L2 - Grounds for processing personal data, obligations for data controllers and processors and data subjects' rights. International data transfers and enforcement

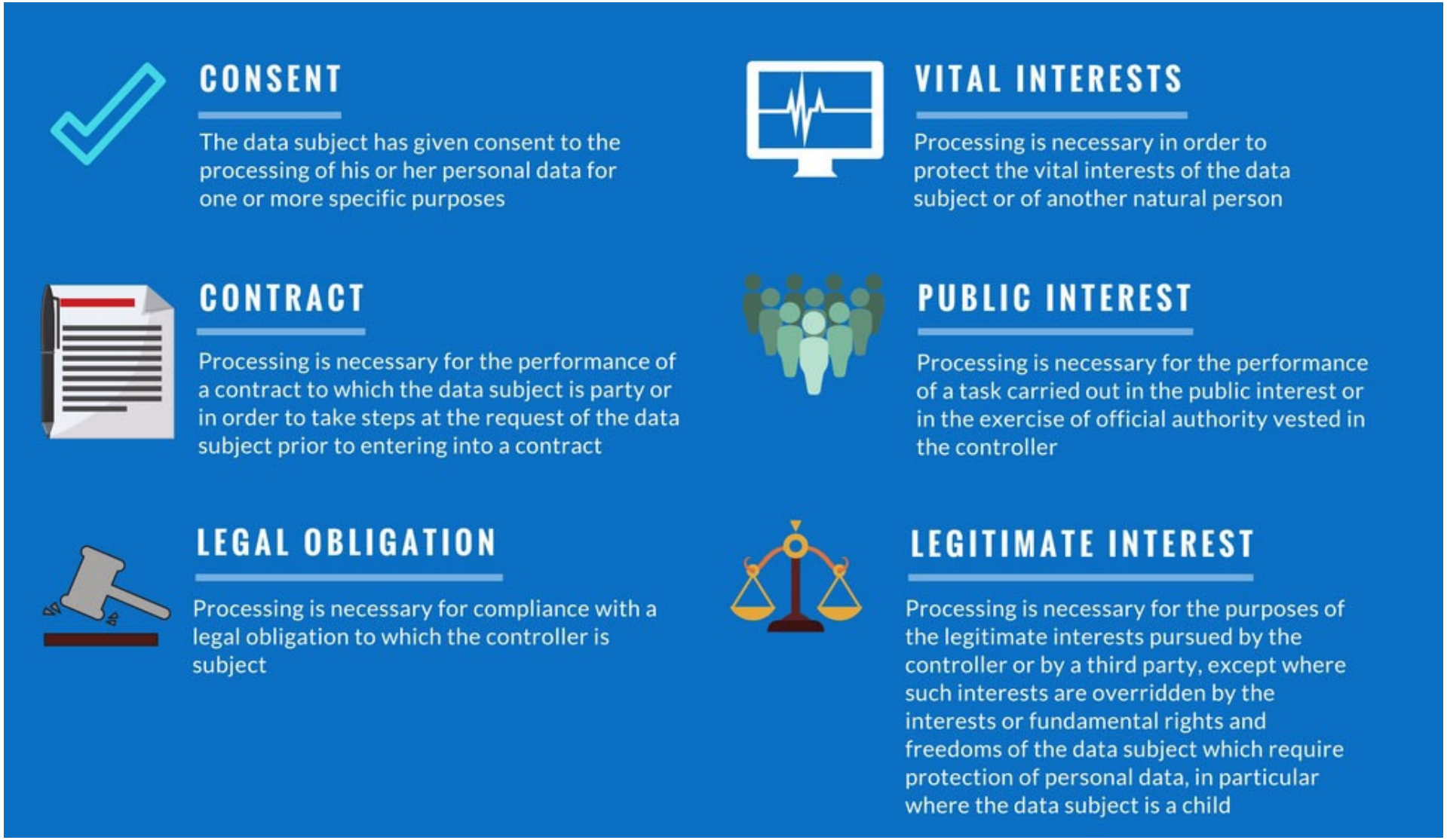
Course: Data Science Regulation and Law

Cluster: Privacy and Data Protection

22 May 2024

1. Grounds for lawful processing of personal data

Legitimate grounds



Consent

To be considered valid under GDPR, it has to be:

