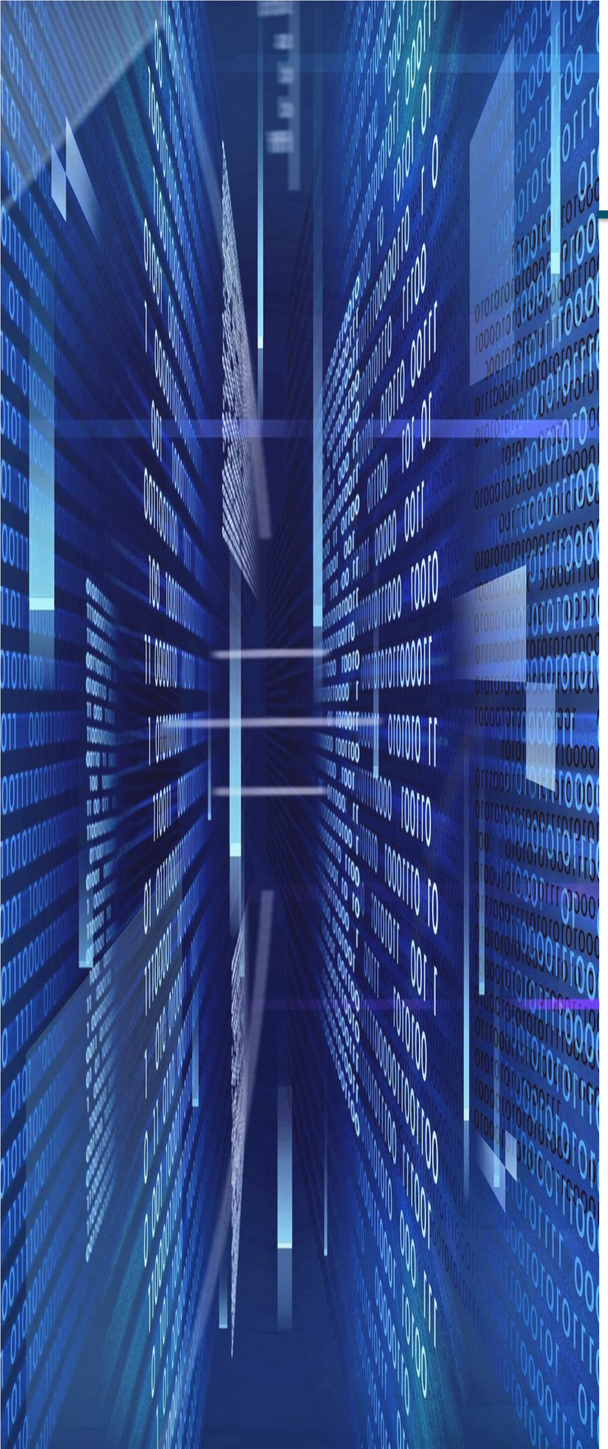


Introduction to Data Protection

Prof. Federica Paci

Lecture Outline

- The legal scene
- Who is who?
  - Data controller, data subject, data processors
- What is personal information?
- GDPR principles and obligations
- Data subjects' rights

Learning Outcomes

- At the end of this lecture you should be able to:
  - Provide a definition of data controller, data subject and data processor
  - Provide a definition of personal data
  - Understand the main data protection principles of GDPR


The legal scene

Starring: at EU level

P Dire ive 1995

EDPB

GDPR 2018

Ok, but what is personal data?

Personal Data

any information relating to an **identified** or **identifiable** natural person ('data subject');

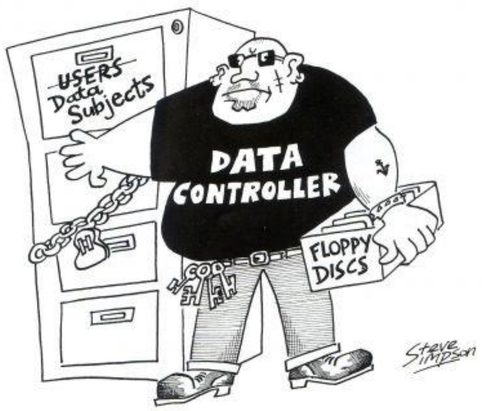
Ex: identification number, one or more factors specific to one’s physical, physiological, mental, economic, cultural or social identity

GDPR: genetic data, biometric data, location data

Who is who?

An identified or identifiable natural person whose personal data are being processed

Who is who?



The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the **purposes** and **means** of the processing of personal data

a natural or legal person, public authority, agency or other body which **processes** personal data on behalf of the controller

Who is who?

“A travel agency sends personal data of its customers to the airlines and a chain of hotels, with a view to making reservations for a travel package. The airline and the hotel confirm the availability of the seats and rooms requested. The travel agency issues the travel documents and vouchers for its customers”.

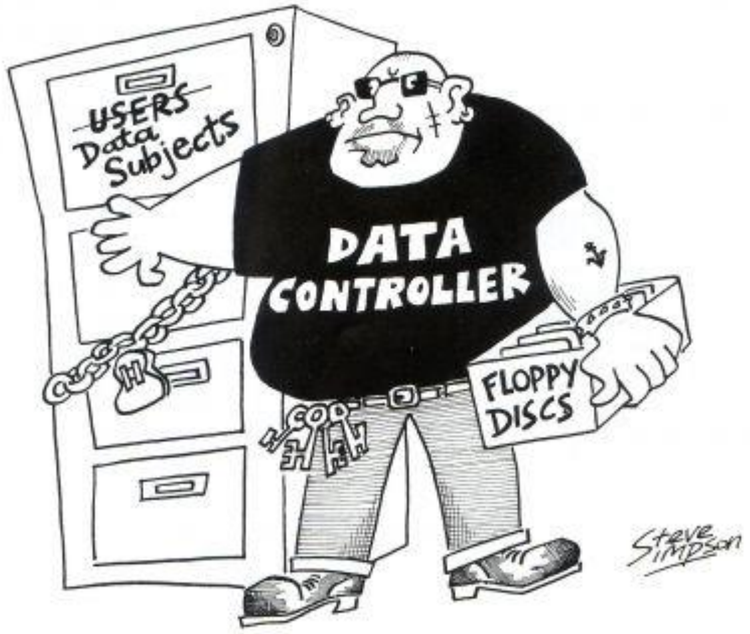
Who is the **data controller**?

“In case of doubt, other elements than the terms of a **contract** may be useful to find the controller, such as the degree of actual control exercised by a party, the image given to data subjects and reasonable expectations of data subjects on the basis of this visibility”. [2010]

Article 29 WP

“Social network service providers provide online communication platforms which enable individuals to publish and exchange information with other users. These **service providers are data controllers**, since they determine both the purposes and the means of the processing of such information. The **users** of such networks, uploading personal data also of third parties, **would qualify as controllers** provided that their activities are not subject to the so-called "household exception"”. [2010]

Article 29 WP



A data controller will have a certain number of obligations

As well as his data processor

3. You shall only collect the data that are necessary to pursue this purpose

4. You shall keep the data for non longer than necessary

5. You shall only keep accurate data

6. You shall keep the data secure

2. You shall process the data for a specified/specific and limited purpose

7. You shall enable data subjects to exercise their rights

1. You shall have a legal basis to process the data

8. You should maintain a record of processing activities

Lawfulness

- Data controllers need to have a lawful basis
- Six possible lawful bases:

1. **Consent:** the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
2. **Contract:** 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;
3. **Legal obligation:** processing is necessary for compliance with a legal obligation to which the controller is subject;
4. **Vital Interest:** processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. **Public interest**: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. **Legitimate interest:** 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.

Consent

Consent of the data subject means any **freely given, specific, informed and unambiguous indication** of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

- **Freely given:** should not generally be a precondition of signing up to a service
- **Specific:** ask consent for each processing purpose and activities
- **Informed:** explain in a clear and concise language
  - the name of the data controller;
  - the name of any third party controllers who will rely on the consent;
  - Purpose(s) for processing
  - Any processing activities
  - Inform individuals can withdraw consent at any time
- **Unambiguous indication** Silence, pre-ticked boxes or inactivity should not constitute consent

Purpose limitation

- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Data controllers have to:
  - specify purposes in privacy information for individuals
  - specify purpose or purposes for processing personal data within the records of processing
  - not process data for purposes incompatible with the initial purposes
- Compatible purpose are archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Data minimization

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Data controllers must ensure the personal data they are processing is:

- adequate – sufficient to properly fulfil the stated purpose;
- **relevant** – has a rational link to that purpose; and
- **limited** to what is necessary – you do not hold more than you need for that purpose.

Accuracy

Personal data shall be **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

Storage Limitation

- Personal data shall be 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

Security

- Personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Accountability

- Data controllers must be able to demonstrate their compliance with GDPR obligations
- They need to put in place appropriate technical and organizational measures to meet the requirements of accountability

The measures include:

- adopting and implementing data protection policies;
- taking a ‘data protection by design and default’ approach;
- putting written contracts in place with organizations that process personal data on your behalf;
- maintaining documentation of the processing activities;
- implementing appropriate security measures;
- recording and, where necessary, reporting personal data breaches;
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals’ interests;
- appointing a data protection officer

A data subject will have a certain number of rights

1. You have a right to be informed (e.g. purpose of the processing)

2. You have a right to access data relating to you

3. You have the right to have the data rectified

4. You have the right to have the data erased if the processing is not legally compliant

5. You have a right to object to certain processing when not based on consent

6. You have a right not to be subject to purely automated decision-making

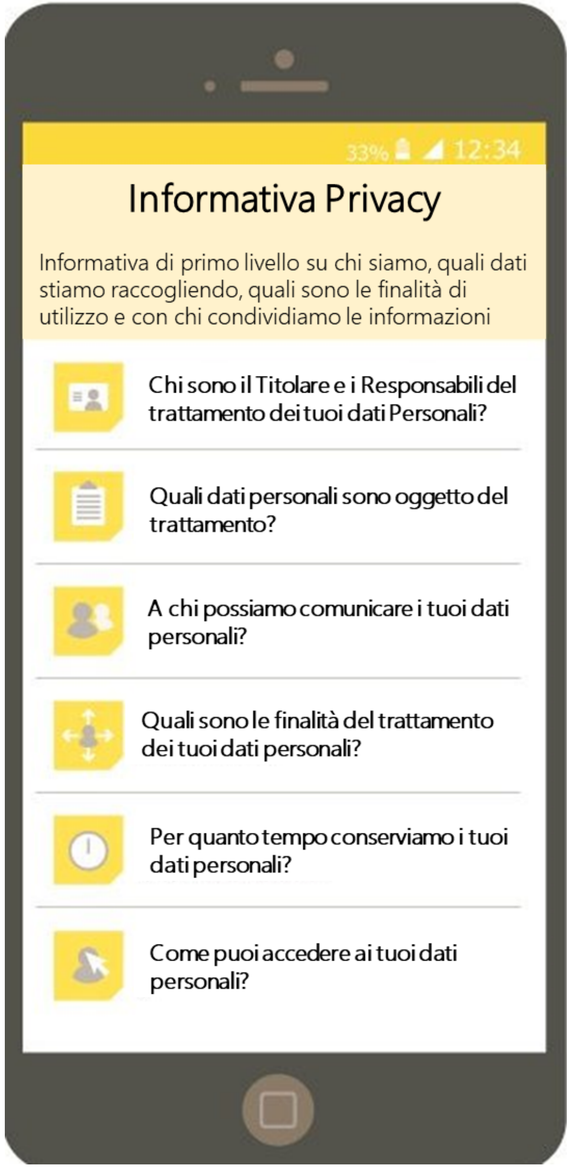
8. You have a right to data portability

Privacy Notices

- Data controllers must tell individuals about their processing in a way that is easily accessible and easy to understand. They must use a clear and plain language
- When data are collected, data controllers must provide a privacy notice:
  - The name and contact details of the organization
  - The purpose for processing
  - The lawful basis for processing
  - The categories of personal data obtained
  - The recipients or categories of recipients of the personal data
  - the details of transfers of the personal data to any third countries or international organizations
  - The retention periods for the personal data
  - The rights available to individuals in respect of the processing

Examples of Privacy Notices

Informativa privacy sintetica		
Ambito	**Informazioni di base**	
TITOLARE DEL TRATTAMENTO (chi decide perché e come i tuoi dati sono trattati)	**VDT Farmaceutica S.p.A.**	*+info*
FINALITA' (qual è lo scopo di trattamento dei dati)	a) **Informazione medico-scientifica** (presentazione medicinali, raccolta richieste campioni,…)	*+info*
	b) **Classificazione e Segmentazione** Attività finalizzate a rendere più efficace l'attività di informazione	*+info*
	c) **Profilazione** Analisi automatizzate di caratteristiche e comportamenti dell'individuo per determinare specifici "profili"	*+info*
LEGITTIMAZIONE (qual è la base legale per il trattamento dei dati)	a) **Informazione medico-scientifica** Consenso dell'interessato	*+info*
	b) **Marketing:** consenso dell'interessato	*+info*
	c) **Profilazione:** consenso dell'interessato	
DESTINATARI (a chi sono comunicati i dati)	I dati non sono diffusi a terzi indeterminati, ma comunicati a specifiche categorie di destinatari, tra cui: - Rete di informatori scientifici del farmaco - Personale interno incaricato del trattamento - Società terze che svolgono attività per conto del Titolare - Società del Gruppo VDT - I dati non saranno ceduti a terz.	*+info*
	Trasferimenti fuori UE: I dati possono essere trasferiti fuori UE nel rispetto della vigente normativa.	*+info*
DIRITTI (quali sono i diritti da esercitare)	accedere, aggiornare, integrare, rettificare, cancellare i dati, chiederne il blocco, opporsi al trattamento, proporre reclamo al Garante Privacy, richiedere la portabilità dei dati (a far data dal 25 Maggio 2018)	*+info*
FONTE DEI DATI (qual è l'origine dei dati trattati)	I dati sono raccolti direttamente presso l'interessato o anche mediante la consultazione di banche dati	*+info*
INFORMAZIONI AGGIUNTIVE	L'informativa completa e altre informazioni sul trattamento dei dati personali sono disponibili nella sezione Privacy del sito www.farmaceuticavdt.it.	*+info*



Reporting Violations

- The GDPR introduces a duty on all organizations to report certain personal data breaches to the relevant supervisory authority. The must do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, They must also inform those individuals without undue delay.
- They should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not they need to notify the relevant supervisory authority or the affected individuals, or both.
- They must also keep a record of any personal data breaches, regardless of whether you are required to notify.

GDPR Fines

- Two levels of fines
- The less severe infringements could result in a fine of up to €10 million, or 2% of the firm’s worldwide annual revenue
- Examples of less severe infringements
  - Fail to report a data breach to the data protection authority
  - Do not appoint a Data Protection Officer
- Severe infringements could result in a fine of up to €20 million, or 4% of the firm’s worldwide annual revenue
- Examples of severe infringements
  - Violation of data protection principles
  - Violation of data subjects' rights
  - Transfer of personal data to international organizations or third party contry

Recommended Readings

- **Guida all´applicazione del Regolamento europeo in materia di protezione dei dati personali.** https://www.garanteprivacy.it/regolamentoue/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali/