National Czech Programme | eosc

# SEVEN ETHICAL PRINCIPALS


## Věra Franková

https://orcid.org/0000-0002-1927-9596




The final document underwent several rounds of review by experts across the Czech research environment.


Co-funded by the European Union

MINISTRY OF EDUCATION, YOUTH AND SPORTS

**National Repository Platform for Research Data (NRP)**
CESNET, association of legal entities
Correspondence address: Generála Píky 430/26, 160 00, Prague
info@eosc.cz; www.eosc.cz

National Czech Programme | eosc

# Seven Ethical Principles

Working with research data requires a responsible approach to their entire life cycle – from the collection and processing to the analysis, archiving, potential sharing and re-use. The underlying ethical principles of working with research data include trustworthiness, transparency, responsibility, long-term sustainability and, last but not least, protection of the interests of research participants. The ethical aspects listed below build upon the FAIR principles (Findable, Accessible, Interoperable, Reusable) of research data management and complement them with some **principles of research integrity** and **open science**, with the aim of enabling their long-term use and their future benefits.

## 1. Trustworthiness

Trustworthiness is both a quality and a value. Being trustworthy means to gain and to keep the trust of others through competence, transparency and consistent behavior. This value applies not only to individuals, organizations, institutions or governments, but also to data, information, evidence and systems. Building trust in research and science, research institutions and scientists is based on collecting, processing and presenting accurate data and research results. That means without **fabrication and falsification**, intentional concealment and plagiarism. Furthermore, trustworthiness is the practical responsibility for data and results management, and it is also manifested in the ability to transparently correct errors.

## 2. Transparency

**Transparency** involves open and understandable disclosure of information about how the data were collected and processed, as well as the methods used to get the results. This can be achieved through careful documentation of scientific work with data, which allows procedures and results to be understood, verified and possibly repeated. Transparency also concerns the management of research data and includes setting **rules for their disclosure**, which clearly define under what conditions, to what extent and for what purposes the data can be shared with others. This setting ensures equal conditions for access to data, supports verification of results and reproducibility, while it also increases trust in scientific and professional work.

Research data can be protected by intellectual property rights, even if they are not part of traditional scientific publications. It is, therefore, necessary to preserve the rights and credits of the authors, and to clearly acknowledge sources when data are shared and reused. This contributes to transparency, mutual trust and advancement of open science.

## 3. Compliance with applicable legislation, institutional rules, professional recommendations and guidelines

Responsible handling of data and information requires knowledge of and compliance with **legal regulations** (e.g. GDPR, cyber security law, copyright law, etc.), institutional rules (e.g. **research data management policies**), and professional and ethical standards that apply to the **given scientific field** and time (e.g. recommendations from **national** and international professional societies or organizations like **UNESCO**, **WMA**, etc.). Together, they define the framework within which the data can be collected, processed, published and shared, in a way that ensures legal compliance and scientific integrity.

## 4. Identification and assessment of possible risks

**Identifying and assessing potential risks** when working with research data ensures the security and responsibility of scientific activities. **Risks can have different nature** – from breach of confidentiality of personal data and misuse of sensitive technical information to non-intentional disclosure of data with the potential of negative impact on society, the environment or national security.

Co-funded by the European Union

MINISTRY OF EDUCATION, YOUTH AND SPORTS

National Repository Platform for Research Data (NRP)
CESNET, association of legal entities
Correspondence address: Generála Píky 430/26, 160 00, Prague
info@eosc.cz; www.eosc.cz

A systematic risk assessment should therefore be carried out before starting to collect or share data within research projects. In the case of research with human subjects, this process should also include the involvement of an ethics committee or, where applicable, an institutional data protection officer. In other areas of research, it is appropriate to consider consulting with data protection legal experts, professionals on environmental protection etc. The measures taken to minimize these risks should be clearly documented.

An example can be shown for personal data, where disclosure or identification may lead to discrimination, stigmatization or categorization of individuals or groups. Additional protection is needed to ensure the interest and well-being of vulnerable groups in research. These include individuals who are more likely to be denied legitimate claims such as physical integrity, autonomy, freedom, social security, unbiased approach or integration into society (e.g. pediatric population, minority population, etc.). Collecting, processing and possible sharing of data of research participants from vulnerable populations must be preceded by an assessment of risks and impact on the vulnerable populations.

# 5. Protection and security of data

Responsible research data management includes their security against loss, unauthorized access, changes or misuse. It relates mostly to the right setting of organizational, technical and physical measures and standards. That includes, for example, encryption of sensitive data, controlling access rights, regular back-up or storing data in a secured storage. The protection of sensitive personal data requires particular attention in order to preserve the privacy of research participants and minimise the risks associated with their misuse. Safety standards should be used for the minimization of risks, even for other types of sensitive and research data in general.

# 6. Privacy protection

Privacy is a fundamental value and right. It affects every aspect of an individual's life, including the social, cultural, political, physical and informational spheres. Protecting it also supports other key human values and rights. Measures to protect privacy should be proportional to the risks, as well as to the benefits that arise from the use of personal data.

Information and data about research participants may only be collected for research purposes with the free (=voluntary) and informed consent of the participant or their legal representative. Participants should be informed about the objectives of their data use, including who has access to the data, how they will be protected, how long they will be stored and what risks are associated with their storage, processing and sharing. They should also be informed about their rights regarding the data. Data should be strictly used in accordance with participant's consent and the approval of the institution's ethics committee. Privacy protection measures include e.g.: controlled access, pseudonymization, anonymization of data and other techniques. Data transfer agreements between individuals and/or organizations that clearly define data handling options are also an important measure.

# 7. Sustainability

Sustainability in the field of research data means preserving their value and usability in the long term. This involves more than just storing the data; it also requires appropriate documentation and archiving to ensure they remain understandable and reusable for future generations of researchers. That means clearly defined institutional and financial responsibilities are required to ensure the continuity of data storage even after the end of individual projects. Sustainability also includes promoting collaboration and data sharing in accordance to the FAIR principles and open science, which increase transparency, verifiability and reproducibility. Data management planning should therefore begin at the research (project) design stage and include secure storage, long-term archiving and mechanisms for future access. Sustainability, in this way, contributes not only to the long-term value of scientific knowledge but also to society's trust in science.

Co-funded by the European Union

MINISTRY OF EDUCATION, YOUTH AND SPORTS

National Repository Platform for Research Data (NRP)
CESNET, association of legal entities
Correspondence address: Generála Píky 430/26, 160 00, Prague
info@eosc.cz; www.eosc.cz