Short Thematic Report

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

Legal update

Country: Slovak Republic

Version of 10 July 2016

FRANET contractor: Centre for the Research of Ethnicity and Culture

Author(s) name(s): Jana Kadlečíková, Ivana Rapošová

1 Description of tasks – Phase 3 legal update

1.1 Summary

*FRANET contractors are requested to highlight in 1 to 2 pages **maximum** the key developments in the area of surveillance by intelligence services in their Member State. This introductory summary should enable the reader to have a snap shot of the evolution during the report period (last trimester of 2014 until mid-2016). It should in particular mention:*

1. *the legislative reform(s)that took place or are taking place and highlight the key aspect(s) of the reform.*
2. *The important (higher) court decisions in the area of surveillance*
3. *the reports and inquiry by oversight bodies (parliamentary committees, specialised expert bodies and data protection authorities) in relation to the Snowden revelations*
4. *the work of specific ad hoc parliamentary or non-parliamentary commission (for example the NSA inquiry of the German Parliament) discussing the Snowden revelations and/or the reform of the surveillance focusing on surveillance by intelligence services should be referred to.*

1. In 2015 and 2016 some major changes took place in Slovak legislation with respect to data retention. The final resolution of the Constitutional Court of the Slovak Republic no.PL. ÚS 10/2014-78[1], which was issued as a conclusion to the legal procedure initiated by the invalidation of the Data Retention Directive 2006/24/EC, triggered a systemic change in the legislation concerning privacy and data protection. Based on this resolution the Act No. 397/2015 was passed in 2015 and came into force on the 1st January 2016[2]. This Act further amends the Acts No. 351/2011 Coll. on Electronic Communications[3], Act No. 301/2005 Code of Criminal Procedure[4] and Act No. 171/1993 on the Police Corps[5]. All three of these Acts transposed Data Retention Directive 2006/24/EC in the past and thus had to be amended if the transposition was to be invalidated in the Slovak legislation system. The new provisions secure a greater control over data retention process and provide more detailed specification of situations in which data could be retained, stored and requested by state bodies. This is limited only to the most serious crimes as e.g. terrorism or threatening the integrity of the country. The amendment also abolishes the preventive blanket retention and storage of data on the side of telecommunication companies - the data could be retained only retrospectively on court request (other than criminal procedure) or court order (criminal procedure). The court request or court order shall, moreover, be issued only in case there are no other legal option how to obtain the information. This applies to the activities of Police force and Intelligence services alike. According to the information provided by the spokesperson of the Slovak information service, based on the article 65, section 7 of the Act no. 351/2011, the Slovak Information Service is currently entitled to acquire telecommunication data only pro futuro and only with the written consent of the lawful judge[6] as opposed to the situation prior to this amendment, when such a consent was not necessary and the data were accessible also retrospectively. Moreover, this amendment provides for an

[1] Slovakia, Constitutional Court of the Slovak Republic (*Ústavný súd Slovenskej Republiky*) Resolution No. PL. ÚS 10/2014-78 from 29 April 2015. Available at http://www.concourt.sk/SearchRozhodnutiav01/podanie.do?id_spisu=572536.

[2]Slovakia, Act No. 397/2015 Coll. which for the purposes of the Criminal Code provides a list of substances with anabolic or other hormonal action and amending and supplementing certain laws (*Predpis č. 397/2015, ktorým sa na účely Trestného zákona ustanovuje zoznamlátok s anabolickým alebo iným hormonálnym účinkom a ktorým sa menia a dopĺňajú niektoré zákony)* from13 November 2015.

[3]Slovakia, Act No. 351/2011 Coll. on Electronic Communications (*Zákon o elektronických komunikáciach*) from 1 November 2011, as amended.

[4]Slovakia, Act. No. 301/2005 Coll. Code of Criminal Procedure (*Trestný poriadok*) from 24 May 2005.

[5]Slovakia, Act. No. 171/1993 Coll. on Police Corps (*Zákon o policajnom zbore*) from 6 July 1993.

[6] Information provided on request by the Slovak Information Service on 13April 2016.

obligation to establish a new monitoring body, the Special Commission of the National Council to supervise the use of information-technological tools that shall secure the surveillance.[7] More detailed information about the Commission will be provided in the next paragraph.

Furthermore, on 1st January 2016 the Act no. 404/2015 Coll.[8] came into force. It amends and supplements the Act no. 166/2003 Coll.[9] on the protection of privacy against unauthorised use of information-technological tools (Act on protection against eavesdropping). The main objective of this Act is to strengthen the control over the use of information and technical resources. According to the Article 8a, section 6 of the aforementioned Act, the controlling function over the use of information technology is executed by the Special Commission of the National Council to supervise the use of information-technological tools established by the National Council. The main aim of this Commission is to check the compliance with the law when it comes to use of information-technological tools by the intelligence services. The Commission has a capacity to check if the competencies of the intelligence services were not abused. However, as the National Council states, the further competencies will be clarified through internal guidelines as soon as the Commission will be established and are now a matter of negotiation.[10] Whereas the already established "old" oversight bodies, mainly the Special Parliamentary Committee to Supervise Slovak Information Service Performance or Military Intelligence performance are entitled to access the information related to the administrative aspects of the Intelligence services, such as its statute, budget allocation, internal guidelines or annual reports (article 5 of the Act 46/1993[11]), the newly forming Special Commission has wider competencies and will be entitled to access the information produced in relation to Intelligence activities in the field of information-technological measures, which includes the access to classified information such as the evidence of information-technological means for a respective period or information on termination of the records. These classified information can be accessed, however handled with the highest caution and any written notes taken based on access to these information shall remain and be stored in the intelligence building under protection (articles 7 - 9 of the Act 404/2015[12]).
It shall consist of 6 parliamentary members and 2 expert members. According to the same article (8a), the Commission should consist of three deputies from governmental coalition, three from opposition and two independent expert members chosen by the parliament. The two independent experts must be over 40 years old and have a career background of a policeman, prosecutor, judge, or in intelligence services profession of legal and security theory and practice or international relations and diplomacy, for at least ten years. They also have to have the most stringent review of the National Security Authority at the top secret level.[13] Parliamentary Members do not need any clearance.[14] The name of the two experts are

[7]Information provided on request by the Ministry of Transport, Construction and Regional Development of the Slovak Republic (*Ministerstvo dopravy, výstavby a regionálneho rozvoja SR*) on 5 October 2015.
[8]Slovakia, Act No. 404/2015 Coll. amending and supplementing ActN. 166/2003 Coll. on the protection of privacy against unauthorised use of information-technological tools and on amendment of certain laws (Act on protection against eavesdropping) (*Zákon, ktorým sa mení a dopĺňa zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane predodpočúvaním) v znení neskorších predpisov*) from 19 December 2015.
[9] Slovakia, Act No. 166/2003 on the protection of privacy against unauthorised use of information-technological tools that amends certain laws (*Zákon 166/2003 z. z. zákon o ochrane pred odpočúvaním*) from 21st May 2003.
[10] Information provided on request by the National Council of the Slovak Republic on 15 June 2016.
[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*) from 21 January 1993.
[12] Slovakia, Act No. 404/2015 amending and supplementing Act No. 166/2003 Coll. on the protection of privacy against unauthorised use of information-technological tools and on amendment of certain laws (Act on protection against eavesdropping) (*Zákon, ktorým sa mení a dopĺňa zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technickýchprostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov*) from 19 December 2015.
[13] Slovakia, Act No. 404/2015 Coll. amending and supplementing Act No. 166/2003 Coll. on the protection of privacy against unauthorised use of information-technological tools and on amendment of certain laws (Act on

not yet know, however, their presence in the Commission will practically change its statute from parliamentary oversight to combined parliamentary and expert oversight. The control shall be done at least once a year at any time, or any time on the own initiative of the Commission or on the initiative of a citizen of the Slovak Republic assuming that the information and the technical means had been used against them. However, the actual result of the review containing information on whether someone is or is not "subjected to supervision" cannot be provided to the citizen who gave the notice. According to the section 13 and 14 of the article 8a, the Commission is on the first instance accountable to the respective Parliamentary Committee (Special Parliamentary Committee to Supervise Slovak Information Service Performance or Military Intelligence performance), which examines their report and if the Committee finds a discrepancy with the law they further report it to the National Council of the Slovak Republic and simultaneously to the Prosecutor General. According to the article 9, the National Council of the Slovak Republic is obliged to organize at least two meetings over the reports provided by the Special Commission and Parliamentary Committees in a year, the Act, however, does not specify any specific remedies the National Council can use. Findings of the report may be published by the media however they may not reveal any confidential (classified) information.[15] The law also stipulates that submitting individual complaint to the commission does not limit in any way the aggrieved party's right to seek judicial remedy or other means of protection.[16] These are most likely in the capacity of the Prosecutor General. The starting date of the operation of the Commission is not specified by the law or by any other resolution. According to the information published by the media, the Commission should start its operation since the 1 January 2017.[17]

On the 1st January 2016, the new Act no. 444/2015 coll.[18] came into force which amends the Act no. 300/2015 Criminal Code[19]. The Act aims to streamline the fight against terrorism by creating legal preconditions in terms of information gathering, extending the possibility of using measures of a preventive nature and not least finish inferring a penalty of prosecution of terrorist offenses, including the related criminal proceedings. With respect to surveillance, the Act amends the Act 46/1993[20] on the Slovak Information Service and Act 198/1994[21] on Military Intelligence and extends their competences towards the use of replacing things and feigned transfer case as legitimate information and operational methods and towards initiating a procedure through which on the incentive of the Slovak Information Service (*Slovenská informačná služba – SIS*) the court might issue an order to abolish the website or access to website that has a content promoting terrorism, or different forms of extremism. This applies only to criminal offences that could cause severe damage to the security of the

protection against eavesdropping) (*Zákon, ktorým sa mení a dopĺňa zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane predodpočúvaním) v znení neskorších predpisov*) from 19 December 2015.

[14]Denník N, (2016), 'Môže byť Galko v komisii na kontrolu odposluchov? Šebej hovorí, že nikdy' 4 May 2016, available at: https://dennikn.sk/451302/moze-byt-galko-komisii-kontrolu-odposluchov-sebej-hovori-ze-nikdy/

[15] Act No. 166/2003 on the protection of privacy against unauthorised use of information-technological tools that amends certain laws, Article 9.

[16] Ibid, Article 8a, Paragraph 15.

[17] Denník N, (2016), 'Môže byť Galko v komisii na kontrolu odposluchov? Šebej hovorí, že nikdy' 4 May 2016, available at: https://dennikn.sk/451302/moze-byt-galko-komisii-kontrolu-odposluchov-sebej-hovori-ze-nikdy/

[18]Slovakia, Act. No. 444/2015 Coll. amending and supplementing the Act No. 300/2005 Z.z. Criminal Code as amended, and which amends certain laws (*Zákon ktorým sa mení a dopĺňa zákon č. 300/2005 Z.z. Trestný zákon v znení neskorších predpisov a ktorýmsa menia a dopĺňajú niektoré zákony*) from 21 December 2015.

[19]Slovakia, Act No. 300/2005 Coll. Criminal Code (Trestný zákon) from 24 May 2005.

[20]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*) from 21 January 1993.

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

state, to economic interests of the state or to protection of the classified information. The further clarification of these threats is not listed.

The legislation governing the competencies and activities of the National Security Authority (*Národný bezpečnostný úrad – NBÚ*) with respect to surveillance has not been altered during the past two years.[22]

However, what remains the Achilles heel of the Slovak legislation with respect to intelligence services is the fact that despite the aforementioned amendments, the major novelties proposed in the draft of the Act no. KM-OPVA-2015/001214 on the Civil Intelligence and Military Intelligence and the amendment of certain laws (the state intelligence and the intelligence services)[23] prepared by the Slovak Information Service in cooperation with a variety of experts from academic and expert backgrounds hasn't been put to the legislation process so far. This proposal is yet considered to be a crucial development in the intelligence services legislation. Despite the partial novelizations of the Act no. 46/1993[24] on the Slovak Information Service and of the Act 198/1994[25] on Military Intelligence, these provisions are considered by experts to be obsolete, mainly not being able to respond to the current security needs and threats (as most of the nowadays threats require different intelligence measures than 20 years ago when these Acts were formulated and thus some protective and intelligence measures are being done on the legal borderline now having a sufficient legal support) and not providing enough security measures, mainly through the weak controlling mechanisms. The new provision entails several crucial amendments that should lead towards greater transparency and accountability of the intelligence services, mainly the unification of the Slovak information Service and Military Intelligence under one organization following the same legal standards and regulations, greater internal control with a possibility of reporting internal violation of rules and greater external control that could systematically respond to citizens' notices in case the violation of law is suspected. The legal proposal has passed the process of interdepartmental commenting already in 2015 and the majority of the comments were incorporated. The fact that the draft of the Act has not been put into the legislation process up to this date had been interpreted as a lack of political will to open this topic prior to the elections taking place in March 2016 by experts and media alike. The adoption of this kind of provision, moreover, requires more than simple parliamentary majority, though putting the proposal into legislative process requires wider political consensus.[26]Therefore it is not clear how quickly and if at all the new governmental coalition will be able to find wider political support for this proposal. The timeframe of the eventual initiation of the legislation process is thus unclear, as much as the extent of the eventual support by the political parties.

2. The most crucial higher court decision was the final resolution of the Constitutional Court of the Slovak Republic no. PL. ÚS 10/2014-78[27], which was issued as a conclusion to the legal procedure initiated by the invalidation of the Data Retention Directive 2006/24/EC, and which triggered a systemic change in the legislation concerning the

[22]Information provided on request by the National Security Authority on 12 April 2016.

[23]Slovakia, Draft of the Act no. KM-OPVA-2015/001214 on the Civil Intelligence and Military Intelligence and the amendment of certain laws (*Návrh zákona o Úradecivilnéhospravodajstva a Vojenskomspravodajstve a o z mene a doplnení niektorých zákonov*) from 27 February 2015.

[24] 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*) from 21 January 1993.

[25]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*), from 30 June 1994.

[26]TA3 (2016), 'The Act on secret services waits for political agreements, the change of the name SIS is possible' (*Zákon o tajných službách čaká na politickú dohodu, v hre aj zmena názvu SIS*), 24 April 2016, available at: http://www.news.sk/rss/clanok/2016/04/952880/zakon-o-tajnych-sluzbach-caka-na-politicku-dohodu-v-hre-aj-zmena-nazvu-sis/ (4th May 2016).

[27] Slovakia, Constitutional Court of the Slovak Republic (*Ústavný súd Slovenskej Republiky*), Resolution No. PL. ÚS 10/2014-78 from 29 April 2015, Available at http://ww

privacy and data protection. The information has been mentioned above and is also elaborated on in detail in our Contribution to the FRA Annual Report 2015.

3. The processes pursued by the Military Intelligence (*Vojenské spravodajstvo – VS*) and by the Slovak Information Service (*Slovenská informačná služba)* following the Snowden revelations are classified and not publicly available. Both of these intelligence bodies deny any kind of information request with respect to measures taken after the affair with the argument they have to remain secret in order to ensure security.[28] The National Security Authority claims not to have taken any additional measures consequent to the affair.[29]

4. The processes pursued by the Military Intelligence and by the Slovak Information Service following the Snowden revelations are classified and not publicly available. Both of these intelligence bodies refused to provide any kind of information related to measures taken consecutive to the affair with the argument they had to remain classified in order to ensure the security of the state.[30] The National Security Authority claims not to have taken any additional measures consequent to the affair[31] and the Data Protection Authority claims not to have any competence over the intelligence services in this respect.[32] However, as can be judged from the draft of the Act no. KM-OPVA-2015/001214 on the Civil Intelligence and Military Intelligence and the amendment of certain laws (the state intelligence and the intelligence services)[33] prepared by the Slovak Information Service, there are certain changes with respect to accountability of the Intelligence employees planned. According to the information available at the Slovak Information Service website, the new proposal of the Act entails a provision allowing that the "members of the intelligence services will have for the first time enshrined in the law the opportunity to report suspected violations of the law of their colleagues directly to the Director of the Intelligence who will be required to deal with such filing in the so-called internal inspection. The novelty lies in the fact that if a member who reported suspected violations of the law by his colleagues could not identify themselves with the decision of the Director of Intelligence, there would be a statutory possibility to report this to the Special Prosecutor, who would investigate the case. The Director of the Intelligence Service would be obliged to provide statutory cooperation. For the first time in last twenty years the "whistleblowing" will become a part of laws on intelligence".[34] This provision is seen as crucial in terms of enhancing the control over intelligence services. However, as stated in the section 1 of this summary, the time frame of this draft of the Act to become a part of the legislation procedure and eventually come into force is not clear.

1.2 International intelligence services cooperation

*FRANET contractors are requested to provide information, in 1 to 2 pages **maximum**, on the following two issues, drawing on a recent publication by Born, H., Leigh, I. and*

w.concourt.sk/SearchRozhodnutiav01/podanie.do?id_spisu=572536

[28]Information provided on request by the Slovak Information Service (13 April 2016) and Military Intelligence (13 April 2016).

[29]Information provided on request by the National Security Authority (12th April 2016).

