25 Slovenia

Aleš Završnik (Ljubljana University); Helena U. Vrabec, (Palantir Technologies, USA-Leiden University, The Netherlands)

25.1 Informed consent

25.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Constitution of the Republic of Slovenia	https://www.ip-rs.si/en/publications/publications-and-guidelines/	Hard Law	The constitution refers to the general right to privacy in Article 35 (protection of right to privacy and personality rights) and to a more specific right to informational privacy in Article 37 (protection of the privacy of correspondence and other means of communication) and particularly Article 38 (the right to data protection).
Personal Data Protection Act (Zakon o varstvu osebnih podatkov, ZVOP-1)	https://www.ip-rs.si/en/legislation/personal-data-protection-act/ (unofficial text in English language) http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3906 (unofficial text in Slovenian language)	Hard law	ZVOP-1 is the main legislative act governing rights, obligations and measures in the field of data protection in the Republic of Slovenia. Adopted in 2007, it stipulates general principles of lawful processing and the rights of the data subject. It also contains provisions regulating some specific fields (direct marketing, video surveillance, biometric data, etc.).
Proposal of the Personal Data Protection Act (Predlog Zakona o varstvu osebnih podatkov, ZVOP-2)	https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-	Legislative proposal	ZVOP-2 will replace ZVOP-1 as the main legislative act in the field of data protection in the Republic of Slovenia and will be aligned with GDPR.

	predpisov/predlog-predpisa.html?id=10208		
Criminal Code (Kazenski zakonik, KZ-1)	http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5050	Hard law	KZ-1 contains criminal law provisions, including provisions referring to data protection and cybersecurity.
Information Commissioner's guidelines and publications	https://www.ip-rs.si/en/publications/publications-and-guidelines/	Soft law	Various guidelines and publications to detail and explain the hard law and the IC's approach to enforcement (click on the titles for links to relevant sources in English): Schengen and your personal data Access to my privacy denied Competencies of the Information Commissioner Guidelines for personal data protection in employment relationships Guidelines regarding the introduction of biometric measures Code of conduct in handling personal data collections Being an informed consumer – who is allowed to handle my personal data and why? Media and the Protection of Personal Data Guidelines regarding digital television and privacy protection Guidelines for preventing identity theft Privacy Impact Assessment in e-Government Projects Guidelines on video surveillance Guidelines for developing information solutions Cloud computing and data protection PIA guidelines for the introduction of new police powers Data – an inexhaustible source of

			business ideas
Other relevant laws		Hard Law	Electronic Communications act, Mass Media Act, Public Procurement act, Patients' Rights Act
Laws setting out administrative details		Hard Law	Inspections act, Administrative Procedure Act

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

(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 Slovenian legislation there are no specific rules relating to these data categories, which are excluded from the scope of national data protection legislation pursuant to Article 7(1) of the Personal Data Protection Act.

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

ZVOP- 1 does not explicitly exclude from its material scope protection of data relating to national security, therefore general data protection rules apply to national security as well.

Name of Authority	Is this an independent body?	Number of employees	Level of activity	Response to requirements, questions, etc. made by the public
Information Commissioner **Informacijski pooblaščenec (pooblaščenka – female version)** **https://www.ip-rs.si/en/**	Yes	Cca 45 do 50 employed by the Information Commissioner. However, the IC office is not only responsible for data protection but also for the requests for access based on the Freedom of Information Act (FOIA requests). Effectively,	Moderate – depending on the availability and funding (e.g., EU funding such as the RAPID project that has enabled the IC to organise trainings on the GDPR for small and medium size companies). Apart from such projects, the Information Commissioner	Whatever question/comment the office of the Information Commissioner receives, they looked into and respond to. In case they receive reports of data protection violations, the IC inspectors either open investigation or issue resolution not to proceed. The IC opinions in which the IC

		this means only half of the staff handles data protection issues.	utilizes social media (Facebook, LinkedIn) to inform and communicate with general public. Lastly, the Information Commissioner opens investigation ex officio: this monitoring function constitutes the largest part of the IC work.	responds to more substantial requests are publicly available. The IC has a duty to open an investigation if they are informed of any violations of data protection. (for example, just recently the IC opened an investigation following the reporting on the Slo-Tech website).

Information regarding Data Protection Authority, Slovenia

(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.?