Freely given
- Genuine choice; data subjects must be able to withdraw consent
- Imbalance of power → may result in invalid consent

Specific
- Specific for the purpose of processing, clear and unambiguous language
- Granular: if more purposes, consent needs to be obtained for each purpose

Informed
- Based on an understanding of the processing event(s), their possible implications and consequences of refusing consent

Unambiguous
- No reasonable doubt on the data subject's intention to consent → inactivity is **not** valid consent

Provable
- 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

Special vs. non-special personal data

Based on the **nature of the personal data,** we can distinguish between:

Special vs non-special personal data → Data that **reveal** religious beliefs, political beliefs, trade union membership, race/ethnic origin, sex life or sexual orientation, health data, biometric data, genetic data

Why are some data considered special?

Due to their nature, they pose a heightened risk to data subjects when processed → processing such data is **prohibited** as a rule, unless some exceptions (e.g., explicit consent) apply (Article 9 GDPR)

Performance of a contract

- Data subject must be party to the contract
- Includes pre-contractual relationships (e.g., checks that need to be performed before entering the contract)
- Personal data must be **necessary** for fulfilling the contract – *objectively* necessary

Legitimate interest

3 Important questions:

1. Is your interest **legitimate**?
(examples: IT/Network/physical security; research; prevention of fraud)

2. Is the processing of data **necessary** to achieve the legitimate interest?
(i.e., is there another way of achieving the identified legitimate interest?)

Legitimate interest

3. Is your interest **overridden** by the rights/interests of the data subject? → Balancing exercise between all the interests at stake

-Assessing the impact requires considering:

- Positive/negative, individual and social
- Severity of risk
- Likelihood to materialize
- Nature of the data (i.e., special categories or not)
- Reasonable expectations of data subjective (privacy policies are important)

-Additional measures to reduce impact:

- Technical/organizational/transparency/accountability

2. Obligations for controllers and processors

Data protection by design

- 1. 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 the processing itself, implement **appropriate technical and organisational 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 default

- 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.

Data controllers: obligations

- Appointment of the data processor(s), if any
- Appointment of sub-processor(s), if any
- Record of processing activities
- Appointment of the DPO
- Cooperation with the DPAs
- Notification of data breaches

Data controllers: obligations in case of high risk

Data breach communication to the data subjects

Data Protection Impact Assessment (DPIA)

