For breaches related to cyber security, N.17(I)/18 provides at article 16 that in case of a failure to comply with its provisions or of the provisions of secondary legislation based on N.17(I)/18 could lead to a fine of up to 10.000 euro and/or imprisonment of up to 6 months.

(ii) Are there administrative fines related to data protection issues?

According to article 32 of the N.125(I)/18, the Commissioner for the Protection of Personal Data may give an administrative fine according to article 83 of the GDPR. Where the person which sustains the fine is a public authority and relates to non-for-profit activity, the fine shall not exceed 200.000 euro.

As it relates to cyber security, according to article 13(κε) of N.17(I)/18, the DSA may give an administrative fine to any person that fails to comply with the provisions of N.17(I)/18 or any secondary legislation based on the said law. Such administrative fine, according to article 30, shall come up to 8.500 euro.

(iii) constitute an official offence or are only prosecuted by the injured party's request?

All criminal offences established under the relevant legislation shall be prosecuted by Cyprus Police via the office of the Attorney General of the Republic (Law Office of the Republic), after a complaint has been made to the police and an investigation have been conducted in order to support the case before the court.

6 Czech Republic

Radim Polčák (Masaryk University) Petra Lančová (Department of Medical Ethics, Faculty of Medicine, Masaryk University, Brno)

6.1 Informed consent

6.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Usnesení č. 2/1993 Sb., o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky (LZPS)	http://www.psp.cz/en/docs/laws/listina.html (English)	Constitutional law	It contains fundamental human rights and freedoms, including the right to the integrity of the person and his or her privacy and the protection of private and family life.

Zákon č. 110/2019 Sb., o zpracování osobních údajů (ZZOÚ)	https://www.zakonyprolidi.cz/cs/2019-110 (Czech)	Hard law	Adopted as an adaptation law to GDPR.
Zákon č. 89/2012 Sb., občanský zákoník (OZ) ***Civil Code***	https://www.cak.cz/assets/pro-advokaty/mezinarodni-vztahy/civil-code.pdf (English)	Hard law	Generally governs privacy, contains also provisions especially dealing with Image and privacy
Zákon č. 329/1999 Sb., o cestovních dokladech	https://www.zakonyprolidi.cz/cs/1999-329 (Czech)	Hard law	Regulates the conditions for issuing and using passports.
Zákon č. 328/1999 Sb. Zákon o občanských průkazech	https://www.zakonyprolidi.cz/cs/1999-328 (Czech)	Hard law	Regulates the issue of identity cards.
Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech	https://www.zakonyprolidi.cz/cs/2000-133 (Czech)	Hard law	Regulates the issue of the use of personal identification number. Explicitly specifies cases where PIN can be used and required.
Zákon č. 372/2011 Sb., zdravotních službách a podmínkách jejich poskytování (ZZS)	https://www.zakonyprolidi.cz/cs/2011-372 (Czech)	Hard law	Regulates some aspects of health care, such as confidentiality, the rule of access for medical documentation, etc.
Zákon č. 106/1999 Sb., o svobodném přístupu k informacím	https://www.zakonyprolidi.cz/cs/1999-106 (Czech)	Hard law	It lays down entities that are obliged under this Act to provide information relating to their

			competence, which are state authorities, territorial self-governing units and their bodies and public institutions.
Zákon č. 181/2014 Sb., o kybernetické bezpečnosti **(ZKB)**	https://www.zakonyprolidi.cz/cs/2014-181 (Czech)	Hard law	Regulates the rights and obligations of persons and the powers of public authorities in the field of cyber security.

Main regulatory tools addressing data protection issues and informed consent in Czech Republic

(i) The GDRP does not apply to purely personal or household activity. Is there any provision under national law for the protection of these data categories?

Generally, the right to privacy regulated as part of the fundamental personality right under §§ 84-90 of the Czech civil code (zákon č. 89/2012 Sb., občanský zákoník, http://obcanskyzakonik.justice.cz/images/pdf/Civil-Code.pdf (English)) provides such protection. We are not aware of any specific provisions in Czech law providing particular protection to personal data processing as purely personal or household activity.

(ii) The GDPR does not apply to national security. Is there any national regulation covering this topic (in terms of data protection issues)?

For personal data protection during activities concerning defensive or security interest of the Czech Republic provides ZZOÚ specific chapter IV (§§ 43-49). The provisions are largely similar to the respective provision of GDPR, the rights of data subjects may be restricted in accordance with the protection of the relevant defensive or security interest. Additional acts that can be considered relevant are the Act on Providing Defence of the Czech Republic (zákon č. 222/1999 Sb. o zajišťování obrany České republiky, https://www.zakonyprolidi.cz/cs/1999-222 (Czech)) and Act on Cybersecurity (with respect to the critical infrastructure, zákon č. 181/2014 Sb. o kybernetické bezpečnosti, https://www.zakonyprolidi.cz/cs/2014-181 (Czech)).

Name of Authority	Link (English version if possible be)	Is this an independent body?	Number of employees	Level of activity (according to your appreciation)?	Response to requirements, questions, etc. made

					by the public
Úřad pro ochranu osobních údajů (ÚOOÚ)	https://www.uoou.cz/en/	Yes	6 inspectors (source: https://www.uoou.cz/inspektori/ds-4697/archiv=0&p1=1059) 28 employees of the supervisory department (data from 18.10.2018, source: https://www.uoou.cz/pocet-zamestnancu-kontrolniho-odboru/ds-5300)	Active, but overburdened	Overburdened, limited capacity to timely respond

Information regarding Data Protection Authorities, Czech Republic

(iii) Does your national legislation introduce a specific definition of "data processing for research purposes"? Does your national legislation define "research in public interest", e.g. referring to Ministerial lists of expected research, etc.?