Personal data may be further processed irrespective of the initial purpose of collection, if conducted for research purposes (Article 17, ZVOP-1: "Processing for historical, statistical and scientific-research purposes"). However, in such case, personal data must be supplied to the data recipient in an anonymized form, unless otherwise provided by statute or if the individual to whom the personal data relate gave prior written consent for the data to be processed without anonymizing. Moreover, the Article defines the obligation to destroy data after processing (unless otherwise provided by statute, or written consent of data subject), and, similarly, the publication of results of processing that needs to be published in anonymized form (unless otherwise provided by statute or consent by the data subject /or by the heirs to the deceased person).

"Research in public interest" is not specifically defined apart from the above-mentioned Article of ZVOP-1 ("Processing for historical, statistical and scientific-research purposes") and indirectly in Article 36 ("Restriction of the rights of an individual"). In the latter case, several rights (explained below) may exceptionally be restricted by statute for reasons of protection of national sovereignty and national defence, protection of national security and the constitutional order of the state, security, political and economic interests of the state, the exercise of the responsibilities of the police, the prevention, discovery, detection, proving and prosecution of criminal offences and minor offences, the discovery and punishment of violations of ethical norms for certain professions, for monetary, budgetary or tax reasons, supervision of the police, and protection of the individual to whom the personal data relate, or the rights and freedoms of others.

The rights that can be restricted are:

- Informing the individual of the processing of personal data (Article 19, ZVOP-1) in case personal data were not collected directly from the individual to whom they relate;

- Right of the individual to information (Article 30, ZVOP-1);
- Right to supplement, correct, block, erase and to object (Article 32, ZVOP-1).

(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?

ZVOP-1 was adopted in 2007 and is not yet aligned with the General Data Protection Regulation. However, it contains several specific safeguards in case of data processing for research purposes (Article 17), namely,

- personal data must be supplied in an anonymized form (unless otherwise provided by statute or with prior written consent of the data subject);
- destruction of data after processing (unless otherwise provided by statute or with prior written consent of the data subject);
- publication in anonymised form (unless otherwise provided by statute or with prior written consent of the data subject or its heir).

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

ZVOP-1 defines sensitive personal data similarly to Article 9 of the GDPR; however, it includes also data on national origin (not only racial and ethnic origin) and the entry in or removal from criminal record or minor offence records.

Processing of sensitive personal data is permitted only in the cases listed exhaustively in Article 13.

During processing of sensitive personal data the data must be specially marked and protected, such that access to them by unauthorised persons is prevented, except in instances from subparagraph 5 of Article 13 (i.e. if the individual to whom the sensitive personal data relate publicly announces them without any evident or explicit purpose of restricting their use) (Para. 1 of Article 14, ZVOP-1). Furthermore, in the transmission of sensitive personal data over telecommunications networks, data must be considered as suitably protected if they are sent with the use of cryptographic methods and electronic signatures such that their illegibility or non-recognition is ensured during transmission (Para. 2 of Article 14, ZVOP-1).

The procedure for implementation of the right of the individual to sensitive information is different (Article 31, ZVOP-1), as the request may be lodged in writing or orally in a record with the data controller once every three months, while in respect to sensitive personal data (and personal data under the provisions of Chapter 2, Part VI of the Act, which is related to video surveillance), once a month.

Specific rules exist for the purposes of direct marketing as data controller may process sensitive personal data only if (s)he possesses the personal consent of an individual, that is explicit and as a rule in writing.

Another specific case relates to connecting filing systems. Filing systems from official records and public books may be connected only if so provided by statute and, in case at least one filing system to be connected contains sensitive data, or if the connecting would result in disclosure of sensitive data (or if implementation of the connecting requires the use of the same connecting code), connecting is not be permitted without the prior permission of the data protection authority (Article 84/3, ZVOP-1).

When expert supervision is provided by the statute (i.e. other statutes, not ZVOP-1), the provisions of ZVOP-1 applies as *lex generalis* (if the statute lacks specific rules on processing of personal data). If in the performance of expert supervision sensitive personal data are processed, the implementer of expert supervision must make an official annotation or other official record of this in the case file of the data controller (Article 90, ZVOP-1).

(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 nationwide or reginal Code of Conduct or national Code of Ethics for data processing albeit the Resolution on the National Research and Development Programme 2011-2020 (ReRIS11-20) stipulates the need to adopt a national ethics code, fairness and best practice in science (point 3.5).

