UNIVERSITY OF PADOVA
DEPARTMENT OF INFORMATION ENGINEERING

Biomedical Wearable Technologies
for Healthcare and Wellbeing

Regulation on data protection

A.Y. 2023-2024

Giacomo Cappon

DEPARTMENT OF
INFORMATION
ENGINEERING
UNIVERSITY OF PADOVA

Privacy

- **Privacy**: the right to a private life, to be autonomous, in control of information about yourself, to be let alone.

- Almost every country in the world recognises privacy in some way.

- Privacy recognised as a universal human right.
  - Universal Declaration of Human Rights (Article 12)
  - European Convention of Human Rights (Article 8)
  - European Charter of Fundamental Rights (Article 7).

Data protection

- The European Charter of Fundamental Rights (Article 8) contains an explicit right to the **protection of personal data**.

- **Data protection** → ensure the fair processing (collection, use, storage) of personal data by public and private sectors.

- **Personal data:** any information related to an identified or identifiable natural (living) person
  - Identifiable natural person: one who can be identified, directly or indirectly, by an identifier such as a name, an identification number, location data, etc.

- Examples of personal data:
  - Names, dates of birth, photographs, email addresses and telephone numbers
  - IP addresses and communication content related to or provided by end-users of communications services

General Data Protection Regulation (GDPR)

- New regulation for data protection adopted by the EU in 2016.
- GDPR is the most comprehensive and progressive data protection regulation worldwide.
- Many global laws are strongly influenced by the EU rules, which are considered the gold standard in data protection law.
- Each EU member state adopted a national regulation on data protection that is compliant with the GDPR.
  - Italian law: **DECRETO LEGISLATIVO 10 agosto 2018, n. 101**. Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
- The GDPR also applies to entities not established in the EU who offer goods and services to individuals in the EU or monitor their behaviour.

GDPR

- The GDPR substituted the **1995 Data Protection Directive,** adopted when there was no massive use of the Internet.

- Over the last 25 years, technology has transformed our lives in ways nobody could have imagined so a review of the rules was needed.

- The GDPR reinforces a wide range of existing rights and establishes new ones
  - Example: the right to erasure (right to be forgotten) → You can request at any time that an organisation delete all your personal data

Living and dead individuals

- The GDPR only applies to the personal data related to an **identifiable living individual.**
- Information relating to a dead person is not subject to the GDPR.
- Single member states are allowed to define their own rules for the protection of dead people.
- Italy has extended the application of the GDPR to dead people with the regulation Decreto Legislativo 101/2018.

Data subject, controller, processor, and Recipient

- **Data subject:** the person whose personal data are collected, held or processed.
- **Data controller**: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
  - It is the official responsible for data protection.
  - The actual processing may be delegated to another party, called the data processor.
- **Data processor**: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
  - The processor only acts "on behalf of the controller" subject to his instructions.
  - The processor may have recourse to a **subcontractor** who processes the data on his behalf.
- **Recipient**: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed.

Data protection officer (DPO)

- **Data protection officer (DPO):** expert in data protection regulation and practices.

- The controller and the processor shall designate a DPO if:
  - the processing is carried out by a public authority or body;
  - regular and systematic monitoring of data subjects on a large scale;
  - processing on a large scale of the special categories of data.

- Tasks of the DPO:
  - to inform and advise the controller or the processor of their obligations according to the GDPR
  - to monitor the compliance with GDPR
  - to provide advice as regards the data protection
  - to cooperate with data protection authorities
  - to act a contact point between the controller, the processor and the data protection authorities.

Data protection authorities

- National **Data Protection Authorities (DPAs)** or Regulators have been established to be the guardians of data protection.
  - The Italian one is: **Garante per la protezione dei dati personali** (**http://www.garanteprivacy.it/**)

- DPAs have the power to investigate, detect and punish violations of data protection rights and obligations.

- In the EU, DPAs must be **independent of any political, governmental or other influence**.

