European Commission

Ethical Review in FP7

Data protection and privacy ethical guidelines

This document was produced on September the 18th 2009

Experts Working Group on data protection and privacy
Chaired by: Caroline Gans-Combe

Special thanks to the Panel Members: Andrew Bottomley, Duarte Carvalho-Oliveira, Costas A. Charitidis, Eva Del Hoyo-Barbolla, Anne Demoisy, Anna Giovanetti, Walter Hannak, James Houghton, David Morton, François Moutou , Jane Lamprill, Antony Lebeau, David Townend, and Mary Sharp.

-

Very special thanks to the Ethics Team : Isidoros Karatzas, Mihalis Kritikos, Yamina Cheikh, Paulette Matkovic Ramirez, Marie Cocquyt, Marco Michelini, Stefan De Vos and François Hirsch

General disclaimer: this document examines the major concepts of data protection and privacy from the point of view of research ethics. It aims at raising awareness about these concepts in the scientific community and at assisting applicants while preparing to submit their project proposals. It does not seek to discuss these concepts in-depth but provides a general overview of their main parameters and some basic suggestions regarding their handling for the purposes of the European Commission's Ethical Review procedure. This document represents an effort to reflect on the experience gained during the operation of the Ethics Review mechanism and to provide some practical guidance, thus it will be regularly updated.

The document contains three sections:

→ 1. The first section consists of an **awareness list** which contains the main questions that need to be taken into account by applicants when dealing with the data protection and privacy aspects of their project - **All relevant definitions are provided within the glossary below**

→2. The second section provides applicants with practical guidance for the identification of the privacy and data protection aspects of their research proposal. It suggests how such issues need to be dealt with in each section of the "Ethical Issues Table" along with a description of the measures that need to be taken in order to comply with the relevant EU rules.

→ the third section includes a **glossary** that defines the major concepts that surround the discussion and application of data protection and privacy rules from an ethical point of view.

Table of Contents

1 - Awareness list:

10 questions that need to be answered on data protection and privacy issues

All relevant definitions are provided within the glossary below

1 – Will any type of personal data be used and/or stored within the framework of the research?

If Yes – Applicants should move to question 2 and the relevant boxes in the Ethical Issues Table need to be ticked.

2 - What kind of human participants/data are involved within the research?

2.1 - categories of human participants

- Patients
- Healthy volunteers (related to health research)
- Volunteers (for surveys, etc…)
- Workers' (e.g.: research lab personnel…)
- Participating researchers' list
- Children
- Vulnerable adults
- Others…..special population groups? Developing countries? etc.

2.2 - categories of data used

- Previously collected data (their sources and usage history)

The content of the data set needs to be specified and copies of appropriate authorizations need to be provided according to the legal requirements of the area where the research is planned to take place.

3 – Are all sensitive data that are planned to be collected really focused on the research question and is relevant for the foreseeable research?

Applicants will need to explain the reasons behind the proposed data collection: Data from different sources should not be amalgamated without making sure that this action is legally possible, especially in cases where a data set might contain information that identifies individuals and information

4 – For how long will the collected data be used?

Usage times need to be specified. On a general point of view, data must be specifically stored solely for as long as the project lasts. Data usage beyond the life of the project is possible but must be closely supervised.

5 – For how long will the collected data be stored and when will it be irreversibly destroyed?

Conservation times need to be specified. Destruction methods need to be illustrated. The costs for both options need to be taken into account when estimating the project's final budget.

6 – Do the applicants have the necessary legal permission to obtain and process the data?

If data are directly gathered from individual study participants, is the planned informed consent system effective?

Informed consent for the proposed project will be required, even if personal data has been collected in the frame of previous research projects: If data from a previously gathered set - either by the applicant or from another project or person – are used, does the initial informed consent cover this complementary use of the data, or does the applicant have to obtain a completely new informed consent for the proposed study The applicants need to discuss these options along with their national/local data protection agency.

7 - How will the collected personal data be securely accessed?