However, the universities have adopted their own Codes of Ethics or Code(s) of Conducts.

For instance, the biggest and the oldest Slovenian university, University of Ljubljana (UL), adopted Ethical Code of Conduct for its researchers and ethics concerns related to personal data protection are checked at four faculties:

- Ethical committee at the Faculty of Social Sciences UL,
- Ethical committee at the Faculty of Arts UL,
- Ethical committee of the Faculty of Education UL,
- Ethical committee of the Faculty of Social Work UL.

The Code of Ethics for Researchers at the UL is based on the following ethical principles (and chapters): 1) Competence; 2) The Conduct of Research (e.g. Objectivity, Conflict of interest, Openness, Responsibility); 3) Confidentiality; 4) Attitude towards Society (e.g. social responsibility and avoid causing harm; respect for private rights, dignity and diversity; equal treatment), and 5) Authorship.

The University of Ljubljana also adopted Guidelines for Ethical Conduct in Research Involving People that includes the following chapters: 1) The need for ethical assessment, 2) Personal data protection (e.g. about de-identification of data, data handling and data storage, destruction of data etc.); 3) Ethical assessment; 4) Participants (e.g. about recruitment, compensation); 5) Research plan; 6) Consent for participation (e.g. the process of obtaining consent, conditions for exceptional oral consent, debriefing of participants).

More about the Code and the Guidelines is available here (in English): https://www.uni-lj.si/research_and_development/ethics_in_research/).

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

Processing of personal data for statistical purposes is defined as providing and displaying aggregate data on mass phenomena (Article 33/3 of the National Statistics Ac, Zakon o državni statistiki, ZDSta). More at: https://www.stat.si/statweb/FundamentalPrinciples/StatConf.

Specific exceptions apply for processing of personal data for statistical (also historical and scientific-research) purposes:

1. In regard to informing the individual of the processing of personal data (Article 19, ZVOP-1) about (A) the data controller and his possible representative (personal name, title or official name respectively and address or seat respectively), and (B) the purpose of the processing of personal data:

- if personal data were not collected directly from the individual to whom they relate, and

- if it would be impossible or would incur large costs or disproportionate effort or would require a large amount of time, or if the recording or supply of personal data is expressly provided by statute.

2. In regard to payment of the cost of supply of personal data in public sector (Article 22/4, ZVOP-1): data controllers in the public sector must supply personal data to data recipient in the public sector without payment of the cost of supply (which is exception to the rule that data controllers are obliged against payment of the cost of supply, to supply personal data to data recipients), unless it involves use for statistical (also historical, and scientific-research) purposes.

3. In regard to protection of personal data of deceased individuals (Article 23/3): data controller may supply data on a deceased individual not only to those data recipients authorised to process personal data by statute (the rule stipulated in Article 23/1 ZVOP-1), but also to any other person intending to use such data for statistical (also historical and scientific-research) purposes if the deceased individual did not prohibit in writing the supply of such personal 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.)

Data processing for research purposes is regulated in Personal Data Protection Act (ZVOP-1) in the same manner as data processing for statistical purposes mentioned in the response to previous question. The new data regulation instruments, such a DPO or DPIA, are not yet implemented in the national data protection law.

25.1.2 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.)

There are no particularities regarding the data subject at the national level.

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

Personal Data Protection Act (ZVOP-1) defines consent as “a voluntary statement of the will of an individual that his personal data may be processed for a specific purpose, and this is given on the basis of information that must be provided to such individual by the data controller pursuant to this Act; personal consent of an individual may be written, oral or some other appropriate consent of the individual.” Compared to the definition of the consent pursuant to the GDPR, the national legislation allows a much broader notion

of consent without the requirement that the expression of an individual's will is also specific, informed and unambiguous.

National legislation also lacks provisions clearly stipulating the conditions for consent, including the right of the data subject to withdraw consent and conditions for the consent of a child.

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

Personal Data Protection Act differentiates between the lawful basis for processing of data in the public and in the private sector.

Regarding processing of special categories of personal data, the national legislation does not include archiving purposes in the public interest, scientific or historical research purposes or statistical purpose as a lawful basis for the processing of this category of personal data as stipulated in 9 (2)(j) of the GDPR. Additionally, the personal data processed for historical, statistical and scientific research purposes have to be transmitted to the data recipient in an anonymised form unless otherwise provided by law or if the data subject consented in writing for the data to be processed without anonymising. This provision severely limits or even completely thwarts the use of personal data for such purposes.

