National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

SLOVENIA

Version of 19 September 2014

Mirovni Inštitut
Neža Kogovšek Šalamon

Summary

[1]. In Slovenia, surveillance is carried out by two state bodies: the Slovene Intelligence and Security Agency (*Slovenska obveščevalno-varnostna agencija–SOVA*), competent for intelligence issues in the civil sector, and the Intelligence and Security Service at the Ministry of Defence of the Republic of Slovenia (*Obveščevalno-varnostna služba Ministrstva Republike Slovenije za obrambo–OVS MORS*), competent for intelligence issues in the military sector. While the former is an autonomous state body responsible directly to the Government, the latter is an organisational unit within the Ministry of Defence. The functioning of SOVA is regulated with the Slovene Intelligence and Security Agency Act (ZSOVA).[1] The functioning of the Intelligence and Security Service at the Ministry of Defence is regulated with the Defence Act,[2] which, however, refers importantly to ZSOVA, meaning that this act is in fact relevant for the functioning of both bodies. The tasks of the Intelligence and Security Service at the Ministry of Defence are further regulated with the Decree on Intelligence and Security Service of the Ministry of Defence.[3]

[2]. The Director of SOVA is appointed by the Government, upon the proposal of the Prime Minister (Article 4 of ZSOVA). SOVA has the power to conduct intelligence and counterintelligence activities and prepares analyses for National Security Council and for all parliamentary committees that need information from SOVA to perform tasks in their own areas of work. Within its surveillance work, SOVA is authorised to acquire, evaluate and transmit from abroad the data which is important for ensuring security, political and economic interests of the State, and data on organisations, groups and persons who, through their activities abroad or in connection with foreign entities, constitute or could constitute a threat to the national security and constitutional order (Article 2 of ZSOVA). In order to fulfil these tasks the agency is authorised by law to gather, evaluate, store and transmit personal data and may also use the registries of personal data of other public and private sector entities. SOVA may transmit data to foreign countries only if they ensure protection of personal data, under a condition that foreign intelligence service will use the data only in accordance with the purposes defined with ZSOVA (Article 12 of ZSOVA). SOVA also has the power to obtain data from other data keepers (private and public), who are obliged to transmit the data to SOVA upon a written request from the Director of SOVA (Article 16 of ZSOVA). Personal data may be kept in the register only until the matter is closed (the matter in the sense of a case file, i.e. a situation or subject that is being dealt with or considered by SOVA; this could be for example surveillance of a specific person or group of persons in relation to a specific activity). When the matter (case) is closed personal data have to be deleted from the register (Article 14, § 3 of ZSOVA). When a matter is closed the documents deriving from the matter have to be archived no later than one year since the closure of the matter (Article 18 of ZSOVA).

---

1 Slovenia, Slovene Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji (ZSOVA)*), 7 April 1999.

2 Slovenia, Defence Act (*Zakon o obrambi*), 20 December 1994.

3 Slovenia, Decree on Intelligence and Security Service of the Ministry of Defence (*Uredba o obveščevalno varnostni službi Ministrstva za obrambo*), 29 July 1999.

[3]. SOVA gathers data in a covert way. To keep its data covert it relies upon the Classified Information Act.[4] The methods of gathering information, defined in law, are i) methods for which court order is not required and ii) methods for which court order is required. Methods for which a court order is not required are authorised with a written order issued by the Director of SOVA. These methods are: a) surveillance of international communication systems, b) orders on covert purchase of things and documents, and c) covert surveillance of public spaces with technical means. The law does not provide for a definition of the term 'international communication systems'. Academic authors define this term as strategic preventive or proactive interception of certain types of communication abroad or from abroad, using information technologies and search keywords. These may not include search parameters that would aim at interception of communication from a specifiable communication line or by a specifiable individual in the Republic of Slovenia.[5] The order on surveillance of international communication systems has to include information on the matter that is subject to surveillance, as well as on means, scope and duration of surveillance. Such surveillance may not focus on a fixed telecommunication line in Slovenia or on a concrete identifiable user of this line in the territory of the Republic of Slovenia (Article 21 of ZSOVA), but it may focus on a telecommunication line or identifiable user of this line located outside Slovenia. Covert surveillance of public spaces using technical means can be authorised if there is a great probability that the needed data will be obtained this way, if such data cannot be acquired in any other way or if acquisition of data in other ways would be related to disproportionate difficulties. The order issued by a Director in such matters can be used only for one time surveillance (Article 22 of ZSOVA). One-time surveillance is understood as the opposite of repeated or multiple-time surveillance. It means that each approved surveillance can be carried out only once in a certain time, as determined in the order allowing surveillance. Any repeated surveillance over a certain individual has to be allowed with an order specifying the reasons for its use.[6]

[4]. Methods for which a court order is required are authorised in advance by the President of the Supreme Court (in case of absence of the President these powers are entrusted to the Vice-president of the Supreme Court, as stipulated in Article 24.c of ZSOVA). These methods cover interception and wiretapping of private correspondence (e-mail, letters and telephone lines). This surveillance has to be justified and is carried out in relation to a defined individual as the motion for issuing such a court order has to include the information on the individual against whom surveillance will be carried out (as required by Article 24., § 2 of ZSOVA). Court orders for these surveillance methods are issued for each case separately if there is a great probability that danger to state security exists, which is evident from:

- covert activities against the sovereignty, independence, territorial integrity and strategic interests of the Republic of Slovenia;

---

4 Slovenia, Classified Information Act (*Zakon o tajnih podatkih*), 25 October 2001.

5 Britovšek, P. (2008), Surveillance of International Communication Systems as an Alleged Interference in the Communication Privacy of an Individual in relation to the Territorial Principle of Rights (Spremljanje mednarodnih sistemov zvez kot domnevni poseg v komunikacijsko zasebnost posameznika v povezavi s teritorialnim principom pravice), Javna in zasebna varnost: zbornik prispevkov / 9. slovenski dnevi varstvoslovja, Bled, 5. in 6. junij 2008; ed. Jerneja Šifrer.

6 Written response provided by SOVA on 9 September 2014.

- covert activities, plans and preparations for carrying out international terrorist operations against the Republic of Slovenia and other acts of violence against a state body and public officials in the Republic of Slovenia and abroad;
- disclosure of information and documents classified in the Republic of Slovenia as state secret to an unauthorised person abroad;
- preparations for armed aggression against the Republic of Slovenia;
- intelligence activities of individuals, organisations and groups to the advantage of foreign states and entities;
- international organised crime activities (Article 24., § 1 of ZSOVA).

[5]. Also, for the court order to be issued, it has to be reasonable to expect that in connection with the activity that is to be put under surveillance a certain means of telecommunications is being used or will be used, whereby it is reasonable to conclude that information cannot be collected in any other way or that collecting information in any other way would endanger people's lives or health (Article 24, § 1 of ZSOVA). Surveillance of national communication systems on the basis of a court order can be carried out for a maximum of three months. In case of justified reasons it can be extended multiple times for three months, but altogether may not last for more than 24 months. Each extension has to be supported with a court order issued by the President of the Supreme Court. If the reasons that justified such surveillance cease to exist, surveillance has to be terminated (Article 24, § 3 of ZSOVA). The data that have been acquired with this method but are of no use for the purpose for which they have been gathered have to be destroyed immediately, after they were examined by the President of the Supreme Court. Other data obtained through such surveillance are kept by SOVA until the matter is closed (Article 24, § 4 of ZSOVA). Under the same conditions the President of the Supreme Court also authorises surveillance of telecommunication systems in Slovenia by way of obtaining telecommunication excerpts. Based on such a court order SOVA may require a telecommunication company to provide an excerpt of communication correspondence. The excerpt may not cover more than six months of traffic data (Article 24.a. of ZSOVA). Based on this provision the communication and postal service providers have to enable SOVA to acquire such data. The type of data that telecommunication service providers have to provide to SOVA are data on the user of the communication connection (upon written request of SOVA), data on the call receiver and call maker, as well as the date, time, duration and other characteristics of the call (upon written order of the President of the Supreme Court). According to the Electronic Communications Act[7] the telecommunication providers had the duty to retain all data for 14 or 8 months (depending on the type of data). On 3 July 2014 the Constitutional Court of the Republic of Slovenia annulled Articles 162-169 that defined data retention duty.[8] The telecommunication providers also have to set appropriate software on their communication systems in a manner requested by the director of SOVA or the President of the Supreme Court (Article 24.b of ZSOVA). These provisions do not provide for a large-scale surveillance of individuals and communication lines based in Slovenia, since the motion to issue a court order has to be individualised, but it can provide for large-scale surveillance of international communication systems for which a court order is not required. The duties of telecommunication providers are further defined with the Electronic Communications Act.[9] In order to carry out covert intelligence activities SOVA may also allow the use of mock documents, issued by a competent body. After the reasons for use of such documents have

[7] Slovenia, Electronic Communications Act (*Zakon o elektronskih komunikacijah*), 20 December 2012.
[8] Slovenia, Constitutional Court, Decision No. U-I-65/13-19 of 3 July 2014.
[9] Slovenia, Electronic Communications Act (*Zakon o elektronskih komunikacijah*), 20 December 2012.

ceased the competent body invalidates the documents which are then archived by SOVA (Article 25 of ZSOVA). There are no guarantees in the law that would prevent the use of this method for large-scale surveillance.