Secured access policy needs to be worked out and clearly specified. It needs to be proportional to the risks involved and the sensitivity of the data, and must clearly state the type of processes - such as password protection, encryption, "need to know basis" principles (i.e. : only the users that need to access the data will be allowed to do so),- that will be implemented. (See glossary for a description of the different means)

8 – How will the data be securely stored: data structure and format?

Data structures such as databases need to be specified - if applicable, it should be specified that identification data will be encrypted and strictly separated from sensitive data such as health data (see glossary) – It should also be specified how the unforeseen data added during the research such as incidental findings will be treated.

9 – How will the data be securely stored: location & hardware?

Conservation methods need to be specified. A non-WAN connected computer server or HARD disk should be preferred. Data should not be stored on a memory stick or other easily lost/accessed media.

10 – How will data transfer be monitored?

Transfer of data outside the EU needs to be identified and specified. The handling process should be specified. Data transfer (between whom and whom) within the project, especially with partners from non-EU countries (developed and/or developing countries) must be given special care due to the variety of legal and administrative standards, bearing into mind that compliance with the relevant EU rules and international/bilateral agreements incorporated into EU law is compulsory. This is because EU legislation requires that the transfer of data outside Europe to be undertaken only to places where there is a local assurance by the proper legal authorities that the level of data protection is at least equivalent to that of the EU area. Applicants need to consider this aspect not only between institutions and companies and the like, but also within companies and the research partnership across geographical borders.

2 - Data protection and privacy in FP7 research proposals

The purpose of this document is to guide applicants:

-in identifying privacy and data protection issues within their proposal;

-in explaining, in the ethics section of the application, how such issues ought to be dealt with within each section of the “Ethical Issues Table” and

-in describing the different measures that might be taken in order to comply with the relevant EU rules including the rules of submission, annex A;

While preparing a proposal, applicants must complete the project’s “Ethical Issues Table”. Depending on the specificities of the program/call for proposals, “privacy and data protection” appear such as

- Privacy
- Consent
- Dual Use
- Research involving developing countries

2.1 - How can the applicant identify the ethical aspects of the privacy and data protection issues within the proposed research?

2.1.1 – Data protection, privacy and legal framework

On the whole, the way data protection and privacy issues are taken into account and formally treated fundamentally depends on the legal environment of each country where the research will take place. However, despite the various differences across the EU, the application of Directive 95/46/EC (Data Protection Directive) guarantees a uniform approach towards these issues. For a detailed picture of the relevant legal framework, see:

http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm**.**

Each – electronic or not – use of data in the frame of the proposed research should comply with the following requirements:

(1) Applicants need to identify the appropriate/competent data protection authority that will provide the relevant authorizations (also when the proposed research is planned to take place in developing countries) and the particular applicable local/national legal requirements on data protection and privacy issues;

(2) Depending on the legal environment, applicants need to provide the appropriate authority with a detailed description of the proposed data collection (and their usage) and the methodology that will be employed for collecting, using and storing of personal data. More information on the relevant institutional contact points (such as the national and local competent authorities) regarding these specific rules is available in the following address:

http://ec.europa.eu/justice_home/fsj/privacy/

Applicants are reminded that compliance with EU rules on data protection and privacy issues is compulsory when applying for EU research funding. In case of non-compliance, applicants incur significant risk (e.g. legal sanction and ethical ramifications such as peer-review difficulties).

2.1.2 - Privacy and research in FP7

Privacy issues arise when data are collected and stored. The handling of digital personal data is of major concern because of the processing possibilities and the potential to link vast amounts of personal data.

This information can be provided from a variety of sources and in various formats such as:

1. Health related records (e.g. patient records, hospital information records, biological traits and genetic material);

2. Criminal records or legal justice investigations and proceedings;

3. State related records, e.g. tax filings;

4. Circulation/travel records such as visas;

5. Residence or various geographic recordings, e.g. GPS localization recordings;

6. Bank records, financial transactions records;

7. Ethnic, religious, dietary or sexual life style identification records;

8. Individual (or collective) day-to-day behaviour studies;

On the whole, privacy concerns any data which, either alone or when linked to other, relate to an identifiable individual or individuals. There is a reasonableness test involved in the linking of data as any data could potentially be linked together to identify an individual. If such information is collected, then the data is subject to the relevant EU data protection standards.

Furthermore, applicants should ask themselves about whether the data, which is planned to be collected within the research project- really, needed for the proper completion of the research. The collection and use of ID & more generally private information must be reduced to a minimum on a “need to use basis” in order to ensure participant safety, an interpretation of results, a treatment of incidental findings and a strict protection of the participant’s data.

2 .1.3 - Informed consent in FP7 research projects

2.1.3.1 – Privacy and informed consent

By signing informed consent documents, research participants agree to a controlled breach of their privacy for a specific purpose and a specific period of time. In case an individual does not agree with such a temporary breach, he/she retains the right to withdraw.

Individuals need to be aware of the:

1. *methods used for handling personal data*
2. *justification for requesting/obtaining their data;*
3. *duration of data use and storage);*
4. *guarantees concerning the rightful use of data;*

Therefore, any research action that might impede privacy requires informed consent.

This means, that, in the Ethical Issues Table if the applicant ticks one of the two privacy topics, the "informed consent" section also needs to be ticked.

2 .1.3.2 - Informed consent is not just about patients.

From a data protection and privacy issues point of view, all study participants present in a research project need to be informed about the planned research use of the collected data independently of the type of data collected. Thus, if a consumer survey is planned within a project, participants to the survey need not only to be informed of how their personal data is planned to be handled, but also to provide appropriate authorisation. Furthermore, the design of the survey must guarantee that only data specifically required for the purposes of the research project will be gathered (unless clearly stated otherwise).

2.1.3.3 – Informed consent processes

Further information on informed consent can be found in the **glossary** below and within the FP7 Ethical Guidelines on the Cordis website: http://cordis.europa.eu/fp7/ethics_en.html

The main aspects of 'Informed consent are the following:'

1. **The potential participant must be given sufficient information in order to be able to make a choice of whether or not to participate that is based on an understanding of the risks and alternatives in an environment, which is free from any coercion;**

2. **The decision of the potential participant on the consent issue must be evidenced. The participant needs to agree that her/his data will be used for a specific research scope and is aware of the meaning of such use;**

When writing a research proposal, applicants must show a detailed understanding of the nature of the information that should be provided to the potential participants. This information must be written in a way that will be understandable to the people who are to be approached as participants; their decision should be based on free will – i.e. the participant's decision not to participate in a survey should not create any negative consequences. Perhaps the most convenient way to show this is to produce a draft information sheet and attach the informed consent protocol to the application.

If applicants wish to include either children or adults who are judged not to have legal competence to consent for themselves in order to participate in research projects, they must prove (1) that the inclusion of such participants is necessary, and (2) that the people who are legally responsibility for them have sufficient information that allows them to make the informed consent choice on their behalf and in their best interests. What is required for each private data user in order to be compliant with the relevant EU and international law is specified here: http://ec.europa.eu/justice_home/fsj/privacy/.

Applicants must provide the European Commission with the needed paper trail and evidence such as sample information sheets (which must be secured to the consent/assent forms), sample consent form and/or explain how they will obtain the proper authorizations or compliance documents from their local or competent authorities.

2.1.4 – Improper use and data protection

Identifying the potential improper use of data is a major question as any potential misuse of information might have unexpected consequences. Case studies show that what seems to be unlinked information can sometime cause important side effects as sensitive or personal information taken out of context can lead to data breach. In addition, there is research that does pose the potential for a dual use, and it is the responsibility of researchers to consider if such a possibility exists and what proportional response is therefore needed.

Applicants therefore need to anticipate if the data they plan to collect could be used in a different context than the one contained in the original protocol thus approaching such data as extremely sensitive.

A review of current legislation on dual use can be found at:
https://www.grip-publications.eu/bdg/g1038.html

Questions that need to be answered by applicants:

1. Can the data obtained within the project have another, reasonably foreseeable, usage?

2. If this is the case, which safeguard measures will put in place so as to protect and control data flow?

3. Have the necessary authorizations for data circulation obtained? Who shall be contacted to assess this need?

2.1.5 – Research, data protection and privacy issues involving non EU Member States and developing countries[1]

Applicants must follow within their project the EU legal framework; these standards should also apply to participants from developing countries[2]. To that end, applicants need to be particularly cautious concerning the "use of local resources" section in the Ethical Issues

[1] For further references, please consult the following documents : *ec.europa.eu/**european**_group_**ethics**/docs/avis17_en.pdf*
[2] Further reading on developing countries : http://hdr.undp.org/en/statistics/

form. This should include an explicit explanation about the protection and proper handling of personal data in developing countries should be safeguarded.

Therefore, if this box is ticked, applicants must explain how they are planning to tackle data protection and privacy issues that relate only to research performed in developing countries. All measures outlined in the above sections must apply also when non-EU Member States are involved.

Prior to any transfer of data outside the EC Member States, applicants should make sure that the place where the data is to be sent has a data protection regime in place that is at least as solid as that required in the EU, or at least conform to the Data Protection Directive's requirements.

It must also be stressed that this section focuses on data's geographical movement. Therefore, even if data is transferred within the same company or research consortium, if such a transfer occurs by crossing geographical boundaries, the issue is relevant. Applicants should seek advice on the issue from their local data protection authority.

Questions that need to be answered by the applicants are:

1. Does any of the research data come from a developing or under economic transition country?

2. Will any of the research outcomes to be implemented within the project include a developing country and the deployment of any kind of personal data?

3. Do any of the resources the project is planning to use come from a developing country?

4. If this is the case, have the necessary measures for protecting and controlling data and – if needed – privacy been designed?

5. Will any data gathered be transferred to a non EC Member State?

6. What are the data privacy standards in the country where the data are obtained? How could the project apply best practices for data storage and processing in that country?

7. Which type of data is being transferred?

8. Have the research participants been informed that their data may be transferred to another country where data protection is not as rigorous as the EU?

2.2 –What are the technical questions that should be asked in order to detect data protection and privacy issues within a project?

This section is dedicated to the technical aspects of data protection and privacy.

At this point it might be needed to take on board the university's/company's, research centre's Chief Technical Officer (CTO) / IT manager if available.

2.2.1 - Data processing

2.2.1.1 – Data storage

Data storage must be secured so as for the data not to become accessible to unwanted third parties and to be protected against disaster and risk.

To that end, the following topics should be considered:

1. Where is the data stored? Data must be stored within a secured environment. If stored electronically, this must be a machine, or set of machines located in a physically secured environment – with controlled access - as well as technically secured: proper temperature control, etc.

2. On which hardware type is the data stored: paper, disk, removable device? Considering the nature of the data used in the project: what will the adapted security processes to be followed? How do they guarantee confidentiality of data?

3. Who has access to the data? Can the data be accessed by any third party? Can the data be copied by any third party?

4. For how long will the data be stored, accessed? What will happen to the data after the end of the study: duration of storage should be justified. Destruction at the convenience of the researcher would appear insufficient, unless clearly stated in the consent form and the approval of the local competent authority. Such deletion of data should be defined as irreversible, or reversible.

5. If stored on a machine, is the storage machine/server equipped with:

- Wifi
- Bluetooth
- USB drive
- On the whole, devices that might ease data duplication of circulation…

6. What data backup policies and processes will be implemented?

Answering these questions will help the applicants assess the data protection and privacy risks within the project and therefore provide a state of the art risk management policy.

2.2.1.2 - Data structure & circulation trends:

Data is a "living material." Data is supposed to be circulated between and modified by different users within a multi-actor research project, which raises issues of potential malevolent usage.

The potential misuse of data can be prevented by:

- Rendering data access difficult to, or unusable by, unwanted (malevolent) third parties;

- Becoming aware of all data circulation trends (cross border circulation, circulation within the project);

- Providing a data-protected/secure legal and technical environment in compliance with the ISO/IEC 27001:2005 standards[3].

To that end, the following questions need to be answered by the applicants:

1. How is the data structured and organised?

- Does one database contains the entirety of the research data?

- Are ID-related information kept in separate databases from other information types in order to ensure that no personal data is obtained without the proper authorisation of the relevant research subjects?

2. Will the data be circulated from one research partner to another within the project? Will the data be provided to any third party? Will the data be circulated within the EU, be transferred to non-EU countries (developing countries)? Is this data circulation strictly needed? If, yes a data circulation plan should be provided?

3. In compliance with **ISO/IEC 27001,** is any encryption process needed? Why? What will be the encryption strategy followed considering the project's needs?

In other words - if the data is to be used for several purposes - is it properly truncated in order to avoid – voluntary or involuntary - improper use.

Applicants must be aware that IT Officers may be able to provide guidance on these issues.

2.2.2 - Risk management & Legal compliance

1–Are all participants to the project aware of the issues beyond data protection and privacy described above? Are they sufficiently trained to handle data protection and privacy within their research project? Does the project include specific training on these topics? Is this demonstrated through a specific work package?

Actions should be taken within the project to ensure that those handling subjects identifiable or sensitive information are made fully aware of their responsibilities and obligations to respect confidentiality in compliance with market standards and best practices (e.g. :ISO/IEC 27001:2005).

Does a specific contractual procedure exist to guarantee confidentiality?

Does the project's budget anticipate sufficient financial funds that can guarantee compliance with the set data control standards?

2 – Are all participants aware of the legal requirements surrounding the use of private data under an electronic form?

The vast majority of the EU members and partners states have implemented regulations concerning data protection issues.

[3] http://www.iso.org/iso/catalogue_detail?csnumber=42103

The full text of these rules can be found in the following web-address: http://ec.europa.eu/justice_home/fsj/privacy/ and http://www.privacyconference2009.org/privacyconf2009/home/index-iden-idimp.html

3 – Has the required authorization for data usage been requested?

The required permits demonstrate compliance to the relevant EU Directives and Regulations. The documents that need to be issued include:

1. data usage information sheet explaining to The European Commission how the obtained data is planned to be stored, used, etc…

2. informed consent forms (or assent from a child/young person), that is to be signed by the participants/research subjects either in paper or electronically (via a specific process such as an opt-in, electronic signature) The participants/research subjects need to agree that his/her data will be used for a specific research purpose and is aware of the future implication of such use. For more on this subject, please refer to the "inform consent section above.

3. whatever the type of research, local/National authorisation or at least a paper trail evidence document showing that the proper authority has been contacted, and for countries where such an authority has not been established, a sample consortium agreement demonstrating how the project will comply with EU law and containing recommendations on these points and what will be the official and national referent on this guarantee. If applicable, the documents through which the relevant data protection and privacy authority is contacted should state that no answer from the so called authority within a period of time implies that the intended data protection and privacy safeguard process is accepted by them.

3 - Glossary

General disclaimer: this glossary summarizes the major concepts of data protection and privacy on an ethical point of view. It does not aim to take into account these concepts in-depth but gives a general definition in order to provide a good understanding of them. Furthermore, if some concepts are omitted this does not mean they should not be considered if there are ethical issues specific to your project. This glossary is a continuous project which will be amended by the European Commission from time to time.

The glossary is built around two separate sections:
1 - General principles of data protection and privacy
2 - Technical aspects

3.1 – General Principles

Assent is voluntary permission given by one who is under the age of consent with no legal status. (Minor) Capacity and competence to assent varies with age, cognitive development, experience of illness and country requirements.

Where sensitive information from adolescents is to be collected, (i.e. about sexual behaviour, pregnancy, or use of recreational drugs) it must be carefully evaluated if parents or legal representatives should be informed. Cultural, social and ethics committee opinions will vary between Member States.

Absolutely no inducement financial or other pressures are allowed to be placed on the investigators, children or their parents/guardians to persuade children to participate in research

Consent and assent must be voluntary and as fully informed as possible and be part of a continuous process, not just a signature on a piece of paper at the beginning of a research project. Finally, the enrolment strategies for the participants should be explained in language they can understand.

Data transfer: transmission of data or data support between information systems through any sort of media

Data privacy: Data privacy involves the right of any individuals to expect that personal information collected about them will be processed securely and will not be disseminated in any form without their written consent. Furthermore, data privacy must not be subject to "mission creep".

Data protection: Data protection consists of a framework of security measures designed to guarantee that data are handled in such a manner as to ensure that they are safe from unforeseen, unintended, unwanted or malevolent use.

Data protection is the technical mechanism to ensure data privacy. Data protection concerns:

- Access to data: who has the right to access each data set? How is this data accessed? Is access to the data properly logged and protected?

- Conservation of the data: where, how and for how long are the data stored and archived? Are the data stored raw, anonymised, structured, or encrypted?

- Accuracy: is there adequate de-multiplication and recovery of the data? Are the data properly updated when applicable and according to the study protocol? Maintained accurately? Are the data properly preserved against potential disaster (data location)?

Data protection concerns all actions deployed in order to ensure the lawful availability and integrity of the data.

Data protection also addresses the potential for intended data transfer outside legally defined boundaries that would require informed consent and that variability of national regulations for the issue be taken into account. Duration of data protection and means of irreversible data removal, if and when intended, should be clearly defined in the research protocol and in the participant information sheet.

Informed Consent: Informed consent is when it can be said with as much certainty as possible that a person has freely given consent based upon understanding as far as possible the aims, risks, benefits of the protocol and a willingness to perform research obligations. It is an agreement to do something or to allow something to happen, made with complete knowledge of all relevant facts, such as the risks involved or any available alternatives. During the informed consent process, it should be indicated who should be contacted in case of unexpected events, withdrawal or asking pertinent questions about the research. Refusal to participate should involve no penalty or loss of benefits to which the participant is otherwise entitled.

Evidence of consent needs to be clear and indisputable, for example a signed paper declaration or a certified dematerialised document using specific identification processes such as opt-in or electronic certificates and signatures must be provided.

Informed Consent is a voluntary positive agreement by someone of legal age and ability who has understood the information, the implications, risks and benefits of the research and willingly agreed to participate. Participants are informed that they can withdraw at any time without having to provide a reason knowing that their withdrawal will not disadvantage their usual relationship with the investigator or the eventual benefits linked to their former participation.

Applicants should also consider how they will be able to show that the level of information was sufficient to allow the particular participants to understand the risks (i.e. to evidence not just their ‘consent’ but their ‘informed’ consent). The important aspect is that the participant needs to agree that her/his data will be used within a specific scope of research and is aware of the meaning of such use.

The informed consent should include information about how the participant’s privacy and data will be protected. (See further in this document) No personal or health record information may be taken or stored from the participant without their written informed consent

Minors, children and vulnerable persons are protected as consent must be asked, and given on their behalf by a parent/guardian or legal representative. However, consent being a continuous process in time, such consent must not be imposed indefinitely on them and must be re asked, for example for children when their reach legal majority.

Except in emergency cases, informed consent must be sought within sufficient time[4], as the patients or healthy volunteers envisaged to participate to the project may wish to think about their decisions and discuss it with others. Any pressure to participate should be avoided. Preferably, independent expert(s) should be made available for answering questions prior to signing the consent forms and consequently the beginning of the intended intervention or enrolment. The level at which this should operate is not fixed, as in so much law the issue is one of proportionality to the risks involved and the sensitivity of the data, so applicants may need to back up their judgment with the opinions of other experts in ethics and law.

Further information on informed consent can be found within the FP7 Ethical Guidelines on the Cordis website: http://cordis.europa.eu/fp7/ethics_en.html

International Data Transfer: Data processing that entails a data transfer outside the European Economic Area.

Personal Data: consist of information relating to an identified or identifiable person ('data Subject' or research participant); An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical appearance, physiological, mental, economic, cultural or social identity;

Processing of personal data' ('processing') consists of any operation or set of operations which is performed on personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

Privacy is a fundamental part of human dignity. It is the human right to refuse interference by others in one's life: it defines the extent to which others can demand information or make choices binding another. It enables individuals to exercise control over the disclosure of their information and over decision-making by them and about them. It is a right that can be claimed by groups of individuals together. Where an individual is incapacitated, his or her privacy can be safeguarded by that individual's legally authorized representative.

In research, therefore, respect for an individual's privacy is safeguarded through a number of mechanisms, including data protection, and informed consent/assent procedures, enabling individuals to choose whether or not to participate in a study and to see the terms under which their involvement is agreed. It is monitored by

1. research ethics committees (through scrutiny of research proposals and, sometimes, on-going review),
2. by the process of law,
3. and most importantly, by self-protection by the individuals through their awareness of the research.

Private information can be derived from various sources and formats. It may include sensitive information like : Health-related records (e.g. patient records, biographic data , medical photographs , diet information, hospital information records, biological traits and genetic material); Criminal records or legal justice investigations and proceedings; State-related records such as tax fillings; Circulation records such as visas; residence or various geographic recordings such as GPS satellite localization recordings; bank record; financial

[4] Best practices suggest ,at least a minimum of full three days notice. A real 'cooling off period' should be built in.

transactions records, as well as religious beliefs, sexual orientation, ethnic identification records. Equally, it can include more general information about individuals. Usually, data are classified according to their level of importance so that users are aware of the type of data that is being collected and protected. If private (personal) data are collected, they must be stored in a secure manner and their access protected in order to avoid improper disclosure. These processes are called **data protection.**

3.2 - Technical aspects

'Anonymisation', 'pseudonymisation' and 'identifiability': 'Anonymous' often means data which does not identify an individual; 'anonymised' means data which has been rendered anonymous; 'pseudonymised' and 'coded' means data where obvious identifiers (e.g. names and addresses) have been replaced with indirect identifiers (e.g. numbers) in the main data set and the indirect identifiers are then held with the obvious identifiers in a separate data set (known as the 'key').

However, the concept operating in European data protection law is the 'identifiability' of an individual from the data. For European data protection law to bind research on personal and sensitive personal data one must ask: is the individual identified either immediately from the data or when that data are combined with other data in the hands of another person. This combination extends only to reasonably foreseeable linkings of data. Therefore, data which is gathered anonymously without any identifiers will be outside the scope of European data protection law; data which is pseudonymised or coded will be within the scope of the law as it is possible to reintroduce the two separate data sets and identify individuals; data which was gathered as identifiable data and then anonymised is subject to the data protection legislation when it contains identifiable data (most importantly at the point of gathering the data, requiring the disclosure by the researcher to the research participant of information including the purpose of the processing and contact details).

Authentication: A process of proving the identity of a computer or computer user. For users, it generally involves user name, password, electronic certificates… Computers usually pass a code that identifies that they are part of a network. In keeping data privacy it is essential to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.

Backup & deletion:

All processes ensuring that a copy exists in case of loss of the original data through accidental deletion. Some examples are listed below:

Disaster recovery: Disaster recovery involves the processes, policies and procedures including backups that are related to preparing for the recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster.

- **Database Shadowing**: A data backup strategy in which a full copy of the user's database is maintained at a remote data centre. Update transactions to the primary database trigger a transmission and similar update to the remote database. A successful recovery is possible from near failure using the shadowed database.

- **Data Synchronization**: The process of accurately reproducing the state of critical information and data to a predetermined point in time before an interruption occurred.

- **Data Wiping**: Data wiping is the process of irreversibly deleting or erasing all data beyond recovery without destruction. It is technically difficult to truly delete information from a computer. Great care must be taken when a computer previously used for research data is reused for other purpose that no remaining identifiable data remains

Brute-Force Attack: Brute-Force Attack is the most widely known password cracking technique. It is a method of defeating an encryption or authentication system by systematically trying every possible code, combination or password until the right one is found. It is also known as an exhaustive search.

Confidentiality: Confidentiality is the basis of trust between parties that prevents disclosure of any data or information to unauthorized individuals or systems.

Cryptography: Cryptography is the study and practice of hiding information. It is a process that assembles principles, means, and methods for the transformation of information in order to hide its content, prevent its undetected modification and/or prevent its unauthorized use.

It consists of transforming clear, meaningful information into an unintelligible, or ciphered, form using an algorithm and/or a key.

Data Theft: Data theft is the act of stealing any data for purposes and recipients other than those intended originally. This could be achieved internally by access to confidential data storage systems/insecure paper records. Data theft has become an increasing problem with the development of removable media devices, which are becoming smaller in size with increased hard drive capacity.
Several types of data theft exist such as “thumb sucking” which is the intentional or unintentional use of a portable USB mass storage device to illicitly download confidential data from a network endpoint, “mp3 slurping” which is the act of using a portable data storage device such as an mp3 to illicitly download large quantities of data by directly plugging it into a computer or “Bluesnarfing” which is the unauthorized access to information from a wireless device through a Bluetooth connection, using, for example, mobile phones.

Data Breach: Data breach involves the unauthorized disclosure of information that compromises the security, confidentiality or integrity of personally identifiable information.

Electronic signature/certificate: is any legally recognized electronic means that indicates that a person adopts the contents of an electronic message

Encryption Within the framework of data protection, Encryption is an electronic procedure for transforming information through cryptography. The level of protection provided by encryption is determined by an encryption algorithm whose strength is measured by the number and size of possible code keys.

File locking: File locking is a technical mechanism that restricts access to a computer file by only allowing one user or process access at any specific time. The purpose of locking is to prevent unauthorised updating or interference with final data. File locking enforces the serialization of update processes to any given file.

One use of file locking is in database maintenance where it can serialize access to the entire physical file underlying a database.

Identity theft (or “Id Theft”): This occurs when someone acquires personal identifiers in order to impersonate someone else with the objective of stealing money, concealing him (her) self from authorities or obtaining other benefits. The person whose identity is used can suffer various consequences when he or she is held responsible for the perpetrator's actions. It is believed to be one of the easiest ways to break security.

Integrity: is the property that ensures that data is not modified without authorization

Mission creep: This means information being collected with permission for one purpose and being used without permission for another reason.

***“Need to know* basis” principles**: when access to the information must be necessary for the conduct of one's official duties.

Non-repudiation: in a computer science sense, is a process through which no user can deny either sending or receiving an electronic transaction.

Password: in computer science, a password is a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource According to computer security experts should ideally contain a mix of letters, characters and numbers and be at least 15 digits long.

Record Locking: Similarly to File Locking, Record Locking is a method of managing shared data on a network by preventing more than one user from accessing the same segment of data at the same time. In a multi-user system, when one person is modifying a record, the record locking properties can be set so as to lock other users out of the record or to verify changes made when two users edit the same record at the same time.

Social engineering: It is a method of accessing privileged information about a computer system or protected data by an unauthorized person masquerading as a legitimate user. It is often regarded as a form of non-technical intrusion that relies mostly on human interaction. One typical example of such trickery is called Phishing. Phishing consists of an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well known and trustworthy Web sites.

Traceability: a method of tracking all electronic and paper data activity.