- **European Data Protection Supervisor (EDPS):** independent supervisory authority responsible for ensuring that EU institutions and bodies comply with data protection law when processing personal data.

Restrictions to the application of GDPR

- In the EU, privacy and data protection are **not absolute rights** and can be limited under certain conditions according to the EU Charter of Fundamental Rights.

- Need to balance the rights to privacy against other EU values, human rights (e.g., right to freedom of expression), public and private interests (e.g., right to freedom of press), and national security.
  - GDPR not applicable if data are used for the purposes of prevention, investigation, detection or prosecution of criminal offences.

- DPAs ensure the balance between privacy and other interests.

Pseudonymised and anonymised data

- **Pseudonymisation:** a technique that replaces or removes information that identifies an individual.
- GDPR definition: *"…the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."*

- Example of pseudonymisation: replacing names and other identifying attributes with a unique identifier.
  - The data controller can still match the unique identifier to the individual having access to relevant additional information.
  - Technical measures must be used to ensure that this additional information is held separately and no one apart the authorized people can retrieve it.

- Pseudonymisation help protecting the privacy of subjects' identity.

- **Remember**: Pseudonymised data are still personal data → subject to GDPR.

Pseudonymised and anonymised data

- **Anonymisation:** a technique that eliminates all the information that identifies an individual.

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

- If at any point we realise that some information allows to re-identify individuals, data should be considered as pseudonymised.

- **Remember**: The GDPR does not apply to personal data that has been anonymised.

GDPR: seven main principles

1. **Lawfulness, fairness and transparency**: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
   - Identify valid grounds under GDPR (known as a 'lawful basis') for collecting and using personal data.

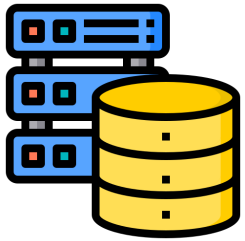
2. **Purpose limitation**: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
   - Purposes for processing must be clear from the start
   - Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are not considered to be incompatible with the initial purposes

GDPR: seven main principles

3. **Data minimisation**: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. **Accuracy**: personal data must be accurate and, where necessary, kept up to date.
   - Personal data that are inaccurate must be erased or rectified without delay.

5. **Storage limitation**: personal data shall be stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed.
   - Personal data may be stored for longer periods only if they are processed for archiving purposes in the public interest, scientific/historical research purposes or statistical purposes.



GDPR: seven main principles

6. **Integrity and confidentiality**: appropriate security of the personal data must be ensured using appropriate technical security measures.
   - Protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

7. **Accountability**: The controller shall be responsible for, and be able to demonstrate compliance with the principles of the GDPR.

Data subjects rights under GDPR

- **The right to be informed**
  - Right to be informed about the collection and use of their personal data.
- **The right of access**
  - Right to access and receive a copy of their personal data, and other supplementary information, including the purpose and period of processing.
- **The right to rectification**
  - Right to have inaccurate personal data rectified or completed.
- **The right to erasure (‘right to be forgotten’)**
  - Right to have personal data erased.
- **The right to object**
  - Right to object to the processing of personal data in certain circumstances.

Data subjects rights under GDPR

- **The right to restrict processing**
  - Right to request the restriction or suppression of their personal data. When processing is restricted, the controller can store the data, but not use it.

- **The right to data portability**
  - Right to move, copy or transfer personal data easily to another controller.

- Rights not to be subject to **automated decision making and profiling**.
  - Right not to be subject to a decision based solely on automated processing, including profiling, which significantly affects him or her.
  - **Profiling**: use of personal data to evaluate or predict certain personal aspects relating to a person, e.g., performance at work, economic situation, health, personal preferences, interests, position…

Data protection by design and by default

- **Data protection by design**:
  - The controller shall implement appropriate technical and organisational measures, e.g., pseudonymisation, which are designed to implement data-protection principles, in an effective manner.

- **Data protection by default**:
  - 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.

