Strengthening resilience

AGAINST ILLEGITIMATE INTERFERENCE

IN THE HIGHER EDUCATION AND RESEARCH ENVIRONMENT

The presented set of documents for enhancing resilience against illegitimate interference in the higher education and research environment has been developed, in response to the requests of Czech higher education and research institutions and in an effort to prevent a fragmented approach by these institutions to the issue of illegitimate interference, within the framework of the Interdepartmental Working Group for Combating Illegitimate Interference in the Higher Education and Research Environment, with significant contributions from the Ministry of Education, Youth, and Sports, the Ministry of the Interior, and the Czech Academy of Sciences, and in consultation with representatives of other Czech higher education and research institutions.

TERMINOLOGY

For the purposes of this methodology and related materials (i.e. *Methodological recommendation defining the minimum scope of due diligence and risk management in cooperation with third parties within the context of strengthening the resilience of the higher education and research environment against illegitimate interference*; *Methodological recommendation for risk management in research security at the institutional level*), the following terms are defined as follows:

Academic Institution

A term used as an alternative for higher education and research institutions, either collectively or individually, depending on the context.

Security Research

Refers to research, development, and innovation activities aimed at identifying, preventing, preparing for, and protecting against illegal actions or actions that intentionally harm (European) communities, individuals, organisations, or structures, including tangible and intangible assets and infrastructure, ensuring operational continuity after such actions, and mitigating their consequences (also applicable in the case of natural disasters and industrial accidents).

Research Security

Organisational and systemic procedures for evaluating and managing security risks in the area of research and education, which reduce the risks associated with illegitimate interference in the higher education and research environment.

The primary goal of research security is the comprehensive protection of the research ecosystem, which also encompasses the protection of national and economic interests.

Sensitive Data/Information

Refers to data and information that an academic institution protects as part of sensitive research and education or considers confidential by its own decision, or that must be protected based on regulatory requirements.

Sensitive Areas of Research and Education

Refers to areas of research and education that carry an increased risk of illegitimate interference and for which enhanced protection is sought, including:

- Critical technologies for the economic security of the EU.
- Selected fields of research and education.
- Selected cooperation with third parties.
- Dual-use goods and technologies, and military material.
- Any other area that an academic institution chooses to classify as sensitive.

Foreign Power

Refers to a foreign state or its authority, or a supranational or international organisation or its authority, as well as any other individuals or legal entities, regardless of nationality or location, involved, even partially, in advancing the interests of a foreign state or organisation through illegitimate interference.

Due Diligence

Refers to a set of measures aimed at eliminating or reducing the risks of illegitimate interference on academic institutions arising from cooperation with third parties.

Identification Data

1. For individuals: name, surname, date of birth, and nationality.
2. For legal persons: name and registered office.
3. In other cases: a designation or name, and any other necessary information to identify the partner unequivocally.

Critical Technologies for the Economic Security of the EU

Refers to a list of technological areas defined in the European Commission's Recommendation of 3 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States[1] and its Annex[2].

---

1 COMMISSION RECOMMENDATION of 3.10.2023 on critical technology areas for the EU's economic security for further risk assessment with Member States; C(2023) 6689 final

2 ANNEX to the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States, C(2023) 6689 final

Illegitimate Interference

Refers to unwanted interference on people, decisions, or processes. This includes foreign malign influence as well as criminal (e.g., corrupt) behaviour and undesirable lobbying. These are usually activities that are covert, deceptive, coercive or corrupt and which the perpetrator of illegitimate interference (foreign power, corruption, lobbying in violation of the law or generally accepted social ethical rules) carries out himself or through a third party and which threaten or damage the interests of higher education and research institutions.
Alternatively, the term foreign interference is also used.

Partner

Refers to any legal or natural person with whom higher education and research institutions are in, or intend to establish, a partnership.

Partnership

A relationship or collaboration established by a cooperation agreement or other written agreement (e.g., memorandum of understanding, distribution of responsibilities in research teams) between an academic institution and a third party. In some cases, it may involve a less formal or even informal contractual relationship (including implied contracts) between an academic institution's employee and a third party.

Employee of a Higher Education or Research Institution/Academic Institution

Refers to a student, intern, academic or research worker, other employees, or individuals in another contractual relationship with the academic institution, as well as others involved in the institution's activities.

Perpetrator of Illegitimate Interference

This term refers to any individual, regardless of whether they act independently or on behalf of a state, company, or organisation, and regardless of the forms and methods of illegitimate interference they employ. The term "attacker" is also sometimes used. They typically pursue their interests in violation of democratic principles, the legal order, and good morals. They seek the easiest possible way to advance their interests, with the vast majority of such activities targeting a specific individual (in this context, a member of the academic community or an employee of the academic institution).

Regional Studies

This refers to academic disciplines focused on the study of local and regional contexts of societal and environmental development, i.e., the context and realities of a given region.

Third Party

This refers to any legal or natural person, public authority, or other entity representing or acting on behalf of a state that is not a member of the European Union (EU)[3], the European Economic Area (EEA)[4], or the European Free Trade Association (EFTA)[5].
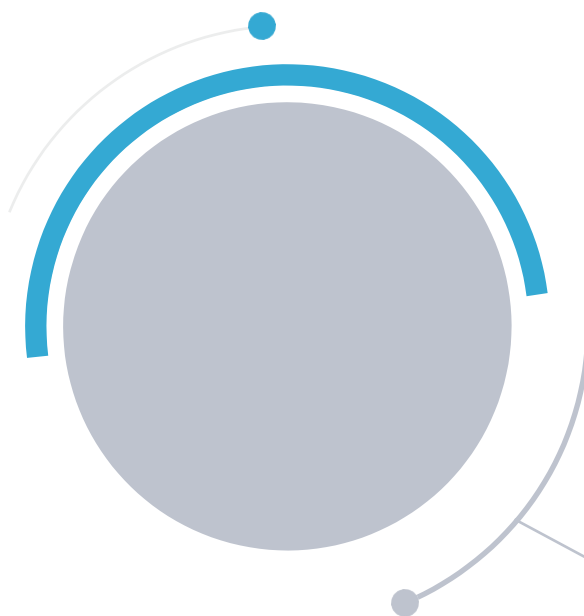
Third Country

This refers to a country other than the Czech Republic. The term "third state" is also used alternatively.

R&D&I or RDI

The acronym R&D&I refers to Research, Development, and Innovation.

Other terms used are interpreted in accordance with the European Commission's Communication on the Framework for State Aid for Research and Development and Innovation (2022/C 414/01).

---

3 https://european-union.europa.eu/easy-read_cs

4 https://www.europarl.europa.eu/factsheets/cs/sheet/169/the-european-economic-area-eea-switzerland-and-the-north; Norway, Iceland and Liechtenstein

5 https://eur-lex.europa.eu/CS/legal-content/glossary/european-free-trade-association-efta.html; Iceland, Liechtenstein, Norway and Switzerland

INTRODUCTION

The development of the international security situation and its impact on the security interests of EU countries, as well as other states within the Euro-Atlantic area, increasingly underscore the necessity of paying due attention to the issue of illegitimate interference. This specific threat significantly disrupts the activities of higher education and research institutions, limiting or endangering their academic rights and freedoms, including their academic independence. Examples of such influence from abroad, whether shared from the USA, the United Kingdom, Canada, Australia, other European countries, or the Czech Republic (CR), demonstrate that this is a real and existing threat. It is important to acknowledge that, at least in the Czech context, only a small fraction of these cases have been publicised or have reached broader awareness within the academic community or the general public.