The term "data processing for research purposes" is used by ZZOÚ in § 16, but not defined. The Czech data protection authority (ÚOOÚ) published a statement concerning the personal data protection in the context of research in 2006 (https://www.uoou.cz/stanovisko-c-2-2006-zpracovani-osobnich-udaju-v-ramci-vedy/d-1485/p1=1881 (Czech)). The conclusions concerning definitions remain applicable despite the changes in the European as well as national personal data protection frameworks. The decisive definition is contained in the Act on R&D Support from Public Sources (zákon č. 130/2002 Sb. o podpoře výzkumu a vývoje z veřejných prostředků, https://www.zakonyprolidi.cz/cs/2002-130 (Czech)), where § 2 contains the definitions of "fundamental research" and "applied research". The "fundamental research" is defined through the reference to Article 2 point 84 of the Commission Regulation (EU) No 651/2014 of 17 June 2014 ('fundamental research' means experimental or theoretical work undertaken primarily to acquire new knowledge of the underlying foundations of phenomena and observable facts, without any direct

commercial application or use in view). The "applied research" is defined in the national act as theoretical or experimental work aimed at acquiring new knowledge or abilities for development of new or significantly improved products, processes or services, including industrial research, experimental development or their combination. The term "research in public interest" is not defined in the national law, although the aforementioned law provides a framework for public financing of research, which implicitly includes consideration of public interest related to the supported research.

(iv) Does your national legislation implement Article 89 of the GDPR, introducing in particular some specific safeguards to adopt in case of data processing for research purposes?

ZZOÚ contains § 16 concerning personal data processing in scientific or historical research. The provision further specifies the requirements pursuant to Article 32 GDPR through recommended measures. These include accent on data minimisation principle; documentation of the processing activities and storage of the records for at least 2 years after the operation; education of the processing individuals in personal data protection requirements; assignment of DPO; restriction of access to processed personal data; pseudonymisation; encryption; measures towards permanent confidentiality, integrity, accessibility and resilience of the processing systems and services; measures for restoration of accessibility and timely access in case of an incident; regular testing, assessment and evaluation of applied technical and organisational measures; special restrictions on transfer to third countries; or special restrictions on processing for other purposes. It further requires limitation of identifiability of the data subjects affected through processing of special categories of personal data pursuant to Article 9 GDPR, unless this measure would be contrary to the protected interests of the data subject. Included is also permissible restricted or delayed application of Articles 15, 16, 18 and 21 GDPR, if necessary, in pursuit of the research purpose of the processing. Article 15 GDPR shall not apply, if the processing is necessary for the purpose of the scientific research and the access to the data would involve disproportionate effort.

(v) Does your national legislation provide specific cases and safeguards for processing sensitive data beyond article 9 of the GDPR? Which cases? Which safeguards?

As stated in the previous answer, § 16 ZZOÚ requires limitation of identifiability of the data subjects affected through processing of special categories of personal data pursuant to Article 9 GDPR, unless this measure would be contrary to the protected interests of the data subject. This is to be understood as requirement for anonymisation or at least pseudonymisation of sensitive data, unless identifiability of the data subject is for him or her beneficial.

(vi) Do you have a national (or some regional) Code(s) of Conducts or national Code of Ethics for data processing in research? Could you please summarize the content of such codes (specifying scope, suggested measures to protect individuals, prohibitions, exemptions, etc.)?

There is no generally applicable Code of Conduct concerning data processing in research in Czech Republic. However, the Czech Academy of Sciences issued its Code of Ethics for Researchers of the Czech Academy of Sciences (http://www.avcr.cz/en/about-us/legal-regulations/code-of-ethics-for-researchers-of-the-czech-academy-of-sciences/index.html (English)), inter alia based on the European Charter for Researchers (2005/251/ES). It mainly concerns the morality and integrity of researchers while conducting research. There are no specific provisions concerning personal data

processing or protection of the data subjects affected by the research. It contains requirement for respect towards the fundamental principles of ethical research provided in the codex while collecting, selection and evaluation of data, taking into account the specifics of the given scientific discipline. It also states that the primary data and documentation of all significant results shall be preserved after publication of the result for a period usual with regard to the given scientific discipline, unless other requirements or legal obligations provide otherwise. The Czech government had a goal to develop an Ethical framework for research in 2005, however this initiative so far did not come to fruition.

(vii) Does your national legislation give specific definitions of data processing for "statistical purposes"? Are there specific rules that apply to such data processing?

ZOOÚ contains no specific definition of data processing for statistical purposes. The aforementioned specification of requirements for scientific and historical research pursuant to § 16 ZOOÚ further apply also to processing for statistical purposes. Indicative towards definition of this term should be the definitions provided in the Act on State Statistical Service (zákon č. 89/1995 Sb. o státní statistické službě, https://www.zakonyprolidi.cz/cs/1995-89 (Czech)). In § 2 letter g) of this act is the "statistical purpose" for the purpose of this act defined as a use for numerical, verbal or graphic description of aggregate events or processes in the society, national economy and environment with the help of statistical information. A statistical information is defined as an information with social, economic, demographic or ecological characteristics, which resulted from an aggregation of individual data.

(viii) Are there any other references to data processing for research purposes in your national legislation? (e.g. duties to have a DPO, duties to perform a DPIA, duty to collect consent, etc.)

As provided in a previous answer concerning § 16 ZZOÚ, aside from data minimisation requirements, access restriction, data transfer restriction and appropriate implementation and revision of technical and organisation measures, the recommended measures also include assignment of a DPO.

6.1.2 Rights of data subjects and data processing

(i) Are there any other references to data processing for research purposes in your national legislation? (e.g. duties to have a DPO, duties to perform a DPIA, duty to collect consent, etc.)

In § 81 OZ is stated that "personality of an individual including all his natural rights are protected and every person is obliged to respect the free choice of an individual to live as he pleases". An individual whose personality rights have been affected has the right to claim that the unlawful interference be refrained from or its consequence remedied. Furthermore, after the death of an individual, the protection of his personality rights may be claimed by any of his close persons.

OZ also contains some right for legal persons. If an unlawful interference with the personality rights of an individual is associated with his activities in a legal person, the right to the protection of his personality rights may also be asserted by that legal person; however, during his life, the legal person may do so only in the name of the individual and with his consent. After the death of an individual, a legal person may claim that the unlawful interference be refrained from and its consequences remedied.

(ii) Are there any special requirements regarding informed consent at the national level?

We are not aware of any special requirements with regard to the general provisions on informed consent. However, the provision in Czech law (§ 89 para. 3 of the Act on Electronic Communications, https://www.mpo.cz/en/e-communications-and-postal-services/electronic-communications/national-legislation-and-regulations/unofficial-consolidated-version-of-the-act-on-electronic-communications--effective-as-at-january-1--2015--156553/ (English, partially outdated)) concerning consent with use of cookies in the online data processing remains divergent from the harmonising provision of the E-Privacy Directive 2002/58/EC, as it sets the opt-out standard, whereas the European law requires the application of opt-in standard. ÚOOÚ released with regards to this issue and GDPR in May 2018 a recommendation for euro-conform interpretation of the national provision (source: https://www.uoou.cz/cookies-a-gdpr/d-29966 (Czech)) , this was however met with critique. The recommendation is currently being reworked pursuant to the recent CJEU decision in the case no. C-673/17, Planet49.

On the other hand, OZ works with different wording, when "svolení" (permission) is used instead of "souhlas" (consent). In is used in the context of using image of an individual, when § 84 OZ states that Capturing the image of an individual in any way that would allow his identity to be determined is only possible with his/her permission. The meaning is the same.

(iii) Are there any special requirements regarding data processing at the national level?

ZZOÚ contains in § 6 exceptions from the requirement on purpose compatibility assessment (Article 6 para. 4 GDPR) for protected interests, unless stated otherwise by the legislator, if the further processing is necessary and adequate for the fulfilment of an obligation or performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The protected interests include: (a) defence or security interests of the Czech Republic; (b) public policy and national security, prevention, investigation or detection of criminal offences, prosecution of criminal offences, execution of criminal penalties and protective measures, ensuring security of the Czech Republic and ensuring public policy and national security, including search for persons and objects; (c) some other important objective of public interest of the European Union or of a Member State of the European Union, in particular an important economic or financial interest of the European Union or of a Member State of the European Union, including monetary, pecuniary, budgetary and taxation matters, matters of financial market, public health and social security; (d) protection of independence of courts and judges; (e) prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; (f) a monitoring, inspection or regulatory function connected to the exercise of official authority in the cases referred to in (a) to (e) above; (g) protection of rights and freedoms of persons; or (h) enforcement of civil law claims.

Furthermore, § 10 ZZOÚ sets an exception form the DPIA obligation, if the personal data processing is required to be carried out under a legal regulation.

(iv) Are there any special requirements to exercise data subject's rights (right of access, correction, deletion of personal data)?

Under § 11 ZZOÚ, certain data subject´s rights may be limited. The exercise of the rights under Articles 12 to 22 GDPR may be limited or postponed in a necessary and reasonable

scope in order to ensure realisation of the protected interests, which are listed in the answer to the previous question (and in § 6 para. 2 ZZOÚ).

Data subject's rights to access are limited in these situations:

1) Processing of personal data for scientific or historical research purposes or for statistical purposes - § 16/3 ZZOÚ data subject's rights shall be postponed, if necessary and proportionate to the purpose of the processing referred above.

2) Processing of personal data for journalistic purposes or for academic, artistic or literary purposes

- § 20 ZZOÚ special rules for the exercise of rights of erasure or rectification of personal data

- § 22 ZZOÚ an objection may be raised only against the specific disclosure of personal data; in doing so, the data subject shall give specific reasons indicating that in the present case the legitimate interest in the protection of his rights and freedoms prevails over the interest in such disclosure.

3) Protection of personal data when processing for the prevention, search or detection of criminal activity, proceeding of criminal offenses, performance of penalties and protective measures, ensuring the security of the security of the Czech republic and the security of the security of the Czech republic (ZZOÚ)

4) Protection of personal data when securing the defence and security interests of the Czech republic (ZZOÚ).

Such limitation must be notified to ÚOOÚ without undue delay in detail set by Art. 23 para. 2 GDPR. This does not apply to processing operations by courts in judicial capacity, which are outside of the supervisory scope of ÚOOÚ (in accordance with Art. 55 para. 3 GDPR). Under § 12 ZZOÚ the communication of a personal data breach to the data subject may also be limited or postponed in order to ensure realisation of the aforementioned protected interests. This shall also be notified to ÚOOÚ as described above.

6.1.3 Minors, sensitive data and other additional categories of data

(i) Are there additional rules beyond the ones enforced by the GDPR for processing special categories of personal data (e.g. sensitive data or data of legal persons/entities)?