Security measures

- Techniques for the **pseudonymisation** and **encryption** of personal data

- Techniques to ensure confidentiality, integrity, availability and resilience of processing systems and services

- Techniques to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- Techniques for regularly testing, assessing and evaluating the effectiveness of security measures

Lawful basis for data processing under GDPR

- The processing of personal data is lawful if at least one of the following applies:
  - **Consent**: the data subject has given clear consent for processing his or her personal data for a specific purpose.
  - **Contract**: the processing is necessary for a contract you have with the individual.
  - **Legal obligation**: the processing is necessary to comply with a legal obligation to which the controller is subject.
  - **Vital interests**: the processing is necessary to protect someone's life.
  - **Public task**: the processing is necessary for performing a task in the public interest.
  - **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

- Data controllers and processors are required to provide information about the lawful basis for processing usually through a privacy notice.

Consent

- Lawful basis based on consent → the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

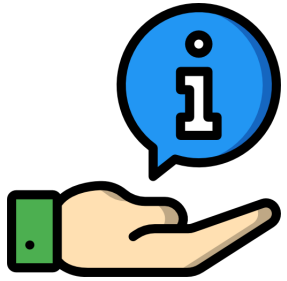
- **Consent:** any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he/she agrees to the processing of his/her personal data.

- The **request for consent** must be clear and presented using plain language.

- The data subject has the **right to withdraw** his or her consent at any time.

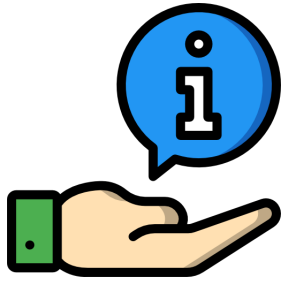
- Withdrawing the consent should be as easy as giving the consent.

Information to be provided before personal data collection



- The **identity and the contact details of the controller**
- The contact details of the **data protection officer** (if applicable)
- The **categories of personal data** concerned
- The **purposes of the processing** and the **legal basis** for the processing
- The **recipients** of the personal data, if any
- If applicable, intention to **transfer** personal data to a third country or international organisation and the existence/absence of an adequacy decision by the European Commission.
- The **period** for which the personal data will be stored, or the criteria used to determine that period.

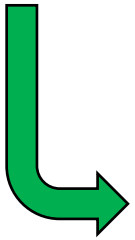
Information to be provided before personal data collection



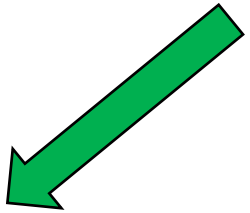
- The existence of the **right to request:**
  - **access** to the personal data
  - **rectification** of the personal data
  - **erasure** of personal data
  - **restriction of processing** of personal data
- The **right to withdraw** consent at any time
- The **right to raise a complaint** with a supervisory authority
- If the provision of personal data is a contractual requirement, the possible **consequences of failure to provide such data**
- The existence of **automated decision-making, including profiling**, and information about the logic involved and the consequences of such profiling

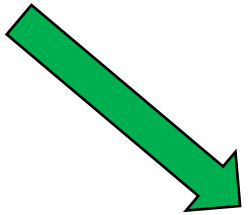
Example: Informed consent form for participating in a research trial

- Planning a research trial in which you collect some personal data.



  - Each participant must provide an explicit consent by which they agree with you processing their data for the purpose of the research.





  - **Information sheet**: document to share the information of the research trial.
  - **Consent form**: form by which the subject provides the consent and agree to participate in the study.

Example of an information sheet template

INFORMATION SHEET FOR STUDY PARTICIPANTS

Study Title: .....

Sponsor's Protocol Code: .....

Sponsor: .....

Research Center: .....

Principal Investigator in the Center: .....

This information sheet is to inform you about a research study that we invite you to participate in. This study has been approved by the Ethics Committee *<PLEASE INCLUDE REFERENCE AND DATE)>*. Before you decide whether you can take part, we would like to explain what is involved in this study and what your participation means. Please, take your time to read the information sheet and ask any questions that may arise.