[6]. SOVA does not have the duty to inform an individual to whom the collected data refers about the fact that the data is being collected, and the individual shall not have the right to have insight in the personal data collection. The two rights of the individual (to be informed, to have insight) may be limited only if the insight would make the task impossible or difficult to fulfil. In order to limit these two rights, administrators of personal data may, at the request of the Director of SOVA, inform the individual to whom the personal data refer only after five years have elapsed from the date of the submission of data to the Agency. (Article 17 of ZSOVA) In case of surveillance with special methods for which an order of the President of the Supreme Court is required, the Director of SOVA shall (after the matter is closed) inform the person to whom the collected data refer, about his or her right to get acquainted with the documents. This right is limited only in cases when there is a justified reason to believe that disclosure of the documents to the person would cause danger for people's life or health or for national security. (Article 24, § 5 of ZSOVA)

[7]. The competence for surveillance related to military issues is entrusted to Intelligence and Security Service of the Ministry of Defence of the Republic of Slovenia (*Obveščevalno-varnostna služba Ministrstva Republike Slovenije za obrambo – OVS MORS*). The General Director of the Service is nominated by the Government on the proposal of the Minister of Defence (Article 82 of the Public Servants Act). OVS MORS has, among others, the power to collect, document and evaluate information, protection of such information and the power to carry out intelligence, counter-intelligence and security tasks. In addition to that, according to Article 34(1) of the Defence Act, the General Director has other powers that are allocated to Director of the Slovene Intelligence and Security Service, which are:

- decide in which cases the Service will use surveillance methods and cooperate with foreign intelligence services (Article 7 of ZSOVA);
- decide on the manner of storing, documenting and archiving the matters/cases of the Service (Article 15 of ZSOVA);
- demand with a reasoned motion to obtain the data from other data keepers or to obtain an insight into the database (Article 16/1 of ZSOVA);
- together with the Director of the Archive of the Republic of Slovenia, determine the time limit in which the closed matter of the Service has to be given to the Archive of the Republic of Slovenia (Article 15 of ZSOVA);
- in consent of the Government, define conditions and manners of acquisition of information with covert cooperation and measures to protect the sources (Article 19/2 of ZSOVA);
- allow surveillance of international communication systems (Article 21 of ZSOVA);
- allow covert surveillance of public spaces with technical means (Article 22 of ZSOVA);
- submit motions for interception and wiretapping of telecommunication means to the President of the Supreme Court (Article 24/1 of ZSOVA);
- inform the President of the Supreme Court about the fact that the reasons for interception and wiretapping of communication in Slovenia have ceased and that such surveillance has ended (Article 24/3 of ZSOVA);
- inform the individual about his/her right to be informed about the materials gathered by the Service (Article 24/5 of ZSOVA);

- demand from telecommunication company information about the user of a certain telecommunication line (Article 24.b/2 of ZSOVA);
- demand from a telecommunication company to install software for surveillance of international communication systems (Article 24.b/2 of ZSOVA); and
- allow the use of mock documents and to demand from a competent body to issue such documents (Article 25/1 of ZSOVA).

[8]. Surveillance conducted by the two bodies is not limited to Slovenia. On the contrary, Article 20 of ZSOVA explicitly provides for surveillance of international communication systems. Namely, according to Article 20, "under the conditions specified in this law, the Agency may use the following special methods of data acquisition: surveillance of international communication systems, covert purchase of things and documents, and covert surveillance of public spaces with technical means". The article is applicable to both SOVA and OVS MORS.

[9]. There are a number of control mechanisms available for oversight of the work of intelligence services. For surveillance of private communication in Slovenia an *ex ante* order of the President of the Supreme Court is required for both SOVA and OVS MORS (however an *ex ante* court order is not required for surveillance of international communication systems). On-going oversight is in the competence of the Parliamentary Commission for Supervision of the Intelligence and Security Services. *Ex post* oversight (which is not on-going) is in the competence Information Commissioner, Administrative Court of the Republic of Slovenia, Budget Inspection of the Ministry of Finance, Court of Audit and Human Rights Ombudsman.

[10]. Safeguards for personal data protection are defined with Personal Data Protection Act.[10] The act is binding for all state (including intelligence and security services) and non-state actors, and its implementation is supervised by the Information Commissioner whose powers are defined with Information Commissioner Act.[11] The Act defines the right to be informed about the fact that the data are being collected and about the purpose of data collection (Article 19 of Personal Data Protection Act), right to insight into the register of personal data, right to obtain a copy of personal data gathered or a confirmation that the data is gathered, right to obtain a list of users to whom the data has been sent (including when, on what grounds and for which purpose they were sent), right to information on sources of data, right to information on the purpose of data evaluation (Article 30 of Personal Data Protection Act) as well as the right to amend, rectify, block and delete the data (Article 32 of Personal Data Protection Act). If the decision of the data keeper on any of these rights is negative (or there is no response), an individual has the right to object directly with this body (Article 32 of Personal Data Protection Act) and also the lodge a complaint at the Information Commissioner (Article 2 of the Information Commissioner Act). There is also a limitation to the rights of individuals specified in the law. Namely, the rights of individuals defined with Article 32 may exceptionally be limited by force of law, for reasons (among others) of protection of state sovereignty and defence, protection of national security and constitutional order of the state, as well as security, political and economic interests of the state. These limitations may be defined only in the scope that is necessary to achieve the purpose of the limitation (Article 36 of the Personal Data Protection Act). These exceptions apply to activities of SOVA and MORS. The Information Commissioner checks on a case-by-case basis whether data protection guarantees cannot be invoked due to these exceptions. The exceptions are therefore not used blankly in relation to

[10] Slovenia, Personal Data Protection Act (*Zakon o varstvu osebnih podatkov*), 15 July 2004.
[11] Slovenia, Information Commissioner Act (*Zakon o informacijskem pooblaščencu*), 30 November 2005.

all the activities of SOVA and OVS MORS, but only in relation to the specific data related to a particular case. None of the relevant acts (in particular ZSOVA or Personal Data Protection Act) explicitly provide for or prohibit non-suspicion-based and indiscriminate large scale surveillance.

[11]. Also, in the event of a breach of his or her rights an individual can always lodge a lawsuit also directly at the Administrative Court of the Republic of Slovenia (Article 34 of the Personal Data Protection Act), after having objected with the body storing the data first. In judicial proceedings before the Administrative Court an individual may claim compensation in accordance with the provisions of the Obligations Act.[12] A prior appeal to the Information Commissioner is not mandatory to seek judicial review at the Administrative Court. However, in case an individual appeals to the Information Commissioner and is not satisfied with the Commissioner's decision on appeal, he or she may claim judicial review at the Administrative Court. Against the judgment of the Administrative Court, an appeal is possible, under certain conditions, to the Supreme Court of the Republic of Slovenia.[13] Against the decision of the Supreme Court (or Administrative Court if the appeal to the Supreme Court is not allowed), an appeal to the Constitutional Court of the Republic of Slovenia is possible.[14]

[12]. There are two other non-judicial remedies available in relation to surveillance. In cases when human rights have been violated by surveillance, an individual has the right to lodge a complaint to the Human Rights Ombudsman. The Ombudsman may carry out an investigation, and issue non-binding opinions with recommendations.[15] If the Ombudsman decides to carry out an investigation, it sends the decision on initiation of investigation to the body under investigation and claims further information and clarifications on the matter, It sets a time limit in which these information and clarifications have to be provided to the Ombudsman. If the body under investigation does not provide the information to the Ombudsman it has to provide reasons due to which additional information could not be provided. If the body under investigation exceeds the time limit set by the Ombudsman the latter informs a hierarchical body the body under investigation is directly responsible to. Refusal to cooperate with the Ombudsman is considered as hindering the work of the ombudsman. About this the Ombudsman may inform the competent parliamentary committee, the parliament or the public. (Article 33 of the Human Rights Ombudsman Act) According to the law, all state bodies, civil servants and holders of public function have a duty to respond to the Ombudsman's invitation to cooperate in investigation and to provide information on the case (Articles 34 and 36 of Human Rights Ombudsman Act). In carrying out an investigation the Ombudsman has the right to have insight into the data and documents that are within the competence of the body under investigation. The Ombudsman may also call witnesses to provide testimony in investigation. Witnesses are obliged to respond to the Ombudsman's invitations (Article 36, § 2 of the Human Rights Ombudsman Act). The Ombudsman may enter the premises of any state body (Article 42/1 of Human Rights Ombudsman Act). After completing the investigation the Ombudsman prepares a report on findings and sends it to the parties involved. They may comment on the report in the time limit set by the Ombudsman. In its final report the Ombudsman states its findings and decides whether the activities of the body under investigation amounted to human rights violations and in what way the violations were

[12] Slovenia, Obligations Act (*Obligacijski zakonik*), 30 October 2001.
[13] Slovenia, Administrative Disputes Act (*Zakon o upravnem sporu*), 28 September 2009.
[14] Slovenia, Constitutional Court Act (*Zakon o ustavnem sodišču*), 8 March 1994.
[15] Slovenia, Human Rights Ombudsman Act (*Zakon o varuhu človekovih pravic*), 20 December 1993.

conducted. Based on its findings the Ombudsman issues recommendations on ways to remedy the violations. The Ombudsman may also propose that a disciplinary procedure is carried out against civil servants who committed the violation (Article 39 of the Human Rights Ombudsman Act). The body under investigation is obliged to inform the Ombudsman in 30 days about the measures taken to remedy the violation. If the body does not respect this duty the Ombudsman may inform the hierarchical body, the competent ministry, the parliament or the public (Article 40 of the Human Rights Ombudsman Act).

