24 Slovakia

Simona Sobotovicova (UPV/EHU)

24.1 Informed consent

24.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
ACT of 29 November 2017 on personal data protection and amending and supplementing certain Acts (hereinafter, the Act) ***(Z Á K O N z 29. novembra 2017 o ochrane osobných údajov a o zmene a doplnení niektorých zákonov)***	https://dataprotection.gov.sk/uoou/sites/default/files/2019_10_03_act_18_2018_on_personal_data_protection_and_amending_and_supplementing_certain_acts.pdf#overlay-context=sk/content/182018#overlay-context=sk/content/182018" (The English version of this Act is not legally binding) file:///C:/Users/Simona/Downloads/ZZ_2018_18_20180525.pdf (binding version in Slovak)	Hard law. The Act implements the GDPR and it was published in the Collection of Laws on 30 January 2018. The Act entered into force on 25 May 2018.	This Act applies to the data protection regulation in Slovakia. It regulates the protection of the rights of natural persons against unauthorised processing of their personal data; rights, obligations, and responsibility during processing of personal data of natural persons and status, activity and organisation of the Office for Personal Data Protection of the Slovak Republic.
Decree of the Office No. 158/2018 Coll. on procedure for Data Protection Impact Assessment **(*V y h l á š k a Úradu na ochranu osobných údajov Slovenskej***	https://www.slov-lex.sk/static/pdf/2018/158/ZZ_2018_158_20180615.pdf (only Slovak version)	Hard law	This regulation provides a legal framework on procedure for Data Protection Impact Assessment.

republiky z 29. mája 2018 o postupe pri posudzovaní vplyvu na ochranu osobných údajov)			

Main regulatory tools addressing data protection issues and informed consent in Slovakia

(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?

Under Slovak legislation the processing of personal data in the course of a household activity as well is excluded from the scope of national data protection regulation [Section 3 (5) (a) of the Personal Data Protection Act]. There is no other specific provision under Slovak law for the protection of these data.

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

On the one hand, the Slovak Data Protection Act (hereinafter, Act) does not apply to the processing of personal data by the National Security Authority for the purposes of performing security screenings and for the purposes of collecting documents on meeting the requirements of judicial competence for decision making for the Judicial Council of the Slovak Republic [Section 3 (5) (c) of the Personal Data Protection Act]. The Act establishes that when taking security measures and assessing the impact on personal data protection, the controller and processor shall apply international norms and security standards, in adequacy manner [Section 78 (11) of the Personal Data Protection Act].

On the other hand, the data protection issues on national security are provided under different legal acts. The most relevant are the following laws[196]: *Act No. 215/2004* Coll. on Protection of Classified Information and on Amendment and Supplementing of certain Acts as amended; Decree of the National Security Authority on Security Employee Examination, on Personnel Security, on Industrial Security and Entrepreneur's Security Project, on Administrative Security as amended, laying down details of Administrative Security of Classified Information (will come into force on 1 January 2020), on Details of Encryption Protection of Information as amended by the Decree *No. 136/2016* Coll, on Security of Technical Devices, on Details Regulating Certification of Mechanical Barrier Devices and Technical Protection Devices and their Use as amended, on Physical Security and Building Security as amended by Decree *No. 315/2006* Coll.; Regulation of the Government of the Slovak Republic *No. 216/2004* Coll. Laying down Fields of Classified Information.

The most relevant is the Protection of Classified Information Act 215/2004. This Act provides that data from the personal security file may be used only to fulfil tasks pursuant to this Act and for the purposes of criminal proceedings and administrative infraction proceedings in the case of unauthorised handling of classified information [Article 33

[196] https://www.nbu.gov.sk/en/authority/legislation/index.html

(3)]. Under this legislation, the Slovak Information Service and the Military Intelligence Service are empowered, in discharging their tasks, to use data from their records and from records and materials resulting from activities of security authorities and military authorities or request data and to maintain in their records data acquired while discharging their tasks under this Act [Article 75 (2) (a) (c)]. This Act contains the different Annexes regarding the data requirements (Annex No. 2, Data Required in the Personal Questionnaire of a Person; Annex No. 3, Data Required in the Personal Security Questionnaire; Annex No. 4, Data Required in the Security Questionnaire of an entrepreneur).

Name of Authority	Link	Is this an independent body?	Number of employees	Level of activity	Response to requirements, questions, etc. made by the public
Office for Personal Data Protection of the Slovak Republic **Úrad na ochranu osobných údajov Slovenskej republiky (Official Slovak Name)**	https://dataprotection.gov.sk/uoou/en	The Office for Personal Data Protection of the Slovak Republic (hereinafter, the Office) is a state administration body with national jurisdiction over the territory of the Slovak Republic. The Office, when exercising its jurisdiction, acts independently and is governed by Constitution of the Slovak Republic, constitutional act, acts, other generally binding legal regulations and international treaties binding upon the Slovak Republic.	46	High	The Office publishes the Annual Report on Data Protection. The most recent Annual Report on Data Protection (28 may 2018- 24 may 2019) was published in September 2019 and could be consulted (Slovak version)in the following link https://dataprotection.gov.sk/uoou/sites/default/files/sprava_o_stave_ochrany_osobnych_udajov_za_obdobie_25.maj_2018_az_24_maj_2019.pdf

Information regarding Data Protection Authority

(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.?