Pursuant to national legislation, automated decision making cannot be based on the data subject's explicit consent. Moreover, the right to obtain human intervention on the part of the controller as one of the fundamental measures to safeguard the data subject's rights and freedoms and legitimate interests in the case of automated decision making is not stipulated in the national legislation.

Slovenian data protection regime is not technologically neutral contrary to Recital 15 of the GDPR. Personal Data Protection Act provides for Sectoral Arrangements, stipulated in Part IV, which provide specific rules governing data processing in the following areas:

- direct marketing,
- video surveillance,
- biometrics,
- records of entry to and exit from premises,
- public books and protection of personal data,
- connecting filing systems,
- expert supervision.

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

Articles 31 and 33 of the Personal Data Protection Act (ZVOP-1) regulate the procedure to exercise the Right of the data subject to information and the Right to supplement, correct, block, erase and to object.

- Both rights may in exceptional circumstances be restricted to the extent necessary to achieve the purpose for which the restriction was provided (Article 36, ZVOP-1). Restriction has to be prescribed in the law for one of the following reasons:

- protection of national sovereignty and national defence;

- protection of national security and the constitutional order of the state;
- security, political and economic interests of the state;
- the exercise of the responsibilities of the police, the prevention, disclosure, detection, proving and prosecution of criminal offences and minor offences;
- the detection and prosecution of violations of ethical norms for certain professions;
- monetary, budgetary or tax reasons;
- supervision of the police;
- protection of the individual to whom the personal data relate;
- the rights and freedoms of others.

Nevertheless, GDPR prescribes that such restriction has to respect the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society, which is not reflected in the national legislation.

The request to exercise the right to information stipulated in Article 30 of ZVOP-1 may be lodged once every three months. If the request relates to sensitive personal data or personal data in relation to video surveillance, it may be lodged every month. Only in exceptional circumstances the request may be lodged within an appropriately shorter period. Depending on the data required, the data controller has to provide information on the same day or within 15 days (in some cases in 30 days). If the data controller fails to provide the information in this period, the request is deemed to be refused.

Similarly, the right to supplement, correct, block, erase and object enshrined in Article 30 of ZVOP-1, may be exercised upon request, if the data subject proves that pertinent personal data is incomplete, inaccurate or not up to date, or that they were collected or processed contrary to the provisions of the ZVOP-1. The data has to be supplemented, corrected, blocked or erased within 15 days, otherwise the request is deemed to be refused.

25.1.3 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)?

There are specific rules on protection of personal data of deceased individuals with a general rule that data controller may supply data on a deceased individual only to those data recipients authorised to process personal data by statute (Article 23 of ZVOP-1).

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

There are no specific rules for processing personal data of children in ZVOP-1. In one of the guidelines the Information Commissioner (DPA) of the Republic of Slovenia explained that general rules of civil law apply.

The new proposal of the Personal Data Protection Act (Zakon o varstvu podatkov, ZVOP-2) stipulates 15 years or more is required for valid consent.

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

There are no specific vulnerable individuals identified in ZVOP-1 apart from the individuals pertaining to a group defined by nationality, race, colour, religious belief, ethnicity, sex, language, political or other belief, sexual orientation, material standing, birth, education, social position, citizenship, place or type of residence or any other personal circumstance (Prohibition of discrimination, Article 4 of ZVOP-1).

25.1.4 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?

Protection of personal data of deceased individuals is stipulated in Article 23 of ZVOP-1. In principle data controller may supply data on a deceased individual only to those data recipients authorised to process personal data by statute. However, three exceptions are possible:

- data controller must supply data on a deceased individual to the person who under the statute governing inheritance is the deceased person's legal heir of the first or second order, if they demonstrate a lawful interest in the use of personal data and the deceased individual did not prohibit in writing the supply of such personal data;

- unless otherwise provided by statute, a data controller may also supply data from the previous paragraph to any other person intending to use such data for historical, statistical or scientific-research purposes if the deceased individual did not prohibit in writing the supply of such personal data;

- if the deceased individual did not issue a prohibition from the previous paragraph, persons who under the statute governing inheritance are his legal heirs of the first or second order may prohibit in writing the supply of his data, unless otherwise provided by statute.