We are not aware of any additional rules in the Czech law in this regard.

Legal persons do not have personal data or personal rights according to Czech law.

However, according to § 83 OZ if an unlawful interference with the personality rights of an individual is associated with his activities in a legal person, the right to the protection of his personality rights may also be asserted by that legal person; however, during his life, the legal person may do so only in the name of the individual and with his consent. If an individual is unable to express his will due to his absence of or inability to reason, consent is not required. After the death of an individual, a legal person may claim that the unlawful interference be refrained from and its consequences remedied.

(ii) Are there any special rules when processing personal data of children? At what age can a minor provide consent according to your regulation?

Pursuant to § 7 ZZOÚ, a minor may provide consent from fifteen years of age on. There are no other special ZZOÚ provisions concerning minors.

(iii) Are there other vulnerable individuals identified in your national legislation?

The Czech ZZOÚ does not contain special provisions in this regard. We are not aware of other Czech legislation that would contain such provisions.

6.1.4 Deceased individuals and personal data

(i) As recital 27 clarifies, the GDPR does not apply to deceased individuals. However, some countries provide people with the right to have all their personal data deleted once they pass away. Some others empower their close relatives to do the same. In some others, these data cannot be used at all without an explicit judicial mandate. What is the situation in your country?

The post mortal protection of personal data is not specifically regulated under the Czech law. Thereby remains primarily applicable the legal framework for post mortal protection of personality rights pursuant to the Czech Civic Code (zákon č. 89/2012 Sb., občanský zákoník, http://obcanskyzakonik.justice.cz/images/pdf/Civil-Code.pdf (English)). Under § 82 para. 2 of the Czech Civic Code, any of close persons of the deceased individual is empowered to protection of his personality rights. A close person of an individual is defined in § 22 para. 1 of the Czech Civic Code as a relative in the direct line, sibling and spouse or a partner under another statute governing registered partnership; other persons in a familial or similar relationship shall, with regard to each other, be considered to be close persons if the harm suffered by one of them is perceived as his own harm by the other. Persons related by affinity and persons permanently living together are also presumed to be close person.

Pursuant to § 84 of the Czech Civic Code, capturing the image of an individual in any way that would allow his or her identity to be determined is only possible with his or her consent. The Czech legal doctrine is not united in the regard, if the substitute consent of one of the close persons is sufficient or if at least implicit (meaning not expressed disapproval) of all close persons of the individual is required.

6.1.5 Accountability and Data Protection Impact Assessment

(i) Does your national regulation introduce further provisions related to general accountability? Any particular requirements? Any specific procedures?

Under § 5 ZZOÚ is expressed an authorisation to process personal data. Controllers may process personal data where it is necessary for compliance (a) with their legal obligation stipulated by law; or (b) with a task carried out in the public interest or in the exercise of official authority vested in the controller. The particular interpretation of this provision in relation to Article 6 para. 1 letters c) and e), para 3 and Article 9 para. 2 GDPR is as of now unclear.

Furthermore, § 62 para. 5 contains a waiver of administrative punishment for breaching the obligations under GDPR for Czech public authorities and bodies (pursuant to Article 83 para. 7 GDPR, for details on the scope of this waiver please refer to this particular provision of ZZOÚ (https://www.uoou.cz/en/assets/File.ashx?id_org=200156&id_dokumenty=1837 (English)). Additionally, § 61 para. 3 ZZOÚ also contains a similar waiver of administrative punishment for breaching the ban on disclosure of personal data imposed by another legal regulation.

(ii) Are data protection impact assessments requirements specified by your national regulation? Any particular requirements? Any specific procedures? Any specific reference to data processing in research?

Czech ZZOÚ contains no particular provisions with specification of the DPIA requirements beyond the wording of GDPR or the directive 2016/680. It merely contains the aforementioned exception in § 10 ZZOÚ, whereas a controller need not carry out assessment of the impact of data processing on personal data protection prior to commencement of personal data processing if such data processing is required by the legal regulation. ÚOOÚ issued in February 2019 national guidelines for DPIA (https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=33193 (Czech)). ÚOOÚ expressly states that this document is predominantly based on the WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248. It contains more detail and reformulates the 9 criteria from the WP 29 guidelines into 10 criteria with three-point scale (critical-significant-low). Each criterion contains explanation or quantitative pointers for each of these values. No specific procedures for DPIA are recommended by ÚOOÚ or in the legislation. We are not aware of any specific references to data processing in research.

6.2 Commercialization of data

6.2.1 General Regulatory Framework

Regulation	Link (English version if possible be)	Type of regulation (hard law, soft law…)	Brief description and scope
Zákon č. 634/1992 Sb. o ochraně spotřebitele	https://www.zakonyprolidi.cz/cs/1992-634 (only Czech, up to date); https://www.mpo.cz/dokument175578.html (English, outdated)	Hard law	Act on Consumer Protection, which also contains regulation of information databases about consumer´s solvency and trustworthiness. It further contains provisions permissible provisions in Terms of Service in a contract with a consumer.
Zákon č. 480/2004 Sb. o některých službách informační společnosti	https://www.zakonyprolidi.cz/cs/2004-480 (only Czech, up to date); https://www.uoou.cz/en/vismo/zobraz	Hard law	Act on Certain Services of the Information Society regulates privacy protection of the users in the

	dok.asp?id_org=200156&id_ktg=1155&p1=1155 (general description in English, outdated)		information society services and permissible dissemination of commercial communication.
Zákon č. 127/2005 Sb. o elektronických komunikacích	https://www.zakonyprolidi.cz/cs/2005-127 (only Czech, up to date); https://www.mpo.cz/en/e-communications-and-postal-services/electronic-communications/national-legislation-and-regulations/unofficial-consolidated-version-of-the-act-on-electronic-communications--effective-as-at-january-1--2015--156553/ (English, partially outdated)	Hard law	Act on Electronic Communications sector. The Chapter V of the act regulates protection of personal data, other forms of data, services and networks for electronic communication. It contains regulation pursuant to the E-Privacy Directive concerning cookies.
Zákon č. 89/2012 Sb., občanský zákoník (OZ) ***Civil Code***	https://www.cak.cz/assets/pro-advokaty/mezinarodni-vztahy/civil-code.pdf (English)	Hard law	Generally governs contracting.

Main regulatory tools addressing data commercialization in Czech Republic.

6.2.2 Practice

(i) In practice, does your country allow contracts based on exchange of personal data for services (for instance, to gain access to an app)?

We are not aware of any particular Czech regulation concerning contractual exchange of personal data for services as a form of payment. Act on Consumer Protection (zákon č. 634/1992 Sb. o ochraně spotřebitele, https://www.mpo.cz/dokument175578.html (English, outdated)) regulates deceptive trade practices towards the consumer, including also deceptive omissions. In this context an omission of information regarding the exchange of personal data for the provided services may constitute a deceptive trade practice. The particular assessment and interpretation are, however, dependent on the specifics of the case and cannot be determined on an abstract level.

(ii) Do you know if these practices are routinely performed?

Previously, it was common for example that downloading an application was subject to a number of consents to provide data, etc. Now, these practices are very limited, as far as I know.

Concerning stipulations about the processing of personal data, they are routinely contained in the terms of service of companies. These terms of service are subject to consumer protection law.

(iii) Does your country have any specific regulation on the remuneration of data subjects if profit is made out of their data?

There is no specific regulation on the remuneration of data subjects for profits made out of their data, unless economic rights of an author under the copyright legislation are taken into consideration.

(iv) Do you have any particular national regulation on the secondary use of data?

The only particular Czech legislation that comes to mind are the provisions on open data use of public sector information under the Act on Free Access to Information (zákon č. 106/1999 Sb. o svobodném přístupu k informacím, https://www.zakonyprolidi.cz/cs/1999-106 (Czech)). The open data available for secondary use are provided through the National Catalogue of Open Data (source: https://opendata.gov.cz/nastroj:narodni-katalog-otevrenych-dat (Czech)).

(v) Do you have any specific protection for metadata or non-personal data in your country?

There is no specific protection provided to metadata or non-personal data in the Czech Republic. Metadata are regulated with regard to permissible scope of data retention under provisions §§ 87-97 of the Act on Electronic Communications (zákon č. 127/2005 Sb. o elektronických komunikacích, https://www.zakonyprolidi.cz/cs/2005-127 (only Czech, up to date); https://www.mpo.cz/en/e-communications-and-postal-services/electronic-communications/national-legislation-and-regulations/unofficial-consolidated-version-of-the-act-on-electronic-communications--effective-as-at-january-1--2015--156553/ (English, partially outdated)).

6.2.3 Nature of Data

(i) How does your country classify data? Is it a product/commodity/good or service? Do you have an additional construct for data?

Current Czech law does not classify data under any particular legal category. The approach to their conception in Czech legal theory is subject to scholarly debate, which indicates the complexity of the issue, especially given the often-misleading linkage of normative provisions to the notion of information rather than data per se. The narrow context in which is classification of data meaningful from the perspective of right *in rem* requires full control of the holder over the data, either through capture on physical data carrier or high level of encryption. However, even then is the classification of data as things redundant, as the rights in rem are bound and carried out on the data carrier, not on the data per se.

Data is an incorporeal thing within the meaning of § 496 OZ (incorporeal things are rights whose nature allows it, and other things without corporeal substance).

Other categories can depend on the nature of this data. For example, artistic work can be protected by copyright. Business data can be protected as trade secrets.

(ii) Except for the Sui Generis Right on the protection of databases, do you have a legislation protecting data in your country (e.g. like copyright)? Are you aware of any mechanisms to determine the value of data?

The Czech Copyright Act (zákon č. 121/2000 Sb., autorský zákon, https://www.zakonyprolidi.cz/cs/2000-121 (Czech, up to date), https://www.wipo.int/edocs/lexdocs/laws/en/cz/cz043en.pdf (English, partially outdated)) provides protection to a scope of works, which are a unique outcome of creative activity. As such, the work may also include e.g. software as well as various works of art. As such, there is no particular accent in the regulation on the data, as the legal protection is bound to the information contained and represented by the data.

The value of data is generally decided through an expert opinion, which uses valuation methods in principle in accordance with the International Valuation Standards issued by the International Valuation Standards Council. Of particular relevance for valuation of data are the respective standards for intangible assets (source: https://www.ivsc.org/files/file/view/id/647).

6.3 Security and cybersecurity

6.3.1 General Regulatory Framework

Regulation	Link (English version if possible be)	Type of regulation (hard law, soft law…)	Brief description and scope
Zákon č. 110/2019 Sb., o zpracování osobních údajů (ZZOÚ)	https://www.zakonyprolidi.cz/cs/2019-110 (Czech)	Hard law	Adopted as an adaptation law to GDPR.
Zákon č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB)	https://www.zakonyprolidi.cz/cs/2014-181 (Czech)	Hard law	Regulates the rights and obligations of persons and the powers of public authorities in the field of cyber security. This Act also incorporates relevant European Union regulations and regulates the security of electronic communications networks and information systems. It shall not apply to information or communication systems handling classified information.

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat	https://www.zakonyprolidi.cz/cs/2018-82 (Czech)	Hard law	It regulates security measures, cyber security incidents, reactive measures, filing requirements in the area of cyber security and data liquidation.

Main regulatory tools addressing security and cybersecurity in Czech Republic

6.3.2 Implementation of EU Law

(i) Are any particular procedures described in your national regulation?

ZZOÚ contains a transposition of the Directive 2016/680 for personal data processing by police forces and national security bodies, which also includes provisions on security procedures and requirements of appropriate technical and organisational measures. Nevertheless, the provisions in principle reiterate the wording of the directive and thereby contain no particular descriptions of procedures.

According to § 14 ZZOÚ in addition to public authorities, the authorities established by law, which carry out statutory tasks in the public interest, are obliged to appoint data protection officers.

ZKB deals with cyber security system. This Act lays down which persons are subject to cyber security obligations. These bodies and persons are:

(a) an electronic communications service provider and an entity providing an electronic communications network;

(b) the authority or person providing the significant network, unless they are the administrator or operator of the communication system referred to in point (a);

(c) the administrator and operator of the critical information infrastructure information system;

(d) the administrator and operator of the critical information infrastructure communication system;

(e) the administrator and operator of a major information system;

(f) f) administrator and operator of the basic service information system,

(g) operator of the basic service;

(h) digital service provider.

Furthermore, it is stated that security measures are divided into organizational and technical measures. These measures are listed in ZKB. Subsequently, the cyber security event and the cyber security incidents are defined and the way of their reporting. Finally, the performance of state administration in this area is regulated, including the establishment of National cyber and information security agency (NÚKIB) and the setting of offenses in this area.

(ii) What is the status of the implementation of the NIS directive in your country towards data protection/security of data?

The NIS directive was implemented through amendments to the Act on Cybersecurity (zákon č. 181/2014 Sb. o kybernetické bezpečnosti) in summer 2017. Apart from the introduction of a new category of obliged entities - a digital service provider - the NIS directive was not very breakthrough for the Czech Republic. The Czech Republic already had a functioning cybernetic framework (for example, adopting a national strategy, establishing a single contact point place, CSIRT team appointments, etc.).

(iii) The GDPR stipulates that appropriate technical and organisational measures to protect personal data must be implemented. Is this prevention reflected in your national regulation?

The detail of the respective provisions of ZZOÚ does not go beyond reiteration of the provisions of the Directive 2016/680 or GDPR. We are further not aware of any document by ÚOOÚ that would provide additional systematic examples or recommendations in this regard.

As discussed above, the ZZOÚ regulate specific rules for fields such as research and statistics, etc. (see part 1). ZKB then adjusts security measures for a specified category of entities (see above).

6.3.3 Personal Data Breach Notification

(i) What requirements in relation to data breach notifications exist in your national regulation? Is this issue regulated in the national implementation of the NIS Directive?

The personal data breach notification requirements are governed by GDPR. ZZOÚ contains only (a) an exception for personal data processing for journalistic purposes or purposes of academic, artistic or literary expression aimed at protection of source or content of the information (§ 19 ZZOÚ) and (b) provisions on personal data breach notification requirements pursuant to the Directive 2016/680 with no particular additional specifications (§ 41 and 42 ZZOÚ). The Act on Cybersecurity (zákon č. 181/2014 Sb. o kybernetické bezpečnosti, https://www.zakonyprolidi.cz/cs/2014-181 (Czech)) contains provisions on notification of a cybernetic security incident, which is however parallel obligation to the personal data breach notification towards respective CERT. The obligations are not mutually exclusive and can occur simultaneously.

As far as cybersecurity is concerned, cyber security event and the cyber security incidents are defined in ZKB. A cyber security event is an event that may cause a breach of information security in information systems or a breach of the security of services or the security and integrity of electronic communications networks. A cyber security incident is a breach of information security in information systems or a breach of security of services and / or security and integrity of electronic communications networks1) as a result of a cyber security incident. ZKB further regulates the way of reporting these events and incidents. NÚKIB keeps records of cyber security incidents.

6.3.4 Supervision of cybersecurity

(i) Does a supervisory body in a narrow sense with enforcement powers exist in your country?

Yes, the National Cyber and Information Security Agency (Národní úřad pro kybernetickou a informační bezpečnost, NÚKIB, https://nukib.cz/en/ (English)) was established as such supervisory body with enforcement powers. It was created in August 2017 through an amendment of the Act on Cybersecurity (zákon č. 181/2014 Sb. o kybernetické bezpečnosti).

(ii) Is in your country an institution like the German BSI (Bundesamt für Sicherheit in der Informationstechnik) established. The Federal Office for Information Security is the national cyber security authority of Germany. It shapes information security in digitisation through prevention, detection and reaction for government, business and society. (https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html) or something similar established? If yes, what are the competences and responsibilities?

Yes, the National Cyber and Information Security Agency (Národní úřad pro kybernetickou a informační bezpečnost, NÚKIB, https://nukib.cz/en/ (English)) is such body. It is the central administrative authority for cyber security, including the protection of classified information in the area of information and communication systems and cryptographic protection. It operates the Government CERT (GovCERT.CZ); cooperates with other Czech as well as international CERT teams and CSIRTs; drafts security standards for information system of the critical information infrastructure and important information systems; determines obliged subjects under the cybersecurity regulation including information system of the critical information infrastructure, important information systems and information systems or providers of basic services; informs the public about cybernetic security incidents; provides analyses and monitoring of cybernetic threats and risks; supports education and research in the area of cyber security. It can issue security measures and award administrative fines for non-compliance with obligations under the Act on Cybersecurity or the issued security measure. It is also in charge of the public regulated service of the Galileo satellite system.

According to § 22 ZKB NÚKIB should:

a) lay down security measures;

b) issue measures;

c) perform specified tasks in selected areas of protection of classified information,

d) keep records pursuant to this Act and under the Act on Protection of Classified Information,

e) impose administrative penalties for non-compliance with obligations stipulated by this Act and the Act on the Protection of Classified Information and on Security Capability

f) act as a coordinating body in a state of cyber danger,

g) cooperate with authorities and persons active in the field of cyber security and cyber defence, in particular with public corporations, research and development workplaces and other CERT type workplaces, and with authorities and persons active in selected areas of protection of classified information,

h) ensure international cooperation in the field of cyber security and in selected areas of protection of classified information,

i) negotiate and concludes agreements on international cooperation in the field of cyber security and in selected areas of protection of classified information,

j) ensure prevention, education and methodological support in the field of cyber security and in selected areas of protection of classified information,

k) ensure research and development in the field of cyber security and in selected areas of protection of classified information,

l) conclude a public contract with the operator of the national CERT,

m) send to the Ministry of the Interior a proposal for critical infrastructure elements in the sector of communication and information systems in the field of cyber security, operated by a state organizational unit, pursuant to the Crisis Act;

n) determine, according to the Crisis Act, the elements of critical infrastructure in the area of communication and information systems in the area of cyber security, except for the elements mentioned in point m),

o) verify every two years the timeliness of the identification of critical infrastructure elements according to points m) and n)

p) designate the basic service operator and the basic service information system,

q) draw up and submit to the Government for approval a national cyber security strategy13) and an action plan for its implementation and update this strategy at least every 5 years,

r) be the single point of contact for ensuring cross-border cooperation on cyber security within the European Union;

s) be a competent authority in the Czech Republic and fulfils information obligations towards the European Commission and the Cooperation Group pursuant to the relevant European Union regulation,

t) inform the public about a cyber security incident pursuant to Section 12 (3),

u) conduct analysis and monitoring of cyber threats and risks,

v) exercise its responsibilities in the field of the public regulated service of the European satellite navigation program Galileo;

w) issued by the Bulletin of the Office, which is published on its website,

x) perform other tasks in the area of cyber security stipulated by this Act and in selected areas of protection of classified information pursuant to the Act on Protection of Classified Information and Security Capability.

(iii) How can damages caused by lack of cybersecurity be claimed (and compensated)? Are such issues sufficiently regulated in your country?

Currently the damages can be claimed in a civil lawsuit on material or non-material damages, inter alia newly also possible based on the direct claim laid in Article 82 GDPR. Additional option is a proceeding on damages of the victim attached to the criminal proceeding in case of damages caused by criminal offence. Cybersecurity offences constitute an official offence according to law (§ 25 ZKB). In case of these offenses

NÚKIB may impose a fine. At this time the Ministry of Justice is preparing a draft law introducing class action lawsuits into the Czech procedural law (source: https://apps.odok.cz/veklep-detail?p_p_id=material_WAR_odokkpl&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=3&_material_WAR_odokkpl_pid=KORNBA9EXSST&tab=detail (Czech)), however the future of this initiative is as of now uncertain.

6.3.5 Enforcement: fines and sanctions

(i) Is a crime related to data protection or cybersecurity punished by a fine or imprisonment?

Yes, Czech Criminal Code (zákon č. 40/2009 Sb., trestní zákoník, https://www.zakonyprolidi.cz/cs/2009-40 (Czech)) contains qualifications concerning data protection as well as cybersecurity. The sanction under § 180 of the Czech Criminal Code for "unlawful processing of personal data obtained in the exercise of public authority or due to breach of duty of confidentiality" can also be imprisonment. The sanction under § 230 of the Czech Criminal Code for "unlawful access to computer system or data carrier" can also be imprisonment. Additional criminal offences concerning cybersecurity include "capture and carrying of access device or password to computer system or other such data" (§ 231 of the Czech Criminal Code) and "damage to record in computer system or on a data carrier and interference with the computer equipment by negligence" (§ 232 of the Czech Criminal Code). For all of these crimes can also under given circumstances be issued fines or temporal ban on given activity.

(ii) Are there administrative fines related to data protection issues?

Yes, additional to the applicable GDPR provisions the ZZOÚ contains two sets of administrative fines. First set under § 61 ZZOÚ applies to infractions by breaching the ban on disclosure of personal data imposed by another legal regulation (e.g. Code of Criminal Procedure) with fine up to 10 000 000 CZK (cca. 400 000 EUR) and increased fine of up to 50 000 000 CZK (cca. 2 000 000 EUR) if committed through press, film, radio broadcast, TV broadcast, internet or other similarly effective medium. § 61 para. 3 ZZOÚ contains a waiver from this sanction for Czech public authorities and bodies.

The second set under § 63 ZZOÚ applies to infractions against the provisions of the act that represent transposition of the Directive 2016/680. The administrative fine is set to up to 10 000 000 CZK (cca. 400 000 EUR).