Under the Slovak legislation there are is not specific definition of "data processing for research purposes". The Data Protection Act provides that personal data shall be collected only for specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with this purpose. But, further processing of personal data for archiving purpose, scientific or historical research purpose, or statistical purpose, if in compliance with special regulation[197] and if appropriate safeguards of the protection of data subject's rights in accordance with section 78 paragraph 8[198], shall not be considered to be incompatible with the initial purpose [Section 7, Principle of Purpose Limitation of the Personal Data Protection Act].

Regarding the "research in public interest" there is no specific definition under Slovak legislation. However, where personal data are processed necessary for the performance of a task carried out in the public interest, where personal data are processed for scientific purpose, historical research purposes or statistical purposes pursuant to section 78 paragraph 8, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest [Section 27 (5) Right to object to personal data processing, Personal Data Protection Act].

(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?

The Slovak law does not deviate significantly from the GDPR.

The legislation regarding the data processing for research purposes provides that where personal data are processed for archiving purpose, scientific purpose or historical research purpose or statistical purpose, controller and processor shall implement reasonable safeguards to protect the rights of data subject. Those safeguards shall involve that appropriate and effective technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation and pseudonymisation [Section 78 (8) of the Personal Data Protection Act].

[197] For example, Act of the National Council of Slovak Republic No. 171/1993 on the Police Forces as amended, Act No. 540/2001 on State Statistics as amended, Act No. 395/2002 on Archives and Registries as amended or Act No. 553/2002 on Disclosure of State Security Authorities in the Period of 1939-1989 and on founding the Nation's Memory Institute as amended (Act on Nation's Memory) as amended.

[198] 78 (8) Where personal data are processed for archiving purpose, scientific purpose or historical research purpose or statistical purpose, controller and processor shall implement reasonable safeguards to protect the rights of data subject. Those safeguards shall involve that appropriate and effective technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation and pseudonymisation.

Where the personal data are processed for scientific purpose or historical research purpose or statistical purpose, the data subject's rights referred to in sections 21 (Right of Access to Personal Data), 22 (Right to rectification of personal data), 24 (Right to restriction of personal data processing) and 27 (Right to object to personal data processing) or in a special regulation may be restricted by special regulation or an international treaty binding upon the Slovak Republic, provided that appropriate conditions and safeguards have been implemented, where such data subject's rights are likely to render impossible or seriously impair the achievement of such purposes, and such restriction of rights of data subject is necessary for achievement of such purposes [Section 78 (9) of the Personal Data Protection Act].

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

Firstly, it must be mentioned that, the Slovak Act mentions that the prohibition to process special categories (Slovak Act uses special categories and not sensitive categories) of personal data shall not apply if processing is necessary for archiving purposes, scientific, historical research purposes, or statistical purposes under this Act, special regulation, or international treaty binding upon the Slovak Republic, which interests are appropriate with regard to the followed objective, respect the essence of the law protecting personal data, and lay down appropriate and specific measures to safeguard fundamental rights and interests of the data subject [Section 16 (2) (k) of the Personal Data Protection Act]. The Act just mentioned the "specific measures to safeguard fundamental rights and interest of the data subject" without providing the definitions of these measures.

Secondly, special categories of personal data may be processed by a competent authority only if data subject has manifestly given his or her personal data, processing is necessary pursuant to a special regulation or an international treaty binding upon the Slovak Republic, or processing is necessary to protect the life, health or property of the data subject or other natural person. The competent authority shall adopt the appropriate safeguard to protect the rights of the data subject [Section 56 (1) (b) (c), 56 (2) of the Personal Data Protection Act].

Thirdly, due to records of processing activities, the obligations referred to the controller (shall maintain a record of processing activities under its responsibility), and to the processor (shall maintain a record of the categories of processing activities carried out on behalf of the controller) shall not apply if the processing includes special categories of data [Section 37 (5) of the Personal Data Protection Act].

Fourthly, the Act establishes the following safeguards:

1. A data protection impact assessment shall in particular be required in the case of processing on a large scale of special categories of personal data [Section 42 (3) (b) of the Personal Data Protection Act].

2. The controller and the processor shall designate a data protection officer where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data [Section 44 (1) (c) of the Personal Data Protection Act].

3. The corporate rules shall specify at least the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security of

personal data, and the requirements in respect of onward transfers to bodies not bound by the corporate rules [Section 49 (2) (d) of the Personal Data Protection Act].