Why are we doing this study?

< STUDY PURPOSES/FUTURE PURPOSES (if any)>

Why have I been asked to take part?

< ADD INCLUSION CRITERIA>

What will happen if I decide not to take part?

< EXPLAIN VOLUNTARY PARTICIPATION AND NO IMPACT ON DISEASE CARE>

What will we need to do if you take part?

< INCLUDE DETAILS ON DATA TO BE COLLECTED AND, THE STUDY PROCEDURES FOR THE COLLECTION>

What are the possible benefits and disadvantages of taking part?

< INCLUDE DETAILS ON THE BENEFITS AND RISKS, if any>.

More information about taking part

Subject Confidentiality

<INCLUDE COMPLIANCE WITH EXPLICIT DATA PROTECTION LAWS (GDRP)>.

< INCLUDE OTHER PEOPLE HAVING ACCESS TO DATA>

< INCLUDE DETAILS OF THE STORAGE PERIOD AND THE STORAGE LOCATION>.

< INCLUDE DETAILS ON THE FURTHER USE OF ANONYMIZED DATA AND SAMPLES AFTER THE END OF THE PROJECT, IF APPLICABLE>.

< INCLUDE DETAILS ON DATA AND SAMPLE TRANSFER AND THE SAFEGUARDES MEASURES ADOPTED, IF ANY>.

< DESCRIBE THE RIGHTS OF THE PARTICIPANT>

< INCLUDE NAME AND CONTACT DETAILS OF THE DATA CONTROLLER>.

< INCLUDE NAME AND CONTACT DETAILS OF THE DATA PROTECTION OFFICER, if applicable>

What will happen in case of incidental findings that might be relevant for study participants' health status?

< DESCRIBE WHAT WILL HAPPEN IN CASE OF INCIDENTAL FINDINGS>.

What will be done with the results?

<INCLUDE INFORMATION ABOUT THE PUBLICATION OF THE ANONYMIZED DATA AND THE RESULTS OF THE STUDY, IF APPLICABLE>.

Who is organizing this research?

<NAME OF THE SPONSOR>

Dr. _____ (center IP)

Hospital _____

Department of _____

Address_____

Example of a consent form template

CONSENT FOR STUDY PARTICIPANTS

Study Title: .....

Sponsor's Protocol Code: .....

Sponsor: .....

Research Center: .....

Code of Patient: .....

I, **(name and surname)** .....

PART I – CONSENT TO THE RESEARCH:

- ☐ have read and understood the information sheet (version ..., date....) provided relating the study *<PLEASE INSERT STUDY TITLE>* and have received a copy of this document.
- ☐ have been able to ask questions which have been answered fully.
- ☐ understand that my participation is voluntary and I am free to withdraw, without giving any reason and my care will not be affected in any way.
- ☐ have had enough time to fully consider my participation in the study.
- ☐ want to be informed of the overall study results at the end of the project.
- ☐ give permission to be informed of incidental findings that might be relevant for my health status.

PART II – CONSENT TO THE DATA PROCESSING:

- ☐ understand that my clinical information may be reviewed by properly authorized individuals as part of the study and that such information will be treated as strictly confidential.
- ☐ am aware of the type of data and samples that will be collected.
- ☐ give permission for using of the samples and data for the study purposes stated in the information sheet.
- ☐ am aware that the persons stated in the information sheet, bound by professional secrecy, will have the authority to access my study data and medical records.
- ☐ agree that anonymised study data will be communicated or published in specialized reports.
- ☐ give permission for storage of the study data and samples until <ENTER DATE>.
- ☐ am aware of the identity of the data controller and of the data protection officer.
- ☐ am aware of the transfer of data from <please include the provider country> to <please include the recipient country>.
- ☐ am aware that I have the right to request access to and rectification or erasure of my personal data or restriction of processing concerning personal data or to object to processing as well as the right to data portability.
- ☐ am aware that if I withdraw from the study, samples will be destroyed and data already collected will be anonymised and may be processed by authorised researchers.