The growing number of cases related to illegitimate interference, including the unlawful transfer of technologies, has compelled states worldwide to take necessary action. In January 2024, the European Commission published a **Proposal for a Council Recommendation on enhancing research security**. In February 2024, the G7 countries released **best practice recommendations for secure and open research**.

RATIONALE

The intention of this presented material is to outline the development of EU policy and the approach of the Czech government towards strengthening research security, with the primary goal of protecting democratic values and principles within the higher education and research environment.

The Czech Republic is part of the European Research Area, whose long-term objective is also to strengthen the stability and resilience of the EU to better cope with future crises.

The aim of this general document is to provide a comprehensive overview and offer guidance on how to approach the issue of illegitimate interference within higher education and research institutions. Beside this general methodology, specific **Methodological Recommendation have been developed, which define the minimum scope of due diligence and risk management in cooperation with third parties within the context of strengthening the resilience of the higher education and research environment against illegitimate interference**. Additionally, there is a **Methodological Recommendation for Risk Management in Research Security at the Institutional Level**. These materials provide concrete recommendations and advice on how to comprehensively assess and manage the risks associated with illegitimate interference in everyday activities at the institutional level. The goal is to offer guidance on understanding the issue and the phases of building institutional resilience, from recognising the reality of this threat in the context of the institution's activities to establishing an adequate system of protective measures and tools, with continuous evaluation always proportionate to the potential risk. The purpose of these documents is not to limit democratic values and principles within the higher education and research environment, but rather to strengthen the independence of their educational and research activities, including international cooperation, as well as to enhance the safety of their employees and students.

The presented methodologies are designed to be holistic and complementary in their mission. This set of materials also serves as a foundation for raising awareness about the issue, aiming to strengthen prevention and improve understanding among all relevant actors involved in the research ecosystem, as well as within society as a whole.

WHY THE HIGHER EDUCATION AND RESEARCH ENVIRONMENT?

Higher education and research institutions are key players in building a functioning European Higher Education Area and European Research Area. They hold a unique position at the crossroads of education, research, and innovation, as well as an irreplaceable role in protecting and promoting European democratic values and shaping new generations.

International cooperation, openness, and academic freedoms are the cornerstones of world-class research, development, and innovation. The internationalisation of research refers to the process of actively involving higher education and research institutions across countries to deepen the impact of research, enabling access to a broader range of resources, technologies, expertise, and perspectives, ultimately leading to more innovative and effective research outcomes.

Higher education and research institutions are particularly vulnerable to illegitimate interference because they operate on the principles of openness and internationalisation. With increasing international tensions and the growing geopolitical significance of research and innovation, higher education and research institutions are increasingly having to confront the risks associated with illegitimate interference within the context of international cooperation. This situation contributes to the fact that the internationalisation of European research is influenced and exploited in ways that not only violate our ethical standards and laws but also threaten our security.

ILLEGITIMATE INTERFERENCE AND RESEARCH SECURITY

From the perspective of the European Commission, as detailed in the **Proposal for a Council Recommendation on enhancing research security**, possible forms of **illegitimate interference within the higher education and research environment** are particularly associated with:

- Undesirable transfer of critical knowledge, know-how and technology that may affect the security of the EU and its Member States, for instance if used for military purposes in third countries.
- Illegitimate interference on research, where research can be instrumentalised by or from third countries in order to diffuse certain narratives or incite self-censorship among students and researchers infringing academic freedom and research integrity in the EU.
- Ethical or integrity violations, where knowledge and technologies are used to suppress or undermine fundamental values, whether in the EU or elsewhere.

Research security focuses on sets of systemic preventive measures that reduce the risks associated with the aforementioned forms of illegitimate interference within the higher education and research environment. Internationally, this initiative is often associated with terms such as "research security", "knowledge security" or "trusted research". The primary goal is the comprehensive protection of the research ecosystem, along with the associated protection of national and Union interests.
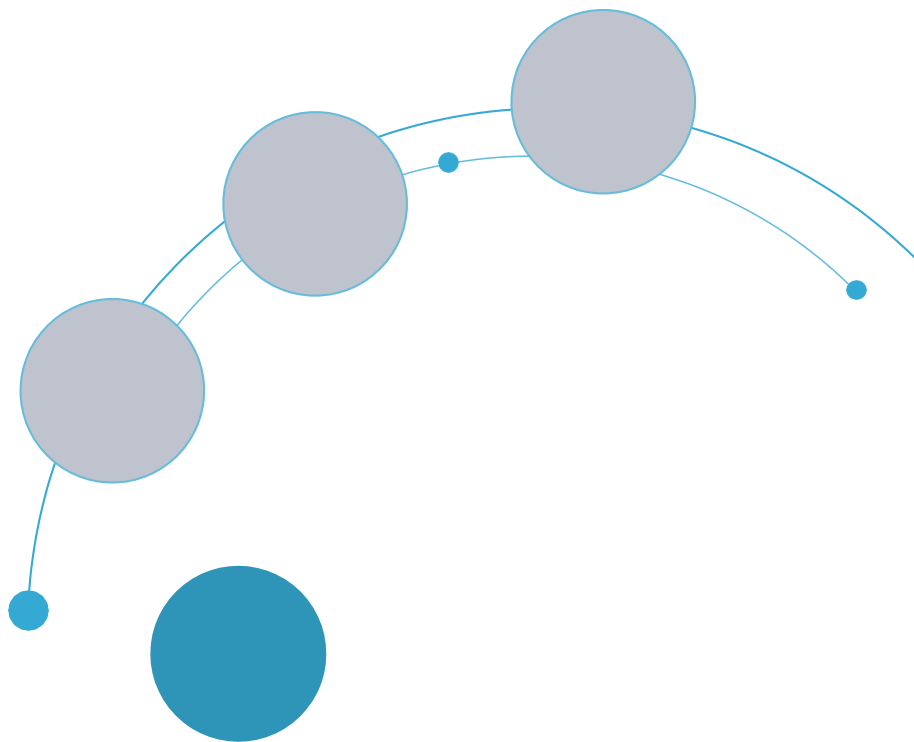
PRINCIPLES

International cooperation in the fields of research, development, and innovation is fundamentally based on a shared understanding of and respect for basic values and principles, such as academic rights and freedoms, research ethics, research integrity, and the principle of open science. The following section of the document will attempt to outline how illegitimate interference can deliberately disrupt and weaken these principles.

ACADEMIC RIGHTS AND FREEDOMS

Since the early history of European universities, academic freedoms have been regarded as a fundamental and characteristic feature of higher education and research institutions. Following the extensive democratisation of Europe and other parts of the world in the second half of the 20th century, academic freedoms and rights ceased to be mere abstract concepts; in many countries, including the Czech Republic, they have been recognised **as specific freedoms enshrined in legislation**. At its core, the concept of academic freedom reflects the idea that it is essential for those working in academia and research to be able to work, and for students to study, without unnecessary restrictions or interference. Recently, academic freedom has been recognised as a fundamental condition of a healthy democracy and a defining feature of democratic governance. Understanding this conceptualisation of academic rights and freedoms is crucial to comprehending the complexity of their potential threats.