4. The competent authority decision which produces an adverse legal effect concerning the data subject cannot be based solely on automated processing of the personal data including profiling, unless authorised by the special regulation or international treaty which the binding upon the Slovak Republic provide otherwise. The special regulation or international treaty which the binding upon the Slovak Republic shall provide appropriate safeguards for protection of the rights of the data subject, particularly the right to obtain verification of the decision from the competent authority by non-automated means. This decision shall not be based on special categories of personal data, unless suitable measures to safeguard the data subject´s rights and legitimate interests are in place [Section 66 (2) of the Personal Data Protection Act]. Profiling that result in discrimination against natural persons on the basis of special categories of personal data shall be prohibited [Section 66 (3) of the Personal Data Protection Act].

(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.)?

In Slovakia, there is no national or regional Code of Conduct or Code of Ethics for data processing in research. However, the research institutes, universities or bodies (for example, Slovak Syndicate of Journalists, Civil Servants, Donors, etc.) who precede the research data, adopted their own Code of Ethics or Code of Conducts which could be freely consulted in English.

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

Under the Slovak legislation there is not specific definition of "statistical purposes". Regarding the rules to statistical data processing, it must be applied the same rules, limitations and safeguards as to research data processing mentioned above.

(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.)

All the references due to data processing for research purposes under Slovak legislation are mentioned previously. Regarding the DPO, there is an online form on the website of the Slovak Data Protection Office which should be completed in order to notify the supervisory authority of the appointment of a DPO. Due to DPIA, the Slovak legislation transposed the DPIA article unless the 35 (4), (5), (6), (10) GDPR provisions, establishing that the controller shall consult each procedures wit data protection officer, where designated, when carrying out a data protection impact assessment [Section 42 (2) of the Personal Data Protection Act].

24.1.2 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.)

All the references due to data processing for research purposes under Slovak legislation are mentioned previously. Regarding the DPO, there is an online form on the website of

the Slovak Data Protection Office which should be completed in order to notify the supervisory authority of the appointment of a DPO. Due to DPIA, the Slovak legislation transposed the DPIA article unless the 35 (4), (5), (6), (10) GDPR provisions, establishing that the controller shall consult each procedures wit data protection officer, where designated, when carrying out a data protection impact assessment [Section 42 (2) of the Personal Data Protection Act].

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

The Slovak Act added a word "serious" regarding the definition of the data subject consent. So, consent of data subject means any serious and freely given, specific, informed and unambiguous indication of data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to such data subject [Section 5 (a) of the Personal Data Protection Act]. The Slovak legislation regarding the conditions for consent to processing of personal data, apart from the GDPR regulation, establishes that, the controller is responsible at any time, to demonstrate that the data subject has consented to processing of his or her personal data [Section 14 (1) of the Personal Data Protection Act].

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

As general rule, the collection and processing of personal data is governed by the GDPR provisions in Slovak legislation. However, there is specific regulation in this respect in the fourth part of the Act mentioned previously [Section 78 of the Personal Data Protection Act]. The Section 78 (5) of the Personal Data Protection Act establishes as well that the controller may also process genetic data, biometric data or data concerning to health on a legal basis under a special regulation or an international treaty binding upon the Slovak Republic.

Regarding the lawfulness of processing, it must be highlighted that the Slovak Act defines the vital interests as the life, health or property. The Act does not set out any additional rules for processing information about criminal offences.

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

In general, there are no significant deviations from the GDPR

Regarding the Right of Access to Personal Data, the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed. Where the controller processes such personal data, the data subject has right of access to the personal data and the following information: the purposes of the personal data processing; the categories of personal data concerned; identification of the recipient or category of recipient to whom the personal data have been or will be disclosed, in particular recipient in third country or international organisations, where possible; the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; the right to request the controller to rectify personal data regarding the data subject or their erasure or restriction or the right to object to processing of the personal data; the right to lodge a complaint to initiate proceedings pursuant to section 100; source of personal data, where the personal data are not collected from the data subject; the existence of automated decision-making, including profiling, referred to in section 28 paragraphs 1 and 4 and, at least in those

cases, controller shall provide information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject [Section 21 of the Personal Data Protection Act].

Data subjects may request deletion of their personal data if the data is inaccurate, incomplete or out of date (in such a case, the data subject may also request correction of the data); the purpose of the processing has ceased; or the law has been breached. It must be mentioned that if erasure of personal data could endanger the rights or law protected interests of a data subject, such data shall be restricted. Such restricted data shall be possible to be processed only for the purpose that prevented them from being erased [Section 65b (4) of the Personal Data Protection Act].

24.1.3 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)?

