Information and technology law course

LECTURE 15 – 13 NOVEMBER 2024

FEDERICA CASAROSA – 2024/2025

European Data strategy

Communication, A European strategy for data, 19.2.2020, COM(2020) 66 final

"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." (p. 5)

We need to make sure we have additional effort related to how data can be organized, processed, used, structured etc.

① Putting on the table what we want to do for the following years. It's a strategy for data (both non personal and personal data)

② Article 114: on the internal market. It intends to protect the internal market. This is them saying what we do in the next years will be for the internal market.

③ I don't own personal data. Connected to that. I can share data with other people, let them process it. But data is still in my database, linked to me. I can "knock on your door" and have a say. In this case we want free flow: possibility of sharing, processing, accessing in the EU and across sectors.
For example health data from Fitbit to android device that is shared to a software. We want still to protect the rights of the data subject. Within the boundaries of GDPR we want to improve and make profit from data flow.

③ Mechanisms should ensure compliance with EU rules, values, data protection etc.

④ We want to make sure that rules for access and use of data are fair, practical and clear.

Challenges for data economy

Availability of data ①

- The value of data lies in its use and re-use.
- Data for the public good
  - G2B + B2B + B2G + G2G ②

Imbalances in market power

Data interoperability and quality ③

- Data interoperability and quality, as well as their structure, authenticity and integrity are key for the exploitation of the data value, especially in the context of AI deployment.

Data governance ④

Data infrastructures and technologies

Empowering individuals to exercise their rights Recall GDPR. Skill control data and exercise my rights.

What are the challenges that I sees?

① Data is the fuel. Make sure that data is available and can be used.

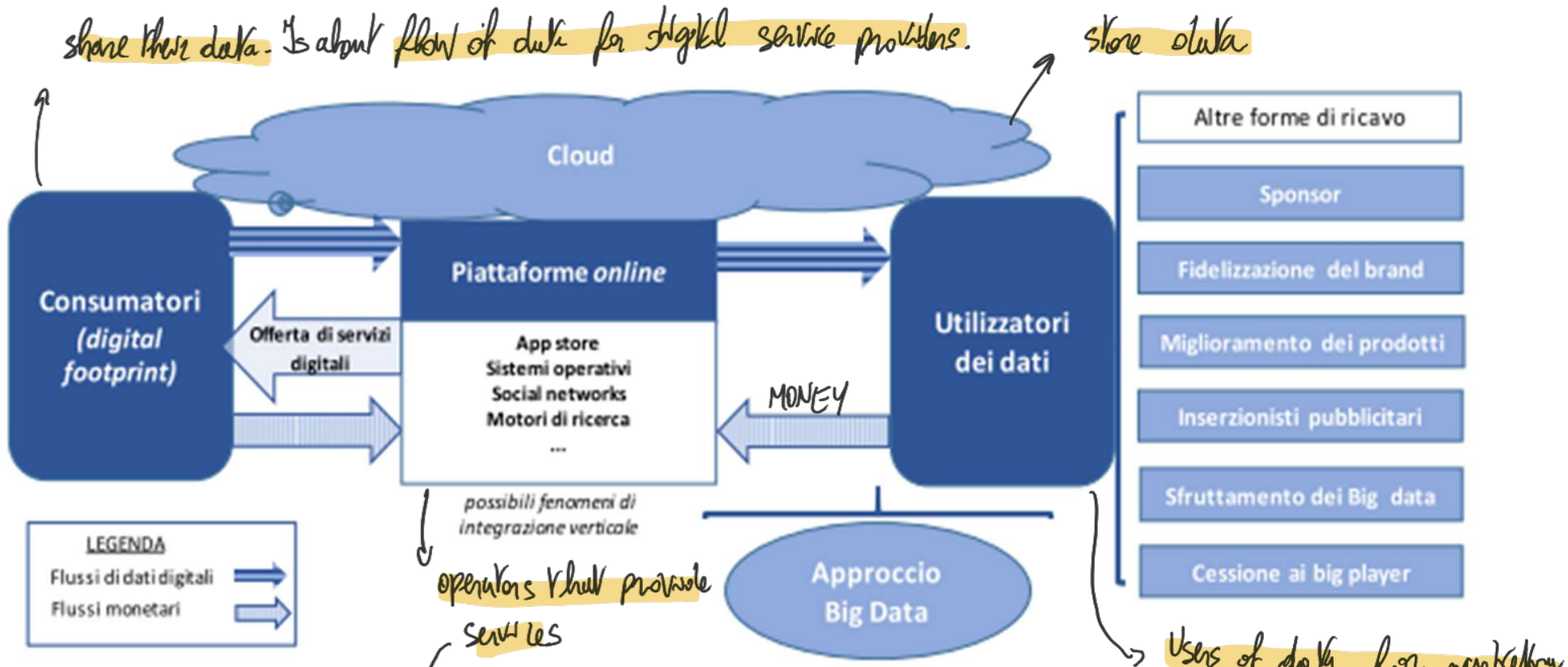
② Means that I have to make sure that there are ways to make data flow between public and private entities (Government / Business)