[13]. In addition, in case of suspicion that surveillance has been carried out unlawfully an individual may lodge a complaint the Parliamentary Commission for Supervision of the Intelligence and Security Services. The act does not explicitly define the duty of the Parliamentary Commission to act upon the complaint. However, this duty can be derived from the wording of the act. Namely, the act states that if the complainant claims that the allegedly unlawful surveillance measures violated his or her rights and if the Commission after the conducted supervision procedure finds unlawfulness, the Commission informs the individual about the supervision (Article 33 of The Parliamentary Supervision of the Intelligence and Security Services Act).

[14]. The described judicial and non-judicial remedies are available in all cases related to personal data protection, regardless of the stage of the surveillance procedure.

Annex 1 – Legal Framework relating to mass surveillance

A- Details on legal basis providing for mass surveillance

Name and type of the mass surveillance-related law	**A definition of the categories of individuals liable to be subjected to such surveillance**	**Nature of circumstances which may give rise to surveillance**	**List purposes for which surveillance can be carried out**	**Previous approval / need for a warrant**	**List key steps to be followed in the course of surveillance**	**Time limits, geographical scope and other limits of mass surveillance as provided for by the law**	**Is the law allowing for mass surveillance in another country (EU MS or third countries)?**
Full name in English and national languages indicating its type – Act of the parliament, Government order, etc.			*National security, economic well-being, etc.…*	*Indicate whether any prior/ex post judicial warrant or a similar permission is needed to undertake surveillance and whether such approval/warrant needs to be regularly reviewed*	*See for example the principles developed by the European Court of Human Rights in the case of Weber and Saravia v. Germany*, (dec.) n°54934/00, 29 June 2006, para. 95 *Steps could include collecting data, analysing data, storing data, destroying data, etc.*	*Clearly state if there are any existing limitations in terms of nationality, national borders, time limits, the amount of data flow caught etc.*	*Please, provide details*
Slovenia, Slovene Intelligence and Security Agency	The act states that SOVA shall collect and	The individuals/ groups who may be subject to	National security and constitutional	For surveillance in public spaces the judicial warrant is	The key steps include: - collection of data	- Interception of private communication	Yes. Article 21 of ZSOVA

Act (*Zakon o Slovenski obveščevalno-varnostni agenciji (ZSOVA)*), 7 April 1999 – Act of the parliament	evaluate information from abroad and provide intelligence on organisations, groups and persons who, through their activities abroad or in connection with foreign entities, constitute or could constitute a threat to the national security and constitutional order. (Article 2, §1 of ZSOVA)	surveillance are those whose activities abroad or in connection with foreign entities, constitute or could constitute a threat to national security and constitutional order. (Article 2, §1 of ZSOVA). This could apply to non-suspicion-based and indiscriminate large scale surveillance if carried out through surveillance of international communication systems for which court order is not required. According to Article 23 it is likely that the security of the state is at risk in cases of:	order.	not required. However, surveillance of private communication through interception of letters and wiretapping has to be authorised by a written order issued for each individual case by the President of the Supreme Court. (Article 23 of ZSOVA). The order has to be requested in advance. It has to specify the individual(s) it applies to. It may only be issued with a maximum validity of three months and it can be extended for maximum periods of three months, but may not last for more than 24 months in total.	- analysing data - storing data and keeping data records - transmitting data - destroying data (Article 12 of ZSOVA).	can be allowed for three months and can be extended, but may not last for more than 24 months in total. (Article 23 of ZSOVA) - The acquisition of the call-related information may be authorised for no longer than six months. (Article 24.a of ZSOVA) - A person who was subject to surveillance may be granted access to his or her file after five years since the data have been transmitted to the Agency. (Article 17, §3 of ZSOVA) Interception of communication for which a court	states: (1) Monitoring of international communication systems and covert purchase of documents and objects shall be authorised by the Director in writing. (2) A warrant for monitoring international communications systems must include: data related to the case to which the special form of information collection refers, the method, scope, and duration. (3) Monitoring of international communications systems must not relate to a determinable

		- covert activities against the sovereignty, independence, territorial integrity and strategic interests of the Slovenia; - covert activities, plans and preparations for carrying out international terrorist operations against Slovenia and other acts of violence against a state body and public officials in Slovenia and abroad; - disclosure of information and documents classified in Slovenia as state secret to an unauthorised person abroad; - preparations for armed aggression against Slovenia;				order is required is limited to the territory of the Republic of Slovenia (Article 24.a of ZSOVA). For surveillance of international communications system no court order is required but such surveillance may not focus on a concrete person or a concrete phone number (but rather on the matter/issue of surveillance). There are no other geographical limitations or limitations concerning citizenship defined in the law.	telecommunications connection or to a specific user of such a connection in the territory of the Republic of Slovenia. (4) A warrant for covert purchase of documents and objects must specify the denomination, contents, quantity and price of the subject of covert purchase. (5) The approval of covert purchase of documents and objects may only apply to a single covert purchase.

		- intelligence activities of individuals, organisations and groups to the advantage of foreign states and entities; - international organised crime activities.					
Slovenia, Defence Act (*Zakon o obrambi*), 20 December 1994 – Act of the parliament This act refers importantly to ZSOVA. Slovenia, Decree on intelligence and security service of the Ministry of Defence (*Uredba o obveščevalno-varnostni službi Ministrstva za obrambo*), 29 July	Defence Act defines the organisational structure and competence of the Intelligence and Security Service at the Ministry of Defence. In defining its powers the Defence Act refers to ZSOVA. According to Article 2, § 1 of the latter, the Intelligence and Security Service at the Ministry of Defence also collects	The individuals/ groups who may be subject to surveillance are those whose activities abroad or in connection with foreign entities, constitute or could constitute a threat to the national security and constitutional order. (Article 2, §1 of ZSOVA). According to Article 23 it is likely that the security of the state is at risk in cases of:	Data is gather to support defence interests of Slovenia, in particular for a purpose of: - establishment of and assessment of military and political security situation and military capacity outside the state that is of special importance for state security; - collection of and analysis of data on conditions in areas where members of	In relation to methods of surveillance, the Defence Act refers to ZSOVA. The latter states that for surveillance in public spaces the judicial warrant is not required. The law states that SOVA may exceptionally collect information by intercepting letters and other means of communication, including telecommunication s (Article 23 of ZSOVA). This type	The key steps include: - collection of data - analysing data - storing data and keeping data records - transmitting data - destroying data (Article 12 of ZSOVA).	- Interception of private communication cannot last for more than 24 months. (Article 23 of ZSOVA). - The acquisition of the call related information may be authorised for no longer than six months. (Article 24.a. of ZSOVA) - A person who was subject to surveillance may be granted access to his or her file after five years since the data	Yes. Article 32, §4 of Defence Act states that surveillance of international communication systems, important for defence interests of the state, is performed by a unit for electronic combat.

1999 – Governmental decree	information on organisations, groups and persons who, through their activities abroad or in connection with foreign entities, constitute or could constitute a threat to the national security and constitutional order. This could apply to non-suspicion-based and indiscriminate large scale surveillance if carried out through surveillance of international communication systems for which court order is not required.	- covert activities against the sovereignty, independence, territorial integrity and strategic interests of Slovenia; - covert activities, plans and preparations for carrying out international terrorist operations against Slovenia and other acts of violence against a state body and public officials in Slovenia and abroad; - disclosure of information and documents classified in Slovenia as state secret to an unauthorised person abroad; - preparations for armed aggression against Slovenia;	Slovenian army carry out their military duties due to obligations to international organisations; - uncovering of and prevention of activities of military organisations and other bodies and organisations that threaten defence interests of the state, Slovenian army or the ministry of defence. (Article 32 of Defence Act)	of surveillance of private communication has to be authorised by a written order issued for each individual case by the President of the Supreme Court. The order has to be requested in advance. It may only be issued with a maximum validity of three months and it can be extended for maximum periods of three months, but may not last for more than 24 months in total.		have been transmitted to the Agency. (Article 17, §3 of ZSOVA) Interception of communication for which a court order is required is limited to the territory of the Republic of Slovenia (Article 24.a of ZSOVA). For surveillance of international communications system no court order is required but such surveillance may not focus on a concrete person or a concrete phone number (but rather on the matter/issue of surveillance). There are no other	

		- intelligence activities of individuals, organisations and groups to the advantage of foreign states and entities; - international organised crime activities.				geographical limitations or limitations concerning citizenship defined in the law.	