25.1.5 Accountability and Data Protection Impact Assessment

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

Legislation currently in force does not provide any provisions, requirements or specific procedures related to general accountability.

The only provision referring to accountability in a broad sense is paragraph 3 of Article 22 of ZVOP-1, which stipulates that data controller is obliged to ensure for each transmission of personal data that it is subsequently possible to determine which personal data were transmitted, to whom, when and on what basis.

(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?

No, data protection impact assessments requirements are not specified by the national regulation. However, the Information Commissioner has set out specifics in the guidelines on PIA (which is the benchmark used to assess PIAs carried over by personal data controllers in the public and private sector). The IC guidelines are also referenced in the proposal for the new data protection act (ZVOP-1).

25.2 Commercialization of data

25.2.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Personal Data Protection Act (Zakon o varstvu osebnih podatkov, ZVOP-1)	https://www.ip-rs.si/en/legislation/personal-data-protection-act/ (unofficial text in English language) http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3906 (unofficial text in Slovenian language)	Hard law	ZVOP-1 is the main legislative act governing rights, obligations and measures in the field of data protection in the Republic of Slovenia. Adopted in 2007, it stipulates general principles of lawful processing and the rights of the data subject. It also contains provisions regulating some specific fields (direct marketing, video surveillance, biometric data, etc.).
Electronic Communications Act	http://www.pisrs.si/Pis.web/cm?idStrani=prevodi (downloadable version)	Hard law	Electronic Communications
Copyright and Related Rights Act	http://www.uil-sipo.si/fileadmin/upload_folder/zakonodaja/ZASP_EN_2007.pdf (note this English version may be outdated)	Hard law	The act sets out rules on copyright, the rights of performers, producers of phonograms, film producers, broadcasting organizations, publishers and makers of databases, and provides details on enforcement of those rights.

Main regulatory tools addressing data commercialization in Slovenia.

25.2.2 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)?

Yes, but only if the individual gives his/her specific consent. The Slovenian Information Commissioner's opinion of Facebook's gathering of personal data via cookies is explained here: https://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/piskotki-odgovori-na-pogosta-vprasanja/ (only in Slovenian). To summarize, consent suffices as legal basis to exchange personal data for services only as long as the controller provides individuals with transparent and thorough information about data processing. Otherwise, the general rules of civil law could apply.

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

If it is the exchange of data for services, then this is something that indeed happens frequently as people are exchanging their personal data with service providers on a daily basis.

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

Slovenian national 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?

As a general rule, personal data has to be collected for a specific purpose and may not be further processed in a manner that is incompatible with these purposes. An exception to the general rule applies in the case of data processing for historical, statistical and scientific-research purposes, however the data has to be transmitted to the data recipient in an anonymised form, unless otherwise provided in the law or data subject have given a written consent for such processing without anonymization.

Additionally, Personal Data Protection Act in its Sectoral Arrangement on Direct Marketing stipulates that the data controller may use the personal data it collected in the course of its lawful activity, also for the purpose of offering goods, services, employment or temporary work through the use of postal services, telephone calls, electronic mail or any other telecommunication means.

In addition, this act sets out special requirements for connecting and cross-referencing databases. This effectively puts limits to secondary uses of data. In addition, certain individual laws specify occasions when secondary use of data is allowed and/or set limits to such specific types of data processing (see for example Register of Companies Act).

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

Classified Information Act; Electronic Communication Act (e.g., traffic data).

25.2.3 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?

To my knowledge, there is no specific classification of data in Slovenia[204].

(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?

Article 141.a of the Copyright and Related Rights Act which sets out requirements for the Sui Generis Right indicates the option that databases are protected by copyright as it mentions that the sui generis right may apply irrespective of the protection by copyright or by other rights.

In June 2019 Slovenia adopted a Regulation implementing 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 in which it determined the authority competent to implement aforementioned Regulation, point of single contact and national online single information point.

Experts are not aware of mechanisms to determine the value of data.

25.3 Security and cybersecurity

25.3.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Information Security Act (*Zakon o informacijski varnosti*, ZInfV)	http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707	Hard Law	The main legislative act in the field of cybersecurity stipulating the measures to achieve a high level of security of networks and information systems in the Republic of Slovenia. The Act implements the NIS Directive in the national legislation.
Personal Data Protection Act (*Zakon o varstvu osebnih podatkov*, ZVOP-1)	https://www.ip-rs.si/en/legislation/personal-data-protection-act/	Hard Law	ZVOP-1 is the main legislative act in the field of data protection in the Republic of Slovenia, pursuant to which personal data has to be protected with organisational, technical and logically-technical measures in order to prevent its destruction, alteration, loss or unauthorised processing.

