities (like having users or employees across the EU), it can designate a "**lead supervisory authority**" (often based on where the company has its main establishment within the EU). This lead authority then becomes the primary point of contact for handling GDPR-related matters for the entire EU, such as investigating complaints or conducting audits.

However, other national DPAs aren't sidelined completely. They can still be involved, especially if the data processing activities have a major impact on individuals within their countries. The lead authority will work with these other DPAs in what's called the "**consistency mechanism**" to make sure decisions are fair and aligned with GDPR across the board.

I love you

The tasks and powers of the Supervisory Authorities

Monitoring and supervision (Art. 57 GDPR)

Advisory functions (Art. 57)

Investigative powers (art. 57 and 58)

Handling complaints (art. 77 GDPR)

Corrective powers (Art. 58 par.2 GDPR)

Section 1

Independent status

Article 51

Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 57

Tasks

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation; (ENFORCES WITH directive we don't have this)

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

(l) give advice on the processing operations referred to in Article 36(2);

Article 58

Powers

1. Each supervisory authority shall have all of the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(b) to carry out investigations in the form of data protection audits;

(c) to carry out a review on certifications issued pursuant to Article 42(7);

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to

① Gather info regarding how processing is carried out. It's an order.

② Warning: it's possible that, by the info I collected you are violating GDPR.

CHAPTER VI
Section 1
Section 2
Article 55
Article 56
Article 57
Article 58
Article 59

manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

Article 83

General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

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

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

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

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

(g) the categories of personal data affected by the infringement;

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

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

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

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

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an

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

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

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

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; Related to security req. also. least relevant ones

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; ex no ask for consent exc...

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX; ban on during processing, withdrawal of consent

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and

Complaints in case of violation

Complaint before Supervisory authority

- preliminary investigation and possible formal administrative procedure that may lead to the adoption of
  - Remedies
  - Administrative sanctions } Corrective pow.

The decision of the supervisory authority may be challenged in court We can complain

DPA can do a wrong decision: 77 allows the possibility to lodge a complaint with a supervisory authority. The fact that we can complain before Supervisory authority for a violation of the GDPR.

If you have a violation of the GDPR, there are two routes: go before DPA, and in this case you have the possibility to challenge the activity of the data controller (and the possibility to have sanctions against the data controller, but no damage); or you go against data controller before a court: here lengthy procedure but then you have possibility to ALSO in case of violation to receive damages in case of suffering from unlawful data processing.

Administrative sanctions under the GDPR (Art. 83)

Administrative sanctions imposed by the DPA

The principles of administrative sanctions

Two groups of fines under the GDPR :

- ✓ up to 10/million or 2% of the annual global turnover if higher;
- ✓ up to 20/million or 4% of the annual global turnover if higher

The accountability principle in the data protection field

- The meaning of the principle

Controller and processors are obliged to ensure that the processing of personal data complies with the relevant rules and must be able to prove compliance at any time (art. 5 par. 2 GDPR)

↳ without previous requests. Up to the data controller, you have to comply and adapt measures.

- Data controller-focused
- Risk-based approach
- The 'elements' of accountability

The accountability principle under the GDPR

- Adoption of codes of conduct, certification mechanisms, data protection seals and marks as facilitating tools to prove compliance with the obligations of the controller (Art. 24 par. 3 GDPR) and of the processor (Art. 28 par. 5 GDPR) as well as mitigating factors of administrative sanctions (Art. 83 par. 2 GDPR)

- Records of processing activities (Art. 30 GDPR)

Responsibility of the controller

- Technical and organisational measures to ensure a level of security appropriate to the risk (Art. 32 GDPR)

- Notification of a personal data breach to the DPA (Art. 33 GDPR)

- Data Protection Impact Assessment (Art. 35 GDPR)

When processing has resulted in a violation, in this case

From ACCOUNTABILITY to LIABILITY

ARTICLE 82 GDPR (Right to compensation and liability)

not just the data subject

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation **shall have the right to receive compensation from the controller or processor for the damage suffered.**

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

Allocating this kind of accountability means it's up to them to show that they comply.