B- Details on the law providing privacy and data protection safeguards against mass surveillance

Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance	**List specific privacy and data protection safeguards put in place by this law(s)**	**Indicate whether rules on protection of privacy and data protection apply:** **only to nationals or also to EU citizens and/or third country nationals**	**Indicate whether rules on protection of privacy and data protection apply:** **only inside the country, or also outside (including differentiation if EU or outside EU)**
Include a reference to specific provision and describe their content	*e.g. right to be informed, right to rectification/deletion/blockage, right to challenge, etc.*	*Please, provide details*	*Please, provide details*
Slovenia, Constitution of the Republic of Slovenia (*Ustava Republike Slovenije*), 23 December 1991, Article 35.	The provision of Article 35 of the Constitution states that 'the inviolability of the physical and mental integrity of every person and his privacy and personality rights shall be guaranteed'.	The provision applies to all persons in the jurisdiction of the Republic of Slovenia, regardless of their nationality.	The constitution applies in the territory of the Republic of Slovenia.
Slovenia, Slovene Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji (ZSOVA)*), 7 April 1999, Article 17.	The law states that when SOVA collects personal data it shall not be bound to inform the individual to whom the data refers and the individual shall not have the right to have insight in the personal data collection. The two rights of the individual (to be informed, to have insight) may be limited only if the insight would make the task impossible or difficult to fulfil. In order to limit these two rights,	The law does not mention nationality of persons under surveillance. It contains general provisions that apply to all persons under surveillance. Under the law foreign nationals are not excluded from surveillance.	The right to be informed and the right to insight apply only inside the country. There are no such safeguards in case of surveillance of international communication systems.

	administrators of personal data may, at the request of the Director of SOVA, inform the individual to whom the personal data refer only after five years have elapsed from the date of the submission of data to the Agency.		
Slovenia, Slovene Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji (ZSOVA)*), 7 April 1999, Article 24, §5.	The provision defines the right to be informed in cases a person's private communication has been under surveillance. The provision states that after the case has been concluded, the Director of the Agency shall inform the person to whom the application of the special form of information collection referred of his/her right to get acquainted with the collected material and in case of a large volume of such material with the report comprising a summary of the collected material. If it is reasonable to conclude that the acquaintance with the material will endanger people's lives and health or the national security, the Director of the Agency may decide not to inform the person concerned of the content of the collected material. The provision does not differentiate between suspicion-based surveillance and non-suspicion	The law does not mention nationality of persons under surveillance. It contains general provisions that apply to all persons under surveillance. Under the law foreign nationals are not excluded from surveillance.	The right to be informed and the right to insight apply only inside the country. There are no such safeguards in case of surveillance of international communication systems.

	based large scale surveillance, therefore it is applicable also in the case of the latter.		
Slovenia, Slovene Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji (ZSOVA)*), 7 April 1999, Article 14	The provision defines deletion and blockage of personal data. The law entitles SOVA to keep a database with personal data of persons who are under systematic long-term surveillance. The provision entitles the Agency to store and manage these data until the end of surveillance activity, and bounds the agency to delete or block the personal data after the surveillance activity is completed.	The law does not mention nationality of persons under surveillance. It contains general provisions that apply to all persons under surveillance. Under the law foreign nationals are not excluded from surveillance.	The right to deletion and blockage apply only inside the country. There are no such safeguards in case of surveillance of international communication systems.
Slovenia, The Parliamentary Supervision of the Intelligence and Security Services Act (*Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb*), 26 February 2003, Article 33, §2	The law defines conditions for parliamentary supervision of SOVA. The provision defines the right of an individual under surveillance to be informed by the parliamentary commission competent for supervision, about the fact that surveillance mechanisms applied against the individual were unlawful.	The law does not mention nationality of persons under surveillance. It contains general provisions that apply to all persons under surveillance. Under the law foreign nationals are not excluded from surveillance.	The law does not define the geographical scope of this safeguard, nor does it limit the scope to the Republic of Slovenia only.
Slovenia, Personal Data Protection Act (*Zakon o varstvu osebnih podatkov*), 15 July 2004, Articles 19, 30, 32, 36.	SOVA is subject to supervision of the Information Commissioner responsible for issues of personal data protection. Personal Data Protection Act defines the following safeguards:	The law does not mention nationality of persons under surveillance. It contains general provisions that apply to all persons under surveillance. Under the law foreign nationals are not excluded	The law is applicable for all bodies keeping records of personal data that are established, situated or registered in the Republic of Slovenia. The law is also applicable in cases when the body keeping the register is not situated in

	The right to be informed about the fact that the data are being collected and about the purpose of data collection (Article 19), right to insight into the register of personal data, right to obtain a copy of personal data gathered or a confirmation that the data is gathered, right to obtain a list of users to whom the data has been sent (including when, on what grounds and for which purpose they were sent), right to information on sources of data, right to information on the purpose of data evaluation (Article 30) as well as the right to amend, rectify, block and delete the data (Article 32). If the decision of the data keeper on any of these rights is negative (or there is no response), an individual has the right to object directly with the body that is storing the data (Article 32). There is also limitation to the rights of individuals specified in the law. Namely, the rights of individuals defined with Article 32 may exceptionally be limited by force of law, for reasons (among others) of protection of state sovereignty and defence, protection of national security and constitutional order of the state, as	from protection.	Slovenia but uses equipment which is situated in Slovenia. (Article 5)

	well as security, political and economic interests of the state. These limitations may be defined only in the scope that is necessary to achieve the purpose of the limitation (Article 36). Data protection safeguards apply to all types of surveillance, suspicion-based and non-suspicion based large scale surveillance. Namely, the Information Commissioner checks on a case-by-case basis whether data protection guarantees cannot be invoked due to these exceptions. The exceptions are therefore not used blankly in relation to all the activities of SOVA and OVS MORS, but only in relation to the specific data related to a particular case.		

Annex 2 – Oversight bodies and mechanisms

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
in English as well as in national language	*e.g. parliamentary, executive/government, judicial, etc.*	*name of the relevant law, incl. specific provision*	*ex ante / ex post / both/ during the surveillance/etc. as well as whether such oversight is ongoining/regularly repeated*	*including the method of appointment of the head of such body **AND** indicate a total number of staff (total number of supporting staff as well as a total number of governing/managing staff) of such body*	*e.g. issuing legally binding or non-binding decisions, recommendations, reporting obligation to the parliament, etc.*
Government of the Republic of Slovenia (Vlada Republike Slovenije)	Government	Slovenia, Slovene Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji (ZSOVA)*), 7 April 1999, Articles 4, 6.	*Ex ante and ex post*, on-going oversight of SOVA. Director of the Agency is responsible to the Government. The Agency has to inform the government on its findings.	The Prime Minister, head of the Government, is nominated by the National Assembly upon the proposal of the President of the Republic (Article 111 of the Constitution).	- Power to appoint and discharge the Director of SOVA. - Power to oversee the work of SOVA. - Right to receive reports of the findings of the Agency. - Right to request reports for the National Security Council, consultative body of the Government.
President of the Supreme Court of the Republic of Slovenia (Predsednik Vrhovnega sodišča	Judicial body (court)	Slovenia, Slovene Intelligence and Security Agency Act (*Zakon o Slovenski*	*Ex ante* and *ex post* oversight of SOVA and Intelligence and Security Service of the Ministry of Defence.	1 person (President of the Supreme Court), in his/her absence Vice-president of the Supreme Court. President of the Supreme Court is nominated by the	– Issuing legally binding decisions: According to Article 24, §1 ZSOVA, interception of private communication in the Republic of Slovenia shall

Republike Slovenije)		*obveščevalno-varnostni agenciji (ZSOVA)*), 7 April 1999, Articles 24, 24.a., 24.c. Slovenia, Defence Act (*Zakon o obrambi*), 20 December 1994, Article 34, §8.		National Assembly upon the proposal of the Minister of Justice, after consulting the opinion of the Judicial Council and assembly of Supreme Court judges (Article 62.a of Courts Act (*Zakon o sodiščih*), 24 March 1994).	be authorised by a written order issued for each individual case by the President of the Supreme Court, if it is very likely that the security of the state is at risk. Each extension of such surveillance has to be authorised ex ante by the President of the Supreme Court (§3). – Irrelevant information obtained this way has to be destroyed, after having been examined by the President of the Supreme Court (Article 24, §4). – Power of the President of Supreme Court to authorise the Agency to obtain information from telecommunication service providers (Article 24.a, §1).
Parliamentary commission for Supervision of the Intelligence and Security Services (Parlamentarna komisija za nadzor obveščevalnih in varnostnih služb)	Parliamentary committee consists of elected members of the parliament.	Slovenia, The Parliamentary Supervision of the Intelligence and Security Services Act (*Zakon o parlamentarnem nadzoru obveščevalnih in*	On-going oversight. Both *ex ante* (right to receive annual work plan) and *ex post* (right to receive reports).	The Commission is established by the National Assembly. It consists of nine members (elected members of the parliament) who are appointed by the National Assembly. The commission has two administrative supporting staff.	– Right to receive reports from intelligence and security services every four months, on their work and on the use of intelligence measures. – Right to receive reports from the Government on matters of special importance for national

		varnostnih *služb*), 26 February 2003, Article 2. Rules of procedure of the Commission for Supervision of the Intelligence and Security Services (*Poslovnik Komisije za nadzor obveščevalnih in varnostnih služb*), 13 July 2004.			security. – Right to demand such reports from the Government or intelligence and security services. – Right to demand a financial report from the Government related to intelligence and security services. – Right to receive from the Government the annual work plan for the intelligence and security services. – Right to examine the premises of intelligence and security services, with or without prior notice. – Right to demand an insight into the documents and data of the intelligence and security services (exempted are documents that would reveal the identity of undercover personnel). – Under certain conditions the Government may decide that oversight be delayed. These conditions are: - oversight would seriously threaten a

					successful implementation of a certain on-going activity of the intelligence service which are of special importance for national security; oversight would seriously threaten a successful implementation of one or more interrelated on-going surveillance measures; there is a serious danger that oversight would endanger the lives of people; or there is a serious danger that oversight would enable the protected source of information. If the Government decides that the oversight is delayed, it has to specify in relation to which surveillance measures the oversight is delayed, legal basis for delay and time of delay which may not exceed three months. The time of delay may be extended for a maximum of six months and the decision on extension has to be adopted with a two-third majority of members of the Parliamentary Commission,

					upon the proposal of the Government. The Government decision can be overruled by two-third majority decision of the Parliamentary Commission. – Right to receive reports from communication service providers on software and technical equipment for supervision, or any changes thereof. – In case communication and postal service providers are ordered to supervise any correspondence, they have a duty to report to the Commission on the execution of such orders every three months. Communication providers have to allow examination visit of the Parliamentary Commission. – Duty to report to National Assembly once a year. The reports are not public. (Articles 13-35)