[204] As a side note, Article 141.a of the Copyright and Related Rights Act (http://www.uil-sipo.si/fileadmin/upload_folder/zakonodaja/ZASP_EN_2007.pdf) defines a database as "a collection of independent works, data or other materials in any form, arranged in a systematic or methodical way and individually accessible by electronic or other means, whereby either the obtaining, verification or presentation of its contents demands a qualitatively or quantitatively substantial investment."

Proposal of the Personal Data Protection Act (*Predlog Zakona o varstvu osebnih podatkov*, ZVOP-2)	https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=10208	Legislative proposal	ZVOP-2 will replace ZVOP-1 as the main legislative act in the field of data protection in the Republic of Slovenia and will be aligned with GDPR.
Electronic Communications Law	http://www.pisrs.si/Pis.web/cm?idStrani=prevodi (downloadable version)	Hard law	Details the responsibility of network operators to adopt appropriate technical and organisational measures to appropriately manage network and service security risks.
Cybersecurity Act	http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707 (no English version available)	Hard law	Specifies entities that are considered to be operators of essential services and determines their duties such as notifying cybersecurity breaches.
The Information Commissioner guidelines on protection of personal data	https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_zavarovanju_OP.pdf (only Slovenian version available)	Soft law	Explanation of legal requirements and best practice to technically and organizationally protect personal data (and a separate set of requirements for protection of sensitive personal data)

Main regulatory tools addressing security and cybersecurity in Slovenia

25.3.2 Implementation of EU Law

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

There are no special procedures described in Slovenian national legislation. Nonetheless in Part V, the proposed data protection act sets out some particular procedures for the following aspects of the GDPR implementation:

- the role of data protection officers;
- the Information Commissioner tasks;
- privacy certifications;
- gathering of data from official databases and registries, and their cross-referencing.

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

Even when data protection provisions and provisions related to the security of data of the NIS directive are transposed in the national legislation, implementation of the NIS directive (Cybersecurity Act) is still in its infant stage. Namely, to make it operational, the responsible Ministry first needs to adopt some implementation regulations that will set up the national security bodies and define their tasks.

(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?

This prevention is only partially reflected in the Slovenian national legislation. Pursuant to Article 24 of the ZVOP-1, protection of personal data shall include organizational, technical and logical-technical procedures and measures in order to protect personal data, prevent the accidental or intentional unauthorized destruction, alteration or loss of data, and unauthorized processing of such data. However, the preventive measures prescribed were pertinent for the intensity of data collection and data processing in 2007, when the Act was adopted and they do not take into account the state of the art and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons as required by the Article 32 of the GDPR.

25.3.3 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?

Personal Data Protection Act (ZVOP-1) does not contain any requirements in relation to data breach notification. Proposal for a new Personal Data Protection Act (ZVOP-2) includes an obligation of a controller and processor of personal data to notify the competent supervisory authority, which corresponds to the notification obligation stipulated in Article 33 of the GDPR.

National legislation implementing NIS Directive (Information Security Act, Zakon o informacijski varnosti, ZInfV) on the other hand, stipulates that any incident has to be notified without undue delay to the competent National Cyber Security Incident Response Centre, which is either SI-CERT or SIGOV-CERT:

a) operators of essential services: obligation to notify incidents having a significant impact on the continuity of the essential services they provide to SI-CERT;

b) operators of digital services: obligation to notify incidents having a substantial impact on the provision of a service that they offer within the Union to SI-CERT;

c) State administration bodies: obligation to notify incidents with a significant impact on the continuous performance of services by state administration bodies to SIGOV-CERT.

in addition, data breach notifications are regulated in the Electronic Communication Act and they will also be part of the amended Data Protection Act (Zakon o varstvu osebnih podatkov 2).