[30]Information provided on request by the Slovak Information Service (13April 2016) and Military Intelligence (13 April 2016).

[31]Information provided on request by the National Security Authority (12 April 2016).

[32]Information provided on request by the Data Protection Authority on 24 June 2016.

[33]Slovakia, Draft of the Act no. KM-OPVA-2015/001214 on the Civil Intelligence and Military Intelligence and the amendment of certain laws (*Návrh zákona o Úradecivilnéhospravodajstva a Vojenskomspravodajstve a o z mene a doplnení niektorých zákonov*) from 27 February 2015.

[34]Information available on the official webpage of the Slovak Information Service

Wills, A. (2015), Making international intelligence cooperation accountable, Geneva, DCAF.[35]

1. *It is assumed that in your Member State international cooperation between intelligence services takes place. Please describe the legal basis enabling such cooperation and any conditions that apply to it as prescribed by law. If the conditions are not regulated by a legislative act, please specify in what type of documents such cooperation is regulated (e.g. internal guidance, ministerial directives etc.) and whether or not such documents are classified or publicly available.*

The Slovak Information Service (SIS) cooperates with other member states' intelligence services especially based on Act no. 46/1993 Coll. on Slovak Information Service, more particularly based on provisions spelled out in Article 1, Paragraph 3, which reads: "When discharging its duties, the information service is entitled to cooperate with other countries' bodies of similar orientation and specialisation as well as with international organisations."

On its official website, SIS states that it currently cooperates with 81 partner intelligence services and is actively involved within the following international intelligence platforms: Club de Berne (CdB), Counter Terrorist Group (CTG), FORUM and Middle European Conference (MEC) and Civilian Intelligence Committee (CIC).[36]

The SIS official website informs that its international cooperation with other intelligence services is also regulated by other internal documents that cannot be further specified as it would constitute a violation of the Act no. 215/2004 Coll. on the protection of confidential information or international agreements that provide the basic framework for this cooperation.[37]

In the field of international cooperation, activities of the National Security Authority of the Slovak Republic are governed by the Act no. 215/2004 Coll. on the protection of confidential information. In its Article 70, Paragraph 4, the law stipulates that "when applying this law, the Authority also cooperates with national security authorities of other states and security authorities of international organisations." The NBÚ informed us that mutual cooperation between the NBÚ and foreign intelligence services could take place only if the intelligence service in question pursued tasks equivalent to those of the NBÚ.[38] Mutual cooperation between the NBÚ and other countries' national security authorities takes place based on applicable international agreements. The list of international agreements concluded to this effect is available on the NBÚs official website[39].

2. *Please describe whether and how the international cooperation agreements, the data exchanged between the services and any joint surveillance activities, are subject to oversight (executive control, parliament oversight and/or expert bodies) in your Member States.*

Mutual cooperation between the SIS and other countries' intelligence services is regulated by international agreements as well as internal rules of international intelligence service

e, available at http://www.sis.gov.sk/aktuality/novinky.html.

[35] HYPERLINK "http://www.dcaf.ch/Publications/Making-International-Intelligence-Cooperation-Accountable" http://www.dcaf.ch/Publication

[36] Slovak Information Service (2015), *Report on the Performance of the SIS in 2014* (chapter 4.4 Cooperation of the SIS with Intelligence Services of Other States), available at: http://www.sis.gov.sk/pre-vas/sprava-o-cinnosti.html

[37]This information was provided at request by the Slovak Information Service on 13 April 2016.

[38]This information was provided at request by the National Security Authority on 8 April 2016.

[39] National Security Authority, International Agreements, available at: http://www.nbusr.sk/sk/pravne-predpisy/ochrana-utajovanych-skutocnosti/medzinarodne-zmluvy.html

associations the SIS is a member of (please see Section 1.2.1.). As far as joint surveillance activities are concerned, mutual cooperation often takes place on the voluntary basis, i.e. outside concrete agreements or contracts that would spell out any rights or obligations of the SIS or its partners.[40]Oversight of joint surveillance activities as well as all other SIS activities is provided by Special Parliamentary Committee to Supervise SIS Performance in compliance with Article 5 of the Act no. 46/1993 Coll. on Slovak Information Service. The law on Slovak Information Service does not specify in more details all areas of SIS activities that shall be subjected to supervision by mentioned Special Parliamentary Committee. The law states more generally type of information and documents on the SIS activities the Special Parliamentary Committee shall be provided by. The law does not specify whether information on join surveillance activities or international cooperation shall be forwarded to the Special Parliamentary Committee. The Special Parliamentary Committee to Supervise SIS Performance does not publish any regular reports.

Participation of the National Security Authority (NBÚ) in joint surveillance activities is regulated by the same rules as its international cooperation in general (please see Section 1.2.1). The NBÚ refused to provide any further information on data exchange within the framework of joint surveillance activities. In general, oversight of its activities is provided by Special Parliamentary Committee to Supervise NBÚ Performance in compliance with Article72, Paragraph 1 of the Act no. 215/2004 Coll. on the protection of confidential information. The National Council of the Slovak Republic also has Special Parliamentary Committee to Examine NBÚ Decisions, which has been established in compliance with Constitutional Law 254/2006 on the Founding and Performance of Special Parliamentary Committee to Examine NBÚ Decisions.

Part of the system of providing oversight is also Special Commission of the National Council to supervise the use of information-technological tools, which was established in compliance with the Act no. 166/2003 Coll. on the protection of privacy against unauthorised use of information-technological tools (Article 8a, Paragraph 1). The commission supervises the application of the Act no.166/2003, which regulates the use of information-technological tools (e.g. wire-tapping devices).

There are no other executive or expert bodies in the Slovak Republic that would perform oversight of data exchanges and/or joint surveillance activities.

[40]This information was provided at request by the Slovak Information Service on 13 April 2016.

8

1.3 Access to information and surveillance

*FRANET contractors are requested to summarise, in 1 to 2 pages **maximum**, the legal framework in their Member State in relation to surveillance and access to information.*
Please refer to the Global Principles on National Security and the Right to Information (the Tshwane Principles)[41](in particular Principle 10 E. – Surveillance) and describe the relevant national legal framework in this context. FRANET contractors could in particular answer the following questions:

1. *Does a complete exemption apply to surveillance measures in relation to access to information?*
2. *Do individuals have the right to access information on whether they are subject to surveillance?*

1. According to the Act 211/2000 on free access to information, all state bodies are required to provide information of public character upon a proper request. However, if the classified information are requested, the state bodies are entitled to deny request to such information with a reference to article 8, of the same Act, that provides that (1) If the requested information constitutes classified information under the Act 215/2004 or is subject to banking secrecy or tax secrecy under a separate law, and the applicant has no authorization, the state body must not make the information available with reference to the this provision.[42] Further the Act no. 46/1993[43] and the Act no. 198/1994[44] under article 17, section 9, specifies, that the information held by the Slovak Information Service are exempt from the entitlements governed by the Act no. 211/2000 on free access to information[45] and the Act no. 428/2002 on personal data protection.[46] Thus the individuals cannot approach these bodies with request to access to classified information.

The principal provision governing the rules of information and object classification and their accessibility is the Act no. 215/2004 Coll. on protection of confidential information[47]. For the purposes of this Act, under article 2, section b, the information is understood as 1. the content of the document, drawing, drawings, maps, photographs, charts or other record, 2. the content of the oral submissions, and 3. the content of an electrical, electromagnetic, electronic or other physical transport medium. The object is understood under article 3, section c, as a 1. tangible medium of listing information, 2. product, 3. equipment, or 4. property. The article 3 of the Act specifies four different categories of information depending from the level of their classification. It distinguishes between the top secret, secret, confidential and reserved information. It further specifies the conditions under which these data can be accessed and lists the specific requirements the person has to meet in order to access them (articles 10 to 42). Besides the other, these entail the security clearance. The Act also specifies the group of publicly accountable persons who are exempt from the obligation

[41] http://www.right2info.org/exceptio ns-to-access/national-security/global-principles#section-10
[42] Slovakia, Act No. 211/2000 coll. on free access to information (*Zákon č. 211/2000 z. z. o slobodnom prístupe k informáciám*) from 13 July 2000.
[43] 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*) from 21 January 1993
[44] 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*), from 30 June 1994.
[45]Slovakia, Act of the National Council of the Slovak Republic No. 211/2000 Coll on free access to information (*Zákon č. 211/2000 Z. z. Zákon o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov*) from 13 July 2000)
[46]Slovakia, Act of the National Council of the Slovak Republic No. 428/2002 Coll on personal data protection (*Zákon č. 122/2013 Z. z. Zákon o ochrane osobných údajov*) from 28 May 2013.
[47]Slovakia, Act of the National Council of the Slovak Republic No. 215/2004 Coll. on the protection of confidential information (*Zákon č. 215/2004 Z. z. o ochrane utajovanýchskutočností a o zmene a doplnení niektorých zákonov*) from 27 April 2004.