Within the EU, academic freedoms are enshrined in **Article 13 of the EU Charter of Fundamental Rights**, which states: "The arts and scientific research shall be free of constraint. Academic freedom shall be respected." This article imposes an obligation to protect and defend this right from pressure or violations by public authorities, as well as from third-party interference.

The paramount importance of academic rights and freedoms is also fully acknowledged in the policies of the European Higher Education Area and the European Research Area. This recognition is reaffirmed by documents from the **Bologna Process** or the **Bonn Declaration on Freedom of Scientific Research** adopted by Member States in 2021.

The Czech Republic's interest lies in maintaining a strong and independent sector of higher education, research, and development, where academic freedoms, academic rights, and freedom of scientific inquiry are guaranteed by Czech laws. The Constitution of the Czech Republic, Act No 111/1998 Coll., on Higher Education Institutions, as well as key documents and statutes of universities, clearly support the protection of academic rights and freedoms, institutional autonomy, self-governance, and freedom of research or action. This demonstrates a broader awareness and understanding of academic rights and freedoms in the Czech context, as outlined above. Some relevant higher education institution documents even specify that higher education institutions are autonomous and independent of power and political structures.

> Despite the fact that **academic freedoms, academic rights, and freedom of scientific inquiry are understood as fundamental values and principles within the higher education and research environment**, **there are increasing concerns** at both the EU and national levels about their potential limitations. Evidence of this can be seen in the growing number of recorded cases of illegitimate interference, which fundamentally infringe on these rights and responsibilities, thereby making the higher education and research environment in the Czech Republic and the EU more vulnerable.

In its working document "**Tackling R&I Foreign Interference**", the European Commission highlights that the internationalisation of the research environment can create situations where higher education and research institutions may interact with institutions or individuals who, on one hand, enrich research or education, but on the other hand, operate in environments where academic and research activities are systematically controlled. International cooperation can thus help to export certain invasive methods or practices into our environment. According to the document, such actions include, for example, monitoring citizens working abroad, their obligation to report regularly to embassies, motivating scientists and students to share information, surveillance, and even censorship of digital communication or online teaching, harassment of certain scientists upon their return home, or harassment of their family members who remained at home during their stay abroad. Exported practices also include pressure on academic publishers in liberal democracies to censor content, denying visas to "unwelcome" scientists seeking to visit repressive countries for academic work, and embedding clauses in cooperation agreements between EU academic institutions that effectively make them complicit in violations of academic rights and freedoms. Lastly, the European Commission's working document points out some covert efforts that pose a threat of illegitimate interference in the higher education and research environment, such as incentivising academics through funding, honorary titles, paid positions, and other privileges.

Given the diversity of universities and research institutions within both the EU and the Czech Republic, **there is no universal guide to address emerging situations**. However, it is essential to establish a strategic approach and systematic risk assessment and management at the institutional level, which will appropriately address the specific needs.

OPEN SCIENCE

Open Science allows for addressing some of the world's most challenging problems and creates cutting-edge research that no single country could achieve on its own. It is important to acknowledge that **there are actors who seek to exploit the principle of Open Science. They deliberately abuse the values of the scientific community to their advantage**, whether for warfare, repression, sabotage, disruption of economic relations, or to bolster their political influence or exert power. In this context, it is critically important to enhance research security and propose measures to protect it.

"**Open Innovation, Open Science, and Open to the World**", also known as the "Three Opens" or "3 Os", were first introduced as EU research and innovation goals in 2015. The international and open nature of science and innovation was presented as a key means of developing new ideas and as a sustainable investment in Europe's future. In 2016, the European Commission defined Open Science as a process based on collaboration and knowledge dissemination through digital technologies and new collaboration tools. Three years later, the European Commission no longer referred to Open Science as a process but as a systemic change leading to better science based on open access, collaboration, communication, knowledge sharing, results, and data, as early as possible in the research process.

However, given the growing strategic competition and the return to power politics, the aforementioned goal of "Three Opens" has become the subject of pressure and interest from certain actors. In response to the tense geopolitical situation, where technology plays a key role in political, economic, and military dominance, democratic states have started to lean towards a so-called "**balanced openness**" and have long been urging higher education and research institutions to intensify international cooperation and develop open collaboration with international partners, but to do so fully in line with the well-known motto "**as open as possible, as closed as necessary**". Recently, more emphasis has been placed on the second part of this motto.

The Open Science policy includes a range of practices applied throughout the entire research cycle, aiming to make knowledge accessible, shareable, and reusable, as well as to foster a transparent, collaborative, and inclusive environment. It is indeed useful to recognise that the principle of Open Science combines "Open Science" (open access to peer-reviewed scientific publications, **FAIR data**, **Open Definition – definition of open knowledge**) and "**Openness of Science**", which seeks to minimise barriers to research collaboration (enabling the mobility of researchers and students, informal collaboration with researchers, sharing information through conferences, workshops, or correspondence, as well as co-launching research among different sectors and groups, including the public). Of the two inseparable aspects of the Open Science principle described above, it is the "Openness of Science" that will be more affected by security measures and where more extensive security processes need to be established.

Although there is broad consensus on the many benefits that Open Science brings to research, a different context and perspective can lead to entirely different considerations. In 2022, the European Commission issued the document **Open Science and Intellectual Property Rights**, which in the context of "as open as possible, as closed as necessary" concerning research data, presents a possible balance between open access on one hand and the protection of intellectual property on the other.

In a similar spirit of **seeking balance**, it is also necessary to approach research security. Unfortunately, it is too often **erroneously argued that protecting research necessarily goes against the principles of Open Science**. There are indeed **legitimate reasons for protecting certain research outcomes and their partial, if any, disclosure.**

Such reasons include the protection of privacy, intellectual property, commercial reasons, and security. This fact is clearly articulated both in European documents that present the principle of **Open Science in Horizon Europe** and in national legislation **under Section 12a(2) of Act No 130/2002 Coll.,** on Support of Research and Development, as amended.

However, when setting relevant measures, it is necessary to **consider proportionality, feasibility, and effectiveness, and always to individually assess whether the implementation of the proposed measure and the associated costs genuinely correspond to the potential threat**. It is only the higher education and research institutions themselves that are familiar with their research, partnerships, internal mechanisms set for personnel processes, or student admissions, and therefore only they can best assess potential risks. By establishing appropriate agreements, they can, for example, prevent later ambiguities and disputes.

> An effective policy supporting research security is one that **respects institutional autonomy and proportionality**, supports the proper establishment and implementation of functional control mechanisms, and goes hand in hand **with open, yet also responsible, science**.

ETHICS AND RESEARCH INTEGRITY

Ethics is most commonly defined as a set of behavioural norms that help distinguish between acceptable and unacceptable behaviour and actions. While most societies have legal rules enshrined in legislation that regulate behaviour or actions, ethical norms are much broader and more informal than written laws.

> Although most societies use laws to enforce generally recognised moral standards, and similar concepts are used in both ethical and legal rules, **ethics and law are not always identical**.

Many fields, institutions, and professions (typically those associated with professional chambers) have adopted norms or codes of conduct that align with their specific intentions and goals. Such documents help individual fields coordinate their activities and bind their actions to these documents, thereby supporting public trust in that field.