25.3.4 Supervision of cybersecurity

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

Information security inspectors of the competent national authority, i.e. the Information Security Administration, are responsible to monitor compliance with the provisions of the Information Security Act. In addition to competences pursuant to the Information Security Act, inspectors may also order measures pursuant to the Inspection Act (Zakon o inšpekcijskem nadzoru), which is a general legislative act regulating inspection. Information security inspectors may supervise:

a) operators of essential services (Article 32 of the Information Security Act);

b) digital service providers (Article 33 of the Information Security Act);

c) state administration bodies (Article 34 of the Information Security Act).

Inspectors have the competence to order various measures in an administrative procedure or impose fines in a minor offence procedure, which are stipulated in Articles 37 - 39 of Information Security Act and Article 38 of the Inspection 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?

At the moment, the competent authority in the field of cybersecurity is the Government Office for the Protection of Classified Information. By the end of 2019 the newly established Information Security Administration, a body within the Ministry of Public Administration (Urad Republike Slovenije za informacijsko varnost) shall gradually assume all of the tasks and responsibilities of the national competent authority and the national single point of contact pursuant to the NIS Directive.

Information Security Administration has numerous competences and responsibilities stipulated in the Information Security Act, among others it coordinates the operation of information security system, provides expert support and opinions in the field of information security, cooperates with other actors in the field of information security, e.g. national CSIRTs (SI-CERT and SIGOV-CERT), Information Commissioner, Agency for Communication Networks and Services of the Republic of Slovenia and law enforcement authorities, organizes training, exercises and education in the field of information security, helps to raise public awareness of information security, promotes and supports information security research and development. Competences of the Information Security Administration are enshrined in Article 27 of the Information Security Act, however additional competences are stipulated in numerous other provisions of the Act.

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

Neither Personal Data Protection Act (ZVOP-1) nor the proposal of the new Personal Data Protection Act (ZVOP-2) address the question of the right to compensation and liability for the damages caused the lack of cybersecurity. Nevertheless, compensation for material and non-material damages may be claimed on the basis of general rules governing the liability for damage stipulated in the Obligations code (Obligacijski zakonik, OZ).

Private insurance companies have also started to offer cyber (liability) insurance policies, which cover third parties' damages claims for both violation of their privacy as well as damages as a result of an incident.

25.4 Enforcement: fines and sanctions

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

Slovenian Criminal Code (KZ-1) stipulates the following criminal offences relating to data protection and cybersecurity, all of which are punished by a fine or imprisonment:

- Article 143: Abuse of personal data (fine or imprisonment of up to 5 years);

- Article 221: Attack on information system (imprisonment of up to 5 years);

- Article 237: Abuse of information system (imprisonment of up to 5 years).

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

In addition to criminal offences, administrative fines (minor offences) may be imposed against the natural or legal person violating data protection rights. Part VII of ZVOP-1 lays down the penal provisions governing the violations of the aforementioned Act and stipulates fines for the following violations:

Article 91: General violations;

Article 92: Violation of the provisions on contractual processing;

Article 93: Violation of the provisions on security of personal data;

Article 94: Violation of the provisions on direct marketing;

Article 95: Violation of general provisions on video surveillance;

Article 96: Violation of the provisions on video surveillance regarding access to official office premises and business premises;

Article 97: Violation of the provisions on video surveillance in apartment buildings;

Article 98: Violation of the provisions on video surveillance in work areas;

Article 99: Violation of the provisions on biometrics in the public sector;

Article 100: Violation of the provisions on biometrics in the private sector;

Article 101: Violation of the provisions on records of entry and exit;

Article 102: Violation of the provisions on connecting filing systems;

Article 103: Violation of the provisions on expert supervision.

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

All criminal offences related to data protection or cybersecurity are officially prosecuted by the public prosecutor (ex officio) and criminal proceedings do not have to be initiated by the injured party.

25.5 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?

Yes, there are national, regional ethical committees and universities' ethics committees that review data protection issues in research projects. There are only two ethics committees established at the national level:

- the "RS National Medical Ethics Committee" (NMEC), responsible for ethical assessment of biomedical research on humans, that are funded by public sources;

- Ethical committee for the experiments on animals for veterinary medicine at the Ministry of agriculture, forestry and food, Administration of the Republic of Slovenia for Food Safety, Veterinary Sector and Plant Protection, which does not conduct ethics review related to personal data protection.