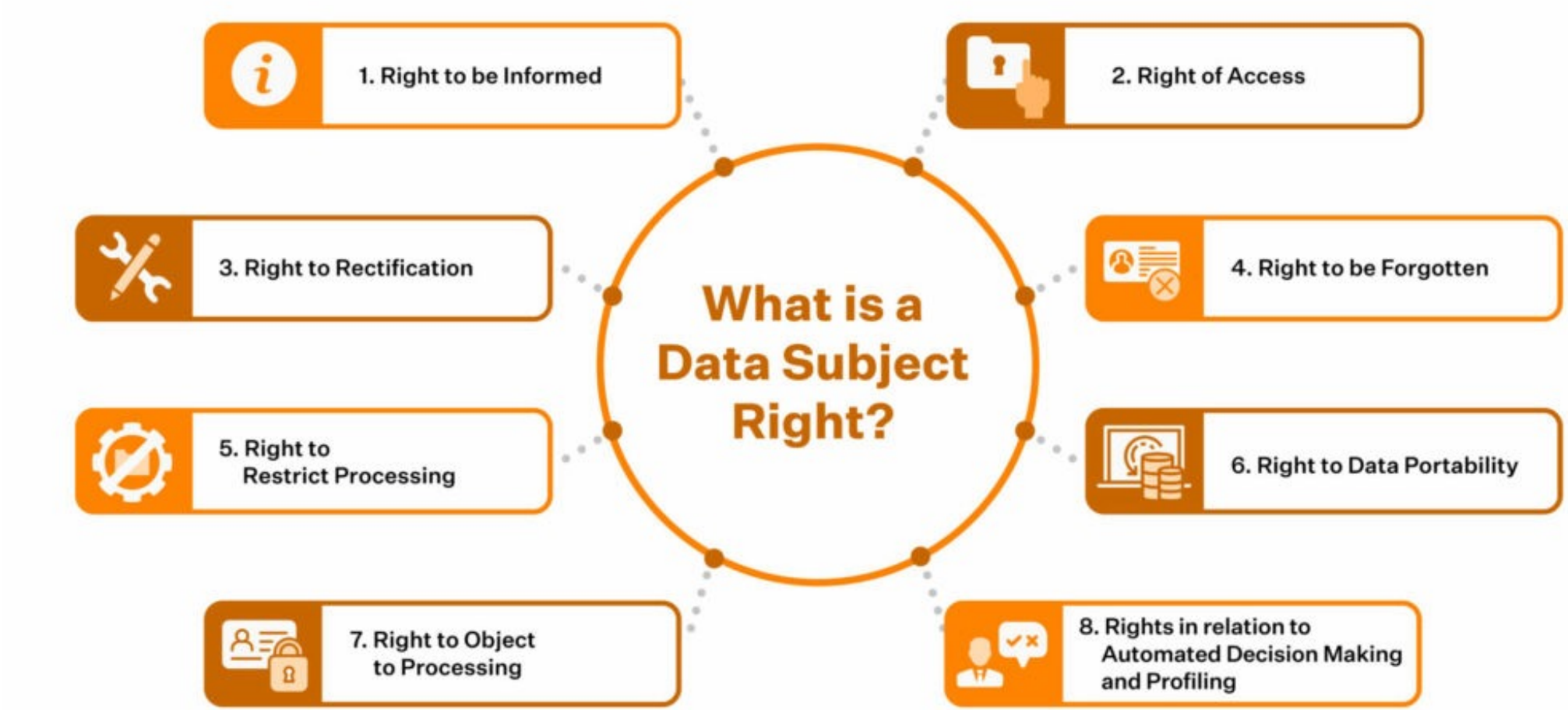
Prior consultation of supervisory authority

Data processors: obligations in case of high risk

- Appointment of sub-processors
- Confidentiality
- Compliance with the controller's instructions
- Records of processing activities

3. Data subject rights

Data subject rights



1. Right to be informed

- Controllers have **a duty to inform** data subjects when personal data are collected about them, and their intended use.
- Not based on data subjects making requests but on controllers providing information about processing, in a **clear and concise way**.
- Information to be provided :
  - Controller's identify and habitual residence/establishment, DPO details if any
  - Legal bases and purposes for processing
  - Categories of personal data processed
  - Recipients
  - Ways data subjects can exercise rights
  - Whether data will be transferred to a third country or international org.
  - The period for which personal data will be stored
  - The existence of automated decision-making
  - Right to **lodge a complaint**

2. Right to access

- The data subject has the right to obtain from the controller a **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 to **information concerning the processing**
- 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, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form
- The right to obtain a copy of data shall not adversely affect the rights and freedoms of other parties

3. 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 processing, the data subject shall have the **right to have incomplete personal data completed**, including by means of providing a supplementary statement.
- Rectifications must occur **without undue or excessive delay** on the part of the controller.

4. Right to erasure

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 **IF**:

1. The request is based **on specific grounds**
2. The right to erasure is not excluded based **on specific exceptions**

4. Right to erasure

Specific grounds:

- No longer necessary to the purposes for which they were collected or otherwise processed;
- The data subject withdraws consent on which the processing is based;
- The data subject objects to the processing;
- The personal data have been unlawfully processed;
- The personal data have to be erased for compliance with a legal obligation;
- The personal data have been collected in relation to the offer of information society services.

4. Right to erasure

Exceptions:

- Exercise of the right of freedom of expression and information;
- Compliance with a legal obligation which requires processing;
- Protection of public interest in the area of public health;
- Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;
- For the establishment, exercise, or defence of legal claims.

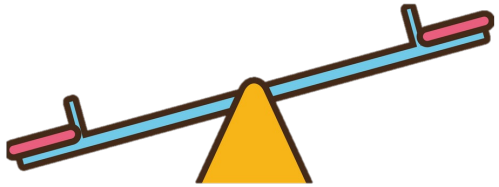
4. Right to erasure

- **Example**

A few years ago, Ted owned a company in the NL, which declared bankruptcy after issues with mismanagement. This information is publicly available in the Dutch company register. Ted requests for his personal data to be erased from the register because it makes it difficult for him to get any investor funding for his new company with a similar business.

Can Ted's request to have his personal data erased be successful? Why?

<u>Ted</u>
Necessity for purpose?



<u>Other rights and interests</u>
Purposes in the public interest

5. Right to restriction of processing

- The data subject shall have the **right to obtain from the controller restriction of processing**
- Where processing has been restricted, 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**.

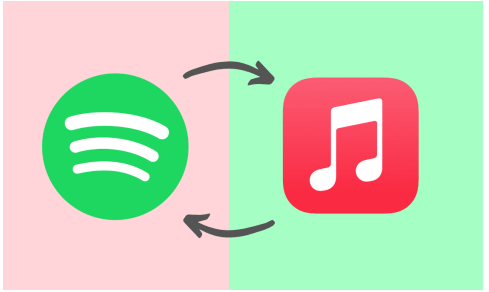
5. Right to restriction of processing

Four cases for restriction of processing:

- 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;
- The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- 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;
- The data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

6. Right to data portability

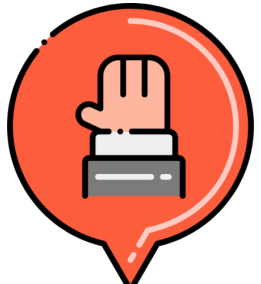
- Data subjects have the right to receive their **personal data that <u>they provided</u>** to a controller in a **structured**, **machine-readable format**, and transmit those data to another controller.
- Two conditions must be met in order for the data subject to be able to exercise this right:
  1. The processing is based on the **consent** legal ground or on the **contract** legal ground
  2. The processing is carried out by **automated** means
- Goal: to avoid 'lock-in' effects and facilitate consumers' choice on the market



7. Right to object

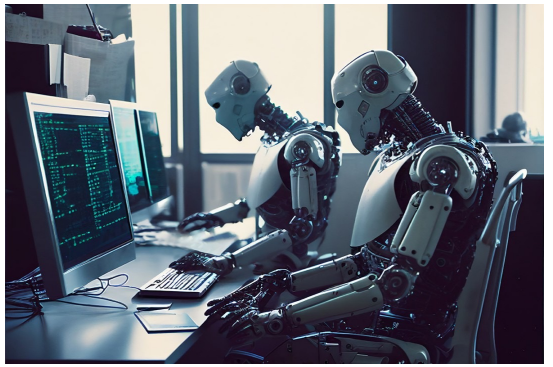
- The data subject shall have the **right to object**, on grounds relating to his or her particular situation, at any time **to the processing of personal data concerning him or her** where processing is necessary:
  - for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
  - for the purposes of the legitimate interests pursued by the controller or by a third party
  - for **scientific or historical research** purposes or **statistical** purposes, on grounds relating to their particular situation (unless this is necessary for public interest)

- The controller shall **no longer process** the personal data **unless** the controller **demonstrates** compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.



8. Right not to be subject to automated decision-making

- Data subjects have the right to **not** be subject to a decision based solely on automated processing, including profiling, which has legal effects or similarly significant effects on them → read: ban on controllers
- Automated decisions = decisions taken using personal data processed solely by automatic means **without** any human intervention.
- Profiling = automated processing using personal data to evaluate certain personal aspects relating to an individual, in particular to analyze or predict aspects concerning that individual



8. Right not to be subject to automated decision-making

- Decision with legal effects – affects data subject's legal rights/legal status/rights under a contract.
  - Examples: entitlement to or denial of a particular social benefit granted by law, such as child or housing benefit, etc.

  OR
- Decision with significant effects – affects data subjects' circumstances to a great extent.
  - Examples: decisions that affect financial circumstances, access to health services, that deny employment, etc.