As a general rule, the Slovak Act transposed all the provisions regarding the processing special categories of personal data. Processing of special categories of data may be carried out without the data subject's consent only if special conditions are met by the regulation as it is mentioned previously. Apart from the GDPR, the Slovak Act provides that the prohibition to process special categories of personal data shall not apply if: processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of public health insurance in accordance with special regulation; processing is carried out in the course of its legitimate activities by a not-for-profit body providing services of general utility, political party or movement, trade union organisation, recognised religious denomination or religious society, and on condition that the processing relates solely to their members or to those natural persons who have regular contact with them in connection with their purposes and that the personal data are not disclosed to the recipient without the written or otherwise reliably provable consent of the data subjects; processing is necessary for preventive occupational medicine, provision of healthcare and services relating to the provision of healthcare, or for the purpose of public health insurance, where such data are processed by healthcare provider, health insurance company, person providing services relating to healthcare provision, or person conducting surveillance over healthcare and the qualified authorised person on its behalf who is bound by the confidentiality obligation with regard to the information he or she has learned during his or her activities, and by the obligation to adhere to the principles of professional ethics; processing is necessary for social insurance, social security of policemen and soldiers, for provision of state social benefits, allowance in support of social integration of individual with severe disability into society, provision of social services, taking the measures under social and legal protection of children and social guardianship, or for provision of help in poverty, or the processing is necessary for purpose to meet the obligations or enforce the rights of controller responsible for processing in the area of labour law and in the area of employment services, if the controller is requested to do so under special regulation14) or under international treaty binding upon the Slovak Republic; processing is necessary due to public interest in the area of public health, or to safeguard high quality and safety of health care, drugs, dietetic foods, or medical devices based on this Act, special regulation, or international treaty binding upon the Slovak Republic laying down appropriate and specific measures to protect rights of the data subject, particularly the confidentiality obligation [Section 16 (2) of the Personal Data Protection Act].

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

Regarding the processing personal data of children, the prohibition to process special categories of personal data shall not apply if processing is necessary for provision of social services, taking the measures under social and legal protection of children and social guardianship [Section 16 (2) (i) of the Personal Data Protection Act].

In Slovakia the age at which a child can provide a valid consent remains at 16 years old..

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

There are not any other vulnerable individuals identified in Slovak legislation apart from the special categories of Personal Data.

24.1.4 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 Slovak Act establishes that, if the data subject dies, the consent requested under this Act or under special regulation2) may be given by a close person to him or her (Section 116 of the Civil Code). The consent shall not be valid if at least one close person gave a written disapproval [Section 78 (7) of the Personal Data Protection Act].

24.1.5 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 the Slovak regulation, the controller shall be responsible for compliance with the fundamental principles of personal data processing, for compliance of personal data processing with the principles of personal data processing and shall be requested to demonstrate such compliance with the data processing principles at request [Section 12 of the Personal Data Protection Act]. The Act adds that the Office imposes fines and administrative fines depending on the individual circumstances of a given case. When deciding about imposing a fine and the level of the fine, the Office considers in particular the level of accountability of the controller or processor with consideration to technical and organisational measures adopted pursuant to section (Data protection by design and by default), sections (Security of processing, Data protection impact assessment) [Section 106 (1) (d) of the Personal Data Protection Act].

(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?

The Slovak Act transposed the data protection impact assessment provisions [unless the 35 (4), (5), (6), (10) GDPR provisions] as mentioned previously.

In Slovakia, the Office has the power to draw up a list of “high risk processing”. Further cases of processing operations that are subject to data protection impact assessment and the procedure in data protection impact assessment pursuant to this Act shall be lay down

by a legislative act of general application issued by the Office [Section 108 (2) of the Personal Data Protection Act].

The Decree of the Office No. 158/2018 Coll. on procedure for Data Protection Impact Assessment provides certain rules in relation to how controllers should carry out the Data Protection Impact Assessment. The Decree does not contain list of processing operations which are subject to the requirement for a data protection impact assessment as envisaged in the article 35 (4) of GDPR.

There is no any special reference to data processing in research under Slovak Act.

24.2 Commercialization of data

24.2.1 General Regulatory Framework

Regulation	Link (English version if possible be)	Type of regulation	Brief description and scope
ACT of 29 November 2017 on personal data protection and amending and supplementing certain Acts (hereinafter, the Act) ***(Z Á K O N z 29. novembra 2017 o ochrane osobných údajov a o zmene a doplnení niektorých zákonov)***	https://dataprotection.gov.sk/uoou/sites/default/files/2019_10_03_act_18_2018_on_personal_data_protection_and_amending_and_supplementing_certain_acts.pdf#overlay-context=sk/content/182018#overlay-context=sk/content/182018 " (The English version of this Act is not legally binding) file:///C:/Users/Simona/Downloads/ZZ_2018_18_20180525.pdf (binding version in Slovak)	Hard law	This Act applies to the data protection regulation in Slovakia. This Act regulates the protection of the rights of natural persons against unauthorised processing of their personal data; rights, obligations, and responsibility during processing of personal data of natural persons and status, activity and organisation of the Office for Personal Data Protection of the Slovak Republic.

Main regulatory tools addressing data commercialization in Slovakia.

24.2.2 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)?

The contracts based on exchange of personal data for services are regulated by Civil law.

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

There is no study, report or any information published about these practices.

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

The Slovak legislation into force legislation does not provide any specific regulation on the remuneration of data subjects if profit is made out of their data.

