COLLECTION OF DECISIONS AND ORDINANCES OF THE UNIVERSITY OF SOUTH BOHEMIA IN ČESKÉ BUDĚJOVICE

Number: R 566 Date: 21 November 2024

Rector's ordinance on strengthening resilience to illegitimate influence at the University of South Bohemia in České Budějovice

Article 1

Introductory provisions

1) International cooperation in research, development and innovation is primarily based on a shared understanding and respect for fundamental values and principles such as academic rights and freedoms, research ethics, research integrity and the principles of open science. However, these fundamental values and principles make higher education and research institutions particularly vulnerable to illegitimate influence.

2) Higher education and research institutions are directly responsible for the management and development of their international cooperation, in accordance with academic freedoms and their autonomy. At the same time, these institutions are fully aware of their role and responsibility towards society and the task of safeguarding democratic and academic values.

3) The aim of this ordinance is to set up internal processes at the University of South Bohemia in České Budějovice (hereinafter referred to as 'USB') in order to strengthen USB's resilience to illegitimate influence (hereinafter also referred to as 'institutional resilience'). In particular, it emphasises the need to spread awareness of this issue across USB, the need for proper education of its employees and students, and the awareness of the personal responsibility of each of them.

4) In the case of higher education and research institutions, institutional resilience should be perceived as the ability to implement a system of measures to strengthen research security against illegitimate influence and to protect their reputation, consisting in particular in safe international research and academic cooperation, including compliance with binding sanction restrictions, in intellectual property management and risk management, especially in areas of research with significant transformative potential of knowledge and technology, in areas related to dual-use technologies and military equipment but also in managing the risk of misuse of knowledge or technology for violating human rights and freedoms.

5) The USB management is committed to the implementation and development of protective measures to enhance research safety at the University of South Bohemia in České Budějovice. The aim of such measures is to prevent and counter threats of illegitimate influence or to ensure the credibility of research conducted at USB.

6) In strengthening its resilience to illegitimate influence, USB draws in particular on generally applicable legislation[1] and public guidance materials related to this area.[2]

7) This ordinance uses generic masculine forms for simplicity in its text.

Article 2

Basic terms

1) 'Illegitimate influence' is a term for unwanted influence on people, decisions or processes. It includes the influence of foreign power but also criminal (e.g. corrupt) behaviour and unwanted lobbying. It usually refers to activities which are covert, deceptive, coercive or corrupt and which are carried out by the originator or perpetrator of illegitimate influence (foreign power, corruption, lobbying in violation of the law or generally accepted social ethical rules), either alone or through a third party, and which threaten or damage the interests of higher education and research institutions.

2) According to the Council Recommendation on Strengthening Research Security,[3] illegitimate influence in research, development and innovation is considered to be, in particular:
(a) the unwanted transfer of critical knowledge, know-how and technology that may affect the security of the EU and its Member States, for example, if used for military or intelligence purposes in third countries,
(b) misuse of research activities to disseminate misinformation based on influence from third countries/parties,
(c) incitement of self-censorship among students and researchers leading to the erosion of institutional autonomy,
(d) violation of scientific ethics or research integrity resulting in the misuse of knowledge and technology to suppress or undermine fundamental democratic values.

3) 'Foreign power' is understood a foreign state or an organ thereof, or a supranational or international organisation or an organ thereof, as well as any other natural persons, regardless of their nationality, and legal persons, regardless of their registered address or place of operation, if they participate, even if only partially, in the promotion of the interests of a foreign state or organisation by means of illegitimate influence.

4) The term 'due diligence' is understood to mean due care representing a set of measures designed to eliminate or reduce the risks of illegitimate influence on higher education and research institutions arising from cooperation with third parties.

5) The term 'balanced openness' refers to the balance between developing open cooperation with international partners on the one hand and enhancing research security on the other.

Article 3

USB Security Manager

1) The USB Security Manager is responsible for the area of USB resilience to illegitimate influence.

2) The USB Security Manager reports directly to the USB Rector and is assigned to the Rector's Office within the organisational structure of the USB Rectorate.

3) USB Security Manager in particular:
(a) sets up and continuously adjusts the system of USB resilience to illegitimate influence,
(b) monitors current developments and receives ongoing training in the area of resistance to illegitimate influence in the higher education and research environment,
(c) keeps the Rector or the Rector's Board informed of changes and the current situation in the area of resistance to illegitimate influence in the higher education and research environment,
(d) regularly assess the risks associated with institutional resilience, including the identification of sensitive areas of education and research at USB[4] (degree programmes, research teams, projects, instruments, equipment or technologies, scientific outputs including research data),
(e) establishes a system and schedule for training USB staff and students to enhance institutional resilience,

(f) provides consultation and advice to USB staff and students on institutional resilience,
(g) receives and maintains records of the reports referred to in Article 6 of this ordinance and records of the risk assessments prepared for partners referred to in Article 8 of this ordinance, including related documents.

4) The USB Security Manager cooperates:
(a) with USB faculty and other constituent parts of USB on institutional resilience through institutional security officers,
(b) with the USB Cybersecurity Manager in the area of information security and cybersecurity,
(c) with the USB Technology Transfer Office Head in the area of intellectual property protection and technology and knowledge transfer,
(d) with the USB Bursar in the area of evaluating restrictions imposed by international sanctions or monitoring regimes and in the area of foreign investment screening,
(e) with the USB Ethics Committee in the field of ethics and research integrity at USB,
(f) with the Occupational Safety and Health and Fire Protection Officer in the area of physical security,
(g) with the USB Research Data Manager in the area of USB research data management,
(h) with other higher education institutions, government authorities, security services, embassies, international organisations and other relevant actors.

Article 4

Institutional resilience officers

1) For individual remits related to the issue of research security at USB, there are designated institutional resilience officers:
(a) economic remit – the Bursar,
(b) personnel remit – the Head of the Rectorate's Human Resources Office,
(c) project remit – the Vice-Rector for Development and Public Relations,
(d) internationalisation remit – the Vice-Rector for International Relations,
(e) science and research remit – the Vice-Rector for Research.

2) Institutional resilience officers, in particular:
(a) cooperate with the USB Security Manager and follow his instructions and recommendations,
(b) methodically manage and cooperate with the relevant persons at faculties (secretaries, heads of human resources offices, vice-deans with relevant remits) or directors of other USB constituent parts (hereinafter referred to as 'responsible persons at constituent parts') within their respective remits,
(c) receive regular training in institutional resilience,
(d) receive information and reports on institutional resilience from employees assigned to the given constitutional part and students enrolled at the constituent part through the responsible persons at constituent parts,
(e) provide consultation and advice on institutional resilience to staff and students of the given constituent part through the responsible persons at constituent parts,
(f) regularly assess and identify at-risk degree programmes, areas of education, disciplines and specific research teams, projects, instruments, equipment and technologies in the given constitutional part in collaboration with the responsible persons at constituent parts.

Article 5

Obligations of staff and students

1) Employees and students of USB are required to conduct themselves in a manner that prevents the possibility of foreign powers influencing USB and prevents the violation of regulations related to international monitoring and sanction regimes.

2) If attempts to exert foreign influence or breaches of the regulations referred to under section 1 occur, staff and students are obliged to report such incidents without undue delay (Article 6 of the ordinance).

3) Before entering into a contractual relationship with an external partner, staff members are required to examine the risks of working with the relevant contractor (Article 8 of the ordinance). This also applies to the conclusion of memoranda and declarations of cooperation.

4) When agreements or memoranda and other documents relating to research and education cooperation are concluded, their content should include the criterion of security and related key conditions, as well as the establishment of rules applicable to foreign relations in the context of receiving delegations or going abroad.

5) Employees are required to complete institutional resilience training and to update their training regularly. Selected staff members who are more likely to be targets of influence, particularly in view of their leadership roles, discipline or field of study, are to receive enhanced training.

6) Students are required to take institutional resilience training if the USB Security Manager decides so.

7) Violation of the obligations under sections 1 to 5 shall be considered a serious violation of obligations arising from legal regulations related to the work performed by the employee within the meaning of Section 52(g) of Act No 262/2006, the Labour Code.

8) Violations of the obligations under sections 1 to 2 and 6 by students shall be considered as violations of the obligations set forth in legal regulations or internal regulations of the University within the meaning of Section 64 of Act No 111/1998, on Higher Education and on Amendments and Supplements to Other Acts (Higher Education Act).

Article 6

Security incident reporting

1) If a staff member or student suspects or attempts to exert foreign influence, or if a situation of illegitimate influence is observed or suspected in the context of cooperation with third parties, or if such a situation is created or suspected retrospectively, he shall immediately report these facts to the responsible person in the constituent part or directly to an institutional resilience officer (Article 4 of the ordinance).

2) The report referred to in section 1 shall indicate who is making it and what it concerns. The USB Security Manager may issue a template for such a report.

3) The responsible person at his constituent part and the relevant institutional resilience officer shall, within a time appropriate to the circumstances and the seriousness of the content of the report, review and forward the report to the USB Security Manager. The USB Security Manager shall, within a timeframe appropriate to the circumstances and the seriousness of the content of the report, evaluate it, provide feedback and recommend a course of action, if appropriate. To do so, he may seek the advice of the responsible person at the constituent part and the relevant institutional resilience officer. Where necessary or appropriate, the USB Security Manager shall report the facts to or consult with government authorities or security services.

4) Serious security incidents are reported by the USB Security Manager to the Rector or Dean along with his recommendation. The Rector or Dean will decide on the next course of action in such cases, normally after

discussion with his Board.

Article 7

Mandatory reporting on international sanctions and monitoring regimes

1) In cases where it is suspected that a prospective student, job applicant, or potential partner collaborating on a research or educational project is from a country subject to international sanctions[5] related to the ban on technical assistance, the faculty student affairs office, the human resources office of the constituent part, or the project team must report this without undue delay to the responsible person at the constituent part, the institutional resilience officer, or directly to the USB Security Manager.

2) The report referred to in section 1 shall indicate who is making it and what it concerns. The USB Security Manager may issue a template for such a report.

3) The USB Security Manager, in liaison with the responsible person at the constituent part or an institutional resilience officer, as appropriate, will recommend further action to the Rector or Dean, depending on the authority in the matter, in particular, whether the admission procedure, selection procedure or project preparation can be continued, or under what conditions. In making this recommendation, he shall be guided by the individual circumstances of the case, the degree programme, the field of study, or the scientific discipline concerned. He is obliged to comply with all generally binding legislation, including informing or obtaining the opinion or permission of the public authorities. The Rector or the Dean shall decide on the further course of action, normally after discussion with his Board.

4) If there is a change in any of the international sanctions regimes that could affect education or scientific research, the USB Security Manager will inform the USB institutional resilience officers and the responsible persons at the constituent parts. The relevant institutional resilience officers will then investigate whether further action needs to be taken in relation to applicants, students, job applicants, employees, contractual or research partners. If such action is necessary, he informs the USB Security Manager. Section 3 shall apply as appropriate.

Article 8

Partner risk assessment (due diligence)

1) Cooperation with third parties is an integral part of the activities of every higher education and research institution. Most of this cooperation is beneficial and has no or minimal risks of illegitimate influence. At the same time, however, there are areas of cooperation between higher education institutions and third parties that carry risks of illegitimate influence to such an extent that it is highly desirable for higher education institutions to try to reduce these risks as far as possible.

2) Due diligence is divided into basic and detailed. Basic due diligence[6] should be applied as widely as possible, ideally whenever a university or research institution is setting up a relationship with a new partner, changing its relationship with an existing partner, or repeatedly during a long-term collaboration. Detailed due diligence[7] should be used particularly when basic due diligence provides information indicating that the collaboration under review carries increased risks.

3) Prior to entering into a contractual relationship with an external partner, in particular, a partnership agreement, research agreement or memorandum and declaration of cooperation, the employees responsible for the preparation of such an agreement or memorandum are required to assess the risks of cooperation with the other party. It is also advisable to check what internal rules and procedures the potential partner institution has in place for cooperation with third parties before starting a specific cooperation.

4) In the event that entering into such a contractual relationship or memorandum poses a risk of damage to the reputation of USB or the employees or students involved, the exercise of foreign influence, violation of restrictions under international monitoring and sanctions regimes, or theft of intellectual property, the employee is required to contact the responsible person at the constituent part, an institutional resilience officer, or the USB Security Manager, who will assess the situation and recommend a course of action.

5) The USB Security Manager may identify selected USB components, degree programmes, areas of education, disciplines, scientific or educational projects, countries of origin of the contractor, or other features of the contractual relationship that require a written risk assessment. This assessment shall then be submitted by the USB Security Manager to the Rector or Dean, as appropriate, along with his recommendation. The Rector or Dean will decide on the next course of action, normally after discussion with his Board.

6) Cooperation is understood here as a broad concept, including documents (contracts, memoranda, etc.), foreign travel, visits by third-party representatives, as well as patronage, funding, gifts and tokens. The USB Security Manager may, through a methodological recommendation for each such activity, specify the elements that such risk assessment must meet.

Article 9

Final provisions

1) The issue of protection of research data in the preparation and conduct of research and its accessibility will be addressed by a separate ordinance of the Rector.

2) Typical situations that may arise in connection with the application of this ordinance and recommendations for these situations are specified in the methodological document 'Implementation recommendations supplementing the Rector's ordinance on strengthening resilience to illegitimate influence at the University of South Bohemia in České Budějovice'.

3) This ordinance comes into force and takes effect on the date of publication in the collection of the Rector's decisions and ordinances in the public section of the USB website.

prof. Ing. Pavel Kozák, Ph.D.
Rector

Prepared by: Vice-Rector for Research, Vice-Rector for International Relations

Distribution list: USB management, Deans of USB faculties, Directors of other constituent parts of USB, USB Cybersecurity Manager, Chair of the USB Ethics Committee, Occupational Safety and Health and Fire Protection Officer

---

[1] In particular, Act No 69/2006, on the implementation of international sanctions, Act No 594/2004, implementing the European Communities regime for the monitoring of exports of dual-use goods and technology, Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 establishing a Union regime for the monitoring of exports, brokering, technical assistance, transit and transport of dual-use goods.

[2] Especially the methodological materials of MEYS:

- Strengthening resilience to illegitimate influence in higher education and research environments,

- Methodological recommendations on research safety risk management at the institutional level,
- Methodological recommendation defining the minimum scope of due diligence and risk management of collaboration with third parties in the context of strengthening the resilience of the higher education and research environment to illegitimate influence (hereinafter referred to as the 'Methodological recommendation on collaboration with third parties'); and
- other materials listed in these guidance materials.

[3] https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=OJ:C_202403510
[4] Article 6 of the Methodological recommendation on cooperation with third parties.
[5] Within the meaning of Section 2 of Act No 69/2006, on the Implementation of International Sanctions.
[6] Article 7 of the Methodological recommendation on cooperation with third parties.
[7] Article 8 of the Methodological recommendation on cooperation with third parties.