Information commissioner of the Republic of Slovenia (Informacijski pooblaščenec Republike Slovenije)	Autonomous and independent state agency competent for issues of data protection and access to public information. Since the law does not limit its competence, the Commissioner is competent for protection of all types of personal data, regardless if they were obtained through suspicion-based or non-suspicion based and indiscriminate large-scale surveillance carried out for the purposes of national security.	Slovenia, Information Commissioner Act (*Zakon o Informacijskem pooblaščencu*), 30 November 2005. read together with Slovenia, Personal Data Protection Act (*Zakon o varstvu osebnih podatkov*), 15 July 2004, Articles 20 and 82.	*Ex post* oversight (in cases of complaints and in cases of inspection procedures).	Information Commissioner is nominated by the National Assembly upon the proposal of the President of the Republic. The mandate of the Commissioner is five years. The person can be nominated as a Commissioner twice. (Article 6 of the Information Commissioner Act). On 31 December 2013 the Information Commissioner had 32 employees (Annual report of the Information Commissioner 2013, p. 22)	– Power to carry out inspection procedure in relation to personal data protection. This includes the power to impose sanctions (monetary and other sanctions that can be issued within inspection procedure). – Power to issue binding decisions on complaints of individuals concerning the right to be informed, to have insight or to obtain information or any other right related to protection of personal data. – Power to issue binding decisions, as a second instance body, in appeals against first instance decisions on (denying) access to public information. (Article 2 of the Information Commissioner Act).

Administrative Court of the Republic of Slovenia (Upravno sodišče Republike Slovenije)	Court competent for judicial review in cases of personal data protection.	Slovenia, Administrative Dispute Act (*Zakon o upravnem sporu*), 28 September 2006	*Ex post* oversight in cases of judicial review of Information Commissioner decisions and in case when judicial review is sought by an individual directly without a prior complaint to the Information Commissioner.	Judges are nominated by the National Assembly on the proposal of the Judicial Council – Slovenia, Courts Act (*Zakon o sodiščih*), 24 March 1994.	– Issuing binding judgments.
Human Rights Ombudsman (Varuh človekovih pravic)	Autonomous and independent state body competent for the protection of human rights and fundamental freedoms.	Slovenia, Constitution of the Republic of Slovenia (*Ustava Republike Slovenije*), 23 December 1991, Article 159. Human Rights Ombudsman Act (*Zakon o varuhu človekovih pravic*), 20 December 1993.	*Ex post* oversight in cases of complaints.	The Human Rights Ombudsman is nominated by the National Assembly upon the proposal of the President of the Republic. The mandate of the Ombudsman is six years. After the expiration of the mandate the same person can be nominated once again as the Ombudsman. (Articles 12 and 14). On 31 December 2013 the Human Rights Ombudsman had 41 employees (Annual report of the Human Rights Ombudsman 2013, p. 368).	– Power to carry out investigations on human rights violations in all state bodies, including intelligence and security services. – Power to receive complaints on and issue reports on its findings and sending the report for comments to the parties involved (it does not have the power to issue binding decisions). – Power to issue recommendations on how to address the human rights violations established. – Power to propose that

					disciplinary proceedings are issued against an official who committed human rights violations, as established by the Ombudsman. – The right to obtain a report in 30 days from the state bodies on how the established violation was addressed and rectified. – In case the response of the state body was insufficient the Ombudsman has the right to inform the entity to whom the said state body is responsible. It can also publish a special report or publish its report in the media, on the expenses of the state body that violated human rights. – Right to enter the premises of any state body. Duty to report annually to the National assembly. (Articles 26-46)

State budget inspection of the Ministry of Finance of the Republic of Slovenia (Proračunska inšpekcija Ministrstva Republike Slovenije za finance).	Organisational unit within the Ministry of Finance, competent for inspection procedures concerning spending of public funds.	Slovenia, Public Finance Act (*Zakon o javnih financah*), 16 September 1999, Article 102.	*Ex post* (upon complaints) and *ex ante* (on the basis of annual work plans) oversight. So far the state budget inspectors have performed five inspection procedures.[16]	The personnel competent to carry out budget inspections comprise of five inspectors plus their head.[17] State budget inspectors are public servants employed in accordance with the Public Servants Act.	– Duty to oversee spending of public funds and to carry out inspection procedures. This includes issuing recommendations, binding decisions and imposing sanctions.
Court of Audit of the Republic of Slovenia (Računsko sodišče Republike Slovenije)	Autonomous and independent state body competent for supervision of state accounts, state budget and spending of public funds.	Slovenia, Court of Auditors Act (*Zakon o računskem sodišču*), 30 January 2001, Article 1.	*Ex post*. The Audits are not regular or and do not necessarily take place annually. The last and only audit of Intelligence Services was in 2008.[18] The report of the Court of audit is not publically available.	Court of Audit has three members, president and two vice presidents. They are nominated by the National Assembly, upon the proposal of the President of the Republic. On 31 December 2013 the number of employees at the Court of Audit was 121, out of these 26 supporting staff (Annual Report of the Court of Audit 2013, p. 80).	- Power to audit all financial aspects of state bodies, including intelligence and security services. (Article 20 onwards) – Power to issue recommendations already in the course of the auditing procedure. – Power to issue audit reports that include measures ordering rectification of problems identified in auditing procedure, in a set deadline.

[16] Written response provided by Budget Inspection on 12 August 2014.
[17] Written response provided by Budget Inspection on 12 August 2014.
[18] Written response provided by Court of Audit on 11 August 2014.

					- Power to demand a report from the state body on measures adopted to address the findings of the Court of Audit. – Duty to file a report to the inspection body or the state prosecutor’s office in case of suspicion of a misdemeanour or criminal act. (Articles 20-30 of the Court of Auditors Act)

Annex 3 – Remedies[19]

Slovene Intelligence and Security Agency Act				
Stages of surveillance process	**Is the subject informed?**	**Does the subject have a right of access to the data collected on him/her?**	**List remedies available to an individual concerned**	**Legal basis for using the available remedies**
	Yes/No	*Yes/No, please provide details if needed*	*Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc.* ***AND*** *please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies.*	*Violation of data protection, private life, specific legislation, etc.*
Collection*	No. Article 17 of ZSOVA states that the Agency is not obliged to inform the individual whom the data concerns about the fact that the	Yes, under Personal Data Protection Act. However, this right can be limited by force of law, for reasons (among others) of protection of state sovereignty and defence, protection of national	- Complaint to the Parliamentary Commission to initiate supervision of intelligence and security service (if data collection is unlawful) - Complaint to the Information Commissioner (if data collection is contrary to data protection safeguards). Against the decision of the Information Commissioner a lawsuit can be lodged to the	- The Parliamentary Supervision of the Intelligence and Security Services Act. - Information Commissioner Act (on the grounds data protection safeguards).

[19] In case of different remedial procedures please replicate the table for each legal regime.

* For the definitions of these terms, please refer to the FRA/CoE (2014), *Handbook on European data protection law*, Luxembourg, 2014, pp. 46-47, available at: http://fra.europa.eu/en/news/2014/council-europe-and-eu-fundamental-rights-agency-launch-handbook-european-data-protection

	data is being collected (§1), and that this right of an individual can be limited if informing the individual would make the task of data collection more difficult (§2). Finally the provision states that the keepers of data collections may inform the person concerned after five years since the data has been transmitted to the Agency, upon a demand of the Director of the Agency (§3).	security and constitutional order of the state, as well as security, political and economic interests of the state. These limitations may be defined only in the scope that is necessary to achieve the purpose of the limitation (Article 36 of Personal Data Protection Act). These exceptions apply to activities of SOVA and MORS. The Information Commissioner checks on a case-by-case basis whether data protection guarantees cannot be invoked due to these exceptions. The exceptions are therefore not used blankly in relation to all the activities of SOVA and OVS MORS, but only in relation to the specific data related to a particular case.	Administrative Court for judicial review. - Direct lawsuit to the Administrative Court. - Complaint to Human Rights Ombudsman (if data collection is connected to human rights violations)	- Personal Data Protection Act. - Human Rights Ombudsman Act (on the grounds of human rights violations – protection of personal data, protection of family and private life etc.)

Analysis*	No.	Yes, under Personal Data Protection Act. However, this right can be limited by force of law, for reasons (among others) of protection of state sovereignty and defence, protection of national security and constitutional order of the state, as well as security, political and economic interests of the state. These limitations may be defined only in the scope that is necessary to achieve the purpose of the limitation (Article 36 of Personal Data Protection Act).	- Complaint to the Parliamentary Commission to initiate supervision of intelligence and security service (if data collection is unlawful) - Complaint to the Information Commissioner (if data collection is contrary to data protection safeguards). Against the decision of the Information Commissioner a lawsuit can be lodged to the Administrative Court for judicial review. - Direct lawsuit to the Administrative Court. - Complaint to Human Rights Ombudsman (if data collection is connected to human rights violations)	- The Parliamentary Supervision of the Intelligence and Security Services Act. - Information Commissioner Act (on the grounds data protection safeguards). - Personal Data Protection Act. - Human Rights Ombudsman Act (on the grounds of human rights violations – protection of personal data, protection of family and private life etc.)
Storing*	No.	Yes, under Personal Data Protection Act. However, this right can be limited by force of law, for reasons (among others) of protection of state sovereignty and defence,	- Complaint to the Parliamentary Commission to initiate supervision of intelligence and security service (if data collection is unlawful) - Complaint to the Information Commissioner (if data collection is contrary to data protection safeguards). Against the decision of the Information Commissioner a	- The Parliamentary Supervision of the Intelligence and Security Services Act. - Information Commissioner Act (on the grounds data protection safeguards).

		protection of national security and constitutional order of the state, as well as security, political and economic interests of the state. These limitations may be defined only in the scope that is necessary to achieve the purpose of the limitation (Article 36 of Personal Data Protection Act).	lawsuit can be lodged to the Administrative Court for judicial review. - Direct lawsuit to the Administrative Court. - Complaint to Human Rights Ombudsman (if data collection is connected to human rights violations)	- Personal Data Protection Act. - Human Rights Ombudsman Act (on the grounds of human rights violations – protection of personal data, protection of family and private life etc.)
Destruction *	No.	Yes, under Personal Data Protection Act. However, this right can be limited by force of law, for reasons (among others) of protection of state sovereignty and defence, protection of national security and constitutional order of the state, as well as security, political and economic interests of the state. These limitations may be defined only in the	- Complaint to the Parliamentary Commission to initiate supervision of intelligence and security service (if data collection is unlawful) - Complaint to the Information Commissioner (if data collection is contrary to data protection safeguards). Against the decision of the Information Commissioner a lawsuit can be lodged to the Administrative Court for judicial review. - Direct lawsuit to the Administrative Court. - Complaint to Human Rights Ombudsman (if data collection is connected to human rights violations)	- The Parliamentary Supervision of the Intelligence and Security Services Act. - Information Commissioner Act (on the grounds data protection safeguards). - Personal Data Protection Act. - Human Rights Ombudsman Act (on the grounds of human rights violations – protection of personal data, protection of

		scope that is necessary to achieve the purpose of the limitation (Article 36 of Personal Data Protection Act).		family and private life etc.)
After the whole surveillance process has ended	Yes, but only in some cases (surveillance of private communication) and under certain conditions (if this would not threaten national security or health and lives of people). (Article 24 §5 of ZSOVA)	Yes, under Personal Data Protection Act. However, this right can be limited by force of law, for reasons (among others) of protection of state sovereignty and defence, protection of national security and constitutional order of the state, as well as security, political and economic interests of the state. These limitations may be defined only in the scope that is necessary to achieve the purpose of the limitation (Article 36 of Personal Data Protection Act).	- Complaint to the Parliamentary Commission to initiate supervision of intelligence and security service (if data collection is unlawful) - Complaint to the Information Commissioner (if data collection is contrary to data protection safeguards). Against the decision of the Information Commissioner a lawsuit can be lodged to the Administrative Court for judicial review. - Direct lawsuit to the Administrative Court. - Complaint to Human Rights Ombudsman (if data collection is connected to human rights violations)	- The Parliamentary Supervision of the Intelligence and Security Services Act. - Information Commissioner Act (on the grounds data protection safeguards). - Personal Data Protection Act. - Human Rights Ombudsman Act (on the grounds of human rights violations – protection of personal data, protection of family and private life etc.)
Defence Act				
Stages of surveillance process	**Is the subject informed?**	**Does the subject have a right of access to the data collected**	**List remedies available to an individual concerned**	**Legal basis for using the available remedies**

		on him/her?		
	Yes/No	*Yes/No, please provide details if needed*	*Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc.* ***AND*** *please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies.*	*Violation of data protection, private life, specific legislation, etc.*
Collection*	No. Article 17 of ZSOVA states that the Agency is not obliged to inform the individual whom the data concerns about the fact that the data is being collected (§1), and that this right of an individual can be limited if informing the individual	Yes, under Personal Data Protection Act. However, this right can be limited by force of law, for reasons (among others) of protection of state sovereignty and defence, protection of national security and constitutional order of the state, as well as security, political and economic interests of the state. These limitations may be defined only in the	- Complaint to the Parliamentary Commission to initiate supervision of intelligence and security service (if data collection is unlawful) - Complaint to the Information Commissioner (if data collection is contrary to data protection safeguards). Against the decision of the Information Commissioner a lawsuit can be lodged to the Administrative Court for judicial review. - Direct lawsuit to the Administrative Court. - Complaint to Human Rights Ombudsman (if data collection is connected to human rights violations)	- The Parliamentary Supervision of the Intelligence and Security Services Act. - Information Commissioner Act (on the grounds data protection safeguards). - Personal Data Protection Act. - Human Rights Ombudsman Act (on the grounds of human rights violations – protection of personal data, protection of

* For the definitions of these terms, please refer to the FRA/CoE (2014), *Handbook on European data protection law*, Luxembourg, 2014, pp. 46-47, available at: http://fra.europa.eu/en/news/2014/council-europe-and-eu-fundamental-rights-agency-launch-handbook-european-data-protection

	would make the task of data collection more difficult (§2). Finally the provision states that the keepers of data collections may inform the person concerned after five years since the data has been transmitted to the Agency, upon a demand of the Director of the Agency (§3).	scope that is necessary to achieve the purpose of the limitation (Article 36 of Personal Data Protection Act).		family and private life etc.)
Analysis*	No.	Yes, under Personal Data Protection Act. However, this right can be limited by force of law, for reasons (among others) of protection of state sovereignty and defence, protection of national security and	- Complaint to the Parliamentary Commission to initiate supervision of intelligence and security service (if data collection is unlawful) - Complaint to the Information Commissioner (if data collection is contrary to data protection safeguards). Against the decision of the Information Commissioner a lawsuit can be lodged to the Administrative Court for judicial	- The Parliamentary Supervision of the Intelligence and Security Services Act. - Information Commissioner Act (on the grounds data protection safeguards).

		constitutional order of the state, as well as security, political and economic interests of the state. These limitations may be defined only in the scope that is necessary to achieve the purpose of the limitation (Article 36 of Personal Data Protection Act).	review. - Direct lawsuit to the Administrative Court. - Complaint to Human Rights Ombudsman (if data collection is connected to human rights violations)	- Personal Data Protection Act. - Human Rights Ombudsman Act (on the grounds of human rights violations – protection of personal data, protection of family and private life etc.)
Storing*	No.	Yes, under Personal Data Protection Act. However, this right can be limited by force of law, for reasons (among others) of protection of state sovereignty and defence, protection of national security and constitutional order of the state, as well as security, political and economic interests of the state. These limitations may be defined only in the scope that is necessary to achieve the purpose	- Complaint to the Parliamentary Commission to initiate supervision of intelligence and security service (if data collection is unlawful) - Complaint to the Information Commissioner (if data collection is contrary to data protection safeguards). Against the decision of the Information Commissioner a lawsuit can be lodged to the Administrative Court for judicial review. - Direct lawsuit to the Administrative Court. - Complaint to Human Rights Ombudsman (if data collection is connected to human rights violations)	- The Parliamentary Supervision of the Intelligence and Security Services Act. - Information Commissioner Act (on the grounds data protection safeguards). - Personal Data Protection Act. - Human Rights Ombudsman Act (on the grounds of human rights violations – protection of personal data, protection of family and private life etc.)

		of the limitation (Article 36 of Personal Data Protection Act).		
Destruction *	No.	Yes, under Personal Data Protection Act. However, this right can be limited by force of law, for reasons (among others) of protection of state sovereignty and defence, protection of national security and constitutional order of the state, as well as security, political and economic interests of the state. These limitations may be defined only in the scope that is necessary to achieve the purpose of the limitation (Article 36 of Personal Data Protection Act).	- Complaint to the Parliamentary Commission to initiate supervision of intelligence and security service (if data collection is unlawful) - Complaint to the Information Commissioner (if data collection is contrary to data protection safeguards). Against the decision of the Information Commissioner a lawsuit can be lodged to the Administrative Court for judicial review. - Direct lawsuit to the Administrative Court. - Complaint to Human Rights Ombudsman (if data collection is connected to human rights violations)	- The Parliamentary Supervision of the Intelligence and Security Services Act. - Information Commissioner Act (on the grounds data protection safeguards). - Personal Data Protection Act. - Human Rights Ombudsman Act (on the grounds of human rights violations – protection of personal data, protection of family and private life etc.)
After the whole surveillance process has ended	Yes, but only in some cases (surveillance of private communication) and under	Yes, under Personal Data Protection Act. However, this right can be limited by force of law, for reasons (among	- Complaint to the Parliamentary Commission to initiate supervision of intelligence and security service (if data collection is unlawful) - Complaint to the Information Commissioner (if data collection is	- The Parliamentary Supervision of the Intelligence and Security Services Act. - Information Commissioner Act

	certain conditions (if this would not threaten national security or health and lives of people). (Article 24 §5 of ZSOVA)	others) of protection of state sovereignty and defence, protection of national security and constitutional order of the state, as well as security, political and economic interests of the state. These limitations may be defined only in the scope that is necessary to achieve the purpose of the limitation (Article 36 of Personal Data Protection Act).	contrary to data protection safeguards). Against the decision of the Information Commissioner a lawsuit can be lodged to the Administrative Court for judicial review. - Direct lawsuit to the Administrative Court. - Complaint to Human Rights Ombudsman (if data collection is connected to human rights violations)	(on the grounds data protection safeguards). - Personal Data Protection Act. - Human Rights Ombudsman Act (on the grounds of human rights violations – protection of personal data, protection of family and private life etc.)

Annex 4 – Surveillance-related case law at national level

Please provide a maximum of three of the most important national cases relating to surveillance. Use the table template below and put each case in a separate table.

No law suit after or based on the revelations by E. Snowden was launched so far in Slovenia.

Case title	U-I-216/07-8
Decision date	4 October 2007
Reference details (type and title of court/body; in original language and English)	Constitutional Court of the Republic of Slovenia (Ustavno sodišče Republike Slovenije)
Key facts of the case (max. 500 chars)	The Director of the Slovene Intelligence and Security Agency (SOVA) addressed a request to the President of the Supreme Court (President) to allow the Agency surveillance of international communication systems. The President interrupted the procedure and lodged a claim for constitutional review of Article 21 of The Slovene Intelligence and Security Agency Act. In the claim the President stated that the term 'surveillance of international communication systems' is not sufficiently defined and that allowing such surveillance would violate the constitutional guarantee of privacy of correspondence and other means of communication (Article 37 of the Constitution).
Main reasoning/argumentation (max. 500 chars)	The Constitutional Court rejected the claim for formal reasons, without adopting a decision on the merits of the case. It established that based on the law the President does not have the competence to authorise surveillance of international communication systems. Such competence would be given only if such surveillance was used in the Slovenian territory or in relation to the person on this territory. The Court concluded that the President of the Supreme Court therefore did not need to use Article 21 of this Act and therefore was not in the position to file a claim for constitutional review of this Act.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	In spite of the fact that there was no decision on the merits, the Constitutional Court confirmed that while surveillance of private correspondence within Republic of Slovenia or in relation to persons at the territory of the Republic of Slovenia requires an order issued by the Supreme Court, such an order is not required for the surveillance of international communication systems. Article 21 of the disputed Act states that surveillance of international communication systems is authorised with an order issued by the Director of the Agency. It is not clear why the Director lodged request for authorisation to the President of the Supreme Court in the first place.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	Since the claim was rejected the disputed legislative provisions remained in power.

Case title	U-I-45/08-21
Decision date	8 January 2009
Reference details (type and title of court/body; in original language and English)	Constitutional Court of the Republic of Slovenia (Ustavno sodišče Republike Slovenije)
Key facts of the case (max. 500 chars)	After conducting an inspection procedure at the Slovene Intelligence and Security Agency (SOVA) the Information Commissioner lodged a claim for constitutional review of Article 21, §1, §2 and §3 of ZSOVA. These provisions define the right of SOVA Director to authorise surveillance of the international communications systems. The inspection procedure showed that such surveillance is carried out after the Director of SOVA approves surveillance of a concrete telephone number, meaning that in practice, such surveillance leads to personal data collection and wiretapping of concrete persons.
Main reasoning/argumentation (max. 500 chars)	The Court rejected the claim for formal reasons, stating that the Information Commissioner may lodge a claim for constitutional review if a question of constitutionality arises in relation to the inspection procedure (as provided under Article 23.a, §6, of the Constitutional Court Act).[20] The Court found that in matter this was not the case. Namely, in inspection procedure the Commissioner was supervising provisions on collection, analysis and transmission of personal data abroad, which has nothing to do with surveillance of communication between foreign communication devices.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	Since the Constitutional Court did not decide on the merits of the case it also did not decide on the question whether the Information Commissioner is competent for supervision of SOVA, taking into account that supervision of SOVA is entrusted to the Parliamentary Commission.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	Since the claim was rejected the disputed legislative provisions remained in power.

[20] Zakon o ustavnem sodišču (Uradni list RS, št. 64/07 - uradno prečiščeno besedilo in 109/12).

Case title	U 422/2006-15
Decision date	4 October 2007
Reference details (type and title of court/body; in original language and English)	Administrative Court of the Republic of Slovenia, Department Nova Gorica (Upravno sodišče Republike Slovenije, Oddelek v Novi Gorici)
Key facts of the case (max. 500 chars)	An individual, who has been involved in written correspondence with SOVA since 1993, lodged a claim to SOVA to provide her with an extract of personal data collected on her by SOVA. SOVA failed to respond the claimant, who consequently lodged a complaint to the Information Commissioner. The latter checked with SOVA and found that the claimant frequently wrote to SOVA and that the content of some of the letters was insulting. Consequently SOVA stopped answering to the claimant. The Commissioner found that SOVA is not collecting personal data of the claimant, and denied the complaint. The claimant sought judicial review before the Administrative Court.
Main reasoning/argumentation (max. 500 chars)	The Administrative Court refused the claim and confirmed the decision of the Information Commissioner. It found that the Commissioner, as provided for by the Personal Data Protection Act, acted in accordance with the law when checking with SOVA whether personal data of the individual are being collected, and that its decision to reject the individual's claim was correct.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The case shows that SOVA is considered as a body that collects personal data and it is therefore bound by Personal data protection Act. SOVA is obliged to enable the Information Commissioner to check whether personal data of a certain individual who claims so, are being collected and analysed. The Information Commissioner can therefore provide an effective remedy for individuals in surveillance leading to data collection also in practice.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	As the individuals' claim was rejected the decision of the Information Commissioner remained in power.

Case title	U-I-65/13-19
Decision date	3 July 2014
Reference details (type and title of court/body; in original language and English)	Constitutional Court of the Republic of Slovenia (Ustavno sodišče Republike Slovenije)
Key facts of the case (max. 500 chars)	The Information Commission lodged a claim for constitutional review of the Electronic Communications Act in relation to provisions that provided for data retention for the period of 14 months for publicly available telephone services and for the period of 8 months for other data. The provisions providing for data retention were included in the law as a result of transposition of EU Directive 2006/24/ES into the Slovenian legal order.
Main reasoning/argumentation (max. 500 chars)	The Constitutional Court first interrupted the procedure since the Court of Justice of the European Union was deciding whether the stated directive was in accordance with the EU law. It interrupted the procedure until the CJEU decided upon the case. Based on the CJEU decision as well as on the basis of the provisions of the constitution, the Constitutional Court found that the provisions providing for indiscriminate data retention were violating Article 38 of the Constitution (right to personal data protection).
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Constitutional Court examined whether the provisions were in line with the principle of proportionality. It found that the legislator had the right to interfere with personal data protection guarantees, however interference measures have to be appropriate and necessary to achieve the legitimate aim - combat against organised crime, state security, defence of the state and constitutional order. The Constitutional Court found that the legislator could have used a less invasive way to achieve these aims.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Constitutional Court annulled the provisions of Articles 162-169 of the Electronic Communications Act and ordered all telecommunication service providers to delete all personal data they were storing based on these provisions. As a result, there are no other provisions in the law that would allow for data retention without a prior authorisation of the competent body.

Annex 5 – Key stakeholders at national level

Please list all the key stakeholders in your country working in the area of surveillance and divide them according to their type (i.e. public authorities, civil society organisations, academia, government, courts, parliament, other). Please provide name, website and contact details.

Name of stakeholder (in English as well as your national language)	**Type of stakeholder** *(i.e. public authorities, civil society organisations, academia, government, courts, parliament, other)*	**Contact details**	**Website**
Slovene Intelligence and Security Agency (Slovenska obveščevalno-varnostna služba – SOVA)	Public authority	Address: Stegne 23c, 1000 Ljubljana, Slovenia T: + 386 (0)1 479 91 01 E: gp.sova(at)gov.si Director: Stane Štemberger	http://www.sova.gov.si/
Intelligence and Security Service of the Ministry of Defence of the Republic of Slovenia (Obveščevalno-varnostna služba Ministrstva Republike Slovenije za obrambo	Public authority	Address: Vojkova cesta 55, 1000 Ljubljana, Slovenia T: + 386 (0)1 471 13 00, 431 90 01, 431 90 13 F: + 386 (0)1 471 90 22 E: gorazd.rednak@mors.si Director: Gorazd Rednak	http://www.mo.gov.si/si/o_ministrstvu/organizacija/obvescevalno_varnostna_sluzba/

Supreme Court of the Republic of Slovenia (Vrhovno sodišče Republike Slovenije)	Court	Address: Tavčarjeva 9, 1000 Ljubljana, Slovenia T: + 386 (0)1 366 44 44 F: + 386 (0)1 366 43 01 E: urad.vsrs@sodisce.si President: Branko Masleša	http://www.sodisce.si/vsrs/
Parliamentary Commission for Supervision of the Intelligence and Security Services (Parlamentarna komisija za nadzor obveščevalnih in varnostnih služb)	Parliamentary Commission	Address: National Assembly, Šubičeva ulica 4, 1102 Ljubljana, Slovenia T: + 386 (0)1 478 94 00 F: + 386 (0)1 478 98 45 E: gp@dz-rs.si	http://www.dz-rs.si/
Government of the Republic of Slovenia (Vlada Republike Slovenije)	Government	Address: Gregorčičeva 20-25, 1000 Ljubljana, Slovenia T: + 386 (0)1 478 1000 F: + 386 (0)1 478 1607	http://www.vlada.si/
National Security Council of the Republic of Slovenia (Svet Republike Slovenije za nacionalno varnost)	Consultative body of the Government	Address: Gregorčičeva 20-25, 1000 Ljubljana, Slovenia T: + 386 (0)1 478 1000 F: + 386 (0)1 478 1607	http://www.vlada.si/