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

Under Slovak Act, the general rule is that personal data shall be collected only for specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with this purpose. Further processing of personal data for archiving purpose, scientific or historical research purpose, or statistical purpose, if in compliance with special regulation and if appropriate safeguards of the protection of data subject's rights mentioned previously, shall not be considered to be incompatible with the initial purpose [Section 7 of the Personal Data Protection Act].

Where the processing of personal data for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a special regulation, the controller shall, in order to ascertain whether processing of personal data for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: a) any link between the purpose for which the personal data have been collected and the purpose of the intended further processing of personal data; b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; c) the nature of the personal data, in particular whether special categories of personal data are processed, or whether personal data related to criminal convictions and offences are processed, d) the possible consequences of the intended further processing of personal data for data subject; and e) the existence of appropriate safeguards, which may include encryption or pseudonymisation [Section 13 (3) of the Personal Data Protection Act].

Moreover, electronic marketing shall be in particular governed by *Act No. 351/2011 Coll. on Electronic Communications*, as amended. Under this Act, processing of the traffic data of a subscriber or user for the purposes of marketing services or the purposes of ensuring value added services by any public network or service providers is possible solely with the prior consent of the subscriber or the user. The prior consent of the recipient of a marketing e-mail shall not be required in the case of direct marketing of similar products and the services of a person, that has obtained electronic contact information of the recipient from the previous sale of its own product and/or service to such recipient and in line with the provisions of the Act.

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

The Slovak legal framework does not provide the specific protection for metadata or non-personal data. However, Slovakia is obliged to apply the Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union[199].

24.2.3 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?

[199] This Regulation aims to ensure the free flow of data other than personal data within the Union by laying down rules relating to data localisation requirements, the availability of data to competent authorities and the porting of data for professional users. Slovakia is bound by the regulation.

Under Slovak legislation there is no any clear or specific data classification as product, commodity, good or service.

(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?

As it is mentioned previously, Slovakia is obliged to apply the Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

There is no specific regulation which refers to the use of databases data.

We are not aware of any mechanisms to determine the value of data.

24.3 Security and cybersecurity

24.3.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Decree no. 164/2013 of the Office for Personal Data Protection of the Slovak Republic on an extent of a safety measures documentation[200]	https://www.dataprotection.gov.sk/uoou/sites/default/files/kcfinder/files/13-z164.pdf (Slovak version)	Hard law	The Decree establishes the scope of adequate technical, organizational and personnel measures (security measures) which must be guaranteed in processing of personal data in the information system and security risks arising from the category of personal data and the way there are processed.
• **Decree no. 117/2014 which amends Decree no. 164/2013 of the Office for Personal Data Protection of the Slovak**	https://www.dataprotection.gov.sk/uoou/sites/default/files/kcfinder/files/117_2014%5B1%5D.pdf (Slovak version)	Hard law	The Decree regulates the security measures which must be guaranteed by the data controller and processor.

[200] The draft of the Decree of the Office for Personal Data Protection on the certification criteria, certification procedures, content of the technical and security documentation and the conditions for the data protection audits, including requirements on professional qualities of data protection auditor, is currently in the preparatory stage.

Republic on an extent of a safety measures documentation			
Act No. 351/2011 Coll. On Electronic Communication as amended	https://www.teleoff.gov.sk/data/files/22211.pdf	Hard law	The Act regulates the protection of privacy and protection of personal data processing in the sector of electronic communication, among others.
Act No. 69/2018 Coll. On cybersecurity	https://www.nbu.gov.sk/wp-content/uploads/legislativa/EN/Act_Cybersecurity.pdf	Hard law	The Act comprehensively regulates the area of cybersecurity and information assurance, it implements basic security requirements and measures necessary for coordinated protection of information and communication managing systems. At the same time it trans in the Collection of Laws under the number 69/2018. This is the first legal norm governing the cybersecurity within the Slovak Republic.
Decree of the National Security Authority No. 165/2018 Coll. that determines identification criteria for respective categories of serious cybersecurity incidents and details of cybersecurity incidents reporting	https://www.slov-lex.sk/static/pdf/2018/165/ZZ_2018_165_20180615.pdf (just Slovak version)	Hard law	The Decree regulates the identification criteria for a cyber security incident (I, II and III stage) category depending on the parameters

Decree of the National Security Authority No. 164/2018 Coll. That determines identification criteria of the operated service (criteria of the essential service)	https://www.slov-lex.sk/static/pdf/2018/164/ZZ_2018_164_20180615.pdf (just Slovak version)	Hard law	The Decree determines the identification criteria of the operated service as it is establishing under EU law.
Decree of the Ministry of Finance of the Slovak Republic No. 55/2014 Coll. On Standards for Information System in Public Administration as amended.	https://www.slov-lex.sk/static/pdf/2014/55/ZZ_2014_55_20190601.pdf (just Slovak version)	Hard law	The Decree regulates the Standards for Information System in Public Administration.

Main regulatory tools addressing security and cybersecurity in Slovakia

24.3.2 Implementation of EU Law

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

Regarding the security obligations, the Slovak Data Protection Act requires that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised, unlawful processing, against accidental loss, erasure or damage of personal data, using appropriate technical or organisational measures [Section 108 (2) of the Personal Data Protection Act]. Controllers and processors must take technical, organisational and personal security measures in accordance with the manner of processing, while taking into account (among other things): the existing technical means; the extent of any risks that could endanger the security or functionality of the filing system; confidentiality considerations; and the importance of the processed personal data; personal data storage control; communication control; personal data transport control [Section 71 of the Personal Data Protection Act].

The security measures are specified as well in the Decree on the Extent of Safety Measures Documentation (164/2013 Coll) and are categorised as either: security documentation; or security projects. Security projects are more detailed and are required if: sensitive personal data is processed and the filing system is connected to the Internet; or the filing system is used to safeguard public interests.

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

On April 1, 2018, Act No. 69/2018 Coll. on cybersecurity came into force. At the same time it transposes European directive on network and information security (NIS

Directive) into Slovak legal order. So, the data protection provisions of the NIS Directive are fully transposed into Slovak legislation.

(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?

Regarding the security of processing of personal data there are implemented the measures as mentioned previously.

Under Cybersecurity Act, the article 20 establishes the Security measures[201]. operators of essential services must notify any incident with significant impact without undue delay (via a single cyber security information system). If the operator of essential services uses an operator of digital services to provide the essential services, the obligation to notify any incident with significant impact is transferred to the operator, i.e. the operator of the digital services will be responsible for this notification (Article 24 of the Cybersecurity Act). A digital service provider is obliged to notify any security incident, regardless of the impact (Article 25 of the Cybersecurity Act). The Cybersecurity Act also permits voluntary reporting of security incidents (Article 26 of the Cybersecurity Act).

24.3.3 Personal Data Breach Notification

(ii) 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?

Regarding the breach notification, there are not any other specific requirements. The Slovak Data Protection Act transposed literally the GDPR (articles 33, 34 of the GDPR) the Notification of a personal data breach to the Office [Section (40) of the Personal Data Protection Act] and Communication of a personal data breach to the data subject [Section (41) of the Personal Data Protection Act].

Due to the Slovak implementation of the NIS Directive, it must be highlighted that there are not specific articles regarding the breach. However, the Slovak Cybersecurity Act transposed all NIS provisions related to the cybersecurity incidents. To this extent, the communication system for cybersecurity incidents reporting and handling of is a communication system that ensures systematic gathering, concentrating, analysing and evaluating of cybersecurity incidents information (Article 8 (2) of the Cybersecurity Act).

The Electronic Communications Act as well establishes some provisions related to the breach. To this extent, the Section 56 (5), Protection of Personal Data provides that in case of a personal data breach, the undertaking that provides public services shall be obliged: a) To notify, without delay, the Office a personal data breach[202]; b) To inform,

[201] For the purposes of this Act, security measures mean tasks, processes, roles and technologies in the organisational, personnel and technical area, whose aim is to ensure cybersecurity during the life cycle of networks and information systems. Security measures performed depending on the classification of information and categorisation of networks and information systems and in compliance with the security standards in the field of cybersecurity are taken in order to prevent cybersecurity incidents and minimise the impact of cybersecurity incidents on the continuity of service operation.

[202] Nature of the personal data breach, effects of the personal data breach, measures proposed or carried out by the undertaking to mitigate the adverse effects of the personal data breach, date of the personal data breach, date of the finding a personal data breach by the undertaking.

without delay, the subscribers and users concerned about the personal data breach, which may adversely affect their personal data or privacy; this shall not apply if the undertaking has demonstrated to the Office that it has implemented appropriate technological protection measures and that those measures were applied to the data concerned by the security breach; such technological protection measures shall render the data unintelligible to the persons not authorised to access it[203]; c) Upon the request of the Office, to inform subscribers and users concerned about the personal data breach where the personal data breach may have an adverse impact on subscribers and users concerned; this shall not apply where the undertaking acted; d) To maintain an inventory of cases of personal data breach, which shall comprise substantial facts related to the breach, its effects and the adopted remedial actions; the inventory shall only comprise the information necessary for this purpose [Section 56 of the Electronic Communications Act]. The contract of the provision of public services shall contain types of measures which may be taken by the undertaking in case of breach of the security or integrity of the network or threat or damage thereof [Section 44 (2) (i) of the Electronic Communications Act]. In case of a particular risk of a breach of the network security, the provider of public services shall be obliged to inform subscribers concerned about such a risk and any possible remedies, including likely costs necessary to avert the threat [Section 64 (5) of the Electronic Communications Act].

24.3.4 Supervision of cybersecurity

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

In Slovakia, the National Security Authority in the field of cybersecurity is a supervisory body which counts with enforcement powers. For example, the National Security Authority handles cybersecurity incidents, declares alerts and warnings of serious cybersecurity incidents, imposes the obligation to take reactive measures and approves the protective measure, performs inspection, issues decisions on imposing remedial measures and levies fines for offences or administrative offences; performs an audit or requests the conformity assessment body to perform an audit at the operator of essential service, among others. All the National Security Authority's competences could be consulted in the article 5 of the Cybersecurity Act.