B2B: how far I should go for transferring info from other?

B2G: how far should I share info to governmental entities?

③ Interoperability: standard to make sure that one system speaks to another. This is the basis for sharing data. Particularly important for AI systems.

④ Control the actors that work in the system.



Rappresentazione sintetica del mercato a due versanti applicato ai dati digitali

2023

Data Act

Data Act

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act)

Article 1 Subject matter and scope

1. This Regulation lays down harmonised rules, inter alia, on:
   - (a) the making available of product data and related service data to the user of the connected product or related service;
   - (b) the making available of data by data holders to data recipients;
   - (c) the making available of data by data holders to public sector bodies, the Commission, the European Central Bank and Union bodies, where there is an exceptional need for those data for the performance of a specific task carried out in the public interest;
   - (d) facilitating switching between data processing services;
   - (e) introducing safeguards against unlawful third-party access to non-personal data; and
   - (f) the development of interoperability standards for data to be accessed, transferred and used. […]

2.This Regulation applies to:
   - (a) manufacturers of connected products placed on the market in the Union and providers of related services, irrespective of the place of establishment of those manufacturers and providers;
   - (b) users in the Union of connected products or related services as referred to in point (a);
   - (c) data holders, irrespective of their place of establishment, that make data available to data recipients in the Union;
   - (d) data recipients in the Union to whom data are made available;
   - (e) public sector bodies, the Commission, the European Central Bank and Union bodies that request data holders to make data available where there is an exceptional need for those data for the performance of a specific task carried out in the public interest and to the data holders that provide those data in response to such request;
   - (f) providers of data processing services, irrespective of their place of establishment, providing such services to customers in the Union;
   - (g) participants in data spaces and vendors of applications using smart contracts and persons whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement.

Approved between 2022/2024. For data governance. This is about "Harmonised rules on fair access to and use of data"

What's the scope?

① Who are those entities? Who's the user? The data holder, recipient?
We had DS, DC, DP.
Data holders may be the DC because they have possibility to hold data.
DR are the ones that will receive data from holders. But who are the users?

NOTE: ② product data and service data to the user of the connected product.
③ Are public sector bodies different than DR? In C we are discussing B2G, in 6 B2B.

Definitions

For the purposes of this Regulation, the following definitions apply:

(1) 'data' means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording;

(2) 'metadata' means a structured description of the contents or the use of data facilitating the discovery or use of that data;

Data Act

Actors

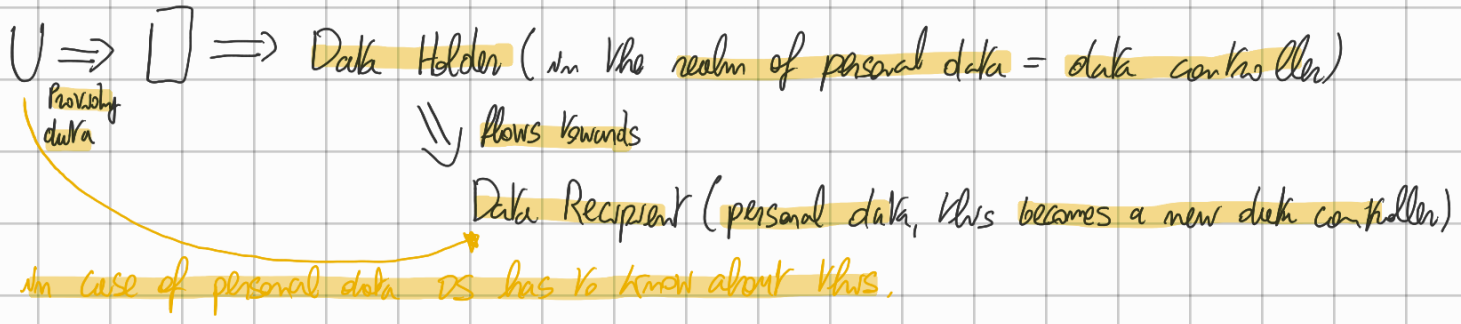
(11) ‘data subject’ means data subject as referred to in Article 4, point (1), of Regulation (EU) 2016/679;

(12) ‘user’ means a natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services;

(13) ‘data holder’ means a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service;

(14) ‘data recipient’ means a natural or legal person, acting for purposes which are related to that person’s trade, business, craft or profession, other than the user of a connected product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation adopted in accordance with Union law;

⑨ Can be the data subject, but user also refers to the legal person. In the system of data we have a user, that owns or can use a connected product. In the realm of personal data, this is also = DS.



We focus on DH.

Data Act : B2G data exchange

Chapter V - Making data available to public sector bodies, the Commission, the European Central Bank and Union bodies on the basis of an exceptional need

Article 14 - Obligation to make data available on the basis of an exceptional need

Where a public sector body, the Commission, the European Central Bank or a Union body demonstrates **an exceptional need**, as set out in Article 15, to use certain data, including the relevant metadata necessary to interpret and use those data, to carry out its statutory duties in the public interest, data holders that are legal persons, other than public sectors bodies, which hold those data shall make them available upon a duly reasoned request

EXCEPTIONAL NEED + PUBLIC INTEREST

Data act and cybersecurity

Article 15 - Exceptional need to use data

1. An exceptional need to use certain data within the meaning of this Chapter shall be limited in time and scope and shall be considered to exist only in any of the following circumstances:

- (a) **where the data requested is necessary to respond to a public emergency** and the public sector body, the Commission, the European Central Bank or the Union body is unable to obtain such data by alternative means in a timely and effective manner under equivalent conditions;
- (b) in circumstances not covered by point (a) and only insofar as non-personal data is concerned, where:
  - (i) a public sector body, the Commission, the European Central Bank or a Union body is acting on the basis of Union or national law and has identified specific data, the lack of which prevents it from fulfilling a specific task carried out in the public interest, that has been explicitly provided for by law, such as the production of official statistics or the mitigation of or recovery from a public emergency; and
  - (ii) the public sector body, the Commission, the European Central Bank or the Union body has exhausted all other means at its disposal to obtain such data, including purchase of non-personal data on the market by offering market rates, or by relying on existing obligations to make data available or the adoption of new legislative measures which could guarantee the timely availability of the data

① Emergency is PoR we need to have.

② How do you define a public emergency? JVs stated in the recitals.

not severable from the other terms of the contract.