At the EU level, the relevant document is the **European Code of Conduct for Research Integrity,** revised in 2023, whose principles apply across all scientific and academic disciplines. The code declares: *"Research is a common enterprise, carried out by many different actors in academic, industry, and other settings. It involves collaboration, direct or indirect, which often transcends social, political, and cultural boundaries. It is underpinned by the freedom to define research questions and develop theories, gather empirical evidence, and employ appropriate methods in an impartial way. Therefore, research draws on the work of the community of researchers and should develop independently of pressure from commissioning parties and from ideological, economic, or political interests. Research integrity is crucial to preserving the trustworthiness of the research system and its results."*

The European Code further outlines the potential consequences and impacts of breaches of research integrity: *"It damages the research processes, degrades relationships among researchers, undermines trust in and the credibility of research, wastes resources, and may expose research participants and subjects, users, society, or the environment to unnecessary harm."*

Although codes issued at the European, national, or institutional levels are very important and useful, like any set of rules, they **do not cover the full range of possible situations**, often conflict with each other, and require substantial interpretation. For this reason, it is crucial that research and academic professionals learn how to interpret, assess, and apply various research norms and rules, and how to make ethical decisions and act ethically in diverse situations. The interpretation of the values and principles guiding research can be influenced by social, political, or technological developments as well as changes in the research environment. Education in research ethics should help address ethical dilemmas that research and academic professionals are likely to encounter during their careers. Simply **familiarising oneself with key concepts, tools, principles, and methods that may be useful in resolving these dilemmas is a preventive and certainly beneficial measure.**

> **Ethical dilemmas** are also **part of international collaboration in research, development, and innovation.** Such dilemmas may arise, for instance, when collaborating with individuals or institutions from countries where basic human rights are not respected. Specifically, doubts may arise about how to proceed with research which results may be used by a foreign partner to violate these rights or to strengthen the military position of that country.

Another potential ethical dilemma may arise when researchers from countries that do not uphold basic human rights are compelled, during their research or upon returning to their country, to use the acquired knowledge for purposes that violate human rights and freedoms.[6] Another ethical dilemma occurs when joint project results are intentionally modified and presented in a way that promotes the political regime of a country that does not respect basic human rights.

It is crucial in the context of international collaboration to be aware of such possibilities at both the institutional and individual levels and to reflect on them throughout the entire research cycle. This includes the initial establishment of contacts and the definition of the subject of international collaboration, through the execution of the project itself, and even the phase after its completion.

---

6 [National knowledge security guidelines | Publication | National Contact Point for Knowledge Security (loketkennisveiligheid.nl)](loketkennisveiligheid.nl)

Higher education and research institutions in the Czech Republic, in addition to their **ethical codes**[7], also **have institutionally established ethical committees**[8] that help address issues related to the ethics of scientific and academic work. Given the potential ethical dilemmas associated with international collaboration in research, development, and innovation as outlined above, it may be appropriate to **reconsider the scope of ethical committees and expand it to include issues related to international collaborations that pose ethical dilemmas**. According to some foreign experiences, the remit of ethical committees should not be focused solely on the methods of conducting research but also on the **unethical use of research results**.[9]

---

7 Code of Ethics for Researchers in the CAS – Czech Academy of Sciences (avcr.cz); Code of Ethics – Charles University (cuni.cz);

8 University of South Bohemia in České Budějovice – Ethics Committee of the USB (jcu.cz); Masaryk University Ethics Commission | Masaryk University (muni.cz)

9 National knowledge security guidelines | Publication | National Contact Point for Knowledge Security (loketkennisveiligheid.nl)

EU INITIATIVES AND TOOLS

The policy of strengthening research security can only be effective if it is properly implemented at all levels - EU, national, and institutional. Each actor has its irreplaceable role and corresponding responsibilities. Coordination at the EU level is an essential prerequisite for preventing the fragmentation of the European Research Area. The ambition of this chapter is to briefly introduce existing or planned EU initiatives and tools for strengthening research security.

DOCUMENTS

In May 2021, the European Commission published the communication **"Global Approach to Research and Innovation"**, which stated that the EU should continue to offer researchers a democratic environment free from political interference, upholding academic rights and freedoms as outlined in the Charter of Fundamental Rights of the EU. **The communication highlighted that academic freedom, integrity, and institutional autonomy are fundamental values of higher education and research institutions in the EU.** The task of the EU and its member states is to support and protect these shared values at the international level and **adhere** to the principles of the **Bonn Declaration on the freedom of scientific research** **when dealing with third parties**. A year later, following this communication, the **"Marseille Declaration"** on international cooperation in research and innovation was presented under the French Presidency of the Council of the EU, emphasising key values and principles relevant to international cooperation in research, development, and innovation, such as the freedom of scientific research, ethics, integrity, open science, and institutional autonomy.

The **G7 meeting** in June 2022 also paid appropriate **attention to research security, academic freedoms, and open science**. In the same year, the European Commission issued the working document "**Tackling R&I Foreign Interference**", aimed at providing information on possible procedures to mitigate the risks of illegitimate interference on higher education and research institutions and support the protection of fundamental values, especially academic rights and freedoms, research integrity, and institutional autonomy.

The European Economic Security Strategy adopted in 2023 notes that, given the changing geopolitical situation and technological advances in recent years, it is also necessary to **strengthen the resilience of the higher education and research environment against illegitimate interference and the associated protection of international cooperation in research, development, and innovation**. Following this document, the **Commission Recommendation on Technological Areas Critical to the Economic Security of the EU** was adopted in October 2023 to assess risks in cooperation with member states.

This recommendation identified ten areas of critical technologies crucial for the EU's economic security:

- Advanced semiconductors technologies
- Artificial intelligence technologies
- Quantum technologies
- Biotechnologies
- Advanced connectivity, navigation, and digital technologies
- Advanced sensing technologies
- Space & propulsion technologies
- Energy technologies
- Robotics and autonomous systems
- Advanced materials, manufacturing, and recycling technologies

At the end of 2023, the **European Commission, in collaboration with member states, initiated a risk assessment of the first four critical technologies**. The assessment aimed to identify the main vulnerabilities and systemic threats in a pan-European context and to prompt the creation of specific and proportional measures in these areas.

In January 2024, the European Commission published a **Communication to the European Parliament and the Council – Strengthening European Economic Security: An Introduction to Five New Initiatives,** which reviewed the EU's activities to date and defined five specific initiatives aimed at strengthening the EU's economic security. They include **the Proposal for a Council Recommendation on enhancing research security**, which is a logical outcome of the preceding initiatives and work of the European Commission and member states over recent years. However, for the first time, the recommendation demonstrates a shared sense of urgency and a common definition of the problems. The proposed measures address all actors involved in the research ecosystem across all levels.

EUROPEAN RESEARCH AREA

Since its inception in 2000 the primary **mission of the European Research Area (ERA)** has been addressing the **fragmentation of research and innovation** systems across EU member states and harmonisation of national policies and programmes for more effective research. **The ERA concept has undergone extensive and gradual development, significantly contributing to addressing current global challenges.** In 2007, the free movement of researchers, scientific knowledge, and technologies was guaranteed by **Article 179 of the Lisbon Treaty**, which was crucial for the future direction of the ERA concept.