to meet the official requirements, who are for instance not obliged to undergo a security clearance and can access classified information from the authority of their post. According to the section 1 of the article 34 of the Act this includes a) the President of the Slovak Republic, b) members of the National Council of the Slovak Republic, c) a member of the Slovak Government, d) a judge of the Constitutional Court of the Slovak Republic, e) The President and Vice-Presidents of the Supreme Audit Office of the Slovak Republic, f) a judge, or g) members of the Judicial Board with respect to determination of prerequisites for judicial competence.[48] With respect to the newly established Special Commission of the National Council to supervise the use of information-technological tools, which shall mainly consist of members of the National Council there is a public discussion if the post provides enough guaranties for them to access the classified information or if they should be also subjected to security control.[49]

2. As stated already in the former section, the Act no. 46/1993[50]and the Act no. 198/1994[51]specify in both cases under article 17, section 9, that the information held by the Slovak Information Service are exempt from the entitlements governed by the Act no. 211/2000 on free access to information[52] and the Act no. 428/2002 on personal data protection.[53] Thus the individuals cannot approach these bodies with request to access the classified information.

However, as referred to also in the section 1.1, pursuant to the Article 8a, section 6, of the Act no. 404/2015 Coll.[54] which came into force on 1st January 2016 there are additional measures accepted in order to enhance protection of individuals against unauthorized surveillance. According to this provision the Special Commission of the National Council to supervise the use of information-technological tools established by the National Council of the Slovak Republic can examine the activities of the Slovak Information Service and Military Intelligence also on the initiative of a citizen of the Slovak Republic assuming that the information and the technical means had been used against them. However, the actual result of the review containing information on whether someone is or is not "subjected to supervision" cannot be provided to the citizen who gave the notice. This provision governs the procedure of the Slovak Information Service and the Military Intelligence respective.

[48]Slovakia, Act of the National Council of the Slovak Republic No. 215/2004 Coll. on the protection of confidential information (Zákon č. 215/2004 Z. z. o ochrane utajovanýchskutočností a o zmene a doplnení niektorých zákonov) from 27 April 2004.

[49]Denník N. (2016), 'Môže byť Galko v komisii na kontrolu odposluchov? Šebej hovorí, že nikdy', 4 May 2016. Accessiblefrom https://dennikn.sk/451302/moze-

[50] 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*) from 21 January 1993

[51] 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*), from 30 June 1994.

[52]Slovakia, Act of the National Council of the Slovak Republic No. 211/2000 Coll on free access to information (*Zákon č. 211/2000 Z. z. Zákon o slobodnom prístupe k informáciám* a o zmene a doplnení niektorých zákonov) from 13 July 2000)

[53]Slovakia, Act of the National Council of the Slovak Republic No. 428/2002 Coll on personal data protection (*Zákon č. 122/2013 Z. z. Zákon o ochrane osobných údajov*) from 28 May 2013.

[54]Slovakia, Act No. 404/2015 amending and supplementing Act No. 166/2003 Coll. on the protection of privacy against unauthorised use of information-technological tools and on amendment of certain laws (Act on protection against eavesdropping) (*Zákon, ktorým sa mení a dopĺňa zákon č. 166/2003 Z. z. o ochrane súkromiapredneoprávnenýmpoužitíminformačno-technickýchprostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane predodpočúvaním) v znení neskorších predpisov*) from 19 December 2015.

1.4 Update the FRA report

FRANET contractors are requested to provide up-to-date information based on the FRA report on Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – mapping Member States' legal framework.

*Please take into account the **Bibliography/References** (p. 79 f. of the FRA report), as well as the **Legal instruments index – national legislation** (p. 88 f. the FRA report) when answering the questions.*

Introduction

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia not mentioned, no specific situation relevant for the analysis.

1 Intelligence services and surveillance laws

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia not mentioned, no specific situation relevant for the analysis.

1.1 Intelligence services

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia not mentioned.
In Slovakia there are three intelligence bodies - The Slovak Information Service, Military Intelligence and the National Security Authority. They are all independent state bodies cooperating with the police force, government or other state bodies when necessary. Their competencies are governed by specific publicly available acts.

1.2 Surveillance measures

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*

3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia not mentioned.
Pursuant to the Act No. 397/2015 which was passed in 2015 and came into force on the 1st January 2016[55] the Slovak legislation does not anymore allow for untargeted data retention. Through this Act the transposition of the Data Retention Directive 2006/24/EC was invalidated in the Slovak legislation. This has directly impacted also Intelligence services which can now request information only pro futuro and based on the written consent of the court.

1.3 Member States' laws on surveillance

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia mentioned, information is correct.
The retention of telecommunication data is governed by the Act No. 351/2011 Coll. on Electronic Communications[56]. Pursuant to the Act No. 397/2015 which was passed in 2015 and came into force on the 1st January 2016[57] the Slovak legislation does not anymore allow for untargeted data retention. Through this Act the transposition of the Data Retention Directive 2006/24/EC was invalidated in the Slovak legislation. Thus the Act No. 351/2011 Coll. specifies, that the telecommunication data can be disclosed to Intelligence bodies only based on the court order. Slovakia thus does not conduct signals intelligence. See also Summary section of this report for further details.

FRA key findings

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia not mentioned, no specific situation relevant for the analysis.

2 Oversight of intelligence services

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*

[55]Slovakia, Act No. 397/2015 which for the purposes of the Criminal Code provides a list of substances with anabolic or other hormonal action and amending and supplementing certain laws (*Predpis č. 397/2015, ktorým sa na účely Trestného zákona ustanovuj ezoznam látok s anabolickým alebo iným hormonálnym účinkom a ktorým sa menia a doplňajú niektoré zákony)* from13 November 2015.
[56]Slovakia, Act No. 351/2011 Coll. on Electronic Communications (*Zákon o elektronických komunikáciach*) from 1 November 2011, as amended.
[57]Slovakia, Act No. 397/2015 which for the purposes of the Criminal Code provides a list of substances with anabolic or other hormonal action and amending and supplementing certain laws (*Predpis č. 397/2015, ktorým sa na účely Trestného zákona ustanovuje zoznam látok s anabolickým alebo iným hormonálnym účinkom a ktorým sa menia a doplňajú niektoré zákony)* from13 November 2015.

12

2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia not mentioned.
Slovakia does not have a very sophisticated oversight system when compared to other countries cited in the report. There are only parliamentary oversight bodies with no remedial power, the newly emerging Commission of the National Council to supervise the use of information-technological tools established by the National Council of the Slovak Republic, no expert bodies and no NGOs or other civic actors specialised on surveillance and data protection. Furthermore, the Slovak ombudsperson and the Data Protection authority have no power over the surveillance conducted by the Slovak Information Service, Military Intelligence and National Security Authority. The lack of control is partially reflected in the draft of the Act no. KM-OPVA-2015/001214 on the Civil Intelligence and Military Intelligence and the amendment of certain laws (the state intelligence and the intelligence services)[58] prepared by the Slovak Information Service (for further details please see the summary of this report).

2.1 Executive control

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia not mentioned.
Pursuant to the article 3 of the Act no. 46/1993 Coll. on the Slovak Information Service[59]and the Act no. 198/1994 Coll. on Military Intelligence[60] the Government of the Slovak Republic provides on-going oversight over their activities. The main competencies of the Slovak government with respect to the Slovak Information Service and Military Intelligence is appointing the director. This is done by the President of the Slovak Republic on the suggestion of the Slovak Government. The Government also decides on the number of employees of the intelligence services and based on the proposal of the Director of intelligence services approve the statute of the intelligence services and adjusts their focus, organization and management.

2.2 Parliamentary oversight

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*

request by the National SecurityAuthority (12 April 2016).
[58]Slovakia, Draft of the Act no. KM-OPVA-2015/001214 on the Civil Intelligence and Military Intelligence and the amendment of certain laws (*Návrh zákona o Úrade civilného spravodajstva a Vojenskom spravodajstve a o zmene a doplnení niektorých zákonov*).
[59]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*) from 21 January 1993.
[60]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*), from 30 June 1994.

13

2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia not mentioned.
The parliamentary oversight is the most developed oversight in the Slovak context. There are 4 parliamentary oversight bodies conducting oversight over the activities of the Slovak Information Service, Military Intelligence and National Security Authority, namely the Special Parliamentary Committee to review decisions of the National Security Authority, Special Parliamentary Committee to supervise the performance of National Security Authority, Special Parliamentary Committee to supervise performance of Slovak Information Service and the Special Parliamentary Committee to supervise performance of Military Intelligence. Their competencies fall within essential powers as defined by the report. Under the current legal provision parliamentary oversight is conducted ex post, and therefore has the character of a subsequent verification of the legality and legitimacy of the activities of the intelligence services. There is a newly forming Special Commission of the National Council to supervise the use of information-technological tools which will have more enhanced powers and will receive notices also from the citizens. Its competencies will be, however, limited to inspection of those notices, the commission will have no remedial power. For further information see the summary under 1.1.

2.2.1 Mandate

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia mentioned, information only partially correct.
As mentioned already in the section 2.2, the competencies of four already established parliamentary oversight bodies in Slovakia fall within the category of essential powers. However, the newly forming Special Commission of the National Council to supervise the use of information-technological tools will have more enhanced powers and will be able to receive notices from citizens and act on its own initiative. Its competencies will be, however, limited to investigation on its own initiative and inspection of notices received, the commission will have no remedial power. According to the section 13 and 14 of the article 8a of the Act 166/2003[61] the Commission is on the first instance accountable to the respective Parliamentary Committee (Special Parliamentary Committee to Supervise Slovak Information Service Performance or Military Intelligence performance), which examines their report and if they find a discrepancy with the law they further report it to the National Council of the Slovak Republic and simultaneously to the Prosecutor General. According to the article 9, the National Council of the Slovak Republic is obliged to organize at least two meetings over the reports provided by the Special Commission and Parliamentary Committees in a year, the Act, however, does not specify any specific remedies the National Council can use. These are most likely in the capacity of the Prosecutor General. The commission is

[61] Slovakia, Act No. 166/2003 on the protection of privacy against unauthorised use of information-technological tools that amends certain laws (Zákon 166/2003 z. z. zákon o ochrane pred odpočúvaním) from 21st May 2003)

14

established pursuant to the Act no. 404/2015 Coll.[62] and will initiate its oversight on 1st January 2017.[63]

2.2.2 Composition

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia not mentioned.
The members of the parliamentary oversight bodies are appointed by the parliament from the members of the National Council of the Slovak Republic.

2.2.3 Access to information and documents

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia not mentioned, no specific situation relevant for the analysis.
According to the section 1 of the article 34 of the Act no. 215/2004 Coll. on the protection of confidential information a) the President of the Slovak Republic, b) members of the National Council of the Slovak Republic, c) a member of the Slovak Government, d) a judge of the Constitutional Court of the Slovak Republic, e) The President and Vice-Presidents of the Supreme Audit Office of the Slovak Republic, f) a judge, or g) members of the Judicial Board with respect to determination of prerequisites for judicial competence can access the classified information.[64] The members of the parliamentary oversight committees are always appointed from the members of the Slovak Parliament, they are not requested to pass any security clearance and can automatically access the classified information if their position in one of the oversight body entitles them to. Whereas the already established "old" oversight bodies, mainly the Special Parliamentary Committee to Supervise Slovak Information Service Performance or Military Intelligence performance are entitled to access the information related to the administrative aspects of the Intelligence services, such as its statute, budget allocation, internal guidelines or annual reports (article 5 of the Act 46/1993[65]), the newly forming Special Commission has wider competencies and will be

[62]Slovakia, Act No. 404/2015 amending and supplementing Act No. 166/2003 Coll. on the protection of privacy against unauthorised use of information-technological tools and on amendment of certain laws (Act on protection against eavesdropping) (*Zákon, ktorým sa mení a dopĺňa zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technickýchprostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov*) from 19 December 2015.
[63]Denník N (2016), 'Môže byť Galko v komisii na kontrolu odposluchov? Šebej hovorí, že nikdy', 4 May 2016, available at https://dennikn.sk/451302/moze-byt-galko-komisii-kontrolu-odposluchov-sebej-hovori-ze-nikdy/

[64]Slovakia, Act of the National Council of the Slovak Republic No. 215/2004 Coll. on the protection of confidential information (*Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností*)
[65] 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*) from 21 January 1993.

entitled to access the information produced in relation to Intelligence activities in the field of information-technological measures, which includes the access to classified information such as the evidence of information-technological means for a respective period or information on termination of the records. These classified information can be accessed, however handled with the highest caution and any written notes taken based on access to these information shall remain and be stored in the intelligence building under protection (articles 7 - 9 of the Act 404/2015[66]).

2.2.3 Reporting to parliament

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia not mentioned, no specific situation relevant for the analysis.

2.3 Expert oversight

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia not mentioned.

2.3.1 Specialised expert bodies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia mentioned, information only partially correct.

In Slovakia, there are no expert oversight bodies up to this date. However, the newly forming Special Commission of the National Council to supervise the use of information-technological tools[67] could be assessed as a quasi-expert oversight body. The Commission shall consist of 6 parliamentary members and 2 expert members.

[66] Slovakia, Act No. 404/2015 amending and supplementing Act No. 166/2003 Coll. on the protection of privacy against unauthorised use of information-technological tools and on amendment of certain laws (Act on protection against eavesdropping) (*Zákon, ktorým sa mení a dopĺňa zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technickýchprostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov*) from 19 December 2015.

[67] Slovakia, Act No. 166/2003 on the protection of privacy against unauthorised use of information-technological tools and on amendment of certain laws (Act on protection against eavesdropping) (*Zákon, ktorým sa mení a dopĺňa zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technickýchprostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov*) from 19 December 2015, Article 8a.

16

According to the article (8a), the Commission should consist of three deputies from governmental coalition, three from opposition and two independent expert members chosen by the parliament. The two independent experts must be over 40 years old and have a career background of a policeman, prosecutor, judge, or in intelligence services profession of legal and security theory and practice or international relations and diplomacy, for at least ten years. They also have to have the most stringent review of the National Security Authority at the top secret level.[68] Parliamentary Members do not need any clearance.[69] The name of the two experts are not yet know, however, their presence in the Commission will practically change its statute from parliamentary oversight to combined parliamentary and expert oversight.

The commission has the power to inspect decisions to deploy information-technological tools and issue protocols on the results of such inspections[70]. The commission subsequently submits the inspection protocols along with the minutes of discussing them within the commission to the applicable parliamentary committee. It is still not known whether these documents could be accessed by public since this issue will be a matter of internal guidelines that are not yet formulated[71]. If the committee finds out the facts that might indicate violations of Act no.166/2003 Coll., it informs the parliament's president and the attorney general about them. The commission is entitled to submit a report on its findings twice a year to be discussed by the National Council. This report shall contain information on every single case of violation of rights by using information-technological tools. Findings of the report may be published by the media however they may not reveal any confidential (classified) information[72]. The law also stipulates that submitting individual complaint to the commission does not limit in any way the aggrieved party's right to seek judicial remedy or other means of protection[73].

2.3.2 Data protection authorities

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

[68] Slovakia, Act No. 404/2015 Coll. amending and supplementing Act No. 166/2003 Coll. on the protection of privacy against unauthorised use of information-technological tools and on amendment of certain laws (Act on protection against eavesdropping) (*Zákon, ktorým sa mení a dopĺňa zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane predodpočúvaním) v znení neskorších predpisov*) from 19 December 2015.

[69] Denník N (2016),'Môže byť Galko v komisii na kontrolu odposluchov? Šebej hovorí, že nikdy', 4 May 2016, available at: https://dennikn.sk/451302/moze-byt-galko-komisii-kontrolu-odposluchov-sebej-hovori-ze-nikdy/

[70] Slovakia, Act no. 166/2003 on the protection of privacy against unauthorised use of information-technological tools that amends certain laws (*Zákon č. 166/2003 Z.z. o ochrane súkromia pred neoprávneným použitím informačno technologických prostriedkov*), from 21 May 2003, Article 8a, Paragraph 13.

[71] Information has been provided by National Council of Slovak Republic on 15 June 2016.

[72] Slovakia, Act no. 166/2003 on the protection of privacy against unauthorised use of information-technological tools that amends certain laws (*Zákon č. 166/2003 Z.z. o ochrane súkromia pred neoprávneným použitím informačno technologických prostriedkov*), from 21 May 2003, Article 9.

[73] Slovakia, Act no. 166/2003 on the protection of privacy against unauthorised use of information-technological tools that amends certain laws (*Zákon č. 166/2003 Z.z. o ochrane súkromia pred neoprávneným použitím informačno technologických prostriedkov*), from 21 May 2003,Article 8a, Paragraph 15.

Slovakia mentioned, information provided is correct.
The DPA in Slovakia has not power over the intelligence services.

2.4 Approval and review of surveillance measures

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia mentioned, information provided is correct.