(63)In situations of exceptional need, it may be necessary for public sector bodies, the Commission, the European Central Bank or Union bodies to use in the performance of their statutory duties in the public interest existing data, including, where relevant, accompanying metadata, to respond to public emergencies or in other exceptional cases. Exceptional needs are circumstances which are unforeseeable and limited in time, in contrast to other circumstances which might be planned, scheduled, periodic or frequent. While the notion of 'data holder' does not, generally, include public sector bodies, it may include public undertakings. Research-performing organisations and research-funding organisations could also be organised as public sector bodies or bodies governed by public law. To limit the burden on businesses, microenterprises and small enterprises should only be under the obligation to provide data to public sector bodies, the Commission, the European Central Bank or Union bodies in situations of exceptional need where such data is required to respond to a public emergency and the public sector body, the Commission, the European Central Bank or the Union

ghlight All Match Case Match Diacritics Whole Words 1 of 18 matches

16:36

(64)In the case of public emergencies, such as public health emergencies, emergencies resulting from natural disasters including those aggravated by climate change and environmental degradation, as well as human-induced major disasters, such as major cybersecurity incidents, the public interest resulting from the use of the data will outweigh the interests of the data holders to dispose freely of the data they hold. In such a case, data holders should be placed under an obligation to make the data available to public sector bodies, the Commission, the European Central Bank or Union bodies upon their request. The existence of a public emergency should be determined or declared in accordance with Union or national law and based on the relevant procedures, including those of the relevant international organisations. In such cases, the public sector body should demonstrate that the data in scope of the request could not otherwise be obtained in a timely and effective manner and under equivalent conditions, for instance by way of the voluntary provision of data by another enterprise or the consultation of a public database.

(65)An exceptional need may also arise from non-emergency situations. In such cases, a public sector body, the Commission, the European Central Bank or a Union body should be allowed to request

light All Match Case Match Diacritics Whole Words 1 of 18 matches

We can get information from a company in case of a major CS incident. But what's the threshold? All incidents are unforeseeable!

① Ex: CS incident in the energy sector that can have cascade effects because energy provider is also providing to other sectors. What is happening? The info of the incident has arrived in the hands of public authority, and the CSIRT has decided that we have the need to understand the consequences of this incident. How far should I go? JMP 13

B2G data exchange

(29) ‘public emergency’ means an exceptional situation, limited in time, such as a public health emergency, an emergency resulting from natural disasters, a human-induced major disaster, **including a major cybersecurity incident,** negatively affecting the population of the Union or the whole or part of a Member State, with a risk of serious and lasting repercussions for living conditions or economic stability, financial stability, or the substantial and immediate degradation of economic assets in the Union or the relevant Member State and which is determined or officially declared in accordance with the relevant procedures under Union or national law;

Data Act and Cybersecurity

Example

A large healthcare provider is targeted by a cyberattack that happened through ransomware inside a DICOM file image of an MRI scan.

↳ standard file for medical purposes

The DICOM file infects the doctor's computer and then reaches the hospital's Picture Archiving and Communication System (PACS).

The ransomware proliferates to the whole hospital network shutting down all the operations and causing data and service unavailability.

Issue: is this public emergency?

Data Act and cybersecurity

Recital (64)

In the case of public emergencies, such as public health emergencies, emergencies resulting from natural disasters including those aggravated by climate change and environmental degradation, as well as human-induced major disasters, such as major cybersecurity incidents, the public interest resulting from the use of the data will outweigh the interests of the data holders to dispose freely of the data they hold. In such a case, data holders should be placed under an obligation to make the data available to public sector bodies, the Commission, the European Central Bank or Union bodies upon their request. The existence of a public emergency should be determined or declared in accordance with Union or national law and based on the relevant procedures, including those of the relevant international organisations. In such cases, the public sector body should demonstrate that the data in scope of the request could not otherwise be obtained in a timely and effective manner and under equivalent conditions, for instance by way of the voluntary provision of data by another enterprise or the consultation of a public database.

- When can a cybersecurity incident become a 'major' one?
  - Which are the criteria?
- Which data should be shared?

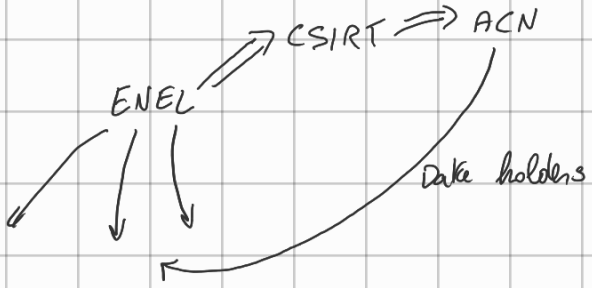
Data Act and cybersecurity

Article 17 Requests for data to be made available

- 1. When requesting data pursuant to Article 14, a public sector body, the Commission, the European Central Bank or a Union body shall:
  - (a) specify the data required, including the relevant metadata necessary to interpret and use those data;
  - (b) demonstrate that the conditions necessary for the existence of an exceptional need as referred to in Article 15 for the purpose of which the data are requested are met;
  - (c) explain the purpose of the request, the intended use of the data requested, including, where applicable, by a third party in accordance with paragraph 4 of this Article, the duration of that use, and, where relevant, how the processing of personal data is to address the exceptional need;
  - (d) specify, if possible, when the data are expected to be erased by all parties that have access to them;
  - (e) justify the choice of data holder to which the request is addressed;
  - (f) specify any other public sector bodies or the Commission, European Central Bank or Union bodies and the third parties with which the data requested is expected to be shared with;
  - (g) where personal data are requested, specify any technical and organisational measures necessary and proportionate to implement data protection principles and necessary safeguards, such as pseudonymisation, and whether anonymisation can be applied by the data holder before making the data available;
  - (h) state the legal provision allocating to the requesting public sector body, the Commission, the European Central Bank or the Union body the specific task carried out in the public interest relevant for requesting the data;
  - (i) specify the deadline by which the data are to be made available and the deadline referred to in Article 18(2) by which the data holder may decline or seek modification of the request;
  - (j) make its best efforts to avoid compliance with the data request resulting in the data holders' liability for infringement of Union or national law.

It's not easy to gather all those sorts of information and explain why I need data. Those guarantee are for the DH, that has tasked them org. on that data.

Plus, take the energy provider example: the DH to which we ask info is not necessarily the attacked entity.



How do I justify my requests? Not easy to put this process in practice but it is done to protect the data holder. Think about pandemic data. Data provision should be done securely and DH are responsible for the data. They need to assure that the DS are protected.

The framework protects users too for this.

Data Act and cybersecurity

Article 17 Requests for data to be made available

- 2. A request for data made pursuant to paragraph 1 of this Article shall:
  - (a) be made in writing and expressed in clear, concise and plain language understandable to the data holder;
  - (b) be specific regarding the type of data requested and correspond to data which the data holder has control over at the time of the request;
  - (c) be proportionate to the exceptional need and duly justified, regarding the granularity and volume of the data requested and frequency of access of the data requested;
  - (d) respect the legitimate aims of the data holder, committing to ensuring the protection of trade secrets in accordance with Article 19(3), and the cost and effort required to make the data available;
  - (e) concern non-personal data, and only if this is demonstrated to be insufficient to respond to the exceptional need to use data, in accordance with Article 15(1), point (a), request personal data in pseudonymised form and establish the technical and organisational measures that are to be taken to protect the data;
  - (f) inform the data holder of the penalties that are to be imposed pursuant to Article 40 by the competent authority designated pursuant to Article 37 in the event of non- compliance with the request; […]

Data Act and cybersecurity

Article 18 - Compliance with requests for data

1. A data holder receiving a request to make data available under this Chapter shall make the data available to the requesting public sector body, the Commission, the European Central Bank or a Union body **without undue delay, taking into account necessary technical, organisational and legal measures**.