Between 2012 and 2020, its policy focused on implementing measures that ensured transnational cooperation, strengthened gender mainstreaming, and supported the optimal circulation of scientific knowledge across the EU. **The main priorities of the ERA were defined in the ERA Roadmap 2015–2020**, which served as an inspirational document for many member states in defining national research, development, and innovation policies.

In 2021, the so-called "**New European Research Area**" was launched through the Council Recommendation on a **Pact for Research and Innovation in Europe**, which also laid down the foundation for the first **Policy Agenda for the European Research Area for 2022–2024**. This agenda defines priority activities that need to be systematically addressed at the national level to achieve the set progress and goals and to strengthen the stability and resilience of the EU to better cope with future crises.

The need for policies and measures to protect academic and research freedoms, institutional resilience, and, more generally, the protection of European democratic values, is more elaborated in the introduction of this methodology. However, it is also important to mention that this significance is also highlighted in key documents of the European Research Area. Therefore, the policy of the European Research Area has **set the protection of academic rights and freedoms in the EU, as well as the related issue of illegitimate interference in higher education and research institutions, as one of its activities, specifically Activity 6, for the 2022–2024 period**.

The primary goal of Activity 6 is to raise awareness of this issue across the EU and to contribute to defining and implementing appropriate measures to address illegitimate interference in the operations of research and higher education institutions. **The Mutual Learning Exercise on Tackling R&I Foreign Interference** was a specific tool used by thirteen member states (including the Czech Republic) to share experiences and knowledge on this issue and to inspire the implementation of potential measures to strengthen the protection of higher education and research institutions at the national level.

The preparation of the Policy Agenda for the European Research Area for 2025–2027 by member states and the European Commission clearly **reflects the importance of the issue related to strengthening research security**. At the same time, it emphasises the need for coordination at the EU level to prevent fragmentation of the European Research Area and to ensure equal conditions and protection of integrity.

HORIZON EUROPE

Horizon Europe is the ninth EU framework programme for research and innovation for the period 2021–2027. With a total allocation of 95.5 billion euros, it is the **largest research and innovation funding programme in the world**.

The aim of Horizon Europe is to facilitate collaboration and enhance the impact of research and innovation on societal development. Simultaneously, the programme serves as an effective tool for implementing EU policies, contributing to addressing current challenges and global issues. Horizon Europe primarily includes initiatives directly related to supporting research and innovation. However, it also contains provisions **protecting the EU's strategic interests**, as defined in the policy on the **internationalisation of research and innovation**.

Horizon Europe was established on 28 April 2021 by **EU Regulation 2021/695**, which defines the rules for participation and dissemination of results. Given the evolving geopolitical situation and the need to protect the EU's economic security, where research, development, and innovation play a crucial role, the **European Commission has decided to utilise and activate protective measures enshrined in the regulation**.

The regulation states that, in order to ensure scientific excellence and in line with **Article 13 of the Charter of Fundamental Rights of the EU,** the programme should support the **adherence to academic rights and freedoms in all countries that utilise its funds. Article 22(5) specifies** that *"...For actions related to Union strategic assets, interests, autonomy or security, the work programme may provide that the participation can be limited to legal entities established only in Member States or to legal entities established in specified associated or other third countries in addition to Member States." Paragraph 5 further mentions "...For duly justified and exceptional reasons, in order to guarantee the protection of the strategic interests of the Union and its Member States, the work programme may also exclude the participation of legal entities established in the Union or in associated countries directly or indirectly controlled by non-associated third countries or by legal entities of non-associated third countries from individual calls for proposals, or make their participation subject to conditions set out in the work programme."*

The European Commission has also decided to exclude entities based in China from the innovation activities of Horizon Europe, in connection with Article 22(6) of the regulation, which states that *"...Where appropriate and duly justified, the work programme may provide for eligibility criteria in addition to those set out in paragraphs 2 to 5 to take into account specific policy requirements or the nature and objectives of the action, including the number of legal entities, the type of legal entity and the place of establishment."*

The European Commission is systematically addressing the mitigation of identified risks to the interests of the EU and also emphasises other relevant articles or paragraphs contained in the regulation. Frequently mentioned is **Article 39** regarding the use and dissemination of results, specifically paragraph 6, which states: *"Unless the work programme provides otherwise, proposals shall include a plan for the exploitation and dissemination of the results. If the expected exploitation of the results entails developing, creating, manufacturing and marketing a product or process, or in creating and providing a service, the plan shall include a strategy for such exploitation. If the plan provides for the exploitation of the results primarily in non-associated third countries, the legal entities shall explain how that exploitation is still to be considered to be in the Union interest."* Another tool is **Article 40(4)**, which addresses the issue of transfer of ownership and granting of licenses:

"Where justified, the grant agreement shall provide for the right for the Commission or the relevant funding body to object to transfers of ownership of results, or to grants of an exclusive licence regarding results, if:

a) the beneficiaries which generated the results have received Union funding;

b) the transfer or licensing is to a legal entity established in a non-associated third country; and

c) the transfer or licensing is not in line with Union interests.

If the right to object is provided for, the beneficiary shall give advance notice of its intention to transfer ownership of results or to grant an exclusive licence regarding results. The right to object may be waived in writing regarding transfers or grants to specifically identified legal entities if measures safeguarding Union interests are in place."

Lastly, the European Commission also highlights the content of **Article 20(1) of the document, which relates to the necessity of concluding security agreements with countries outside the EU:** *"Actions carried out under the Programme shall comply with the applicable security rules and in particular rules on the protection of classified information against unauthorised disclosure, including compliance with any relevant Union and national law. In the case of research carried out outside the Union using or generating classified information, it shall also be necessary that, in addition to the compliance with those requirements, a security agreement shall have been concluded between the Union and the third country in which the research is to be conducted."*

Included in the Economic Security Package, presented by the European Commission in January 2024, was also a consultation document, the **White Paper on Options for Strengthening Support for Research and Development Involving Dual-Use Technologies** highlighting that a significant number of technologies crucial for the EU's economic security have dual-use potential,. In the context of the changing geopolitical situation and the associated new challenges, risks, and threats, the European Commission finds it increasingly important to support research and development involving technologies with dual-use potential. Apart from stimulating discussion, the **White Paper presents possible adjustments to the conditions of the EU Framework Programme for Research and Innovation**, which currently supports research and development activities focused solely on civilian use.

The European Commission, together with member states, **has recently begun discussions on preparing the upcoming tenth EU Framework Programme for Research and Innovation**, also in the context of strengthening research security. Given the aforementioned list of activated measures and initiatives, it is clear that the new generation of security measures will significantly influence the shape of the programme that will replace the current Horizon Europe programme from 2028 onwards. Experiences from previous framework programmes related to the strategic interests of the EU can certainly offer valuable insights. Therefore, it is not out of place to be inspired by the motivational saying "**fortune favours the prepared mind**" in the coming years.

NATIONAL LEVEL

The Czech Republic (CR) is among the world's most democratic and economically advanced countries and is well aware of its responsibility to respond to the current risks associated with the internationalisation of research, development, and innovation. Drawing from its own experience with a totalitarian regime and the transition to democracy, the CR leverages this knowledge to establish relevant measures within the context of democratic principles and EU policies, fulfilling its duty to help higher education and research institutions responsibly address the situation. The following chapter outlines initiatives and measures at the national level that relate to the issues of illegitimate interference, strengthening institutional resilience, and ensuring research security.

KEY DOCUMENTS ON SECURITY ISSUES

The current security environment and threats to the Czech Republic are described in the **Security Strategy of the Czech Republic 2023**, which also **contributes to assessing security issues within the higher education and research environment**. The strategy highlights the interconnectedness of security threats, where internal and external security, security in the physical and online realms, and the security of the state, society, and individuals cannot be separated. It emphasises a whole-government and whole-society approach, where not only each institution but also every citizen contributes to ensuring security through their behaviour and approach.

In the context of the document's content, the Czech Republic must be capable of active prevention and management of economic pressure or influence operations, including the issue of illegitimate interference in the higher education and research environment. Czechia's task is to prevent certain state and non-state actors from gaining economic or technological advantage through illegitimate practices or directly harming private companies, higher education and research institutions, or national interests. According to the strategy, a key role in managing these threats lies in ensuring proper institutional and personnel protection mechanisms. The Security Strategy also points to risk actors who pose a global security threat and increasingly assert their interests by attempting to reshape the current rules-based international order. They utilise tools of hybrid influence as well as the openness of international cooperation in the higher education and research environment.

> Through the published strategy, the CR also declares its active approach and readiness to create a safe environment for conducting world-class research, development, and innovation. Simultaneously, it emphasises that **ensuring the secure implementation of research, development, and innovation, as well as the safe deployment of technologies, is a crucial** condition for the further development of the Czech economy.

Information related to the security situation and threats to the CR is also reflected in the annual reports of the **Security Information Service (BIS)**. The BIS has been drawing attention to the risks and threats of illegitimate interference by foreign powers in the context of international cooperation in higher education and research environments for a long time. It also stresses the need to raise awareness of this issue within society, the importance of proper education for employees of relevant institutions, and the recognition of personal responsibility.

The National Cyber and Information Security Agency (NÚKIB) plays a key and irreplaceable role in safeguarding the cyber security of the Czech Republic. Its challenging task is regularly summarised in the **Annual Reports of the National Cyber and Information Security Agency**, which also reflect on the higher education and research environment. Through its extensive activities and awareness efforts, the NÚKIB highlights the fact that **higher education and research institutions possess valuable information** that is often and easily **targeted by cyber espionage**. In the context of the current geopolitical tensions and an increasingly digital world, cyber security is not just the concern of a few institutions or individuals but depends on the responsible approach of all of us.

METHODOLOGICAL AND SYSTEMIC SUPPORT

The increasing media coverage of domestic and international events and cases concerning the international cooperation of higher education and research institutions in recent years has led to a greater awareness of the need to protect relevant institutions from illegitimate interference.

In response to this issue, in 2021, the Ministry of the Interior developed the **Counter Foreign Interference Manual for the Czech Academic Sector**, which primarily provides a summary of advice and recommendations, as well as guidelines on how to deal with situations involving influence by foreign powers, and how to react and proceed. The manual does not aim to describe all possible ways in which influence by foreign powers on higher education and research institutions might occur but focuses on describing basic techniques and procedures. Experience shows that it is not always possible to prevent all threats in their breadth and complexity, but it is good to be aware of them and to prepare for them. In 2022, in response to further cases and in cooperation with the Czech Academy of Sciences for its internal use, the **CAS Manual for Counter Foreign Interference** was issued.

The Czech government, by its **Resolution No 794 of 25 October 2023,** on the proposal to expand the system to strengthen the resilience of public administration against illegitimate interference, instructed the First Deputy Prime Minister and Minister of the Interior **to enable higher education and research institutions to undergo training focused on the issue of illegitimate interference, organised by the Ministry of the Interior**.

In the spring of 2023, the Ministry of Education, Youth, and Sports established a platform called the **Interdepartmental Working Group for Combating Illegitimate Interference in Higher Education and Research**, which main goal is to delve deeper into the issue of illegitimate interference and to create a system of appropriate measures that will contribute to strengthening and protecting the higher education and research environment at the national level, fully within the context of EU policy. The group's members represent the Ministry of Education, Youth, and Sports; the Ministry of the Interior; the Ministry of Industry and Trade; the National Cyber and Information Security Agency; the Financial Analytical Office; the Research, Development, and Innovation Council; and the Office of the Minister for Science, Research, and Innovation. Representatives of the Czech Academy of Sciences and higher education institutions participate in the group's meetings as permanent guests.

The group's intention is also to prepare a **set of methodological materials** (such as the presented set of documents for increasing resilience to illegitimate interference in the higher education and research environment) to help assess potential risks of international cooperation relevant to all actors involved in the research, development, and innovation ecosystem in the CR. They should create possible guidelines for setting up internal mechanisms necessary to strengthen institutional resilience to illegitimate interference.

A key action at the national level with a significant impact on research security and the strengthening of institutional resilience in higher education and research institutions is the fact that the **Ministry of Education, Youth, and Sports, as the Managing Authority of the Jan Amos Komenský Operational Programme**, has also incorporated this issue into the planned **Research Environment call**, specifically into **Activity 9 – Setting up a System to Increase Institutional Resilience to Illegitimate Influence**. This call, published in June 2024, aims to support the development of capacities, knowledge, and skills of managerial, research, and other staff of research organisations in the area of strategic research and development management, with the goal of increasing their professional capacity for managing research organisations and strategically managing research and development, and creating internationally competitive conditions and a resilient, secure environment for conducting excellent research and development. Higher education and research institutions can thus take advantage of this incentive to internally set up the necessary management mechanisms, systematically institutionalise them, and safeguard the personnel for this agenda. Raising awareness of this issue and ensuring the education of employees is a mandatory part of implementing Activity 9.

The development of research security policies at the national level will be influenced by proactive actions and the future incorporation of related issues into key strategic or legislative instruments. Higher education institutions, in accordance with the obligation given by Act No 111/1998 Coll., on Higher Education Institutions and Amending and Supplementing Other Acts, must annually submit an **annual report on the activities of the university and an annual report on the management of the university to the Ministry of Education, Youth, and Sports**. **Starting in 2025, the outline of the annual report on the activities of the university** will also include a section related to the **issue of strengthening resilience against illegitimate interference**. At the end of 2023, a **draft of a new Act on Research, Development, Innovation, and Knowledge Transfer and amending certain acts** was presented.

It also mentions issues related to research security and the need to strengthen institutional resilience against illegitimate interference in the research environment. Another potential systemic measure could be incorporating this topic into subsequent measures of the **National Policy of Research, Development and Innovation of the Czech Republic 2021+** or into the **Methodology for the Evaluation of Research Organisations and Programmes of Purpose-Oriented Support for Research, Development, and Innovation**.

INTERNATIONAL PARTNERS

As an equal member and partner of the EU, the Czech Republic actively contributes to strengthening the resilience of the European Research Area through various measures and within the context of the aforementioned activities. However, **it also finds it beneficial to collaborate and allow the exchange of experiences and the sharing of good or bad practices related to research security with other democratic states outside the EU**. The Czech Republic believes that only such an approach can help protect democratic higher education and research institutions worldwide and make them more resilient. **In recent years, the Czech Republic has established close cooperation in this area, particularly with the United Kingdom and the United States of America** and recognises that the international expert meetings held with representatives from both countries have brought many useful insights to the national context. **The recommendations of the British Rectors' Conference on research security** are certainly an inspiring document, as are the guidelines from the **UK's National Protective Security Authority (NPSA) on research security or the** practical guidelines **published by the University of Liverpool**. Equally thought-provoking is the US government document **(NSPM-33) on the National Security Strategy for US Government-Supported Research and Development or the ASCE programme,** which leverages the expertise of universities to address threats posed by foreign adversaries to US academic institutions.

> **The Czech Republic will continue to strive to deepen cooperation and share relevant information with democratic states regarding research security**, as it is primarily in its own interest to strengthen the trust of international partners and simultaneously demonstrate readiness to protect the higher education and research environment from hostile intentions.

INTERCONNECTED AGENDA

The Czech Republic is fully aware that the **issue of illegitimate interference within the higher education and research environment is closely intertwined with a wide range of activities that require careful attention in the context of international cooperation.** These include sanctions policies and mechanisms, research on dual-use technologies, export control of dual-use goods, the field of technical assistance and intangible transfer of technologies, foreign investment screening, cyber security, and the protection of the reputation of Czech higher education and research institutions.

The following documents and activities can contribute to deepening awareness of the areas related to strengthening research security:

- In 2021, the Ministry of the Interior developed the **Counter Foreign Interference Manual for the Czech Academic Sector**, which primarily offers a summary of advice and recommendations, as well as guidelines on how to handle situations involving illegitimate interference by foreign powers, and how to respond and proceed. In 2022, the Czech Academy of Sciences Manual for Limiting Illegitimate Interference by Foreign Powers was published.

- In 2021, the Financial Analytical Office introduced a methodological tool primarily intended for higher education and research institutions, titled **Technical Assistance and Intangible Technology Transfer Handbook,** which addresses restrictive measures within the framework of international sanctions and the related issue of intangible technology controls. This handbook is set to be updated in 2024.

- In 2022, the Czech Customs Administration launched an awareness initiative called **Let's Protect Europe Together,** aimed at fostering partnership, cooperation, and assistance to the business community and academia in preventing the illegal proliferation of goods, technologies, and information subject to export controls.

- The Ministry of Industry and Trade regularly reports (**via annual reports)** on the operation of the foreign investment screening mechanism, which may be relevant in some cases, particularly for spin-offs dealing with emerging and disruptive technologies.

- In 2023, the Ministry of Education, Youth, and Sports dedicated the **6th edition of the National Day of Large Research Infrastructures to the issue of illegitimate interference, focusing on raising awareness and resilience**. The record from this conference contains a wealth of valuable information related to this issue from both national and international perspectives.

INSTITUTIONAL LEVEL

The aim of the following chapter is to provide a general overview of the scope and possibilities for addressing the issue of illegitimate interference within higher education and research institutions, fully in line with institutional autonomy and academic freedoms. At the same time, this chapter seeks to deepen understanding of the issue and explore the possibility of establishing the process of strengthening research security at the institutional level, from the moment of recognising the reality of the threat to the implementation of protective measures and procedures, always adequate to the potential risks faced by the institution.

POSITION OF HIGHER EDUCATION AND RESEARCH INSTITUTIONS

The European Commission, in its Economic Security Package presented in January 2024, strongly emphasises the changes in the international environment. Growing strategic competition and a return to power politics are influencing international relations, resulting in threats that are more diverse, unpredictable, and often hybrid[10].

---

10 Hybrid threats, in the context of the Council's proposed Recommendation on Strengthening Research Security, refer to cases where state or non-state actors attempt to exploit the EU's vulnerabilities for their own gain by using a coordinated combination of measures (e.g., diplomatic, military, economic, and technological) without formally waging war.

Not only are scientific values such as academic freedom, ethics, research integrity, and the principle of openness under pressure, but there is also a risk of unwanted knowledge transfer and the misuse of research outcomes. Scientific knowledge and its resulting applications are increasingly being strategically used by some states to globally demonstrate economic, political, and military power. **Higher education and research institutions are therefore finding themselves in increasingly challenging situations related to the risks of unwanted transfer of critical technologies to countries where they may be used in violation of [fundamental human rights](#) or to strengthen the military power of these countries.** Although such cooperation is not always prohibited or legally regulated in the CR, it is advisable to subject it to proper evaluation.

> **Defining and setting up effective measures to** strengthen research security and the resilience of higher education and research institutions against illegitimate interference is, according to the **[Proposal for a Council Recommendation on enhancing research security](#),** **often associated with balancing and finding possible solutions in "grey areas", where certain forms of international cooperation in research, development, and innovation are not prohibited but are still undesirable because they are unethical or pose risks to national and, not to say, EU security**.

RESPONSIBILITY

Higher education and research institutions, in accordance with academic freedoms and institutional autonomy as laid down by national legislation, their statutes, founding charters, and other relevant documents, **are responsible for the development and management of their international cooperation.** They are also fully aware of their role and responsibility to society and their obligation to protect democratic and academic values. This responsibility is declared by many of them through their signing of the **[Magna Charta Universitatum](#)**, accepted by over a thousand institutions worldwide.

The European Commission and the Czech government are interested in providing support to higher education and research institutions through relevant tools to make informed decisions and help them manage risks related to illegitimate interference. They are also keen to engage in open and constructive dialogue to anticipate and mitigate any potential side effects of security measures. Such dialogue will ultimately strengthen the support and impact of defined measures. However, in the end, and in relation to institutional autonomy, the **responsibility and implementation of specific measures lie fully with the higher education and research institutions themselves.**

The principle that "security is a collective responsibility with individual accountability" is also relevant in the context of research security. It aptly highlights the role and responsibility of the individual researcher. The best way to ensure the academic freedom of individual researchers and teams is to allow them to make as many decisions for themselves as possible. Where this is not feasible because the potential risks are too great or there are too many moral or other doubts, the institution should ensure the possibility of professional consultation or the option to leave the decision to a superior. In this respect, it is extremely important for higher education and research institutions to provide their staff with adequate **support in identifying and assessing risks and to determine at what level decisions can best be made**.[11]

---

11 [Knowledge-security-Academy-Position-Paper-October-2023.pdf](#)

Ultimately, responsibility for international cooperation in research, development, and innovation, for knowledge exchange, and for the protection of institutional autonomy and academic freedom rests with the management of the respective institution. It is also their task to provide support in assessing and finding compromises that need to be made at lower levels.

Lastly, it is the **responsibility of the Czech government to raise awareness of this issue, create appropriate support conditions, whether in the form of systemic or methodological measures or relevant information**, and thus help higher education and research institutions to responsibly and safely handle the current situation.

PROACTIVE APPROACH

Only a responsible approach by the institutions themselves to illegitimate interference will help protect the reputation of the Czech higher education and research environment, safeguard academic rights and freedoms, ensure research openness, and enable institutions to maximise the benefits of their research efforts. At the same time, this approach sends a clear signal that the criterion of research security is properly incorporated into their institutional environment and daily operations.

A proactive approach by higher education and research institutions to the threats of illegitimate interference ultimately **helps to**:[12]

- Protect the institution's reputation.
- Protect the reputation of the research team.
- Protect the reputation of individual researchers.
- Prevent unauthorised access to valuable research, sensitive, or personal data of the institution.
- Prevent the loss of potential future partners, grants, contracts, or talented researchers.
- Protect academic freedom and research openness.
- Prevent the questioning of trust in the research results or data of the institution.
- Prevent the loss of research data.
- Prevent the loss of intellectual property, patent opportunities, and potential financial income.
- Avoid competitive disadvantages in relevant research fields.
- Prevent foreign governments from gaining unauthorised commercial, technical, or intellectual advantages.
- Avoid legal or administrative consequences.
- Prevent economic disadvantages and threats to the security of the CR, the EU, and NATO.
- Uphold principles of social responsibility and maintain ethical standards.

---

12 Research Foundation – Flanders – Knowledge security (fwo.be)

MEASURES

Higher education and research institutions are encouraged in EU policies and documents related to strengthening research security, specifically in the **Council Recommendation on Enhancing Research Security,** to enhance research security through the responsible implementation of measures related to **risk management, risk assessment, and the execution of due diligence**. Institutions are further urged to have thorough knowledge of their potential partners and suppliers and, in line with their organisational structure, to distribute internal decision-making processes hierarchically for high-risk cases. When entering into agreements, memoranda, or other documents related to research collaboration, institutions should, according to the European Commission, include security criteria and associated key conditions, as well as establish rules for international relations, including receiving delegations or travelling abroad. This issue should also be properly reflected in personnel policies, as well as in the educational and training offerings and tools of the institution. It is essential to secure the physical and cyber spaces and implement measures that ensure access to areas such as laboratories, research infrastructures, databases, or systems that may contain sensitive information, only under clearly defined conditions. To ensure individual security, it is crucial and necessary to prevent all forms of direct or indirect discrimination and stigmatisation.

Specific measures, based on the above recommendations from the European Commission, should be implemented by higher education and research institutions **in proportion to the risks they face**. **The following pillars can serve as a supporting system**:

- **Risk Management:** Institutions should systematically institutionalise the agenda, set up internal processes and mechanisms that support their resilience in proportion to the risks related to the focus of their research activities, and define measures and a risk management system associated with internationalisation.

  A more detailed elaboration of this risk management pillar and the institutional handling of the issue is the subject of the **Methodological Recommendation for Risk Management in Research Security at the Institutional Level, developed in parallel with this general document**.

- **Due Diligence and Risk Management in Collaboration with Third Parties:** Institutions may assess potential risks associated with potential research partners or suppliers by conducting due diligence; informing decision-making bodies of possible risks; assessing the potential of technologies and/or research; verifying the absence of conflicts of interest; and establishing clear rules related to risk management in collaboration with third parties when entering into international research, development, and innovation collaborations, and when receiving foreign delegations or travelling abroad.

  A more in-depth exploration of this area is the subject of the **Methodological Recommendation defining the minimum scope of due diligence and risk management in cooperation with third parties within the context of strengthening the resilience of higher education and research environment against illegitimate interference**.

- **Communication, Education, and Sharing Experiences:** Institutions should have a plan to raise awareness of issues related to illegitimate interference and to strengthen institutional resilience and research security; they should provide training to staff, students, and others involved in international collaboration or other activities relevant to these issues; and they should aim to build a knowledge community and share experiences and best practices.

  The **Counter Foreign Interference Manual for the Czech Academic Sector** published by the Ministry of the Interior in 2021 can be used as a basic material, offering primarily a summary of advice and recommendations on how to recognise and respond to illegitimate interference.

The Czech Government Resolution No 794 of 25 October 2023, on expanding the system to strengthen public administration's resilience against illegitimate interference, allows higher education and research institutions to undergo training on the issue of illegitimate interference provided by the Ministry of the Interior.

- **Cybersecurity:** Institutions should, in line with the relevance of the Cybersecurity Act, reflect the supportive materials issued by the National Cyber and Information Security Agency when ensuring their cybersecurity. At a minimum, institutions should implement online educational courses focused on cybersecurity available on the **osveta.nukib.gov.cz** portal.
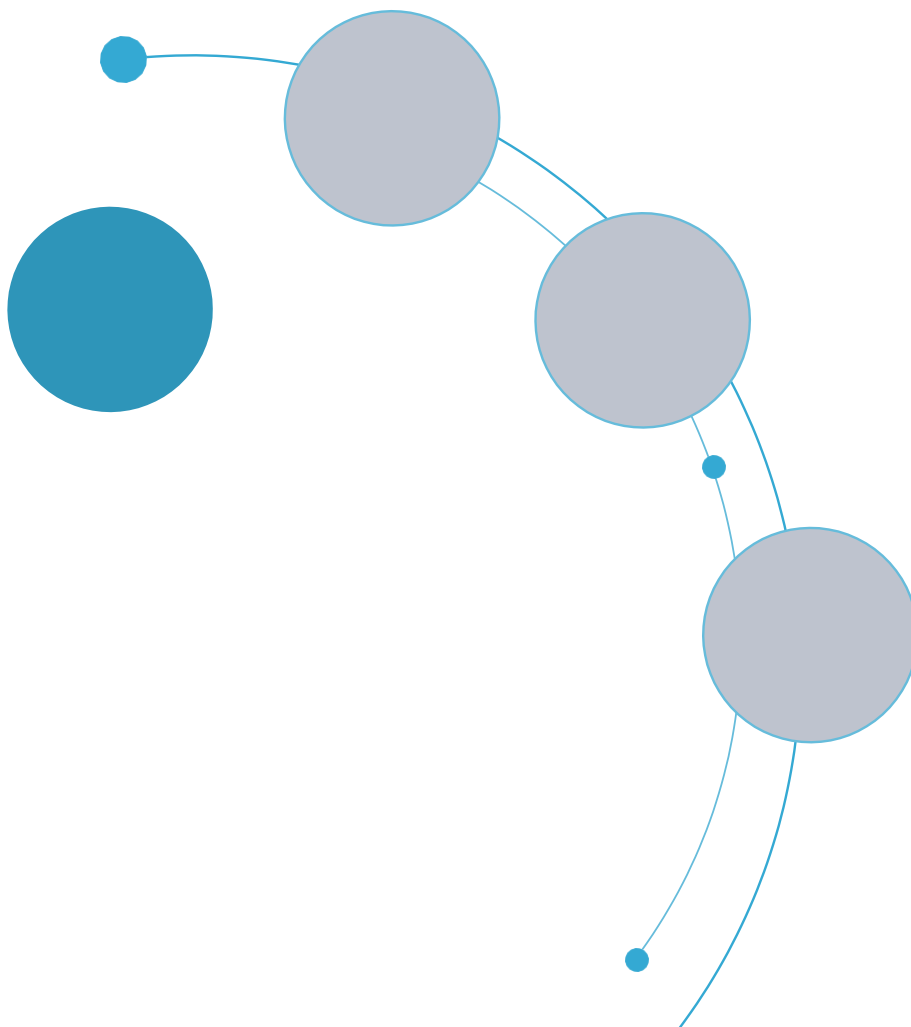
CONCLUSION

Only through raising awareness of the issue of illegitimate interference, adopting a proactive approach, and implementing appropriate and proportionate measures that connect institutional, national, and international levels, can the resilience of Czech higher education and research institutions be strengthened. This, in turn, will enhance the security of the European research area and the related economic security of the EU, as it is particularly true here that the stronger the individual components, the more resilient and stable the whole.