At the regional level, medical centres in towns Celje and Maribor, conduct ethics assessment of research, but are not authorized to approve a project financed by the national Slovenian Research Agency (Agencija za raziskovalno dejavnost, ARRS), or the ministry, responsible for science. There are two specialized ethics committees assessing ethics compliance of research projects: Ethics Committee of the Institute of Oncology Ljubljana and State Commission for Infertility Treatment and Procedures of Biomedically-Assisted Procreation.

However, these national and regional do not primarily focus on ethics issues related to personal data protection. Research projects, master, doctoral theses etc. are assessed at universities, which adopted their own codes of ethics. For instance, the biggest Slovenian university, University of Ljubljana (UL), adopted Ethical Code of Conduct for its researchers. UL also offers templates of informed consent forms and information sheets to facilitate ethics compliance. Moreover, several of the University's members, i.e. faculties, established their own ethics committees and ethics concerns related to personal data protection are checked at four faculties of the UL:

- Ethical committee at the Faculty of Social Sciences,
- Ethical committee at the Faculty of Arts,
- Ethical committee of the Faculty of Education,
- Ethical committee of the Faculty of Social Work.

More about the ethics compliance and committees established at the University of Ljubljana: https://www.uni-lj.si/research_and_development/ethics_in_research/.

Finally, the calls published by the (national) Slovenian Research Agency (ARRS) explicitly demand from the applicants to address ethics issues and explain mitigating measures,

related to human participants, biological samples, personal data, genetic information and animals.

Aspects of data protection that the review bodies focus on are related to informed consent procedures, safety and equality. For example the Guidelines for Ethical Conduct in Research Involving People of the University of Ljubljana) includes the following topics:

- the enrolment of participants:

o participants have the ability and are able to freely decide whether to participate;

o participants are under no pressure to participate;

o participants have not been offered remuneration in excess of compensation of costs;

o participants have not been promised unrealistic benefits and advantages;

o participants have been appropriately presented with the study;

o the application is enclosed with an example of an appropriate protocol of addressing candidates for the study;

- the method is appropriate

o the method enables a reply to the posed research question;

o the process poses no danger to participants;

o the process does not pose excessive burden on participants;

o the process does not involve unnecessary or excessive exposure to stress;

o the process does not involve unnecessary or excessive exposure to offensive or emotionally difficult stimuli and content;

o the application has been enclosed with an example of appropriate non-standard stimuli or instruments;

- deceit / transparency of research

o participants have been informed on the actual purpose of the research;

o the purpose of the research has been suitably presented before its execution;

o in case the research requires deceit or naive participants, the protocol should include an appropriate debriefing of participants after the completion of the research;

- extraordinary situations

o in the case of extraordinary situations (identification of a danger or threat to participants or other persons), an appropriate protocol for action has been prepared and enclosed;

Ethics assessments are conducted before the actual research starts, e.g. according to the Code of Ethics of the University of Ljubljana and the open calls of the Slovenian Research Agency (ARRS). During the implementation of the research project, ethics checks may be conducted as well, but this is extremely rare in practice and more exception to the rule.

(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?

Funding bodies, such as the national Slovenian Research Agency (ARRS), require ethics self-assessment from the applicants to their open calls from 2006. However, the ethics checks during implementation phase of the research projects that the Agency funds are not systematically conducted and remain underdeveloped. The Agency does not offer support in the sense of, for instance, providing templates of informed consent form, or similar guidance for applicants.

(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 national legislation that implements Dual-Use Regulation no 428/2009 of 5 May 2009 and Council Joint Action of 22 June 2000 concerning the control of technical assistance related to certain military end-uses (2000/401/CFSP) consists of:

- Act Regulating the Control of Exports of Dual-Use Items (Zakon o nadzoru izvoza blaga z dvojno rabo, ZNIBDR); and

- Decree on procedures for issuing authorisations and certificates and on competence of the Commission for the Control of Exports of Dual-Use Items (Uredba o načinu izdaje dovoljenj in potrdil ter vlogi Komisije za nadzor izvoza blaga z dvojno rabo).

However, there is no guidance for researchers when dual use items may be involved, e.g. similar to Guidance notes of the H2020, such as:

- Guidance note — Research involving dual-use items, or

- Guidance note — Research with an exclusive focus on civil applications.

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

26 Spain

Aliuska Duardo (UPV/EHU), Lorena Campillo (UPV/EHU), Iker Conal (UPV/EHU),

26.1 Informed consent

26.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos	https://www.boe.es/boe/dias/2018/1	Hard law	This law aims to: