Ad hoc information request: National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

SLOVAK REPUBLIC

Version of 6 October 2014

Center for the Research of Ethnicity and Culture (CVEK)
Eva Kovačechová

Summary

[1]. There is an on-going discussion on adopting a new national intelligence law. It was about to come into force on 1 January 2015, but the law was not yet adopted. The law assumed establishing new name of the Slovak Information Service (The Civil Intelligence Bureau) and it was supposed to elaborate more precisely about certain issues in the law. There were concerns that the new law would bring more powers to the Prime Minister towards intelligence services.[1] Nevertheless, the law was not yet adopted.

A- Slovak Information Service

[2]. Slovak Information Service [*Slovenská informačná služba*] (SIS) is established under the Act No. 46/1993 Coll. on the Slovak Information Service. The Information Service is a state body of the Slovak Republic which shall fulfil tasks in the protection of the constitutional establishment, public order, security of the State and interests of the State concerning the foreign policy and economy to the extent circumscribed by this act.[2]

[3]. Within the scope of its functions the Information Service shall collect, accumulate and analyse information. Its activities in relation to the use of information-technical means without the prior consent of the person whose privacy is infringed upon by the state body are regulated by the Act. 166/2003 Coll. on the Protection of the privacy against unauthorized use of information and technical means (Act on the Protection against Interception).[3]

[4]. SIS is entitled to request the assistance, documents or information from the government and other bodies, legal entities and individuals in case they may contribute to clarifying the facts important for the tasks specified by the law. To the extent necessary, the SIS has the right to access the information and personal data from the information systems of the state bodies even without the informing and consent of the person concerned.[4]

[5]. Any enterprise providing telecommunication services is required upon a written request and with the consent of the court or upon a court order to

[1] TERAZ.SK (2014) '*New law on intelligence services should be valid since January 2015*' http://www.teraz.sk/slovensko/spravodajske-sluzby-novy-zakon/73267-clanok.html.

[2] Slovakia, Act of the National Council of the Slovak Republic No. 46/1993 Coll., on the Slovak Information Service (*Zákon Národnej rady Slovenskej republiky č. 46/1993 Z.z. o Slovenskej informačnej službe*), 21 January 1993.

[3] Slovakia, Act of the National Council of the Slovak Republic No. 166/2003 Coll.on the Protection against Interception (*Zákon Národnej rady Slovenskej republiky č. 166/2003 Z.z. o ochrane pred odpočúvaním*), 24 April 2003.

[4] Slovakia, Act of the National Council of the Slovak Republic No. 46/1993 Coll. on the Slovak Information Service (*Zákon Národnej rady Slovenskej republiky č. 46/1993 Z.z. o Slovenskej informačnej službe*), 21 January 1993.

provide SIS with the data that are subject to telecommunications privacy in writing or electronically in an encrypted form and understandable way.[5] The Criminal Procedure Act uses term "court order",[6] while the Act on Protection against Interception uses the term "consent of the court".[7] Both court order and consent of the court are issued in identical court procedures.

[6]. Oversight over the Information Service activities shall be carried out by the National Council of the Slovak Republic, which shall establish a special Oversight Body comprised of members of the National Council. If the Oversight Body discovers any violation of the Act No. 46/1993 Coll., they are obliged to notify the National Council of the Slovak Republic and the Prosecutor General. Depending on the nature of the violation, the Government of the Slovak Republic shall also be informed.[8]

[7]. Within the scope of its functions the Information Service shall collect, accumulate and analyse information originating from Slovak Republic as well as from abroad.

[8]. The Information Service collects, accumulates and analyses information on:

I. activities threatening the constitutional establishment, territorial integrity and sovereignty of the Slovak Republic,
II. activities directed against the security of the Slovak Republic,
III. activities of foreign intelligence services,
IV. organized criminal activity and terrorism,
V. matters potentially capable of seriously threatening and/or inflicting damage upon the economic interests of the Slovak Republic,
VI. threat and/or disclosure of information and matters protected according to special regulations or international agreements or international protocols.

[9]. The Information Service shall collect, accumulate and analyse information on activities arising abroad which are directed against the constitutional

[5] Slovakia, Act of the National Council of the Slovak Republic No. 351/2011 Coll. on the Electronic Communication (*Zákon Národnej rady Slovenskej republiky č. 351/2011 Z.z. o elektronických komunikáciách*), 14 September 2011.

[6] Slovakia, Section 116 of the Act of the national Council of the Slovak Republic No. 301/2005 Coll. Criminal Procedure Act (*Zákon Národnej rady Slovenskej republiky č. 301/2005 Z.z. Trestný poriadok*), 24 May 2005.

[7] Slovakia, Act of the National Council of the Slovak Republic No. 166/2003 Coll.on the Protection against Interception (*Zákon Národnej rady Slovenskej republiky č. 166/2003 Z.z. o ochrane pred odpočúvaním*), 24 April 2003.

[8] Slovakia, Act of the National Council of the Slovak Republic No. 46/1993 Coll. on the Slovak Information Service (*Zákon Národnej rady Slovenskej republiky č. 46/1993 Z.z. o Slovenskej informačnej službe*), 21 January 1993.

establishment and security of the Slovak Republic and information necessary for the implementation of its interests concerning the foreign policy.[9]

[10]. SIS collects, accumulates and analyses information. It develops and operates information systems, in which personal data of individuals and information about things or facts related to its tasks are processed.

[11]. Information on the conduct of adolescents less than 14 years of age cannot be entered into files.[10] The Information Service shall be required to ensure protection of personal data processed in its information systems and information kept in file from disclosure, abuse, damage or unauthorised destruction and loss. In cases where information kept in files of the Information Service is no longer required for the fulfilment of established duties, or be it for any legal reason, the Information Service shall be required to store the data in a way which would prevent anyone, with the exception of a court, from obtaining access to it.[11] Information and technical means can be used only when necessary, as defined in the Act on Protection against Interception,[12] and solely to achieve the purpose of carrying out the tasks of the state. [13] Information and technical means are in particular electrotechnical, radiotechnical, phototechnical, optic, mechanical, chemical and other technical means and mechanisms.[14] They may be used only with the prior written permission of the statutory judge for the necessary time, up to a maximum of 6 months. This shall be repeatedly extended based on a new application, but always to a maximum of 6 months. It is not possible to appeal against the approval decision. The statutory judge, who issued the consent, is obliged to systematically examine the duration of the reasons for

[9] Slovakia, Act of the National Council of the Slovak Republic No. 46/1993 Coll. on the Slovak Information Service (*Zákon Národnej rady Slovenskej republiky č. 46/1993 Z.z. o Slovenskej informačnej službe*), 21 January 1993, Section 2.

[10] Slovakia, Act of the National Council of the Slovak Republic No. 46/1993 Coll. on the Slovak Information Service (*Zákon Národnej rady Slovenskej republiky č. 46/1993 Z.z. o Slovenskej informačnej službe*), 21 January 1993, Section 17.

[11] Slovakia, Act of the National Council of the Slovak Republic No. 46/1993 Coll. on the Slovak Information Service (*Zákon Národnej rady Slovenskej republiky č. 46/1993 Z.z. o Slovenskej informačnej službe*), 21 January 1993, Section 17.

[12] Slovakia, Act of the National Council of the Slovak Republic No. 166/2003 Coll.on the Protection against Interception (*Zákon Národnej rady Slovenskej republiky č. 166/2003 Z.z. o ochrane pred odpočúvaním*), 24 April 2003, Section 3: "Information and technical means may be used only if it is inevitable in democratic society to ensure security of state, defense of the state, prevention and clarification of criminal activities, or to protect rights and freedoms of others."

[13] Slovakia, Act of the National Council of the Slovak Republic No. 166/2003 Coll.on the Protection against Interception (*Zákon Národnej rady Slovenskej republiky č. 166/2003 Z.z. o ochrane pred odpočúvaním*), 24 April 2003, Section 3 paragraph 2.

[14] Slovakia, Act of the National Council of the Slovak Republic No. 166/2003 Coll.on the Protection against Interception (*Zákon Národnej rady Slovenskej republiky č. 166/2003 Z.z. o ochrane pred odpočúvaním*), 24 April 2003, Section 2.

the use of information and technical resources. If the reasons no longer exist, he/she shall decide without delay on completion of their use.[15]

B- Millitary Intelligence

[12]. a. Millitary Intelligence [*Vojenské spravodajstvo*] (MI) is established by the law.[16] It is a special service that performs the role of securing intelligence defence of the Slovak Republic.

[13]. b. Within the scope of its functions the Military Intelligence shall collect, accumulate and analyse information. Its activities in relation to the use of information-technical means without the prior consent of the person whose privacy is infringed upon by the state body is regulated by the Act. 166/2003 Z.z. on the protection of the privacy against unauthorized use of information and technical means (Act on the Protection against Interception).[17]

[14]. MI is entitled to request the assistance, documents or information from the government and other bodies, legal entities and individuals in case they may contribute to clarifying the facts important for the tasks specified by the law. To the extent necessary, the SIS has the right to access the information and personal data from the information systems of the state bodies even without the informing and consent of the person concerned.[18]

[15]. Any enterprise providing telecommunication services is required upon a written request and with the consent of the court, or solely upon a court order, to provide MI with the data that are subject to telecommunications privacy in writing or electronically in an encrypted form and understandable way. [19]

[16]. c. Oversight over the Military Intelligence activities shall be carried out by the National Council of the Slovak Republic, which shall establish a special Oversight Body comprised of members of the National Council. This body is

[15] Slovakia, Act of the National Council of the Slovak Republic No. 166/2003 Coll.on the Protection against Interception (*Zákon Národnej rady Slovenskej republiky č. 166/2003 Z.z. o ochrane pred odpočúvaním*), 24 April 2003, Section 4.

[16] Slovakia, Act of the National Council of the Slovak Republic No. 198/1994 Coll. on Military Intelligence (*Zákon Národnej rady Slovenskej republiky č. 198/1994 Zb. o vojenskom spravodajstve*), 30 June 1994.

[17] Slovakia, Act of the National Council of the Slovak Republic No. 166/2003 Coll.on the Protection against Interception (*Zákon Národnej rady Slovenskej republiky č. 166/2003 Z.z. o ochrane pred odpočúvaním*), 24 April 2003.

[18] Slovakia, Act of the National Council of the Slovak Republic No. 198/1994 Coll. on Military Intelligence (*Zákon Národnej rady Slovenskej republiky č. 198/1994 Zb. o vojenskom spravodajstve*), 30 June 1994.

[19] Slovakia, Act of the National Council of the Slovak Republic No. 351/2011 Coll. on the Electronic Communication (*Zákon Národnej rady Slovenskej republiky č. 351/2011 Z.z. o elektronických komunikáciách*), 14 September 2011.

different from the Oversight body controlling SIS.[20] If the Oversight Body discovers any violation of the law, they are obliged to notify the National Council of the Slovak Republic.[21]

[17]. d. Within the scope of its functions the Military intelligence shall collect, accumulate and analyse information originating from Slovak Republic as well as from abroad.

[18]. e. The Military Intelligence collects, accumulates and analyses information on:

i. activities threatening the constitutional establishment, territorial integrity, sovereignty and defensiveness of the Slovak Republic,
ii. activities of foreign intelligence services,
iii. terrorism,
iv. matters potentially capable of seriously threatening and/or inflicting damage upon the military and economic interests of the Slovak Republic,
v. threat and/or disclosure of information and matters protected according to special regulations or international agreements or international protocols.

[19]. The Military Intelligence shall collect, accumulate and analyse information on activities arising abroad which are directed against the constitutional establishment and security of the Slovak Republic and information necessary for the implementation of its interests concerning the foreign policy.[22]

[20]. MI collects, accumulates and analyses information. It develops and operates registers, in which personal data of individuals and information about things or facts related to its tasks are gathered, preserved and processed.

[21]. Information on the conduct of adolescents less than 15 years of age cannot be entered into files.[23] The Military Intelligence shall be required to ensure protection of personal data processed in its information systems and

[20] Special oversight body of the National Council of the Slovak Republic to control Military Intelligence Service (*Osobitný kontrolný výbor NRSR na kontrolu činnosti Vojenského spravodajstva*) http://www.nrsr.sk/web/Default.aspx?sid=vybory/vybor&ID=132.

[21] Slovakia, Act of the National Council of the Slovak Republic No. 198/1994 Coll. on Military Intelligence (*Zákon Národnej rady Slovenskej republiky č. 198/1994 Zb. o vojenskom spravodajstve*), 30 June 1994.

[22] Slovakia, Act of the National Council of the Slovak Republic No. 198/1994 Coll. on Military Intelligence (*Zákon Národnej rady Slovenskej republiky č. 198/1994 Zb. o vojenskom spravodajstve*), 30 June 1994.

[23] Slovakia, Act of the National Council of the Slovak Republic No. 198/1994 Coll. on Military Intelligence (*Zákon Národnej rady Slovenskej republiky č. 198/1994 Zb. o vojenskom spravodajstve)*, 30 June 1994, Section 17.

information kept in file from disclosure, abuse, damage or unauthorised destruction and loss. In cases where information kept in files of MI is no longer required for the fulfilment of established duties, or be it for any legal reason, MI is entitled to destroy the data. [24] Information and technical means can be used only when necessary, as defined in the Act, and solely to achieve the purpose of carrying out the tasks of the state. They may be used only with the prior written permission of the lawful judge for the necessary time, up to a maximum of 6 months. This shall be repeatedly extended based on a new application, but always to a maximum of 6 months. It is not possible to appeal against the approval decision. The statutory judge, who issued the consent, is oblidged to systematically examine the duration of the reasons for the use of information and technical resources. If the reasons no longer exist, he/she shall decide without delay on completion of their use.[25]

C- National Security Authority

[22]. National Security Authority [*Národný bezpečnostný úrad*] is the main body of state administration for the protection of classified information, cipher service and electronic signature.[26]

[23]. Within the scope of its functions the National Security Authority shall search, collect, accumulate and analyse information necessary for acquaintance with classified information. Such information is collected in individual cases in order to gather information about specific persons who are aiming to gain safety authorisation for acquaintance with classified information. The Act on NSA does not entitle NSA to conduct anonymous massive surveillance. The main role of the NSA is to protect classified information, mainly through preventive measures that create conditions for personal security, industrial security, administrative security, physical and building security, and information security.

[24]. The National Security Authority collects information throught its own means from other state and municipal authorities, as well as other legal entities. The NSA also works with information collected by the Slovak Information Service (SIS), Military Intelligence Service (MI) and Police. SIS and MI shall at request of NSA provide information on security reliability of

[24] Slovakia, Act of the National Council of the Slovak Republic No. 215/2004 Coll. on the Protection of classified information (*Zákon Národnej rady Slovenskej republiky č. 215/2004 Z.z. o ochrane utajovaných skutočností*), 11 March 2004.

[25] Slovakia, Act of the National Council of the Slovak Republic No. 166/2003 Coll.on the Protection against Interception (*Zákon Národnej rady Slovenskej republiky č. 166/2003 Z.z. o ochrane pred odpočúvaním*), 24 April 2003.

[26] Slovakia, Act of the National Council of the Slovak Republic No. 215/2004 Coll. on the Protection of classified information (*Zákon Národnej rady Slovenskej republiky č. 215/2004 Z.z. o ochrane utajovaných skutočností*), 11 March 2004.

nominees, security clearence of the nominees at the place of their residence and on the security of the environment in which the nominee lives, the occurrence of potential secutiry risks and other information requested by NSA in terms of the Act. SIS and MI administrate record and registry connected to protection of classified information.[27]

[25]. However, what is interesting in relation to the collective pursuit, is its competences acquired in 2014. [28] NSA provides basis for the decision making process performed by the Judicial Council on the presumption of judicial competence of all existing judges and candidates for judges. In this context, NSA collects information on judges or candidates for judges, which are:

i. records of the Police Force, Slovak Intelligence Service, Military Intelligence,
ii. verifications carried out in the place of permanent residence,
iii. Information requested from the municipality in which the person has a permanent or temporary residence,
iv. information from checks on the safety of the environment in which the person lives and moves, and the possibility of occurrence of risks,
v. the information requested from other state bodies, other legal persons, natural persons - these persons are obliged to provide it. [29]

[26]. NSA evaluates the collected information and sends the evaluation to the Judicial Council. Based on this evaluation the Judicial Council decides whether the judge/candidate has fulfilled the conditions of judicial competence. [30] In the case regarding judge, the decision of the Judicial Council may be reviewed by the Constitutional Court of the Slovak Republic. Candidate for judge does not have any remedies available. [31]

[27]. NSA has jurisdiction in the Slovak Republic.

---

[27] Slovakia, Act of the National Council of the Slovak Republic No. 215/2004 Coll. on the Protection of classified information (*Zákon Národnej rady Slovenskej republiky č. 215/2004 Z.z. o ochrane utajovaných skutočností*), Article 75, 11 March 2004.

[28] Slovakia, Act amending and supplementing the Act No. 385/2000 Coll. and changing and supplementing selected sections from Act No. 195/2014 Coll. (*Zákon č. 195/2014 Z.z., ktorým sa mení a dopĺňa zákon č. 385/2000 Z.z. a ktorým sa menia a dopĺňajú niektoré zákony*), 04 July 2014.

[29] Slovakia, Act of the National Council of the Slovak Republic No. 215/2004 Coll. on the Protection of classified information (*Zákon Národnej rady Slovenskej republiky č. 215/2004 Z.z. o ochrane utajovaných skutočností*), 11 March 2004, Sections 69a and 69b.

[30] Slovakia, Act of the National Council of the Slovak Republic No. 185/2002 Coll. on the Judicial Council (*Zákon Národnej rady Slovenskej republiky č. 185/2002 Z.z. o Súdnej rade*), 11 April 2002.

[31] Slovakia, Act of the National Council of the Slovak Republic No. 38/1993 Coll. on the Organisation of the Constitutional Court (*Zákon Národnej rady Slovenskej republiky č. 38/1993 Z.z. o organizácii Ústavného súdu Slovenskej republiky, o konaní pred ním a o postavení jeho sudcov*), 20 January 1993.

[28]. NSA provides basis for decision process performed by the Judicial Council at the written request of its chairman and in order to ensure the basis for a decision of the Judicial Council on the presumption of judicial competence.

[29]. NSA collects information, evaluates it and sends the evaluation to the Judicial Council.[32]

[30]. NSA shall collect such information as is necessary to verify the fulfilment of the prerequisites of judicial competence and also for the decision of the Constitutional Court of the Slovak Republic on the complaint against the decision of the Judicial Council. The judge, who according to the decision of the Judicial Council does not fulfil the judicial competence, which should guarantee that the function will be carried out properly, can lodge a complaint with the Constitutional Court. A complaint may also be lodged by the Minister of Justice, if the Judicial Council decided that the judge fulfilled the conditions of the judicial competence, whereas NSA documents do not justify this conclusion.[33]

[32] Slovakia, Act of the National Council of the Slovak Republic No. 215/2004 Coll. on the Protection of classified information (*Zákon Národnej rady Slovenskej republiky č. 215/2004 Z.z. o ochrane utajovaných skutočností*), 11 March 2004, Sections 69a and 69b.

[33] Slovakia, Act of the National Council of the Slovak Republic No. 38/1993 Coll. on the Organisation of the Constitutional Court (*Zákon Národnej rady Slovenskej republiky č. 38/1993 Z.z. o organizácii Ústavného súdu Slovenskej republiky, o konaní pred ním a o postavení jeho sudcov*), 20 January 1993, Section 74da.

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)?
Act on Electronic Communications No. 351/2011 Coll, 14 September 2011	Users (subscribers as well as end-user) who use public services - electronic communications services. This includes any natural person or a legal person who uses electronic communication services.	Enterprise (i.e. any person who provides a service network or service in electronic communications) is required to retain traffic data, location data, and data of communicating parties following the date of communication during: a) Six months in case of Internet	Any electronic communications enterprise is required to retain data related to every user (§ 58 subsection 5). On the basis of a written request and without delay, the enterprise shall be obliged to provide data to the bodies acting in the criminal proceedings, court and other state bodies (i.e. Slovak	The enterprise shall retain the data for a period specified by the law, without no further decision of a competent state authority or court. However, providing the law enforcement body, court or other lawful state body (i.e. Slovak Information Service, Military Intelligence) with the	Enterprise (i.e. any person who provides a service network or service in electronic communications) is required: - to retain traffic data, location data, and data of communicating parties of all its users following the date of the communication (§ 58, subsection 5). - to provide the law enforcement body, court or other lawful state body (i.e. Slovak	The law does not provide any definition of the geographic scope. Enterprise (i.e. any person who provides a service network or service in electronic communications) is required to retain traffic data, location data, and data of communicating parties following the date of	Act provides no information about mass monitoring in another country.

		access, Internet electronic mail and calling through Internet, and b) Twelve months in case of other types of communication. (§ 58 ods. 5 zákona) The enterprise shall retain data in the scope in which it produces or processes it while provisioning a service or network. The undertaking shall retain the data related to the unsuccessful call attempts which the undertaking produces or processes and retain in terms of the telephone numbers, or records in case of the Internet data. (§ 58 ods. 6) The effectiveness of the provisions	Information Service, Military Intelligence) for the purposes of investigation, detection and prosecution of criminal offences related to the terrorism, illegal trading, organized criminal activity, leakage and threatening of the concealed facts and to criminal offences committed by dangerous grouping (§ 58 subsection 7). ! The effectiveness of the provisions under § 58, subsection 7 have been temporarily suspended by the decision of the Constitutional Court of the Slovak Republic dated 04.23.2014 in the matter led under file PL. CC 10/2014 (Decision published in the	data is carried out on the basis of: - A written request - With the consent of the court or on the court order. (§ 63 ods. 6) ! The effectiveness of the provisions under § 63, subsection 6 have been temporarily suspended by the decision of the Constitutional Court of the Slovak Republic dated 04.23.2014 in the matter led under file PL. CC 10/2014 (Decision published in the Collection of Laws under no. 128/2014 Coll).	Information Service, Military Intelligence) (§ 58 ods. 6) with the retained information based on a written request and under the conditions specified by the law (§ 63 subsection 6). -to administer annual statistics on the retained data which should not contain the personal data (§ 58 subsections 8 and 9). - to provide the Ministry of Transport, Construction and Regional Development with the annual statistics. The Ministry shall subsequently submit statistics to the European commission. (§ 58 subsection 9). - to ensure that the data shall be subject to the relevant technical and organisational measures, to protect the data against accidental or unlawful	communication during: a) Six months in case of Internet access, Internet electronic mail and calling through Internet, and b) Twelve months in case of other types of communication. (§ 58 subsection 5 zákona) ! The effectiveness of the provisions under § 58, subsection 7 have been temporarily suspended by the decision of the Constitutional Court of the Slovak Republic dated 04.23.2014 in the matter led under file PL. CC 10/2014 (Decision published in the Collection of Laws	

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)?
		under § 58, subsection 7 have been temporarily suspended by the decision of the Constitutional Court of the Slovak Republic dated 04.23.2014 in the matter led under file PL. CC 10/2014 (Decision published in the Collection of Laws under no. 128/2014 Coll).	Collection of Laws under no. 128/2014 Coll).		destruction, accidental loss or alteration, unauthorised or unlawful storage, processing, access or publishing and to ensure that the data can be accessed only by the authorised persons (§ 58 subsection 10). - to ensure that the data, except those that have been provided and secured, shall be destroyed at the end of the period of retention (§ 58 subsection 10, letter d) - on the basis of a written request, the enterprise providing public networks or public services shall be obliged to provide	under no. 128/2014 Coll).	

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)?
					other state bodies with online, direct and continuous access to the subscribers´ data of its own network or services in an electronic form and also on a physical information carrier (§ 63 subsection 5). - to provide other state body, for the purposes of fulfilling its tasks under special regulations and on the basis of a written request and with the court´s consent or on court´s order, with the data which are subject to telecommunications secrecy in a written form or in an		

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)?
					encrypted electronic form (§ 63 subsection 6) - to operate public networks or provide public services by means of such technology, including its individual parts and software, which makes it possible to connect and operate the equipment for listening and tapping of traffic in a network owned by the state (§ 63 subsection 7). ! The effectiveness of the provisions under § 58, subsections 5-7 and § 63, subsection 6 have been temporarily suspended by the decision of the Constitutional Court of		

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)?
					the Slovak Republic dated 04.23.2014 in the matter led under file PL. CC 10/2014 (Decision published in the Collection of Laws under no. 128/2014 Coll).		
Act on the Protection of Personal Data No. 122/2013 Coll.	This Act applies to everyone who processes personal data, determines the purpose and means of processing or provides personal data for processing (§ 2 subsection 1). The person concerned shall mean any natural person whose personal data are being processed (§	The controller shall process personal data without the consent of the data subject if the purpose of the processing of personal data, group of data subjects and the list of personal data or their scope is stipulated in directly enforceable legally binding act of the European Union,	The processed personal data may be provided, made available or disclosed in the filing system without the data subject's consent only if a special Act stipulates the purpose of provision, making available or disclosure, a list of personal data that may be provided, made	This Act does not provide special provisions on providing the third parties with the personal data of the persons concerned without their consent – it only contains reference to the specific laws.	As soon as the purpose of processing is fulfilled, the controller shall provide for destruction of personal data without undue delay. This does not apply if personal data are a part of the registration record. The controller shall ensure the destruction of personal data without undue delay even if:	As soon as the purpose of processing is fulfilled, the controller shall provide for destruction of personal data without undue delay. If the recording is not used for the purposes of criminal proceedings or proceedings	Act provides no information about mass monitoring in another country.

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)?
	4 subsection 2, letter a).	an international treaty, which is binding for the Slovak Republic, or in this Act. (i.e. The Act on Protection of Personal Data) (§ 10 subsection 1). Also the public space might be monitored without the explicit consent, however, only for the purposes provided by the law, and such space shall be clearly marked as being monitored, except when required by a separate law (§ 15, subsection 7).	available or disclosed, as well as the third parties to which personal data are provided or a group of recipients to which personal data are made available (§ 10 ods. 2 a 3). The above mentioned special acts can be Act No 40/1993 coll. on State Citizenship, the Act No 483/2001 Coll. on Banks, the Act No 305/2005 Coll. on Social-legal protection of Children, the Act No 400/2009 Coll. on State Service. Space accessible to the public can be		- the reasons which prevented obtaining of the consent of the data subject ceased to exist - the data subject requested in a written form the termination of his/her personal data processing (§ 17).	concerning misdemeanours, the person who made it shall be obliged to destroy it at the latest within 15 days from the day following after the day on which the recording was made, unless otherwise stipulated by a special Act (§ 17).	

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)?
			monitored only if it is clearly marked as being monitored and only for the purposes of: - The protection of public order and security, - Detection of crime, - Breach of security of the State, - Protection of property or health (§ 15 subsection 7).				
Act on the Protection of classified information No. 215/2004 Coll., 11 March 2004.	- Persons involved in the protection of classified information - General courts judges and candidates for judges	National Security Authority (NSA) provides the materials necessary for security vettings (§ 10, § 16). osobitné postavenie SIS, VS	NSA ensures the basis for the protection of classified information through the creation of conditions of personnel security, administrative	In order to perform a security vetting it is required (besides other statutory conditions) to obtain a consent of the person concerned. If a special law provides otherwise, also a natural person,	The law does not mention any specific procedures on how to deal with the obtained information after the completion of the security vetting. NSA is obliged to stop collecting and	The law does not encompass any time limits, geographical scope and other limits of mass surveillance.	Act provides no information about mass monitoring in another country.

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)?
		a PZ pri vykonávaní bezpečnostných previerok špecifických osôb NSA provides the basis for the decision making process of the Judicial Council of the Slovak Republic on the presumption of judicial competence - in relation to the judges as well as to the candidates for judicial positions (§ 69a, § 69b).	security, the encryption protection of information, physical security, building security, security of technical devices and industrial security (§ 6). NSA provides a basis for verification of the facts which should be met in order to prove the judicial competence. Collected information include: - A completed questionnaire - Information about a person from the	commission or other authority may request performing the safety check of a nominee, if stipulated by a special law (§ 10, § 16). At the written request of the Head of the Judicial Court NSA provides basis for the verification of the facts to meet the preconditions of the judicial competence.	evaluating data for verification of the judicial competence eligibility on the basis of judicial notice of the President of the Judicial Council (§ 69a subsection 1) NSA keeps a file regarding a natural person which is based on all the relevant information obtained to determine person's judicial competence as a judge. Data from this file can only be used to decide on the fulfilment judicial competence criteria (§ 69a subsection 6). NSA is required to evaluate the collected data and send the evaluation to the		

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)?
			records of the Police Force, Slovak Intelligence Service and Military Intelligence, - Information about the person from the checks carried out at the place of his/her permanent residence by the Police Force, Slovak Intelligence Service, Military Intelligence - Information requested from the municipality in which the individual has his/her permanent		Judicial Council within five months after receiving the request (§ 69 subsection 1)		

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)?
			or temporary residence, - Details of the checks carried out by the Police Force, Slovak Intelligence Service or Military Intelligence about the security of the environment and the possibility of potential security risks, - Information about the individuals requested from the other state bodies, other legal entities and individuals (§ 69a, subsection 2).				

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)?
Act of the National Council of the Slovak Republic No. 198/1994 Coll. on Military Intelligence	The law does not specify anything in this regard besides the condition that the data on minors younger than 15 years should not be kept in the files of the Military Intelligence (§ 17 subsection 2).	To decide about the surveillance of persons by the Military Intelligence within the scope of its functions is in the competence of the Minister of Defence or other authorized person (§ 11 subsection 2).	The procedure of exaction, use and evidence of informational and operational resources is determined by the Minister of Defence (§ 11 subsection 7). Military Intelligence performs the role of ensuring intelligence security of the Slovak Republic (§ 1 subsection 1). The use of information-technical means is regulated by the Act. 166/2003 Coll. and they could be used only if it is	To decide about the surveillance of persons and things by the Military Intelligence within the scope of its functions is in the competence of the Minister of Defence or other person authorized by the Minister of Defence (§ 11 subsection 2). The procedure of exaction, use and evidence of informational and operational resources is determined by the Minister of Defence (§ 11 subsection 7). The information-technical means may be used only under prior written consent	Military Intelligence: - collects data, - stores data, - uses data on persons who have a direct link to the fulfilment of the Military Intelligence´s task and duties. - ensures the protection of the stored data against disclosure, unauthorized destruction or damage - data are destroyed when they are no longer needed to fulfil the tasks, or if there are other legal reasons.	The law does not contain specific provisions.	The law does not specify.

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)?
			inevitable in a democratic society - to safeguard the security and defence of the country, - to prevent and reveal criminal activities, or - to protect the rights and freedoms of other persons (§ 3).	of a judge and only during necessary time period, which may not exceed 6 months. This time period may be prolonged for necessary time. If there are more types of information-technical means to be used, there must be specific written consent of a judge for each of them. The application for consent to use information-technical means must be written and it must in particular encompass specific type of information-technical means, locality, time period, identification of a person against			

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)?
				whom the information-technical means are to be used, justification of using information-technical means. There is no remedy against court decision. (The Act No. 166/2003 Coll. On Protection against Interception, Section 4)			
Act of the National Council of the Slovak Republic No. 46/1993 Coll. on the Slovak Information Service	The law does not specify anything in this regard besides the condition that the information on the conduct of adolescents less than 14 years of age cannot be	The Director, or – in his absence - a deputy delegated by him , shall decide on the use of surveillance of persons or matters in the fulfilment of	The Slovak Information Service is a state body of the Slovak Republic which shall fulfil tasks in the protection of the constitutional establishment,	The Director, or – in his absence - a deputy delegated by him, shall decide on the use of surveillance of persons or matters (§ 11 subsection 2).	Slovak Information Service: - collects data and create data files (§ 11, § 17),	The law does not contain specific provisions.	The law does not specify.

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)?
	entered into files of the Slovak Information Service (§ 17 subsection 2).	the duties of the Slovak Information Service within the scope of its activities (§ 11 subsection 2).	public order, security of the State and interests of the State concerning the foreign policy and economy (§ 1 subsection 2). Within the scope of its functions the Information Service shall be authorized to create and maintain files in which information on subject matter and persons having a direct connection to the fulfilment of the duties of the Slovak Information Service decreed by the Act is accumulated, kept and used (§ 17 subsection 1). The use of information-	Details on the use and record keeping of informational-operational means including the surveillance of persons and thing shall be regulated by the Director (§ 11 subsection 7). The information-technical means may be used only under prior written consent of a judge and only during necessary time period, which may not exceed 6 months. This time period may be prolonged for necessary time. If there are more types of information-technical means to be used, there must be	- maintain data files (§ 11) - use data (§ 17) - ensure protection of personal data processed in its information systems and information kept in file from disclosure, abuse, damage or unauthorised destruction and loss. (§ 17 ods. 3) - In cases where information kept in files of the Slovak Information Service is no longer required for the fulfilment of established duties, or be it for any legal reason, the Information Service shall be required to store the		

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)?
			technical means is regulated by the Act. 166/2003 Coll. and they could be used only if it is inevitable in a democratic society - to safeguard the security and defence of the country, - to prevent and reveal criminal activities, or - to protect the rights and freedoms of other persons (§ 3 By using information-technical means, the essential right or freedom can be infringed upon only to the inevitable extent and for a period of time not	specific written consent of a judge for each of them. The application for consent to use information-technical means must be written and it must in particular encompass specific type of information-technical means, locality, time period, identification of a person against whom the information-technical means are to be used, justification of using information-technical means. There is no remedy against court decision.	data in a way which would prevent anyone (with the exception of a court) from obtaining access to it (§ 17 subsection 6). - destruction of the data is regulated by the internal regulation (§ 17 subsection 8).		

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)?
			longer than inevitable to attain the legal goal, to which it serves (§ 3).	(The Act No. 166/2003 Coll. On Protection against Interception, Section 4)			
Act of the National Council the Slovak Republic No. 171/1993 Coll. on the Police Force	The Act does not further specify.	Police force is an armed security force which performs the tasks in matters of internal order, security, combating crime and with regards to these tasks it also uses surveillance and monitoring of persons and subject matters (§ 1 subsection 1)	The Police Force is authorised to use information-technical means while performing tasks connected to: -combat of terrorism and legalisation of incomes from criminal activities, - disclosure of international organised crimes and organised criminal activities related to illicit manufacturing,	The order to intercept and record telecommunications shall be issued by the presiding judge of a panel prior to the commencement of criminal prosecution, or by a judge for pre-trial proceedings on a motion from a prosecutor. If the matter bears no delay and a prior order from a judge for pre-trial proceedings cannot be obtained, the order may be issued by a	The Police Force shall: - Process personal data, - Exchange information and personal data with other bodies of EU Member States in order to fulfil the tasks of the Police Force for the purposes of criminal proceedings - Establish information systems for the processing of personal data	The Act does not further specify besides the fact that the Police Force shall examine regularly, at least once in every three year, if the processed personal data remains necessary for the tasks performed by the Police Force (§ 69 subsection 8).	Police force has no competence outside the Slovak Republic.

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)?
			possession and spread of narcotic and psychotropic substances and poisons, precursors and nuclear materials, - smuggling, fraud and counterfeiting of money, stamps or bonds, - the disclosure of other extremely serious criminal acts, - providing protection and help to the threaten witness and protected witness or of legalised person and agent,	prosecutor before the commencement of criminal prosecution or in pre-trial proceedings, unless the interception and recording of telecommunications involves the entry into the dwelling of a person; such order shall have to be confirmed by a judge for pre-trial proceedings within 24 hours of its issuance; failing that, the order shall become null and void and the information obtained on its basis may not be used for the purposes of criminal proceedings and shall have to be immediately destroyed in a	- if the information and personal data are no more necessary for the tasks the Police Force shall immediately liquidate them, block them anonymize them - examine regularly, at least once in every three years, whether the processed personal data remain necessary for the fulfilment of the tasks performed by the Police Force (§ 69 - § 69g).		

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)?
			- disclosure of tax evasions and illicit financial transactions, - disclosure of deliberate criminal offences which are liable to imprisonment for at least 2 years, or other deliberate criminal offences which are prosecuted pursuant to the international agreement binding for the Slovak Republic (§ 36).	prescribed manner (§ 115 of the Criminal Procedure Code No. 301/2005 Coll.).			
Act No. 166/2003 Coll. on the Protection of Privacy against the Unauthorised Use	Anyone - Act does not specify the range of persons.	This Law stipulates the conditions required for the use of information - technical means	Information-technical means (ITM) shall be used only if it is inevitable in a	The statutory judge who has granted the approval to use the information-technical means (ITM) can, on	- Obtaining information - Making a copy of audio, visual, audio visual recording	Using ITM for the necessary period at maximum of six months. Always could be repeatedly	The act does not further specify.

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)?
of Information-technical means and on Amendment and Supplementation of Certain Laws (Act on the Protection against Interception), from April 24, 2003.		without the prior consent of the person whose privacy is infringed upon by the state body, which uses the information-technical means. Information-technical means are in particular electro-technical, radio-technical, photo-technical, optic, mechanic, chemical and other technical means and facilities that are used in a covert manner - to trace, open, examine and evaluate mail and other deliveries, - to intercept and record	democratic society to safeguard the security and defence of the state, to prevent and reveal criminal activities, or to protect the rights and freedoms of other persons. By using information-technical means, the essential right or freedom can be infringed upon only to the inevitable extent and for a period of time not longer than inevitable to attain the legal goal, to which it serves (§ 3).	the basis of a new request, extend the duration of the time period, but in each case for no longer than other six months. Statutory judge who gave permission to use the ITM has to systematically monitor the duration of the reasons for their use (§ 4). In an exceptional case, if there is a reasonable suspicion of a crime being committed and information-technical means might be used by the Police Force to fulfil its tasks, if the case is to be dealt with immediately and the approval of the statutory judge	- Destruction of records (§ 7).	extended for a maximum of six months (§ 5). The law sets no geographical limits of use.	

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)?
		telecommunication activities, - to make and use video, audio and other recordings. (§ 2) This Law does not apply to the use of information-technical means in the criminal proceeding (§ 1). I.e. The Act on Protection against Interception applies only on activities of civil or military intelligence services in their activities, outside the criminal investigation and prosecution procedures.		cannot be obtained in advance, the Police Force may use information-technical means without a prior approval. The Police Force shall be required to notify the statutory judge of the use of the information-technical means subsequently within one hour from the beginning of their use. If the Police Force does not obtain a subsequent written approval of the statutory judge within 12 hours from the beginning of the use of ITM, the use of these means shall be immediately ceased (§ 5).			

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)?
		Information-technical means can be used by the Police Force, Slovak Information Service, Military Intelligence, Corps of Prison and Judiciary Guards, and Customs Board (§ 2).					

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)**
Constitution of the Slovak Republic no. 460/1992 Coll., Section 19, subsections 2 and 3 - the right to privacy: - The right to protection from unauthorized interference in private and family life. - The right to protection against unauthorized collection, disclosure or other misuse of his person. Section 22: privacy of correspondence, delivered messages and other documents, personal data protection	- The right to protection from unauthorized interference in private and family life - The right to protection against unauthorized collection of personal data on one's person - The right to protection against unauthorized disclosure of data on one's person - The right to protection against unauthorized misuse of data on one´s person - The right to personal data protection	This right applies to "everyone", that is for each person in the jurisdiction of the Slovak authorities, i.e. not only the citizens of the Slovak Republic, but also for EU citizens and / or third country nationals, while in the territory of the Slovak Republic.	The legislation of the Slovak Republic adopted by the legislature (or constitutional) authority shall be valid throughout the territory of the Slovak Republic and in all places, where the Slovak Republic assumes jurisdiction.

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)
Act No. 351/2011 Coll. on Electronic Communications Any enterprise providing a public network or service shall be obliged to ensure technically and organisationally confidentiality of communications and the related traffic data which are conveyed by means of its public network and public services. Tapping, listening, storage or other kinds of interception or surveillance of communications and the related data by persons others than users or without the consent of the users concerned, shall be prohibited in particular unless stipulated otherwise	- the right to the confidentiality of information Any enterprise providing a public network or service shall be obliged to ensure technically and organisationally confidentiality of communications and the related traffic data which are conveyed by means of its public network and public services. Recording, listening, storage or other kinds of interception or surveillance of communications and the related data by persons others than users or without the consent of the users concerned, shall be prohibited in particular unless stipulated otherwise by this Act (§ 55 subsection 3). - the right to the protection of personal data Protection of personal data shall apply to the subscribers and users who are a natural	Those rules apply not only to the citizens of the Slovak Republic, but for every person who is a party to and a user of electronic services to businesses. Privacy applies to users and subscribers who are natural persons. (§ 56 subsection 1)	The legislation of the Slovak Republic adopted by the legislative body shall be valid throughout the territory of the Slovak Republic and in all places, where the Slovak Republic is to assume jurisdiction.

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)
by this Act (§ 55 subsection 3). Any person who stores or obtains access to the information stored on the device of the end user is eligible to do that only if the user granted a permission based on the concise and clear information about the purpose of the information use. The obligation to obtain a consent does not apply to the law enforcement bodies and other state bodies (§ 55 subsection 5).	Person (§ 56 subsection 1) - right to be informed on the collection and processing of personal data: The enterprise shall be obliged to inform the subscribers of the types of personal data which are gathered and processed, on the legal reason, purpose and duration of processing them. Such information shall be provided at the latest at the conclusion of a contract of the provision of public services (§ 56 subsection 4). - right to be informed when of personal data breaches: In case of a personal data breach, the enterprise that provides public services shall be obliged: a) immediately notify the Regulatory Authority for Electronic		

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)
	Communications and Postal Services on a personal data breach, b) immediately inform the subscribers and users of the of personal data breaches, which may adversely affect the personal data or privacy (unless the enterprise provides evidence of appropriate technological protection measures) c) at the request of the Regulatory Authority for Electronic Communications and Postal Services inform the subscribers and users of a breach of privacy if the personal data breach may have a negative impact on the subscribers and users, d) maintain an inventory of personal data breaches. (§ 56 subsection 5)		

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)
	- right to anonymization of personal data: The enterprise may process location data other than traffic data, relating to the subscriber or user public network or public service only if they are made anonymous, or with their consent, to the extent and for the time necessary to provide value-added services. (§ 57 subsection 2) - The right to liquidation or data anonymization: Traffic data relating to subscribers and users shall not, without the consent of the person concerned, be kept. The enterprise is required upon termination of the transmission of the message to immediately discard or anonymize it, except exceptions regulates by the law.		

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)
	(§ 57 subsection 4) - The right of subscriber / user to temporarily refuse the data processing: If the subscriber or user has consented to the processing of location data other than traffic, the enterprise is obliged to allow him to decide every time he/she connects to the network or for each transmission of a message to temporarily refuse the processing of location data in a simple and free way. (§ 57 subsection 8) - Right to the disposal of the mandatory retained data: The enterprise ensures that the data are at the end of the period of retention are destroyed, besides the data secured and data provided to national authorities.		

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)
	(§ 58 subsection 10, letter d) - The right to protection of telecommunications privacy: Anyone who comes to his subject into contact with the provision of networks and services, the use of services, accidentally or otherwise, is obliged to keep telecommunication privacy. The telecommunications privacy may be disclosed to the Regulatory Authority for Electronic Communications and Postal Services of electronic communications and postal services, subscribers and users concerned, its authorized agent or legal successors, unless the law provides otherwise. Telecommunications privacy means: - The content of messages transmitted, - Related data communicating parties,		

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)
	- Operational data, - Location data (§ 63 subsection 2 and 3)		
Act No. 122/2013 Coll. on Protection of Personal Data § 28: Rights of the person concerned in relation to an operator which processes personal data.	The data subject shall be entitled to request upon a written application from the controller a) confirmation whether his personal data are or are not being processed, b) information about the state of processing of his personal data in the filing system in a generally intelligible form and in the extent under Section 15 subsection 1 letters a) to e) Numbers 1 to 6; if a decision under Paragraph 5 is issued, the data subject shall be entitled to familiarize himself with the procedure of the processing and evaluating of operations, c) exact information, in a generally intelligible form, about the source	This Act applies to everyone who processes personal data, determines the purpose and means of processing or provides personal data for processing. (§ 2 subsection 1) The Act on Protection of Personal Data applies to SIS and MI surveillance activities only partly – the law stipulates that its certain provisions does not apply to processing personal data which are inevitable to secure public interest, if operator (processing entity) fulfils its legal duties to ensure: - security of Slovak Republic, - defence of Slovak Republic,	This Act also applies to the controllers, which do not have a registered office, organizational unit, business premises or permanent residence on the territory of a) the Slovak Republic but they are located abroad at a place, where the law of the Slovak Republic takes precedence based on an international public law, b) a Member State, provided that for the purposes of personal data processing they use fully or partially automated means or other than automated means of processing located on the territory of the Slovak Republic, while such means of processing are not used solely for the transfer of personal data through the territory of the Member States. (§ 2 subsection. 2)

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)
	from which the controller obtained his personal data for their processing, d) list of his personal data, in a generally intelligible form, which constitute the subject of the processing, e) rectification or erasure of his inaccurate, incomplete or not updated personal data, which constitute the subject of the processing, f) erasure of his personal data, if the purpose of their processing was fulfilled; if any official documents containing personal data constitute the subject of the processing, he may request their returning, g) erasure of his personal data which constitute the subject of processing if there was a violation of the Law,	- public order and security, etc. (§ 3) These are the provisions which does not apply to SIS and MI: - obligations of operator processing personal data, (§ 6 / 2 – 5) - processing or personal data via subcontractor (§ 8 / 5), - obligation of operator to inform the person of whom he/she stores the personal data (§ 15 / 1,2,8), - rights of an affected person to seek certain information from an operator processing data of such person (§ 28 / 1) - the obligation of an operator to provide data from his/her records (§	

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)
	h) blocking of his personal data due to the cancelation of the consent for personal data processing before its expiration if controller processes personal data based on the consent of the data subject. (§ 28)	44).	
Act No. 300/2005 Coll. Criminal Code § 196 - § 198: Breach of Privacy of Correspondence Crime is committed by anyone who intentionally breaches: a) the privacy of letter correspondence through spying or opening a sealed letter or other written communication delivered	- The right to protect the privacy of communications - The right to protection against unauthorized handling of personal data - The right to protection against unauthorized disclosure or access the privacy of documents, audio, video or other recording, computer data or other private document - The right to protect the confidentiality of oral expression, or other personal characteristics.	Those rules apply not only to the citizens of the Slovak Republic, but for every person who is in the territory of the Slovak Republic. Criminally responsible for the commission of an offense is a Slovak citizen or an alien who is in the territory of the Slovak Republic residence. (§ 4)	Violation of rules under the Criminal Code (i.e. assessment punishable offense under the Penal Code) refers to the act that was committed on the territory of the Slovak Republic. Offense shall be deemed committed on the territory of the Slovak Republic even if: - the Act was committed at least partly in the territory of the Slovak Republic, - the act was committed outside the Slovak Republic, but the actual breach or threat to an interest protected by the Penal Code was in the territory of the Slovak Republic, - The offense was committed on board of a vessel flying the flag of the Slovak Republic or on board of an aircraft

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)
by postal service or in other habitual manner, b) the privacy of information transferred via electronic communication service, or c) the privacy of private transfer of computerized data to the computer system, out of it or within it, including electromagnetic radiation from computer system transferring such computerized data, d) divulges a private information which he got knowledge of from a closed letter or other written communication delivered by postal			registered in the register of the Slovak Republic (§ 3).

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)
service or in other habitual manner that were not addressed to him, or from the information transferred via electronic communication service, or e) makes use of such information, f) in breach of a generally binding legal regulation, manufactures, procures for him self or another, or possesses the equipment capable of intercepting the information transferred via electronic communication service, shall be liable to a term of imprisonment of up to three years.			

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)
§ 377: Breach of Confidentiality of Spoken Utterance and Other Expression of Personal Nature: Crime is committed by any person who breaches the confidentiality of private spoken utterance or other expression of personal nature by its unlawful recording, and makes such recording accessible to a third person or uses it otherwise, and thus causes serious prejudice to the rights of another, shall be liable to a term of imprisonment of up to two years.			

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)
§ 376: Crime is committed by any person who unlawfully breaches the secrecy of an instrument or other written document, audio recording, video recording or other recording, computer data or other document kept private by another through disclosing them or making them accessible to a third person, or using them otherwise, and thus causes serious prejudice to the rights of another. § 377: Breach of Confidentiality of Spoken			

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)
Utterance and Other Personal Expression: Crime is committed by any person who breaches the confidentiality of private spoken utterance or other personal expression by its unlawful recording, and makes such recording accessible to a third person or uses it otherwise.			

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 ongoing/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.*
Vláda Slovenskej republiky (The Government of the Slovak Republic)	government	Act of the National Council of the Slovak Republic No 46/1993 Coll. on the Slovak Information Service	The Government provides on-going oversight: -The Government shall determine the manning levels of the SIS and on the recommendation of the Director shall approve the Statute of the SIS, which will modify the objectives, organization and administration of the SIS (§ 3 para 4) Depending on the nature of the case the Government of the Slovak Republic shall be informed about	The Government is consisting of the Prime Minister, Deputies and other ministers. The prime Minister is appointed by the President of the Slovak Republic. Other ministers are appointed by the President of the Slovak Republic upon proposal of the Prime minister. (Constitution of the Slovak Republic, Art. 109, 110, 111)	The Government decides through its resolutions (uznesenie) and regulations (nariadenie). (Constitution of the Slovak republic, Article 118 and 120)

			violation of the Act on SIS. (§ 5 para 4)		
Úrad na ochranu osobných údajov Slovenskej republiky (The Office for personal data protection)	public administrative authority (executive)	Act on the Protection of Personal Data No. 122/2013 Coll. The Office for Personal Data Protection is an administrative authority with nationwide activities, which performs the supervision personal data protection and contributes to the protection of fundamental rights and freedoms of natural persons with regard to the processing of their personal data. (§ 45 subsection 1)	The Office for Personal Data Protection of the Slovak Republic is an independent state authority which performs the supervision of data protection and contributes to the protection of fundamental rights and freedoms with regard to the processing of personal data. Activities of the Office shall not apply to cases where personal data are processed by intelligence and the National Security Authority. If personal data is processed by intelligence services or National Security Authority, the supervision over the personal data protection is performed by the National Council of the	At the head of the office is Chairman, who shall be elected and recalled by the National Council of the Slovak Republic on the proposal of the Government. The term of office is five years and may be appointed for no more than two consecutive terms. The Chairman is deputised by the Deputy Chairperson, who is appointed and dismissed by the Government on the proposal of the Chairman of the Office. The term of office is five years and may be appointed for no more than two consecutive terms. Number of employees: 38	The Office shall issue generally binding legal regulations to implement the Act (ie. by laws), participating in the preparation and comments on draft laws and other generally binding legal regulations on the protection of personal data, make recommendations binding opinions, methodological guidelines, agreed. The Office issues decisions, carries special registration, imposes sanctions.

			Slovak Republic (i.e. Parliament). (§ 46 subsection 5)		
Výbor NR SR na preskúmavanie rozhodnutí Národného bezpečnostného úradu (Committee of the National Council of Slovak Republic to review decisions of the National Security Authority)	parliamentary body	Constitutional Act No. 254/2006 Coll. on the establishment and operation of the Committee of the National Council to review decisions of the National Security Authority The Committee shall review the decisions of the National Security Authority, if stipulated by law. (Article 3)	The Committee shall review the decision of the National Security Authority - it operates ex post in certain cases, stipulated by law. (§ 30 of the Act No 215/2004 Coll. On Protection of classified information) The Committee decides upon appeal filed against the decision of NSA: - on findings that a person does not fulfil the precondition to have access to classified information (§ 26 para. 2), - on dismissing the authorisation to acquaintance with classified information (§ 29), - on findings that entrepreneur does not	At the head of of the Committee is a Chairman, deputised the Deputy Chairman. 11 Members - Members of the National Council, elected by the National Council of the Slovak Republic on the basis of proportional representation according to the number of members of political parties or movements	Committee makes decisions by a simple majority of members present. The Committee starts it procedure upon receiving the appeal, statement to the appeal and the relevant documents concerning the appealed decision of the NSA. The Committee shall: - dismiss the appealed decision and return the case back to NSA to issue a new decision, or - dismiss the appeal. The decision of the Committee must be justified. The decision is binding and is subject to the court review – by the Supreme Court. (Art. 4 of the Constitutional Act No 254/2006 coll.))

			fulfil the conditions for issuing an industrial security certificate (§ 50 para 2), - on findings that entrepreneur stopped fulfilling the conditions for issuing an industrial security certificate (§ 50 para 5), - on issuing the authorisation to get acquainted with classified information in connection with duties under international agreement (§ 60 para 7).		
Osobitný kontrolný výbor NR SR na kontrolu činnosti Národného bezpečnostného úradu (Special Body of the National Council of the Slovak Republic for the oversight over the activities of the National Security Authority)	parliamentary body	Act No. 350/1996 Coll. on the Rules of Negotiation Procedure of the National Council of the Slovak Republic Act No. 215/2004 Coll. on the protection of classified information	The Body exercises control activities of the Authority continuously. While the Committee of the National Council of Slovak Republic to review decisions of NSA is authorised to review certain specified decisions of NSA (listed above), the Special body of the National Council of the Slovak Republic for the	According to the Act No. 215/2004 Coll. National Council elects at the beginning of each term committee members, determines their number, composition and method of work of this body (§ 72 of Act No. 215/2004 Coll.) The Body members are elected by the National Council on the basis of proportional representation of parliamentary club(s) members and given a specified number of members	The Body announces the violation of the Act No. 215/2004 Coll. to the National Council of the Slovak Republic, Prosecutor General and depending from the nature of matter also informs the Government. (§ 72 of Act No. 215/2004 Coll.) Hearings of all special supervising parliamentary bodies are not public. The outcomes of the discussion by the Body may be discussed by the plenum of the Parliament.

		The National Council of the Slovak Republic executes supervision over activities of the National Security Authority, through special supervision body consisting of Members of Parliament. (§72 subsection 1 Act No. 215/2004 Coll.)	oversight over the activities of the NSA has power to provide overall supervision over NSA.	of the Committee (§ 60 of Act no. Coll. 350/1996) The Body currently has 14 members - Members of the National Council.	Legislation does not stipulate any further details.
Osobitný kontrolný výbor NR SR na kontrolu činnosti Slovenskej informačnej služby (Special Body of the National Council of the Slovak Republic on the oversight of the activities of Slovak Information Service)	parliamentary body	Act No. 350/1996 Coll. on the Rules of Negotiation Procedure of the National Council of the Slovak Republic Act of the National Council of the Slovak Republic No. 46/1993 Coll. on the Slovak Information Service	The Body exercises oversight over SIS activities continuously. There are no conclusions publicly available. The website of the Special Body contains only invitations to the hearings of the Body.	At the beginning of each term in office, the National Council of the Slovak Republic shall elect members to the Oversight Body, and determine the number of members, the organization and method of work of this body. (§ 6 of the Act No. 46/1993 Coll.) The Oversight Body members are elected by the National Council on the basis of proportional representation of parliamentary club(s) members	The Body announces the violation of the Act No. 46/1993 Coll. to the National Council of the Slovak Republic, Prosecutor General and depending from the nature of matter also informs the Government. (§ 5 of Act No. 46/1993 Coll.). Hearings of all special supervising parliamentary bodies are not public. The outcomes of the discussion by the Body may be discussed by the plenum of the Parliament.

		Supervision of the activities of the Slovak Information Service is executed by the special supervising body of the National Council of the Slovak Republic composed out of Members of Parliament. (§ 5 of the Act No. 46/1993 Coll.)		and given a specified number of members of the Oversight Body (§ 60 of Act no. Coll. 350/1996) The Body currently has 15 members - members of the National Council of the Slovak Republic.	Legislation does not stipulate any further details.
Osobitný kontrolný výbor Národnej rady Slovenskej republiky na kontrolu činnosti Vojenského spravodajstva (Special Body of the National Council of the Slovak Republic on the oversight over Military Intelligence)	parliamentary body	Act No. 350/1996 Coll. on the Rules of Negotiation Procedure of the National Council of the Slovak Republic Act No. 198/1994 Coll. on Military Intelligence Supervision of the activities of the Military Intelligence is executed by the special supervising body	The Body exercises oversight over Military Intelligence activities continuously. The conclusions from the Special Body are not publicly accessible.	At the beginning of each term in office, the National Council of the Slovak Republic shall elect members to the Oversight Body, and determine the number of members, the organization and method of work of this body. (§ 6 of the Act No. 198/1994 Coll.) The Oversight Body members are elected by the National Council on the basis of proportional representation of parliamentary club(s) members and given a specified number of members of the Oversight Body (§ 60 of Act no. Coll. 350/1996)	The Body announces the violation of the Act No. 198/1994 Coll. to the National Council of the Slovak Republic (§ 6 subsection 4 of the Act No. 198/1994 Coll.) Hearings of all special supervising parliamentary bodies are not public. The outcomes of the discussion by the Body may be discussed by the plenum of the Parliament. Legislation does not stipulate any further details.

		of the National Council of the Slovak Republic composed out of Members of Parliament.		The body currently has 15 members - members of the National Council of the Slovak Republic.	

Annex 3 – Remedies[34]

[Act No. 351/2011 Coll. on Electronic Communications]				
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*	Yes – the user gives an explicit consent, or, in case the collection of data directly follows the law, the user's consent is not required	yes (§ 56 ods. 4)	Extrajudicial dispute resolution pursuant to Act no 351/2011 (§ 75 et seq) is performed by the Regulatory Authority for Electronic Communications and Postal Services (administrative authority) The action on the protection of personality under the Civil Code No. 40/1964 Coll (§ 11 et seq) is	Breach of the obligations arising from the Act No. 351/2011 Coll.on Electronic Communications

[34] 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

	user consent is not required also if the information is obtained by the law enforcement body or other state body (§ 55 subsection 5) Other state body shall include armed security body, armed body and state body that fulfils task with regard to protection of constitutional regime, state defence, inner order and state security. (§ 55 subsection 6)		performed by the district court, the regional court decides on the appeal.	

Analysis*	Yes - only with the explicit consent of the user, except for the situations in which the information is obtained by the law enforcement bodies or other state bodies (§ 55 paragraph 5).	yes (§ 56 ods. 4)	Extrajudicial dispute resolution pursuant to Act no 351/2011 (§ 75 et seq) is performed by the Regulatory Authority for Electronic Communications and Postal Services (administrative authority) The action on the protection of personality under the Civil Code No. 40/1964 Coll (§ 11 et seq) is performed by the district court, the regional court decides on the appeal.	Breach of the obligations arising from the Act No. 351/2011 Coll.on Electronic Communications
Storing*	Yes – the user gives an explicit consent, or, in case the collection of data directly follows the law, the user's consent is not required user consent is not required also if the information is obtained by the law enforcement body or other	yes (§ 56 ods. 4)	Extrajudicial dispute resolution pursuant to Act no 351/2011 (§ 75 et seq) is performed by the Regulatory Authority for Electronic Communications and Postal Services (administrative authority) The action on the protection of personality under the Civil Code No. 40/1964 Coll (§ 11 et seq) is performed by the district court, the regional court decides on the appeal.	Breach of the obligations arising from the Act No. 351/2011 Coll.on Electronic Communications

	state body (§ 55 subsection 5)			
Destruction *	the user is not specifically informed on the liquidation of data	yes (§ 56 ods. 4)	Extrajudicial dispute resolution pursuant to Act no 351/2011 (§ 75 et seq) is performed by the Regulatory Authority for Electronic Communications and Postal Services (administrative authority) The action on the protection of personality under the Civil Code No. 40/1964 Coll (§ 11 et seq) is performed by the district court, the regional court decides on the appeal.	Breach of the obligations arising from the Act No. 351/2011 Coll.on Electronic Communications
After the whole surveillance process has ended				

[Act No. 122/2013 Coll. on Protection of Personal Data]				
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*	Yes, besides the exceptions provided by the law	yes	Legal proceedings on personal data protection (§ 62 and following) are performed by the Office for personal data protection (administrative authority), the Chairmen of the Office decides on appeals. The action on the protection of personality under the Civil Code No. 40/1964 Coll (§ 11 et seq) is performed by the district court, the regional court decides on the appeal.	violation of data protection

* 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

Analysis*	Yes, besides the exceptions provided by the law	yes	Legal proceedings on personal data protection (§ 62 and following) are performed by the Office for personal data protection (administrative authority), the Chairmen of the Office decides on appeals. The action on the protection of personality under the Civil Code No. 40/1964 Coll (§ 11 et seq) is performed by the district court, the regional court decides on the appeal.	violation of data protection
Storing*	Yes, besides the exceptions provided by the law	yes	Legal proceedings on personal data protection (§ 62 and following) are performed by the Office for personal data protection (administrative authority), the Chairmen of the Office decides on appeals. The action on the protection of personality under the Civil Code No. 40/1964 Coll (§ 11 et seq) is performed by the district court, the regional court decides on the appeal.	violation of data protection
Destruction*	The obligation of data disposal is regulated by the law, therefore explicit consent is not required.	yes	Legal proceedings on personal data protection (§ 62 and following) are performed by the Office for personal data protection (administrative authority), the Chairmen of the Office decides on appeals. The action on the protection of personality under the Civil Code No. 40/1964 Coll (§ 11 et seq) is performed by the district court, the regional court decides on the appeal.	violation of data protection

After the whole surveillance process has ended			Legal proceedings on personal data protection (§ 62 and following) are performed by the Office for personal data protection (administrative authority), the Chairmen of the Office decides on appeals. The action on the protection of personality under the Civil Code No. 40/1964 Coll (§ 11 et seq) is performed by the district court, the regional court decides on the appeal.	violation of data protection

[Act No. 215/2004 Coll. on the Protection of Classified Information]				
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[*]	yes	yes	Committee of the National Council of Slovak Republic to review decisions of	While objecting to the decision on the inability to fulfil the criteria

[*] 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

			the National Security Authority (Constitutional Act No. 254/2006 Coll on the establishment and operation of the Committee of the National Council to review decisions of the National Security Office) - in the review of the decision on nominee´s incapability to meet the conditions for acquaintance with classified information. Committee's decision is reviewable by the Supreme Court of the Slovak Republic (According to Section 5 of the Act no. 254/2006 Coll) In the case of judges: Based on the evaluation of the information provided by the NSA Judicial Council of the Slovak Republic decides on the presumption of judicial competence (Act no. 185/2002 Coll on the Judicial Council of the Slovak Republic), the decision of the Judicial Council is to reviewable by the Constitutional Court of the Slovak Republic.	necessary to become eligible for acquitance with the classified information (or eventually on the inability to meet the judicial competence criteria) it is possible to object also to the activities of NSA performed when collecting the information on the person concerned.
Analysis*	yes	yes	Committee of the National Council of Slovak Republic to review decisions of the National Security Authority (Constitutional Act No. 254/2006 Coll on the establishment and operation of the Committee of the National Council to review decisions of the National Security Office) - in the review of the decision on nominee´s incapability to	While objecting to the decision on the inability to fulfil the criteria necessary to become eligible for acquitance with the classified information (or eventually on the inability to meet the judicial competence criteria) it is possible to object also to the activities of NSA performed when collecting the

			meet the conditions for acquaintance with classified information. Committee's decision is reviewable by the Supreme Court of the Slovak Republic (According to Section 5 of the Act no. 254/2006 Coll) In the case of judges: Based on the evaluation of the information provided by the NSA Judicial Council of the Slovak Republic decides on the presumption of judicial competence (Act no. 185/2002 Coll on the Judicial Council of the Slovak Republic), the decision of the Judicial Council is to reviewable by the Constitutional Court of the Slovak Republic.	information on the person concerned.
Storing*	yes	yes	Committee of the National Council of Slovak Republic to review decisions of the National Security Authority (Constitutional Act No. 254/2006 Coll on the establishment and operation of the Committee of the National Council to review decisions of the National Security Office) - in the review of the decision on nominee´s incapability to meet the conditions for acquaintance with classified information. Committee's decision is reviewable by the Supreme Court of the Slovak Republic (According to Section 5 of the Act no. 254/2006 Coll)	While objecting to the decision on the inability to fulfil the criteria necessary to become eligible for acquitance with the classified information (or eventually on the inability to meet the judicial competence criteria) it is possible to object also to the activities of NSA performed when collecting the information on the person concerned.

			In the case of judges: Based on the evaluation of the information provided by the NSA Judicial Council of the Slovak Republic decides on the presumption of judicial competence (Act no. 185/2002 Coll on the Judicial Council of the Slovak Republic), the decision of the Judicial Council is to reviewable by the Constitutional Court of the Slovak Republic.	
Destruction *				While objecting to the decision on the inability to fulfil the criteria necessary to become eligible for acquitance with the classified information (or eventually on the inability to meet the judicial competence criteria) it is possible to object also to the activities of NSA performed when collecting the information on the person concerned.
After the whole surveillance process has ended				

[Act of the National Council of the Slovak Republic No. 198/1994 Coll. on Military Intelligence]				
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	no	The affected person may object to the procedure conducted by the Military Intelligence in potential criminal proceedings against him/her. Otherwise they would never learn that MI collects, stores and processes information their person. Another option is to pursue complaint on the protection of the personality under the Civil Code No. 40/1964 Coll (§ 11 et seq), processed by the district court, the regional court decides on appeals. If Military Intelligence performs security checks on its employees, the decision on compliance is reviewable	Violation of data protection, private life.

* 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

			by the Supreme Court of the Slovak Republic (Act no. 215/2004 Coll, § 30)	
Analysis*	no			
Storing*	no			
Destruction *	no			
After the whole surveillance process has ended	no			

[Act of the National Council of the Slovak Republic No. 46/1993 Coll. on the Slovak Information Service]				
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	no	The affected person may object to the procedure conducted by the Slovak	Violation of data protection, private life.

* 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

			Information Service in potential criminal proceedings against him/her. Otherwise they would never learn that SIS collects, stores and processes information their person. Another option is to pursue complaint on the protection of the personality under the Civil Code No. 40/1964 Coll (§ 11 et seq), processed by the district court, the regional court decides on appeals. If Slovak Information Service performs security vettings on its employees, the decision on compliance is reviewable by the Supreme Court of the Slovak Republic (Act No. 215/2004 Coll, § 30)	
Analysis*	no	no	The affected person may object to the procedure conducted by the Slovak Information Service in potential criminal proceedings against him/her. Otherwise they would never learn that SIS collects, stores and processes information their person. Another option is to pursue complaint on the protection of the personality under the Civil Code No. 40/1964 Coll (§ 11 et seq), processed by the district	Violation of data protection, private life.

			court, the regional court decides on appeals. If Slovak Information Service performs security checks on its employees, the decision on compliance is reviewable by the Supreme Court of the Slovak Republic (Act No. 215/2004 Coll, § 30)	
Storing*	no	no	The affected person may object to the procedure conducted by the Slovak Information Service in potential criminal proceedings against him/her. Otherwise they would never learn that SIS collects, stores and processes information their person. Another option is to pursue complaint on the protection of the personality under the Civil Code No. 40/1964 Coll (§ 11 et seq), processed by the district court, the regional court decides on appeals. If Slovak Information Service performs security vettings on its employees, the decision on compliance is reviewable by the Supreme Court of the Slovak Republic (Act No. 215/2004 Coll, § 30)	Violation of data protection, private life.
Destruction *	no	no	The affected person may object to the procedure conducted by the Slovak Information Service in potential	Violation of data protection, private life.

			criminal proceedings against him/her. Otherwise they would never learn that SIS collects, stores and processes information their person. Another option is to pursue complaint on the protection of the personality under the Civil Code No. 40/1964 Coll (§ 11 et seq), processed by the district court, the regional court decides on appeals. If Slovak Information Service performs security checks on its employees, the decision on compliance is reviewable by the Supreme Court of the Slovak Republic (Act No. 215/2004 Coll, § 30)	
After the whole surveillance process has ended	no	no	The affected person may object to the procedure conducted by the Slovak Information Service in potential criminal proceedings against him/her. Otherwise they would never learn that SIS collects, stores and processes information their person. Another option is to pursue complaint on the protection of the personality under the Civil Code No. 40/1964 Coll (§ 11 et seq), processed by the district court, the regional court decides on appeals.	Violation of data protection, private life.

			If Slovak Information Service performs security checks on its employees, the decision on compliance is reviewable by the Supreme Court of the Slovak Republic (Act No. 215/2004 Coll, § 30)	

[Act of the National Council of the Slovak Republic No. 171/1993 Coll. on Police Force]				
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	Yes, the person concerned may request the information on what personal data is processed by the Police Force, whom was it	The person concerned may initiate proceedings under Act no 122/2013 Coll. Privacy Policy - acting Office for Personal Data Protection (administrative authority), on appeal (decomposition) decided by the	violation of data protection, private life

* 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

		made available, correct the inaccurate data and request destruction or blockage of false or unnecessary data. The Police force would not provide such information if it jeopardized the investigation, the official procedure, criminal proceedings, the person concerned or other persons, if it was necessary to ensure public order or national security, or if so stipulated by a special law. (§ 69c)	President of the Office for Personal Data Protection The person concerned may initiate the proceedings under the Act No. 122/2013 Coll. on Protection of Personal Data. The proceedings on personal data protection (§ 62 and following) are performed by the Office for personal data protection (administrative authority), the Chairmen of the Office decides on appeals. The person concerned may object to the procedure of the Police Force- if the criminal proceedings was initiated and the person has the status of the accused (defendant) or aggrieved. Another option is to pursue complaint on the protection of the personality under the Civil Code No. 40/1964 Coll (§ 11 et seq), processed by the district court, the regional court decides on appeals.	
Analysis*	no	Yes, the person concerned may request the information on what personal data is processed by the Police	The person concerned may initiate proceedings under Act no 122/2013 Coll. Privacy Policy - acting Office for Personal Data Protection (administrative authority), on appeal	violation of data protection, private life

		Force, whom was it made available, correct the inaccurate data and request destruction or blockage of false or unnecessary data. The Police force would not provide such information if it jeopardized the investigation, the official procedure, criminal proceedings, the person concerned or other persons, if it was necessary to ensure public order or national security, or if so stipulated by a special law. (§ 69c)	(decomposition) decided by the President of the Office for Personal Data Protection The person concerned may initiate the proceedings under the Act No. 122/2013 Coll. on Protection of Personal Data. The proceedings on personal data protection (§ 62 and following) are performed by the Office for personal data protection (administrative authority), the Chairmen of the Office decides on appeals. The person concerned may object to the procedure of the Police Force- if the criminal proceedings was initiated and the person has the status of the accused (defendant) or aggrieved. Another option is to pursue complaint on the protection of the personality under the Civil Code No. 40/1964 Coll (§ 11 et seq), processed by the district court, the regional court decides on appeals.	
Storing*	no	Yes, the person concerned may request the information on what personal data is	The person concerned may initiate proceedings under Act no 122/2013 Coll. Privacy Policy - acting Office for Personal Data Protection	violation of data protection, private life

		processed by the Police Force, whom was it made available, correct the inaccurate data and request destruction or blockage of false or unnecessary data. The Police force would not provide such information if it jeopardized the investigation, the official procedure, criminal proceedings, the person concerned or other persons, if it was necessary to ensure public order or national security, or if so stipulated by a special law. (§ 69c)	(administrative authority), on appeal (decomposition) decided by the President of the Office for Personal Data Protection The person concerned may initiate the proceedings under the Act No. 122/2013 Coll. on Protection of Personal Data. The proceedings on personal data protection (§ 62 and following) are performed by the Office for personal data protection (administrative authority), the Chairmen of the Office decides on appeals. The person concerned may object to the procedure of the Police Force- if the criminal proceedings was initiated and the person has the status of the accused (defendant) or aggrieved. Another option is to pursue complaint on the protection of the personality under the Civil Code No. 40/1964 Coll (§ 11 et seq), processed by the district court, the regional court decides on appeals.	
Destruction *	no	Yes, the person concerned may request the information on what	The person concerned may initiate proceedings under Act no 122/2013 Coll. Privacy Policy - acting Office for	violation of data protection, private life

		personal data is processed by the Police Force, whom was it made available, correct the inaccurate data and request destruction or blockage of false or unnecessary data. The Police force would not provide such information if it jeopardized the investigation, the official procedure, criminal proceedings, the person concerned or other persons, if it was necessary to ensure public order or national security, or if so stipulated by a special law. (§ 69c)	Personal Data Protection (administrative authority), on appeal (decomposition) decided by the President of the Office for Personal Data Protection The person concerned may initiate the proceedings under the Act No. 122/2013 Coll. on Protection of Personal Data. The proceedings on personal data protection (§ 62 and following) are performed by the Office for personal data protection (administrative authority), the Chairmen of the Office decides on appeals. The person concerned may object to the procedure of the Police Force- if the criminal proceedings was initiated and the person has the status of the accused (defendant) or aggrieved. Another option is to pursue complaint on the protection of the personality under the Civil Code No. 40/1964 Coll (§ 11 et seq), processed by the district court, the regional court decides on appeals.	
After the whole surveillance process has ended	yes – if not jeopardizing the fulfilment of the tasks of the Police Force and		The person concerned may initiate proceedings under Act no 122/2013 Coll. Privacy Policy - acting Office for	violation of data protection, private life

	personal data were not destroyed, Police Force shall notify the person concerned that his/her personal data are stored (§ 69a)		Personal Data Protection (administrative authority), on appeal (decomposition) decided by the President of the Office for Personal Data Protection The person concerned may initiate the proceedings under the Act No. 122/2013 Coll. on Protection of Personal Data. The proceedings on personal data protection (§ 62 and following) are performed by the Office for personal data protection (administrative authority), the Chairmen of the Office decides on appeals. The person concerned may object to the procedure of the Police Force- if the criminal proceedings was initiated and the person has the status of the accused (defendant) or aggrieved. Another option is to pursue complaint on the protection of the personality under the Civil Code No. 40/1964 Coll (§ 11 et seq), processed by the district court, the regional court decides on appeals.	

Annex 4 – Surveillance-related case law at national level

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

Case title	IV. ÚS 216/2013
Decision date	18.04.2013
Reference details (type and title of court/body; in **original language and English** **[official translation, if available])**	*Ústavný súd Slovenskej republiky* [The Constitutional Court of the Slovak Republic]
Key facts of the case **(max. 500 chars)**	The applicant alleged a violation of their rights under the Constitution (Article. 22, personal data protection) and the Convention (Article. 8) by the interception and recording of telecommunications ordered by the District Court and suggested by the Regional Prosecutor's Office. The applicant was the subject of criminal proceedings for serious crime, illicit manufacture of narcotic drugs and psychotropic substances, precursors and poisons, their possession and trafficking. He alleged that in his criminal case the telecommunication recording has been used as evidence, although it was created for the purpose of another person´s criminal case, with the consent for the interception

	of different phone number. Moreover, this record had been taken even before the commencement of a prosecution of the complainant.
Main reasoning/argumentation **(max. 500 chars)**	The applicant complained that contrary to the Criminal Procedure Code neither the proposal of the Regional Prosecutor's Office nor the order of the District Court for the interception was sufficiently justified even though specific facts justifying the invasion to privacy must be stated. Objected proposal of the prosecution and court´s order, however, were justified only formally and, therefore, illegal. As it follows, records obtained in such manner cannot be used as a legal evidence.
Key issues (concepts, interpretations) clarified by **the case** **(max. 500 chars)**	Subsidiarity powers of the Constitutional Court for the protection of personal data
Results (sanctions) and key consequences or **implications of the case** **(max. 500 chars)**	The Constitutional Court dismissed the complaint for the lack of jurisdiction. It stated that the criminal proceedings in the case of complainant has not yet been completed. It also stated that criminal proceedings is from its beginning to its end a continuous process, in which the implementation of individual actions and implementation of fundamental rights and freedoms protective measures may be part of the competencies exercised by the authorities in criminal proceedings

	and they are liable to corrections in case of failures. Usually, the misconduct and measures violating the fundamental rights and freedoms could be objected at the Constitutional Court only after the end of the proceedings.

Case title	III. ÚS 97/2012 (case followed by the public and known as "Gorilla")
Decision date	20.11.2012
Reference details (type and title of court/body; in **original language and English** **[official translation, if available])**	*Ústavný súd Slovenskej Republiky* [The Constitutional Court of the Slovak Republic]
Key facts of the case **(max. 500 chars)**	The applicant alleged a violation of their rights under the Constitution and the Convention, including the right to privacy (Article. Paragraph 10. 2 of the Constitution and Art. 8 of the Convention). The violation should have been done by the use of information and technical means in his apartment.

Main reasoning/argumentation **(max. 500 chars)**	The applicant complained that the Slovak Information Service used against him the information acquired through technical means for the creation of video and audio recordings of his apartment. Consent to the execution of records was given by the regional court. Although the complainant was not allowed to inspect the file, one document was supposed to indicate that the information acquired by the SIS, had been a subject of trade and other illegal activities. The applicant complained that the SIS proposal for interception lacked relevant reasons and, therefore, it was not sufficiently justified why the complainant´s flat was to be tapped. Also the principle of the inevitable time was not respected. Court nevertheless issued a consent to the interception, without justification, and it was not clear whether it was issued by the legal judge. Therefore, the order was considered to be illegal and unconstitutional. In addition, the duration of the consent was later prolonged. The complainant argued that the case was a systemic failure of the oversight function of the court.
Key issues (concepts, interpretations) clarified by **the case** **(max. 500 chars)**	The Constitutional Court inspected whether the decision of the regional court, which granted consent for the use of information-technical means in the complainant's apartment, did not interfere with the complainant´s privacy. The Constitutional Court further inspected whether the decision issued by the regional court and the procedure were legal and constitutional.

Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Constitutional Court found that the rights of the complainant were violated. According to the Constitutional Court: - Limitations and conditions of the consent for the use of information and technical means were too loose, thus there was no guarantee of the strict proportionality of the interference in pursuit of a legitimate aim, - The applicant had no opportunity to object against eavesdropping, as this was learned only after a considerable time lag, while from the alleged consent of the tribunal it was not clear on what grounds the consent had been issued. The grounds must be evident even when the case is confidential. - In the consent issued by the court the formal reference to the provision of the Act is not sufficient unless the specific circumstances are further specified.

Case title	PL. ÚS 10/2014
Decision date	23.04.2014

Reference details (type and title of court/body; in **original language and English** **[official translation, if available])**	*Ústavný súd Slovenskej Republiky* [The Constitutional Court of the Slovak Republic]
Key facts of the case **(max. 500 chars)**	The Constitutional Court preliminary discussed the petition of 31 Members of Parliament on compliance of certain provisions (Art. 58 para 5-7, Art. 63 para 6) of the Act No. 351/2011 Coll. on Electronic Communications, certain provision (Art. 116) of the Criminal Code No 300/2005 Coll., and certain provisions (Art. 76a para 3) of the Act No. 171/1993 Coll. on Police Force with the Constitution of the Slovak Republic (Articles 13 para. 4, 16 para 1, 19 para. 2 and 3, 22, 26) and with the Charter of fundamental rights and freedoms (Art. 7 para. 1, 10 para. 2 and 3, 13, 17), Conventions on protection of human rights and fundamental freedoms (Art. 8 and 10) and Charter of fundamental rights of the European Union (Art. 7, 8, 11 and Art. 52 para. 1). The Constitutional Court preliminary suspended effectivity of Articles 58 / 5-7 and 63 / 6 of the Act on Electronic Communications. The information about the preliminary decision was published in the Collection of Laws under No. 128/2014. The decision, however, is not published on the web page of the Constitutional Court.

Main reasoning/argumentation **(max. 500 chars)**	Since the decision is not published on the web page of the Constitutional Court, this information is not yet available (until the final decision is published).
Key issues (concepts, interpretations) clarified by **the case** **(max. 500 chars)**	Since the decision is not published on the web page of the Constitutional Court, this information is not yet available (until the final decision is published).
Results (sanctions) and key consequences or **implications of the case** **(max. 500 chars)**	The Constitutional Court preliminary suspended the effectivity of Articles 58 / 5-7 and 63 / 6 of the Act on Electronic Communications.

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**
Slovenská informačná služba **[Slovak Information Service]**	*intelligence service*	*Vajnorská 39, 831 04 Bratislava 3* Phone contact: +421/02/44 25 90 21, 02/44 25 90 63 e-mail: info@sis.gov.sk	*http://www.sis.gov.sk/index.html*
Vojenské spravodajstvo **(Military Intelligence)**	military intelligence service	inaccessible	Does not exist

Národný bezpečnostný úrad **[National Security Authority]**	public authority - security agency	Budatínska 30, 850 07 Bratislava 57 Phone contact: +421/02/6869 1111 e-mail: podatelna@nbusr.sk	http://www.nbusr.sk/sk/index.html
Úrad pre reguláciu elektronických komunikácií a poštových služieb **[Regulatory Authority for Electronic Communications and Postal Services]**	public authority – administrative body	Továrenská 7, 828 55 Bratislava24 telefonický kontakt: +421 2 57 881 111 e-mail: e-podatelna@teleoff.gov.sk	http://www.teleoff.gov.sk/
Úrad na ochranu osobných údajov [The Office for personal data protection]	public authority – administrative body	Hraničná 12, 820 07 Bratislava 27 Phone contact: +421/2/32313214 E-mail: statny.dozor@pdp.gov.sk	http://www.dataprotection.gov.sk/uoou/
Výbor NR SR na preskúmanie rozhodnutí Národného bezpečnostného úradu (Committee of the National Council of the Slovak Republic	parliamentary body	Národná rada Slovenskej republiky Nám. Alexandra Dubčeka 1, 81280 Bratislava e-mail (general e-mail of the National Council): info@nrsr.sk Phone contact : +421 2 5972 1255	http://www.nrsr.sk/web/Default.aspx?sid=vybory/vybor&ID=133

to review decisions of the National Security Authority)		Fax: +421 2 5441 5468	
Osobitný kontrolný výbor NR SR na kontrolu činnosti Národného bezpečnostného úradu (Special Body of the National Council of the Slovak Republic for the oversight over the activities of the National Security Authority)	parliamentary body	Národná rada Slovenskej republiky Nám. Alexandra Dubčeka 1, 81280 Bratislava Phone contact: + 421 2 5972 1670 e-mail: okvnbu@nrsr.sk	http://www.nrsr.sk/web/Default.aspx?sid=vybory/vybor&ID=130
Osobitný kontrolný výbor NR SR na kontrolu činnosti Slovenskej informačnej služby (Special Body of the National Council of the Slovak Republic on the oversight of the activities of the Slovak Information Service)	parliamentary body	Národná rada Slovenskej republiky Nám. Alexandra Dubčeka 1, 81280 Bratislava Phone contact : +421 2 5972 1670 e-mail: okvsis@nrsr.sk	http://www.nrsr.sk/web/Default.aspx?sid=vybory/vybor&ID=131

Osobitný kontrolný výbor Národnej rady Slovenskej republiky na kontrolu činnosti Vojenského spravodajstva (Special Body of the National Concil of the Slovak Republic on the oversight of the activities of the Military Intelligence)	parliamentary body	Národná rada Slovenskej republiky Nám. Alexandra Dubčeka 1, 81280 Bratislava Phone contact : +421 2 5972 1670 email: okvvs@nrsr.sk	http://www.nrsr.sk/web/Default.aspx?sid=vybory/vybor&ID=132
Asociácia bývalých spravodajských dôstojníkov (The Association of Former Intelligence Officers)	NGO	Nevädzová ulica 5, 82101 Bratislava e-mail: absdslovakia@gmail.com	http://www.absd.sk/uvodna_stranka#

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

Reports of the Slovak Information Service (available only for years 2011 and 2012):

http://www.sis.gov.sk/for-you/sis-annual-report.html

Components of the Annual Reports of the National Security Authority (available only in Slovak):

http://www.nbusr.sk/sk/o-urade/informacie-pre-verejnost/komponent-vyrocnej-spravy.html

Report on state of provision of universal service and postal payment service (available for years 2012 and 2013, only in Slovak):

http://www.teleoff.gov.sk/index.php?ID=8711

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

   The annual reports of the Office for Personal Data Protection:

   http://www.dataprotection.gov.sk/uoou/en/node/44

3. Non-governmental organisations (NGOs)

Reports from the conferences on intelligence services organised by the Association of the Former Intelligence Officers in co-operation with Law Faculty of Paneuropean University Bratislava:

http://www.absd.sk/zborniky

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

Academics:

Hrubala, J. (2011), 'Judicial Orders and Decicions "sui generis" Interfering with Privacy – Potential Errors and Potential Consequences', *Justičná revue,* Vol. 63, No. 10, pp. 1346 – 1356.

Tothova, M. (2011), 'Eavesdropping and Tapping of Telephone Communication and its Usage in Order to Reveal and Prove Corruption', *COFOLA 2011: the Conference Proceedings*, Brno, Masaryk University.

https://www.law.muni.cz/sborniky/cofola2011/files/normotvorba/Tothova_Marcela_5725.pdf

Sepesi, P. (2011), 'Illegal Eavesdropping and Tapping of Telephone Communication – Decision of the Constitutional Court', *Učená právnická spoločnosť*, 18 January 2011.

http://www.ucps.sk/nelegalne_odposluchy_hovorov

Media:

Webnoviny.sk (2014), '*We Need Trustworthy Body for Eavesdropping, the Experts Say',* 25 July 2014.

http://www.webnoviny.sk/slovensko/clanok/848876-potrebujeme-doveryhodny-urad-na-odpocuvanie-tvrdia-experti/

Kernova, M. (2014), 'Shall Journalists Declassify Eavesdropping and Private E-mails?', *SME blog*, 6 June 2014.

http://omediach.blog.sme.sk/c/358510/maju-novinari-zverejnovat-odposluchy-a-sukromne-maily.html

Pravda (2014), '*In Case of Eavesdropping the Judges were not yet Testifying*', 24 July 2014.

http://spravy.pravda.sk/domace/clanok/324814-v-kauze-odpocuvania-este-nevypovedali-ani-sudcovia/

Krbatova, L. (2014), '*Case of Eavesdropping is still in a Drawer of Centes*', *Pravda*, 7 August 2014.

http://spravy.pravda.sk/domace/clanok/326135-centes-musi-kauzu-odpocuvania-novinarov-ukoncit-do-oktobra/

Pravda (2014), '*Were Politics Tapped during Lipsic?*', 22 June 2014.

http://spravy.pravda.sk/domace/clanok/321637-odpocuvali-politikov-za-lipsica/

SME (2013), '*Nicholson was Tapped because of Valko. He taught English the Murdered*', 30 October 2013.

http://www.sme.sk/c/6989646/nicholsona-policajti-odpocuvali-pre-valka-zavrazdeneho-ucil-anglictinu.html

SME (2013), '*The Judges Approve almost any Eavesdropping (Review)',* 1 November 2013.

http://www.sme.sk/c/6991400/sudcovia-podpisu-takmer-kazde-odpocuvanie-prehlad.html

TREND (2011), '*The Prime Minister will Dismiss Galko from Function*', 22 November 2011.

http://ekonomika.etrend.sk/ekonomika-slovensko/premierka-odvola-galka-z-funkcie.html

Kernova, M. (2011), '*Gucik Secretly Tapped Galko. The Recording was Performed Live',* medialne.trend.sk, 22 November 2011.

http://medialne.etrend.sk/televizia/gucik-si-nahral-galka-zaznam-pustil-live.html

Kernova, M. (2011), '*Analytics: Political Power Interfere with Media Freedom'*, medialne.trend.sk, 21 November 2011.

http://medialne.etrend.sk/tlac/analytici-politicka-moc-zasahuje-do-slobody-medii.html

Kernova, M. (2011), '*Galko did not Deny Eavesdropping, he did not Respond to Journalists'*, medialne.trend.sk, 21 November 2011.

http://medialne.etrend.sk/tlac/galko-odpocuvanie-nepoprel-novinarom-neodpovedal.html

eTrend (2011), '*Many Eavesdroppings, too Little Public Information',* 14 December 2011.

http://www.transparency.sk/sk/vela-odpocuvani-primalo-verejnych-informacii/

Meseznikov, G. (2011), *'Media-Intelligence game "As always"'*, Hospodarske noviny, 25 November 2011.

http://www.ivo.sk/buxus/docs/publicistika/subor/Mesez_HN_25_11_2011.pdf