I give consent to the participation in this research study

_____	_____	_____
Name of Study Participant	**Date**	**Signature**

(Please write in capital letters)

I declare that I have fully informed above mentioned participant about this research study. If during the study new information becomes available that could influence the consent of the participant or can help to provide new treatment or healthcare, I will immediately inform them.

_____	_____	_____
Name of Researcher	**Date**	**Signature**

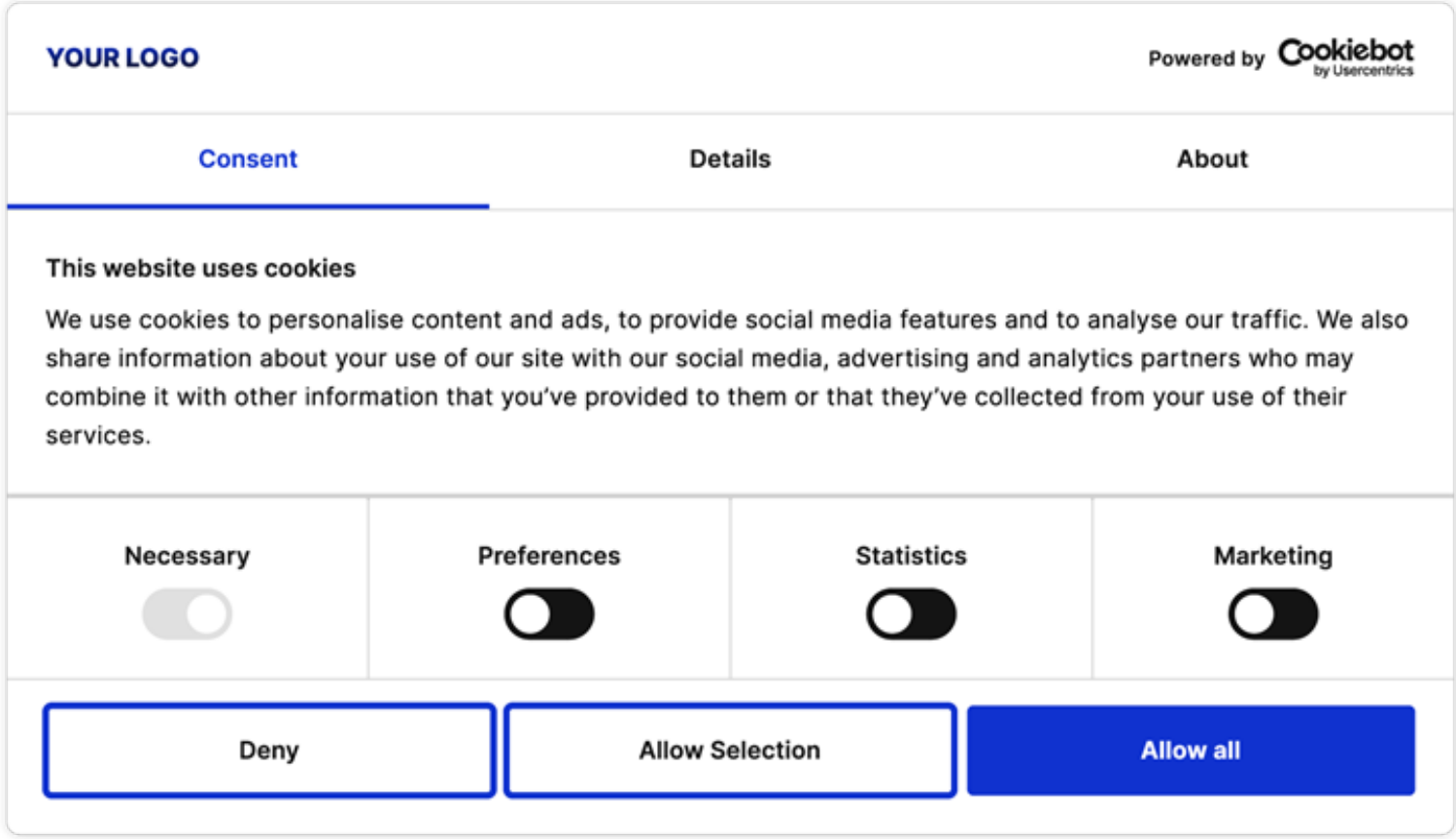
(Please write in capital letters)

One copy to study participant, one to case notes, one to study file.