FRA key findings

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia not mentioned, no specific situation relevant for the analysis.

3 Remedies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The standard of protecting individuals' rights and remedy in the case of violating these rights is relatively low in the Slovak Republic as the country only has parliamentary oversight bodies established. Other government institutions and agencies that provide oversight of fundamental rights implementation such as, for instance, Data Protection Authority of the Slovak Republic and Office of the Public Defender of Rights (i.e. ombudsman) do not have any powers whatsoever with respect to intelligence services. Slovakia does not have any expert oversight body, either. While the parliament's oversight bodies provide oversight of intelligence services' performance in the field of surveillance, they do not have any power of remedy in individual cases of violating fundamental rights. The only option for the individuals that seek remedy in concrete cases of violation is to turn to courts of justice; however, it is fair to question the effectiveness and sufficiency of this remedy given the overall condition of Slovakia's judicial system and the current quality of Slovak courts' decision-making.

3.1 A precondition: obligation to inform and the right to access

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The observation made in FRA Report,[74] i.e. that the obligation to information and the right to access is not provided, continues to apply to the Slovak Republic. Intelligence services are not required to inform individuals that they are being subjected to surveillance before, during or after the surveillance operation. Similarly, individuals do not have the right to access data and information that are being gathered on them by intelligence services.

The Data Protection Authority of the Slovak Republic does not have any powers to interfere in any way with surveillance operations as performed by intelligence services. The office does not have any binding power that would entitle it to instruct intelligence services to inform individuals that they have been, are being or will be subjected to surveillance or to allow them to access the data gathered during surveillance operations. The Office of the Public Defender of Rights (i.e. ombudsman) lacks this kind of power as well.

According to valid laws, the Slovak Information Service has the right to process personal data and to request such data from other public organs that are obliged to provide them to it. The persons in question are not informed that their personal data are being gathered and processed.[75]The SIS gathers and processes these data through its information systems; the details regarding protection of these data, the regime of accessing them and the way of authorising their disclosure and provision are regulated by an internal decree issued by the SIS director.[76]

Like the SIS, the Military Intelligence also has the right to process personal data and to request such data from other public organs that are obliged to provide them; in this case, however, the valid law does not regulate any regime of accessing these data. As a result, the person in question is not informed that it is being subjected to surveillance and has no right to request access to these data.

The Act no. 46/1993[77] and the Act no. 198/1994[78] under article 17, section 9, specifies, that the information held by the Slovak Information Service are exempt from the

[74]FRA (2015), *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU*, p. 62.
[75]Slovakia, Act No. 46/1993 Coll. on Slovak Information Service, Article 15, from 15 February 1993, Paragraph 2.
[76]Slovakia, Act No. 46/1993 Coll. on Slovak Information Service, Article 17, from 15 February 1993, Paragraph 8.

[77] 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*) from 21 January 1993

[78] 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*), from 30 June 1994.

entitlements governed by the Act no. 211/2000 on free access to information[79] and the Act no. 428/2002 on personal data protection.[80] Thus the individuals cannot approach these bodies with request to access to classified information.

The only exception when valid laws stipulate the obligation to inform individuals that they have been subjected to surveillance is the situation when information-technological tools (e.g. wire-tapping devices) have been used against the person in question, either during criminal proceedings or during proceedings that preceded them, provided that the use of information-technological tools has not led to finding facts that would be relevant to criminal proceedings. In such a case, the obtained records must be destroyed and the protocol on destroying them must be made part of the criminal file.[81]The person in question must be informed of destroying the records by a police officer, a procurator or a judge. At the same time, the person in question must be informed of the right to demand examining legitimacy of the surveillance order as well as records of the telecommunications operator.[82]

3.2 Judicial remedies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Since existing oversight bodies do not have any remedial functions for the time being, judicial remedies are the only means of remedy currently available in the Slovak Republic.

According to information provided by the Slovak Information Service (SIS)[83], the regime to demand judicial remedies in cases involving surveillance has not been amended in the Slovak Republic over the past two years. Since the right to individuals' sanctity and privacy is guaranteed by the Slovak Constitution, these fundamental rights and freedoms can only be breached in the extent spelled out in Article 1, Paragraph 4 of Act no. 46/1993 Coll. on Slovak Information Service, as amended.

3.2.1 Lack of specialisation and procedural obstacles

[79]Slovakia, Act of the National Council of the Slovak Republic No. 211/2000 Coll on free access to information (Zákon č. 211/2000 Z. z. Zákon o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov) from 13th July 2000)

[80]Slovakia, Act of the National Council of the Slovak Republic No. 428/2002 Coll on personal data protection (*Zákon č. 122/2013 Z. z. Zákon o ochrane osobných údajov*) from 28 May 2013.

[81]Slovakia, Act No. 301/2005 Coll. (Code of Criminal Procedures), from 2 July 2005, Article 115, Paragraph 8.

[82]Slovakia, Act No. 301/2005 Coll. (Code of Criminal Procedures), from 2 July 2005, Article 115, Paragraph 9.

[83]This information was provided at request by the Slovak Information Service on 13 April 2016.

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia lacks courts or judges that would specialise in protection of personal data or protection of fundamental rights with respect to surveillance. Of all the activities and operations that fall within the realm of surveillance, only the use of so-called information-technological tools (e.g. wire-tapping devices) must be authorised by a court (either beforehand or, in justified cases, additionally), i.e. the applicable regional court or the Specialised Criminal Court, provided the matter falls within its sphere of competence[84]. Similarly, Slovakia lacks courts or judges that would specialise in matters related to gathering and processing personal data or performing surveillance.

In Slovakia there are no non-governmental organisations that would specialise in providing legal counselling or legally representing individuals in matters related to violation of fundamental rights in the process of performing surveillance.
In cases of violation of one's rights to privacy, individuals can complaint at the court in civil or criminal proceeding. In civil proceeding individual may object to violation of right to privacy under the Civil Code (mainly the part Protection of personality – sections 11-16)[85]. According to Civil Proceedings Code for Adversarial Proceedings the accusation submitted by the plaintiff shall also contain those evidence whose nature admits that they may be attached to the accusation[86]. The legislation does not stipulate any further details what kind of evidence shall be attached to the accusation. In the criminal proceeding provisions of the Criminal Code may be applied (section 194a, 374)[87]. The section 194a defines that privacy in dwellings is protected by the law and that collecting information about inhabitants of the dwelling by using the information-technological tools or other technical tools without consent of the person(s) concerned is prohibited. The section 374 on unauthorized handling of personal data says that personal data collected by public authorities, or within the exercise of employment or function may not be disclosed, made available or published.

3.2.2 Specialised judges and quasi-judicial tribunals

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

[84] Act No. 166/2003 Coll. on the protection of privacy against unauthorised use of information-technological tools that amends certain laws, from 21 May 2003, Article 4, Paragraph 1.
[85] Slovakia, Act No. 40/1964 Coll. Civil Code (*Zákon č. 40/1964 Z.z. Občiansky zákonník*) from 5 March 1964.
[86] Slovakia, Act No. 160/2015 Coll. Civil proceedings code for adversarial proceedings, from 17 July 2015, Article 132, Paragraph 3.
[87] Slovakia, Act No. 300/2005 Coll. Criminal Code (*Zákon č. 300/2005 Z.z. Trestný zákon*) from 2 July 2005.

21

Slovakia lacks specialised judges that would focus on cases with respect to performing surveillance. Similarly, there are no quasi-judicial tribunals that would adjudicate on practical issues related to performing surveillance.

3.3 Non-judicial remedies: independence, mandate and powers

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

None of the non-judicial oversight bodies established in Slovakia has a remedial function.

Parliamentary oversight bodies:

- **Special Parliamentary Committee to Supervise Performance of Slovak Information Service** – if the committee establishes violation of Act no. 46/1993 Coll. on Slovak Information Service, it must immediately report the violation to the National Council of the Slovak Republic and the Office of Attorney General of the Slovak Republic; depending on the nature of the violation, it may also report it to the Government of the Slovak Republic.[88] The committee does not have the mandate to deal with individual complaints.
- **Special Parliamentary Committee to Supervise Performance of Military Intelligence** – if the committee establishes violation of Act no. 198/1994 Coll. on Military Intelligence, it must immediately report the violation to the National Council of the Slovak Republic.[89] The committee does not have the mandate to deal with individual complaints.
- **Special Parliamentary Committee to Supervise Performance of National Security Authority** – if the committee establishes violation of Act no. 215/2004 Coll. on the protection of confidential information, it must immediately report the violation to the National Council of the Slovak Republic and the Office of Attorney General of the Slovak Republic; depending on the nature of the violation, it may also report it to the Government of the Slovak Republic.[90] The committee does not have the mandate to deal with individual complaints.
- **Special Commission of the National Council to supervise the use of information-technological tools**[91] - the commission has the power to deal with motions filed by individuals who suspect violations of their rights guaranteed by the Act no. 166/2003 Coll.[92]

[88]Slovakia, Act No. 46/1993 Coll. on Slovak Information Service, from 15 February 1993, Article 5, Paragraph 4.
[89]Slovakia, Act No. 198/1994 Coll. on Military Intelligence, from 9 August 1994, Article 5, Paragraph 4.
[90]Slovakia, Act No. 215/2004 on the protection of confidential information, from 27 April 2004 Article 72, Paragraph 3.
[91]Slovakia, Act No. 166/2003 on the protection of privacy against unauthorised use of information-technological tools that amends certain laws, from 21 May 2003 Article 8a, Paragraph 1.
[92]Ibid, Article 8a, Paragraph 6.

22

Other oversight bodies

Data Protection Authority of the Slovak Republic – this body does not have any supervisory powers or remedial functions with respect to intelligence services. According to the Act on the Protection of Personal Data, in case personal data are processed by intelligence services or the National Security Authority, the oversight with respect to personal data protection is provided by the National Council of the Slovak Republic in compliance with a special regulation.[93]

Office of the Public Defender of Rights (i.e. ombudsman)–according to the Act on Public Defender of Rights, the ombudsperson's sphere of competence does not include any government institutions and agencies including intelligence services.[94]

Expert oversight bodies are not established at all in the Slovak Republic.

3.3.1 Types of non-judicial bodies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Non-judicial bodies do not have a remedial function in the Slovak Republic. The Data Protection Authority of the Slovak Republic, the Office of the Public Defender of Rights and applicable parliamentary committees to provide oversight of intelligence services' performance do not have the power to accept individuals' complaints and issue decisions on the remedy of individual violations of fundamental rights in the process of performing surveillance.

The most recent change in the field of non-judicial bodies is the founding of a new special supervisory commission by the National Council of the Slovak Republic. By passing Act no. 404/2015 Coll. that amended Act no. 166/2003 Coll. on the protection of privacy against unauthorised use of information-technological tools, as amended, the parliament established the Commission of the National Council to supervise the use of information-technological tools.[95] The commission has the power to deal with motions filed by individuals who suspect violations of their rights guaranteed by the Act no. 166/2003 Coll.[96]

[93] Slovakia, Act no. 122/2013 on the protection of personal data, from 28 May 2013, Article 46, Paragraph 5; Slovakia, Act no. 215/2004 on the protection of confidential information, from 27 April 2004, Article 42, Paragraph 8.

[94] Slovakia, Act No. 564/2001 on Public Defender of Rights, from 23 December 2001, Article 3, Paragraph 2.

[95] Slovakia, Act No. 166/2003 on the protection of privacy against unauthorised use of information-technological tools that amends certain laws, from 21 May 2003, Article 8a, Paragraph 1.

[96] Ibid, Article 8a, Paragraph 6.

23

The commission has the power to inspect decisions to deploy information-technological tools and issue protocols on the results of such inspections[97]. The commission subsequently submits the inspection protocols along with the minutes of discussing them within the commission to the applicable parliamentary committee. It it is not known yet whether the protocols and minutes issued by the commission will be confidential or public, this issue will be a matter of internal guidelines that are not yet formulated[98].

If the committee finds out the facts that might indicate violations of Act no.166/2003 Coll., it informs the parliament's president and the attorney general about them. The commission is entitled to submit a report on its findings twice a year to be discussed by the National Council. This report shall contain information on every single case of violation of rights by using information-technological tools. Findings of the report may be published by the media however they may not reveal any confidential (classified) information.[99] The law also stipulates that submitting individual complaint to the commission does not limit in any way the aggrieved party's right to seek judicial remedy or other means of protection.[100] In other words, the law grants the commission a recommendation and information function rather than a remedial one.

3.3.2 The issue of independence

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

In Slovakia, the make-up of parliamentary oversight bodies largely depends on the actual make-up of the parliament because special committees established to supervise intelligence services and other security agencies comprise exclusively members of the National Council of the Slovak Republic.

The new Commission of the National Council to supervise the use of information-technological tools has eight members. Six of them are recruited from members of parliament, more concretely members of committees to supervise intelligence services and the Parliamentary Committee on Defence and Security. The remaining two commission members need not be members of parliament but they are elected by the assembly based on a joint proposal submitted by Parliamentary Committee on Defence and Security, Special Parliamentary Committee to Supervise Performance of Slovak Information Service and Special Parliamentary Committee to Supervise Performance of Military Intelligence.[101]

[97] Ibid, Article 8a, Paragraph 13.
[98] Based on the information sent by the National Council of the Slovak Republic on 15 June 2016.
[99] Slovakia, Act no. 166/2003 on the protection of privacy against unauthorised use of information-technological tools that amends certain laws (*Zákon č. 166/2003 Z.z. o ochrane súkromia pred neoprávneným použítím informačno technologických prostriedkov*), from 21 May 2003, Article 9.
[100] Ibid, Article 8a, Paragraph 15.
[101] Ibid, Article 8a, Paragraphs 2 and 3.

24

3.3.3 Powers and specialisation of non-judicial remedial bodies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*
   Please see subsection 3.3.

FRA key findings

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

In the case of Slovakia, it is important to note that the only situation when the person in question must be informed that it has been subjected to surveillance (or to deployment of information-technological tools) is when such tools have been deployed during criminal proceedings (or during proceedings that preceded them), provided that the use of information-technological tools has not led to finding facts that would be relevant to criminal proceedings (for further information please see Section 3.1).

While the recently established Commission of the National Council to supervise the use of information-technological tools has the right to deal with individual complaints, it is not authorised to inform the complainants whether they have been subjected to surveillance or not.

In Slovakia, the only way of legal remedy in cases of violating fundamental rights by subjecting individuals to surveillance is to turn to a court. Of various types of oversight bodies, Slovakia has only parliamentary ones and even they do not have the remedial function with respect to individual complaints.

Conclusions

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Slovakia not mentioned. No country specific information relevant for analysis.

1.5 Check the accuracy of the figures and tables published in the FRA report (see the annex on Figures and Tables)

1.5.1 Overview of security and intelligence services in the EU-28

- *Please, delete all lines not referring to your country in the table below (see Annex p. 93 of the FRA Report)*
- *Check accuracy of the data*
- *Add in track changes any missing information (incl. translation and abbreviation in the original language).*
- *Provide the reference to the national legal framework when updating the table.*

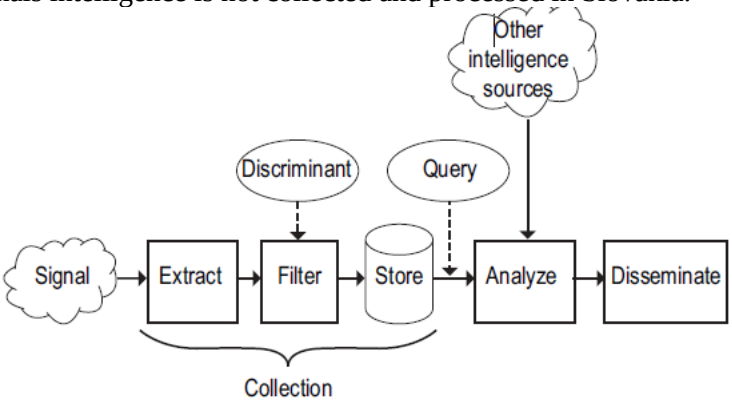
The information regarding Slovak intelligence services is correct.