(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?

In Slovakia, at the beginning 2018, the National Security Authority started the operation of a specialized workplace which, after the adoption of the Cybersecurity Act on April 1, 2018, started to fulfil the tasks of the National CSIRT unit. On September 1, 2019, the unit was transformed into the National Cybersecurity Center SK-CERT. The SK-CERT

[203] Description and manner of the personal data breach, contact points where more information can be obtained, and measure recommended to mitigate adverse effects of the personal data breach.

does within the organizational structure of the Authority have the status of a separate unit. The Authority provides through SK-CERT services related to the management of security incidents, elimination of their consequences and subsequent recovery of information systems in cooperation with the owners and operators of these systems. The other SK-CERT activities include analytical activities, research, security awareness building and providing cybersecurity education.

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

Under Slovak legislation into force, neither the Data Protection Act nor the Cybersecurity Act addresses how to claim the lack of cybersecurity.

The Data Protection Act transposed literally the GDPR Right to compensation and liability article (Article 82 GDPR) unless the last provision.

Regarding the Cybersecurity Act, the Authority shall be liable for the damage caused to the operators of essential services, digital service providers, their employees or to the person reporting the cybersecurity incident, which was caused by notification. The Authority ensures non-stop protection of data and information processed under this Act from illegal disclosure, abuse, damage, unauthorised destruction, theft and loss in the manner according to specific legal regulation [Article 12 (5), (7) of the Cybersecurity Act]. The operator of essential service is not liable for the damage incurred to another entity by limitation of continuity of essential service at cybersecurity incident handling. The Authority is liable for the damage caused by limited continuity of essential service due to the cybersecurity incident by carrying out the obligations in the manner according to the previous sentence [Article 19 (8), (7) of the Cybersecurity Act].

24.4 Enforcement: fines and sanctions

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

Under the Slovak Criminal Code as amended, a person is liable to a term of imprisonment of up to one year if, without lawful authority, they communicate, make accessible or disclose: (i) personal data of another person obtained in connection with the execution of public administration or with the exercise of constitutional rights of a citizen; or (ii) personal data of another person obtained in connection with the execution of his own profession, employment or function, and thus breaches his own obligation prescribed by a generally binding legal regulation. The offence set out above is punishable by up to two years' imprisonment in certain circumstances where there are aggravating factors (Article 374 of the Criminal Code). Related to the Cybersecurity, the Slovak Criminal Code specifies five crimes expressly connected to cyberspace: unauthorised access to a computer system; unauthorised intervention in a computer system; unauthorised intervention in computer data; unauthorised capture of computer data; and procurement and possession of access devices and computer system passwords and other such data. However, many cybercrimes (for example, phishing attacks) are still prosecuted as common crimes (for example, fraud), (Articles 247- 247d of the Criminal Code).

Regarding the Cybersecurity Act, a natural person commits an offence by violating the obligation, providing false information in the notification, violating any of the obligations, not adopting security documentation, not having proceeded in compliance with the technical, organisational or personnel measures adopted by the operator of essential

service. The Authority may levy a fine from EUR 100 to EUR 5,000 for an offence. The general regulation on offences is applied to offences and related hearings. The offences are heard by the Authority and the Authority levies the fines. Fines for offences constitute state budget revenue [Article 30 (1), (2), (3), (4), (5) of the Cybersecurity Act].

The legal entity/operator of the essential services or a digital service provider may be sanctioned and fined between EUR 300 and 1% of annual turnover (provided it does not exceed EUR 300,000).The authority will also be authorised to impose fines between EUR 300 and EUR 100,000 to anyone, who does not provide the required information relating to national cyber security strategy. When determining the amount of fines, the authority will take into account the seriousness of the administrative offense/tort, in particular the manner of committing it, the duration, consequences and circumstances in which it was committed (Article 31 of the Cybersecurity Act).

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

The Data Protection Act transposed literally the administrative offences and fines related to data protection issues as it is established in GDPR. The Office may also impose an administrative fine up to €2 000 to a person that is not a controller or processor for not providing requested cooperation to the Office, the Office may also impose an administrative fine to the controller or processor, or representative of controller or processor, up to €2 000 if it does not ensure adequate conditions, up to €10 000 if it obstructs the performance of an inspection [Section (105) (1), (2) of the Personal Data Protection Act]. It must be highlighted that Office imposes fines and administrative fines depending on the individual circumstances of a given case. When deciding about imposing a fine and the level of the fine, the Office considers in particular: the nature, severity, and duration of the breach, nature, scope or purpose of personal data processing, as well as the number of data subjects affected, and scope of damage if applicable, possible guilty for breaching of personal data protection, measures that the controller or processor had adopted to mitigate damages suffered by data subjects, the level of accountability of the controller or processor with consideration to technical and organisational measures, previous breaches of the personal data protection by the controller or processor [Section (106) (1) of the Personal Data Protection Act].

The Cybersecurity Act provides as well the administrative offences regulation in the Article 31 of Cybersecurity Act.

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

The general rule is the prosecution by the injured party’s request. Nevertheless, under the Cybersecurity Act, the Authority task is referred to handle cybersecurity incidents, declares alerts and warnings of serious cybersecurity incidents, imposes the obligation to take reactive measures and approves the protective measure; sends early warnings; gathers domestic reports on cybersecurity incidents; gathers reports on cybersecurity incidents from abroad and ensures cooperation with international organisations and authorities of other states when handling cybersecurity incidents of cross-border nature; performs inspection, issues decisions on imposing remedial measures and levies fines for offences or administrative offences or performs an audit or requests the conformity assessment body to perform an audit at the operator of essential service. The criminal offences related to data protection or cybersecurity are officially prosecuted by the public prosecutor.

24.5 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?

Regarding the research Ethics Committees in Slovakia it must be highlighted that the Slovak Republic current system of ethics review in Slovakia (SR) was gradually established since 1990. It consists of the National Ethics Committee (working at the Ministry of Health), and of the mutually independent local (hospital) and regional (research) ethics committees - (R)ECs. It is based on a specific law (Act No. 576/2004 on health care and on services related to health care and Act No. 362/2011 on medicinal products and medical devices) and decentralized. The Committees review data protection issues in research projects.

The Act No. 576/2004 on health care and on services related to health care establishes the provisions regarding biomedical research (articles 26-34) available in Slovak version. The Ethics Committee of the Ministry of Health is appointed by the minister of health according to the provisions of the Law No. 576/2004 Coll. on health care as an advisory body on questions of bioethics, including those connected with ethics of biomedical research and clinical trials.

It is also serves as a consulting body for the 'local' and 'regional' ECs in the SR. The committee only exceptionally performs the ethics review of projects or protocols for a specific research project (when for example, there is no other relevant or responsible ethics committee for the specific project).

Local Ethics Committees are established by directors of health care facilities or biomedical research institutions. They are to review protocols of Clinical Trials (CTs) or biomedical research projects planned to be performed in that facility/institution, and to provide a follow up of the research approved.

These ECs may also be required to advice the director of the facility/institution on ethical issues arising from the health care provision by the facility/institution, so to function also as the so-called "clinical ethics committees". Health care institutions, however, can establish different ethics committees to deal with 'research' or with “clinical” ethics.

Regional Ethics Committees are appointed by the regional state authority. Their task is to review and monitor the conduct of multicentre CTs and multicentre biomedical research projects (with an exception of the review of 'local aspects' of CTs/research projects), as well as of CTs/research projects performed on the outpatient basis (via doctors'/specialists' offices).

They also may be required to advice the regional state authority (e. g. the regional state physician) on ethical issues arising from the health care provision in the region.

In Slovakia, Slovak Research and Development Agency (SRDA) is the research and development grant agency in the Slovak Republic. It was established by the Act

No.172/2005 in July 2005 and it is a successor of the previous agency functioning since 2001. SRDA is the instrument for distribution of public finances for research and development on the competitive basis in Slovakia. SRDA is responsible for research and development promotion in all research fields, including international research cooperation (https://www.apvv.sk/buxus/docs/agentura/predpisy-externe/statute-srda.pdf). Under the Statute of the Slovak Research and Development Agency, there are not specific provisions regarding the review data protection issues in research projects.

Due to the research in the field of biomedical sciences, it must be highlighted the Institute of Medical Ethics and Bioethics (IMEB), http://www.bioethics.sk/. The IMEB brings news and professional information from the field of bioethics and information about the activities, research and educational projects and publications of IMEB – including the complete archive of the IMEB journal Medical Ethics & Bioethics. It also informs about the activities of the Institute of Health Care Ethics (IHCE) of the Slovak Medical University in Bratislava. IMEB and IHCE closely collaborate according to the mutual collaboration agreement signed in 2001 by Director of IMEB and by the Rector of SMU. Under the Statute of IMEB (just in Slovak version), there are not specific provisions regarding the review data protection issues in research projects.

(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?

The Slovak Research and Development Agency (SRDA) does not publish any templates of informed consent form, or similar guidance for applicants referred to the data protection impact assessment.

(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?

The Slovak Republic regulates the export of dual-use goods and technologies by Act No. 39/2011 Coll. on dual-use items through individual, global, general export or transfer permits, which are issued at the request of the Ministry of Economy of the Slovak Republic (MOE). The MOE can ask other competent bodies for their views concerning applications for the export of dual-use items. A negative view of the Ministry of Foreign Affairs regarding the particular export is binding on the MOE.

The Slovak Republic is a member of the EU Customs Union, which applies a uniform trade relations regime to third countries that is binding on all EU member states. The EU closely monitors compliance with international trade rules and, in case of violations, takes measures to protect its interests, for example, by applying embargos and bans on investments.

I am not aware of any national specific researchers and innovators working projects and tools on security-sensitive technologies which could be used in order to protect against industrial espionage and other confidentiality breaches.