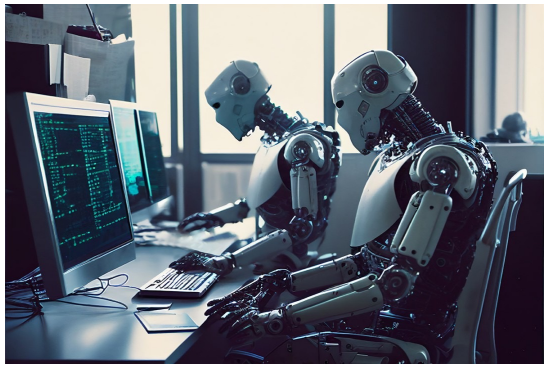
8. Right not to be subject to automated decision-making

Exceptions

This right does not apply where the processing:

- is necessary for entering into, or performance of, a contract between the data subject and a data controller;
- is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- is based on the data subject's explicit consent.

+ implementation of **suitable measures and safeguards**: e.g. a mechanism for human intervention to provide individuals with the option to appeal, which triggers a human review ; algorithmic auditing, etc.



4. International data transfers

International data transfers

- The GDPR aims to prevent the risk that personal data might be processed outside EU to circumvent GDPR rules. This is against goal of ensuring a high level of protection to personal data.
- The protection should follow the personal data, **wherever it goes**
- **But what about international transfers of data occurring on a regular basis, which are highly facilitated by digital technologies?**

International data transfers

1

Adequacy decision

2

Appropriate safeguards

3

Derogations

Adequacy decisions

- If a country has an adequacy decision → free flow of personal data
  - As of 2023: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zeeland, Republic of Korea, Switzerland, UK, Uruguay, US
- For an adequacy decision to be issued, the European Commission needs to assess the level of data protection in the third country by looking at their national law and applicable international obligations – rights, remedies, etc.
- Decision is granted only if the third country offers a level of protection of personal data that is **'essentially equivalent'** to that ensured by EU law
- See the *Schrems* saga

Appropriate safeguards

- If there is no adequacy decision, personal data can still be transferred by means of appropriate safeguards between the parties making the transfers (i.e., controllers and processors).
- Instruments that can establish appropriate safeguards:
  - **Binding Corporate Rules** – multinationals based in many countries can transfer personal data within their corporate group. Must be approved by the Data Protection Authority.
  - **Standard data protection clauses (SCCs)**– adopted by the EU Commission *or* by national Data Protection Authorities and approved by the Commission.
  - **Approved code of conducts**
  - **Approved certification mechanism**

Derogations

In the absence of both an adequacy decision, and appropriate safeguards, transfers may still be justified in the following 7 circumstances:

- the data subject gives explicit consent for the data transfer
- the data subject enters – or is preparing to enter – into a contractual relationship where the transfer of data abroad is necessary;
- to conclude a contract between a data controller and a third party in the interests of the data subject;
- for important reasons of public interest;
- to establish, exercise or defend legal claims;
- to protect the vital interests of the data subject;
- for the transfer of data from public registers (this is an instance of prevailing interests of the general public to be able to access information stored in public registers).

Even if none of these apply, a transfer can still occur if: the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject. Controller must provide safeguards & inform supervisory authority and data subjects of the legitimate interest.

TUTORIALS

TUTORIALS

- Please read carefully the Opinion of the Advocate General and the judgment of the Court of Justice in the *Google Spain* case. Please try to focus on the differences in their conclusions (which significantly diverge) and on the reasons behind them
- It is not necessary (nor required) that you capture all the legal technicalities of the case in the reasoning of both AG and ECJ: let's try to focus on the essence of their arguments on the different points
- If you don't understand something in particular, please be prepared to share your question(s) at the beginning of the tutorial: we will not explore the case but just summarize the main findings of the Court
- Once read the opinion and the judgment, please focus on the following points/questions…

TUTORIALS

- Do you agree that companies based outside the European Union should comply with EU data protection law when it comes to the processing of data of European residents?
- Do you agree that a search engine service provider carries out a processing of personal data any time it retrieves information from the Internet, on third-parties' websites, based on the prompts input by its users?
- Do you agree that a search engine service provider acts as controller in respect of the personal data it indexes when providing search results to its users?
- Do you agree that a search engine like Google is tasked with evaluating whether a request to obtain the removal of links to personal data should be accepted or rejected?

LinkedIn

Marco Bassini

Assistant Professor of Fundamental Rights and Artificial Intelligence at Tilburg University

Thank you!

m.bassini@tilburguniversity.edu