Information Commissioner of the Republic of Slovenia (Informacijski pooblaščenec Republike Slovenije)	Public authority	Address: Zaloška 59, 1000 Ljubljana, Slovenia T: + 386 (0)1 230 97 30 F: + 386 (0)1 230 97 78 E: gp.ip@ip-rs.si	https://www.ip-rs.si/
Human Rights Ombudsman (Varuh človekovih pravic)	Public authority	Address: Dunajska cesta 56, 1109 Ljubljana, Slovenia T: + 386 (0)1 475 00 50 F: + 386 (0)1 475 00 40 E: info@varuh-rs.si	http://www.varuh-rs.si/
State budget inspection of the Ministry of Finance of the Republic of Slovenia (Proračunska inšpekcija Ministrstva Republike Slovenije za finance)	Public authority	Address: Ministry of Finance, Budget Supervision Office, Fajfarjeva 33, 1000 Ljubljana, Slovenia T: + 386 (0)1 369 6900 F: + 386 (0)1 369 6914 E: mf.unp@mf-rs.si	http://www.unp.gov.si/en/
Court of Audit of the Republic of Slovenia (Računsko sodišče Republike Slovenije)	Public authority	Address: Slovenska cesta 50, 1000 Ljubljana, Slovenia T: + 386 (0)1 478 5888 F: + 386 (0)1 478 5891 E: sloaud@rs-rs.si	www.rs-rs.si
Administrative Court of the Republic of Slovenia (Upravno	Court	Address: Fajfarjeva 33, 1000 Ljubljana, Slovenia T: + 386 (0)1 47 00 100 F: + 386 (0)1 47 00 150	http://www.sodisce.si/usrs/

sodišče Republike Slovenije)		E: Urad.Uprlj@sodisce.si	
Faculty of Social Sciences, University of Ljubljana (Fakulteta za družbene vede Univerze v Ljubljani)	Academia	Address: Kardeljeva ploščad 5, 1000 Ljubljana, Slovenia T: + 386 (0)1 5805-100 F: + 386 (0)1 5805-101 E: fdv.faculty@fdv.uni-lj.si	http://www.fdv.uni-lj.si
Fakultate za varnostne vede Univerze v Mariboru (Faculty of Criminal Justice and Security of the University of Maribor)	Academia	Address: Kotnikova 8, 1000 Ljubljana, Slovenia T: + 386 (0)1 3008 300 F: +386 (0)1 2302 687 E: fvv@fvv.uni-mb.si	http://www.fvv.uni-mb.si/
Mirovni institute (The Peace Institute)	NGO	Address: Metelkova 6, 1000 Ljubljana, Slovenia T: + 386 (0)1 234 77 20 F: + 386 (1)234 77 22 E: info@mirovni-institut.si	http://www.mirovni-institut.si/
Amnesty International Slovenije (Amnesty International) Slovenia	NGO	Address: Beethovnova 7, 1000 Ljubljana, Slovenia T: + 386 (0)1 426 93 77 F: + 386 (0)1 426 93 65 E: amnesty@amnesty.si	http://www.amnesty.si/
Transparency International Slovenje – Društvo Integriteta (Transparency	NGO	Address: Povšetova 37, 1000 Ljubljana, Slovenia T: + 386 (0)40528279 E: info@integriteta.si	http://integriteta.si/

International Slovenia – Association Integriteta)			
Inštitut za elektronsko participacijo (Institute for Electronic Participation)	NGO	Address: Povšetova 37, 1000 Ljubljana, Slovenia T: + 386 (0)41 365 529 E: info@inepa.si	http://www.inepa.si/

Annex 6 – Indicative bibliography

Please list relevant reports, articles, studies, speeches and statements divided by the following type of **sources *(in accordance with FRA style guide)***:

1. Government/ministries/public authorities in charge of surveillance

Slovenia, Parliamentary Commission for Supervision of the Intelligence and Security Services (*Parlamentarna komisija za nadzor obveščevalnih in varnostnih služb*) (2011), Annual Report for 2010 – public part (*Letno poročilo za leto 2010 – javni del*).

Slovenia, Government of the Republic of Slovenia (*Vlada Republike Slovenije*) (2008), Final Report of the Working Group for Assessment of Work of the Slovene Intelligence and Security Agency (*Zaključno poročilo delovne skupine za oceno dela Slovenske obveščevalno-varnostne agencije*), No. T- 022-2/2007-30, 30 September 2008.

Slovenia, Slovene Intelligence and Security Agency (*Slovenska obveščevalno-varnostna agencija*) (2011), Report on Activities of the Slovene Intelligence and Security Agency in relation to the issue of archive materials of former Service of State Security (*Poročilo o aktivnostih Slovenske obveščevalno-varnostne agencije v zvezi s problematiko arhivskega gradiva nekdanje SDV*), No. 020-4/2010/59, 2 February 2011.

2. National human rights institutions, ombudsperson institutions, national data protection authorities and other national non-judicial bodies/authorities monitoring or supervising implementation of human rights with a particular interest in surveillance

Slovenia, Human Rights Ombudsman (*Varuh človekovih pravic*) (2012), Annual Report for 2011.

Slovenia, Information Commissioner of the Republic of Slovenia (*Informacijski pooblaščenec Republike Slovenije*) (2008), Claim for Constitutional Review (*Zahteva za oceno ustavnosti*), 6 March 2008.

Slovenia, Information Commissioner of the Republic of Slovenia (*Informacijski pooblaščenec Republike Slovenije*) (2009), Non-binding opinion No. 0712-184/2009/2 (*Neobvezno mnenje št. 0712-184/2009/2*), 23 April 2009.

Slovenia, Information Commissioner of the Republic of Slovenia (*Informacijski pooblaščenec Republike Slovenije*) (2014), Annual Report for 2013 (Letno poročilo za leto 2013).

Slovenia, Administrative Court of the Republic of Slovenia (*Upravno sodišče Republike Slovenije*) (2007), Judgment No. U 422/2006-15, 4 October 2007.

Slovenia, Constitutional Court of the Republic of Slovenia (*Ustavno sodišče Republike Slovenije*) (2009), Ruling No. U-I-45/08-21, 1 January 2009.

Slovenia, Constitutional Court of the Republic of Slovenia (*Ustavno sodišče Republike Slovenije*) (2007), Ruling No. U-I-216/07-8, 4 October 2007.

3. Non-governmental organisations (NGOs)

No reports, articles or other comprehensive written sources produced by the NGOs in Slovenia on the subject were identified. The only relevant sources that could be provided are the following:

Your life is Being Recorded: Establishing Society of Surveillance through Information and Telecommunication Technologies (Vaše življenje se snema: Vzpostavljanje družbe nadzora preko informacijskih in komunikacijskih tehnologij), The Peace Institute Forum, 17 October 2013, video available at: https://www.youtube.com/watch?v=776JhIxAsNY.

Public Statement at the International Day of Telecommunication and Information Society (Izjava za javnost ob Mednarodnem dnevu telekomunikacij in informacijske družbe), Institute for Electronic Communication, 17 May 2013, available at: http://www.inepa.si/institut-inepa/novice/225-mednarodni-dan-telekomunikacij-in-informacijske-druzbe.html.

4. Academic and research institutes, think tanks, investigative media report.

Anžič, A., Golobinek, R. (2003), Slovenian Model of Parliamentary Oversight of Intelligence and Security Services (*Slovenski model parlamentarnega nadzorstva nad obveščevalnimi in varnostnimi službami*), *Teorija in praksa*, 40(6), pp. 1058-1073.

Britovšek, P. (2008), Surveillance of International Communication Systems as an Alleged Interference in the Communication Privacy of an Individual in relation to the Territorial Principle of Rights (Spremljanje mednarodnih sistemov zvez kot domnevni poseg v komunikacijsko zasebnost posameznika v povezavi s teritorialnim principom pravice), Javna in zasebna varnost: zbornik prispevkov / 9. slovenski dnevi varstvoslovja, Bled, 5. in 6. junij 2008; ed. Jerneja Šifrer.

Garb, G. (2007), Forms of Secret Operations of Intelligence and Security Services of the Republic of Slovenia (*Oblike tajnega delovanja obveščevalno-varnostnih služb Republike Slovenije*), Master Thesis, Mentor Dr. Drago Zajc, Co-mentor Dr. Iztok Prezelj, Faculty of Social Sciences of the University of Ljubljana.

Ilinčić, S. (2006), Parliamentary Oversight of Intelligence and Security Services in the Republic of Slovenia (*Parlamentarno nadzorstvo obveščevalnih in varnostnih služb v Republiki Sloveniji*), Diploma Thesis, Mentor Dr. Andrej Anžič, Faculty of Social Sciences of the University of Ljubljana.

Kokalj, M. (2006), Slovene Intelligence and Security Agency as an Autonomous Government Service (*Slovenska obveščevalno-varnostna agencija kot samostojna vladna služba*), Diploma Thesis, Mentor dr. Miro Haček, Faculty of Social Sciences of the University of Ljubljana.

Kuralt, M. (2009), Forms of Oversight of the Work of Slovene Intelligence and Security Agency (*Oblike nadzorstva nad delom Slovenske obveščevalno varnostne agencije*), *Varstvoslovje*, pp. 2-11.

Lindič, M. (2013), Internal Supervision of Intelligence and Security Services (*Notranji nadzor obveščevalno varnostnih služb*), Diploma Thesis, Mentor dr. Franc Željko Županič, Faculty of Criminal Justice and Security of the University of Maribor.

Štarkel K. T. (2011), (Un)lawfulness of Functioning of Intelligence Service: Case Study of Sova Affair (*(Ne)zakonitost delovanja obveščevalne službe: analiza primera afere Sova*), Diploma Thesis, Mentor dr. Iztok Prezelj, Faculty of Social Sciences of the University of Ljubljana.

Vehovec, T. (2003), Re-structuring of Intelligence and Security System in Slovenia (*Prestrukturiranje obveščevalno-varnostnega sistema v Republiki Sloveniji*), Diploma Thesis, Mentor dr. Marjan Brezovšek, Faculty of Social Sciences of the University of Ljubljana.