Additionally, § 62 para. 5 ZZOÚ contains a waiver of administrative punishment for breaching the obligations under GDPR for Czech public authorities and bodies (pursuant to Article 83 para. 7 GDPR, for details on the scope of this waiver please refer to this particular provision of ZZOÚ (https://www.uoou.cz/en/assets/File.ashx?id_org=200156&id_dokumenty=1837 (English)).

(iii) Do data protection offences constitute an official offence or are only prosecuted by the injured party's request?

Data protection offences constitute an official offence according to law. Damages may also be claimed in civil litigation.

6.4 Governance

(i) At least in the biomedical sciences research involving human participants usually is subject to ethical review by research ethics committees or similar bodies. Data protection, however, not only affects the biomedical sciences, but potentially all fields of research. Are you aware of any committees (e.g. research ethics committees, ethical review boards) or agencies (e.g. national research funding agencies, national security agencies) in your country that review data protection issues in research projects? If yes, are reviews mandatory and governed by specific guidelines or regulations? Do you know which aspects of data protection review bodies focus on? Are reviews only conducted before the actual research starts or is the research process monitored as well?

The research review committees and ethical review boards at public research institutions (primarily public universities and research institutes) should be taking the aspect of personal data processing into consideration in their broader assessments of the particular research projects. Of particular note is the Committee for Ethics of Research established by the Czech Academy of Sciences (http://www.avcr.cz/cs/o-nas/struktura/vedecka-rada-av-cr/komise-pro-etiku-vedecke-prace/ (Czech)). Similarly the agencies for public funding of research, i.e. Czech Science Foundation (https://gacr.cz/en/) and Technology Agency of the Czech Republic (https://www.tacr.cz/en/homepage/) take measures concerning data processing into consideration as part of the assessment criteria for proposed research projects requesting funding.

On the other hand, in the Czech Republic we have multicentre and local ethics committees assessing biomedical sciences research involving human participants. These ethics committees however do not review data protection issues at all. The reason is following:

Our State Institute for Drug Control (*"Státní ústav pro kontrolu léčiv"*; SÚKL), which is administrative authority in field of Drug Control and Drug research, issued a notice to the sponsors of clinical trials that SÚKL will not assess or approve documents related to the processing and protection of personal data.[77] In this notice there is also stated that "*the sponsor should submit to ethics committee separate documents concerning the processing and ensuring the protection of personal data in accordance with GDPR, together with a statement that the data protection will ensure the protection of personal data required by GDPR. It is the responsibility of the sponsor (personal data controller) that the documents relating to the processing and ensuring the protection of personal data, including any consents and information transmitted to the subjects, comply with GDPR and the relevant legislation on personal data processing in the Czech Republic. The Ethics Committee will not comment on these documents. Compliance with GDPR and the applicable legislation in the Czech Republic is therefore the obligation and responsibility of the contracting authority.*"

Because of this statement, compliance with the GDPR is assessed neither by the SÚKL nor by the ethics committees. It is common for institutions in which such research is conducted (typically a teaching hospitals) to conclude a research cooperation agreement concerning also data protection (including the control of informed consent, etc.).

Thus, the only control by state authority can only come ex post through the ÚOOÚ

[77] GDPR – Obecné nařízení o ochraně osobních údajů [online]. Státní ústav pro kontrolu léčiv [cit. 30. 10. 2019]. Dostupné z: http://www.sukl.cz/leciva/gdpr-obecne-narizeni-o-ochrane-osobnich-udaju

(ii) What instruments (e.g. ethics self-assessments at the proposal stage), if any, do research funding agencies and other research supporting bodies in your country use to promote data protection in ICT R&I? Do they facilitate the use of these instruments or data protection impact assessments by providing tools (software or other), templates or guidelines?

We are not aware that the Czech Science Foundation (https://gacr.cz/en/) or the Technology Agency of the Czech Republic (https://www.tacr.cz/en/homepage/) had taken any specific measures towards promoting of data protection in ICT R&I or facilitated the use of any particular instruments or DPIA methods. Both agencies issued statements about their compliance with the data protection framework, which however do not concern particularities of the supported instruments or tools (source: https://www.tacr.cz/dokums_raw/novinky/GDPR_souhrn.pdf (Czech) and https://gacr.cz/uredni-deska/ochrana-osobnich-udaju-a-gdpr-v-grantove-agenture-ceske-republiky/ (Czech).

(iii) Are there any national regulations or procedures that specify what to consider when ICT R&I involves defence technology, dual use technology or is affected by embargoes? If yes, who are the bodies responsible for monitoring and enforcement? Are there any tools researchers and innovators working on security-sensitive technologies can use in order to protect against industrial espionage and other confidentiality breaches?

Security research falls within the domain of the Ministry of Interior, which provides regulatory framework and relevant strategic plans and concepts (source: https://www.mvcr.cz/vyzkum/clanek/zakladni-informace-o-bezpecnostnim-vyzkumu-bezpecnostni-vyzkum.aspx (Czech)). We are not privy to the information regarding available tools to protect against industrial espionage and other confidentiality breaches for participating researchers and innovators. We are not aware of any publicly available information in this regard aside from aforementioned framework and strategic documents, which however do not contain any specific information on this topic.

On the other hand, customs Administration of The Czech Republic controls the export of dual use technology. This control generally does not prohibit or restrict the legal export of controlled technology, but individual deliveries are not allowed if there is a risk of abuse. It helps prevent possible damage to the political, security or business interests of the state, as well as prevent damage to the business interests of an entrepreneur, even by unintentional involvement in undesirable activities.

7 Denmark

Jesper Lund (IT-Political Association of Denmark), Sofie Flensburg (University of Copenhagen)

7.1 Informed consent

7.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope