Ethical rules for processing for statistical or scientific research purposes
pursuant to art. 20, paragraph 4, of Legislative Decree 10 August 2018, n. 101 - 19 December 2018
(Published in the Official Journal no. 11 of 14 January 2019)

Ethical rules apply to all processing carried out for statistical and scientific purposes - in accordance with the methodological standards of the relevant disciplinary sector - which is owned by universities, other research bodies or institutes and scientific societies, as well as researchers operating in the field of said universities, bodies, research institutes and members of said scientific societies.
The ethical rules do not apply to processing for statistical and scientific purposes connected with health protection activities carried out by healthcare professionals or healthcare bodies, or with comparable activities in terms of significant personalized impact on the interested party, which remain governed by the relevant provisions. The research carried out for the latter purposes is instead subject to general provisions dedicated to the medical-health sector.

Duties of the Project Manager:

1. The research is carried out on the basis of a project drawn up in accordance with the methodological standards of the relevant disciplinary sector, even in order to document that the processing is carried out for suitable and effective statistical or scientific purposes.
2. The research project referred to in paragraph 1, also:
   a. specifies the measures to be adopted in the processing of personal data, in order to guarantee compliance with these ethical rules, as well as with the legislation on the protection of personal data;
   b. identifies any data controllers;
   c. contains a declaration of commitment to comply with these ethical rules. A similar declaration is also signed by the subjects - researchers, managers and persons authorized to process - who are involved in the continuation of the research;
3. The owner deposits the project at the university or research body or scientific society to which he/she belongs, which takes care of its conservation, in confidential form (consultation of the project being possible solely for the purposes of applying the legislation on personal data), for five years from the scheduled conclusion of the research;
4. In the processing of health-related data, the subjects involved observe the confidentiality and security rules to which healthcare professionals are required or comparable confidentiality and security rules.

The Project Manager is also required to:

1. provide the information to the interested parties, so that it is clear whether the activities involve research or health protection;
2. collect consent;

Consent to the processing of data suitable for revealing the state of health is, therefore, generally necessary. When expressing their consent to a medical or epidemiological investigation, the interested party is asked to declare whether or not they want to know about any unexpected discoveries that may emerge about them during the research.
The consent of the interested party is not necessary when all the required conditions are met simultaneously in the art. 110 of Legislative Decree 196/2003:

Art. 110 (Medical, biomedical and epidemiological research)

1. The consent of the interested party for the processing of data relating to health, for the purposes of scientific research in the medical, biomedical or epidemiological field, is not necessary when the research is carried out on the basis of legal or regulatory provisions or the law of the European Union in accordance with Article 9, paragraph 2, letter j) of the Regulation, including the case in which the research is part of a biomedical or health research program

envisaged pursuant to Article 12-bis of Legislative Decree 30 December 1992, n. 502, and an impact assessment is conducted and made public pursuant to articles 35 and 36 of the Regulation. Consent is also not necessary when, due to particular reasons, informing the interested parties is impossible or involves a disproportionate effort, or risks making the achievement of the objectives of the research impossible or seriously jeopardized. In such cases, the data controller adopts appropriate measures to protect the rights, freedoms and legitimate interests of the interested party, the research program is the subject of a reasoned favorable opinion from the competent ethical committee at local level and must be subjected to prior consultation with the Guarantor pursuant to article 36 of the Regulation.
2. In case of exercise of the rights of the interested party pursuant to article 16 of the Regulation in relation to the processing referred to in paragraph 1, the rectification and integration of data are noted without modifying the latter, when the result of such operations does not produce significant effects on the search result.
3. If necessary, obtaining the prior opinion of the Ethics Committee.

General authorizations from the Guarantor

The Guarantor for the protection of personal data has issued:

- Provisions relating to the processing of personal data carried out for scientific research purposes (general authorization n. 9/2016) https://www.garanteprivacy.it/web/guest/home/docweb/-/docwebdisplay/docweb/9068972#5
- Provisions relating to the processing of genetic data (general authorization n. 8/2016) https://www.garanteprivacy.it/web/guest/home/docweb/-/docwebdisplay/docweb/9068972#4

Data dissemination

Data suitable for revealing the state of health of the interested parties, as well as data relating to sexual life and racial and ethnic origin used for the conduct of the study cannot be disclosed.
The results of the research may be disseminated in aggregate form, or in ways which do not make the interested parties identifiable even through indirect identifying data, even in the context of publications.

Custody and security

There is an obligation to implement adequate technical and organizational measures to guarantee a level of security appropriate to the risk (art. 32 GDPR), which include, among others, where appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the confidentiality, integrity and availability of processing systems and services on a permanent basis;
- the ability to promptly restore the availability and access of personal data in the event of a physical or technical incident;
- a procedure to regularly test, verify and evaluate the effectiveness of technical and organizational measures in order to guarantee the security of processing.

The phase of data storage or archiving (and, possibly, collection and conservation of biological samples), the subsequent phase of processing the same information and transmitting it to any external subjects who collaborate with the implementation of the research, must be taken into consideration.
In particular, the following are adopted:

- suitable measures to guarantee data protection from the risks of: unauthorized access to data, theft or partial or complete loss of storage media, portable and fixed processing systems (for example, through the partial or complete application of cryptographic technologies file system or database, or through the adoption of other IT protection measures that make the data unintelligible to non-legitimate subjects);
- secure communication protocols based, for instance, on the use of cryptographic standards in electronic data transmission;

- labeling techniques, in the conservation and transmission of biological samples, using identification codes, or other solutions which, considering the number of samples used, make them not directly attributable to the interested parties, allowing the latter to be identified only in case of necessity.

With specific reference to the processing operations of research data stored in a centralized database, it is necessary to adopt, among others:

- suitable authentication and authorization systems for authorized personnel based on the tasks and access and processing needs, taking care of using credentials valid for the duration of the research and of deactivating them at the end of the research;
- procedures for periodic verification of the quality and consistency of the authentication credentials and authorization profiles assigned to those authorized to process;
- audit log systems for controlling access to the database and for detecting any anomalies.

Data transfers abroad

Article 1, paragraph 3 of EU Regulation 2016/679: within the European Union and the European Economic Area (Iceland, Norway, Liechtenstein) there are no limits related to the protection of personal data.

It is always necessary to evaluate the technical methods and assign the correct level of security (pseudonymisation, encryption, encryption techniques, ...) in relation to the type of data: common or particular (related to health, genetic, biometric, judicial ...).

Articles 44 to 49 of EU Regulation 2016/679: the transfer of personal data to countries not belonging to the European Union is in principle prohibited, if specific guarantees are not present:

- adequacy of the third country recognized by decision of the European Commission;
- in the absence of adequacy decisions by the Commission, adequate guarantees of a contractual or contractual nature that must be provided by the owners involved (including binding corporate rules - BCR, and standard contractual clauses);
- in the absence of any other prerequisite, use of exceptions to the transfer ban applicable in specific situations (Article 49 of the Regulation).

The GDPR establishes the obligation for the Data Controller, where this is carried out by a public administration, to designate a Data Protection Officer. The Data Protection Officer has consultancy duties towards the Data Controller and the subjects designated or authorized to process and has supervisory duties on compliance with the Regulation.

For doubts or clarifications you may contact the Personal Data Protection Officer DPO by writing to: dpo@iusspavia.it

To find out about the legislation you can consult:

Regulation on the protection of personal data implementing EU Regulation 2016-679.pdf

Definitions:

Personal data - any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more elements characteristic of his or her physical, physiological, genetic, psychological, economic, cultural or social identity;

Non-EU Third Countries – Countries not belonging to the European Economic Area (EEA, i.e. EU + Norway, Liechtenstein, Iceland);

Privacy contacts - natural persons, appointed by the internal data processing manager (Department Director, Manager), who have the task of supporting the Manager in all activities relating to the processing of personal data, of interfacing with the DPO for all activities relating to the correct management of the protection of personal data and for any communication linked to the application of the relevant legislation;

Data Controller - the natural or legal person, public authority, service or other body which, individually or together with others, determines the purposes and means of the processing of personal data" (art. 4. par. 1 point 7 of (EU) Regulation 2016/679- GDPR)-IUSS represented by the Dean;

Processing - any operation or set of operations performed with or without the help of automated processes and applied to personal data or sets of personal data, such as collection, recording, organization, structuring, storage, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, comparison or interconnection, limitation, cancellation or destruction.