Websites using cookies and GDPR

- **HTTP cookies:** small blocks of data created by a Web server while a user is browsing a website, needed for some crucial functions of browsers (e.g., to track the session state).
-
- Cookies can store enough data to **potentially identify the user** without his/her consent.
  - Used by advertisers to track users' online activity so that they can target them with highly specific advertisements.
  - They can be considered personal data subject to GDPR!
- **Compliance with the GDPR** imposes that Web servers using cookies must:
  - receive users' consent before using any cookies except those that are strictly necessary;
  - provide accurate and specific information about the data each cookie tracks and its purpose in plain language before consent is received;
  - document and store user consent;
  - allow users to access the service even if they refuse the use of certain cookies;
  - allow easy withdrawal of consent.

Example of an informed consent form for the use of cookies



Special categories of personal data (Art 9)

Personal data revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- data concerning physical or mental health
- data concerning sexual life or sexual orientation
- genetic data or biometric data (physical, physiological or behavioural characteristics which allow or confirm the unique identification of a person

The processing of these kind of data **shall be prohibited**.

Conditions for use of special categories of personal data

Exceptions in which special personal data can be processed:

- the data subject gives explicit **consent** to the processing of those personal data;
- processing is necessary for carrying out the **obligations** and exercising specific rights of the controller or of the data subject;
- processing is necessary to protect the **vital interests** of the data subject or of another person and the data subject is physically or legally incapable of giving consent;
- processing is done within an organization for **legitimate purposes**, solely for members of the organization, and data are not disclosed outside the organization without the consent of the data subject;
- the personal data are manifestly made **public** by the data subject;
- …

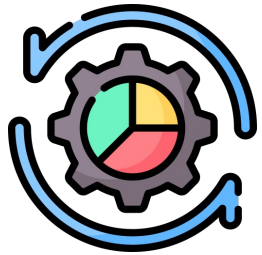
Conditions for use of special categories of personal data

- …
- processing is necessary for the establishment, exercise or defence of **legal claims**;
- processing is necessary for reasons of **public interest**;
- processing is necessary for the purposes of preventive or occupational **medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems;
- processing is necessary for reasons of **public health**, such as protecting against serious cross-border threats to health;
- processing is necessary for archiving purposes in the public interest, **scientific** or historical research purposes or statistical purpose.

Records of processing activities

Each **controller** shall maintain a **record of processing activities** under its responsibility. The record shall contain these information:

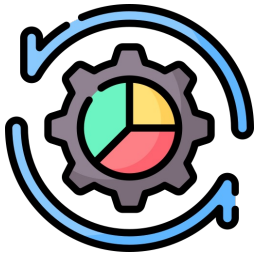
- name and contact details of the controller;
- purpose of processing;
- the categories of data subjects and the categories of personal data;
- the categories of recipients to whom the personal data are disclosed;
- where applicable, transfers of personal data to a third country;
- where possible, time limits for erasure of the different categories of data;
- where possible, a description of the security measures adopted.



Records of processing activities

Each **processor** shall maintain a **record of processing activities** carried out on behalf of the controller. The record shall contain these information:

- name and contact details of the processor and of the controller;
- the categories of processing carried out;
- where applicable, transfers of personal data to a third country;
- where possible, a general description of the security measures adopted.



Secondary use of the personal data

- **Secondary use of the personal data**: the controller intends to further process the personal data for a purpose other than that for which the personal data were collected

- Prior to that further processing, the controller shall provide the data subject with **information on that other purpose** and any relevant further information.