	Civil (internal)	**Civil (external)**	**Civil (internal and external)**	**Military**
SK	National Security Authority/*Národný bezpečnostný úrad* (NBÚ)		Slovak Information Service/*Slovenská informačná služba*(SIS)	Millitary Intelligence/*Vojenské spravodajstvo* (VS)

1.5.2 Figure 1: A conceptual model of signals intelligence

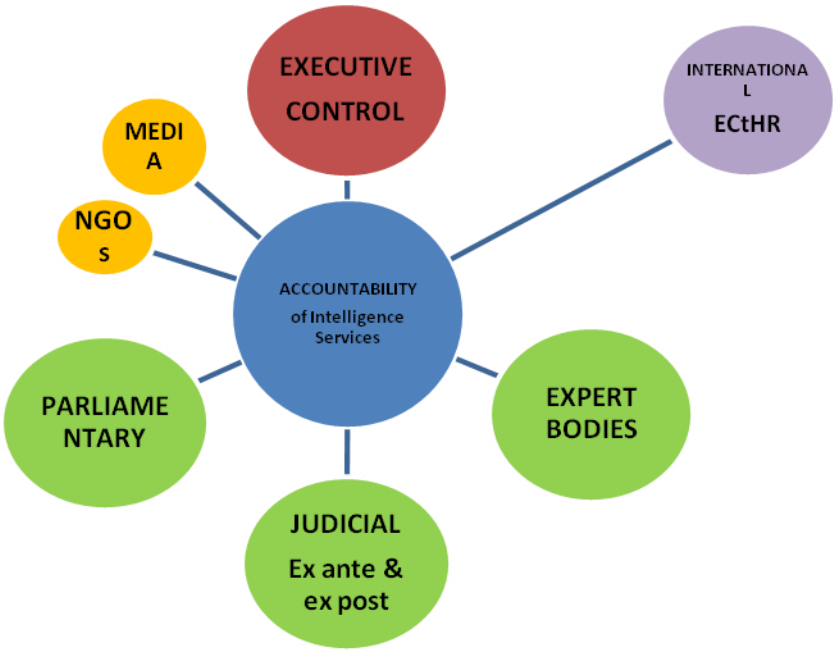
- *Please, provide a reference to any alternative figure to Figure 1 below (p. 16 of the FRA Report) available in your Member State describing the way signals intelligence is collected and processed.*

Signals intelligence is not collected and processed in Slovakia.



1.5.3 Figure 2: Intelligence services' accountability mechanisms

Please confirm that Figure 2 below (p. 31 of the FRA Report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

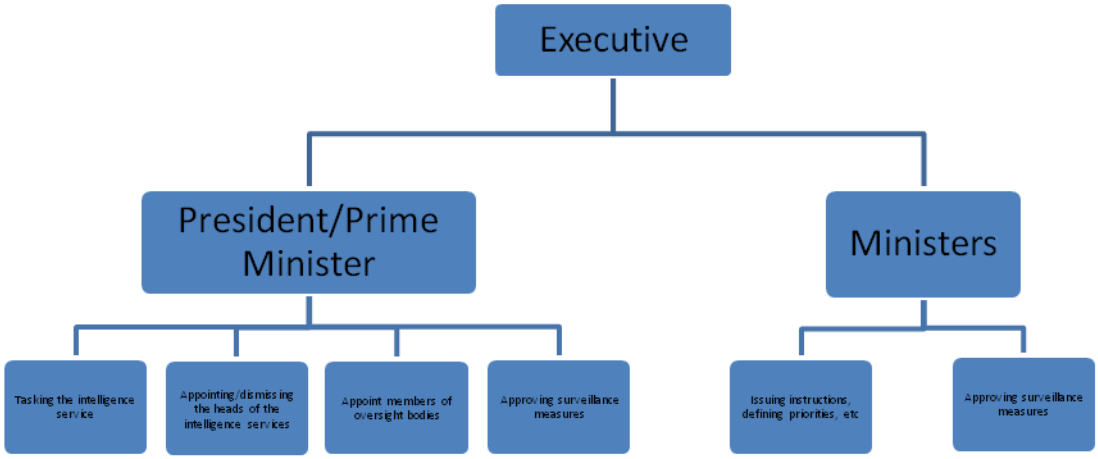


Expert bodies are not established in Slovakia. The new parliamentary Commission to Supervise the Use of Information-Technological Tools might be considered as a quasi-expert body since it consists not only of members of parliament but also of two experts.

1.5.4 Figure 3: Forms of control over the intelligence services by the executive across the EU-28

Please confirm that Figure 3 below (p. 33 of the FRA Report) properly captures the executive control over the intelligence services in your Member State. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

The information in Figure 3 refers to the situation in Slovakia properly except of the point that the president/prime minister appoints members of oversight bodies since there are only parliamentary oversight bodies whose members are appointed by the parliament.



1.5.5 Table 1: Categories of powers exercised by the parliamentary committees as established by law

Please, delete all lines not referring to your country in the table below (see p. 36 of the FRA Report)
Please check the accuracy of the data. Please confirm that the parliamentary committee in your Member State was properly categorised by enumerating the powers it has as listed on p. 35 of the FRA Report. Please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

Slovak parliamentary oversight bodies have essential powers beside the new Commission to Supervise the Use of Information-Technological Tools that can receive individual complaints and issue recommendations.

Member States	Essential powers	Enhanced powers
SK	X	

Note: Finland, Ireland, Malta and Portugal do not have parliamentary committees that deal with intelligence services.

1.5.6 Table 2: Expert bodies in charge of overseeing surveillance, EU-28

Please, delete all lines not referring to your country in the table below (p. 42 of the FRA Report). Please check the accuracy of the data. In case of inaccuracy, please suggest

any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

The information is correct however the new Commission to Supervise the Use of Information-Technological Tools might be considered as a quasi-expert body since two members of the commission are not members of parliament but experts.

EU Member State	Expert Bodies
SK	N.A.

1.5.7 Table 3: DPAs' powers over national intelligence services, EU-28

Please, delete all lines not referring to your country in the table below (p. 49 of the FRA Report). Please check the accuracy of the data. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

The information regarding the powers of the DPA in Slovakia is correct.

EU Member State	No powers	Same powers (as over other data controllers)	Limited powers
SK	X		

Notes: No powers: refers to DPAs that have no competence to supervise NIS.

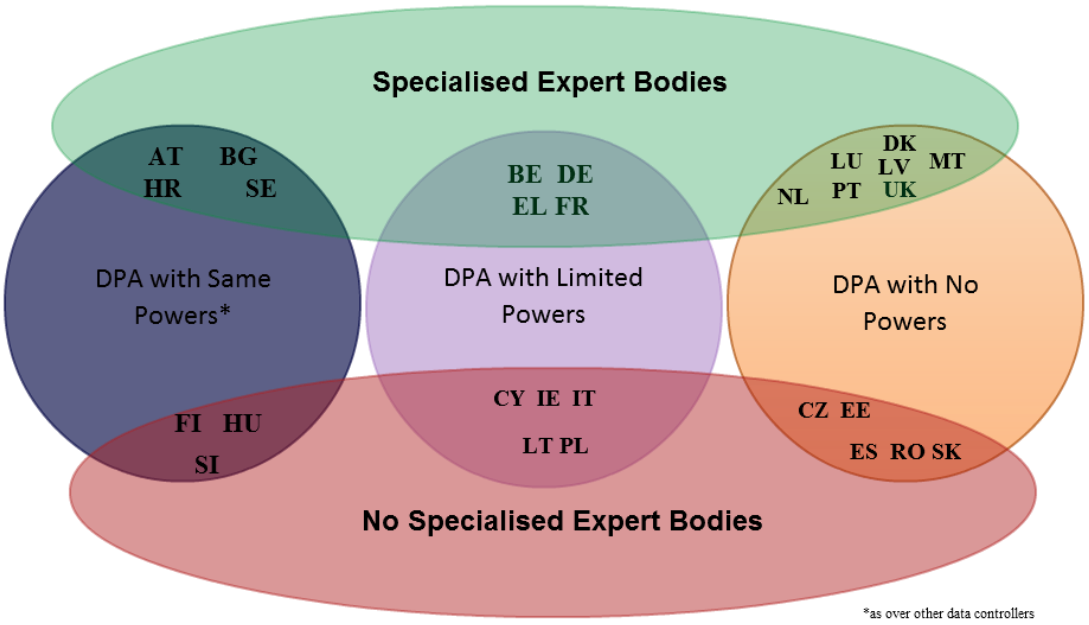
Same powers: refers to DPAs that have the exact same powers over NIS as over any other data controller.

Limited powers: refers to a reduced set of powers (usually comprising investigatory, advisory, intervention and sanctioning powers) or to additional formal requirements for exercising them.

1.5.8 Figure 4: Specialised expert bodies and DPAs across the EU-28

Please check the accuracy of Figure 4 below (p. 50 of the FRA Report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

The information regarding the situation in Slovakia is correct, however as we have mentioned in previous sections the new Commission to Supervise the Use of Information-Technological Tools might be considered as a quasi-expert body since two members of the commission are not members of parliament but experts.



1.5.9 Table 4: Prior approval of targeted surveillance measures, EU-28

Please, delete all lines not referring to your country in the table below (p. 52 of the FRA Report). Please check the accuracy of the data. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

The information regarding the situation in Slovakia is correct.

EU Member State	Judicial	Parliamentary	Executive	Expert bodies	None
SK	X				

1.5.10 Table 5: Approval of signals intelligence in France, Germany, the Netherlands, Sweden and the United Kingdom

Please check the accuracy of Table 5 below (p. 55 of the FRA Report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

The signals intelligence is not collected in Slovakia, the information is correct.

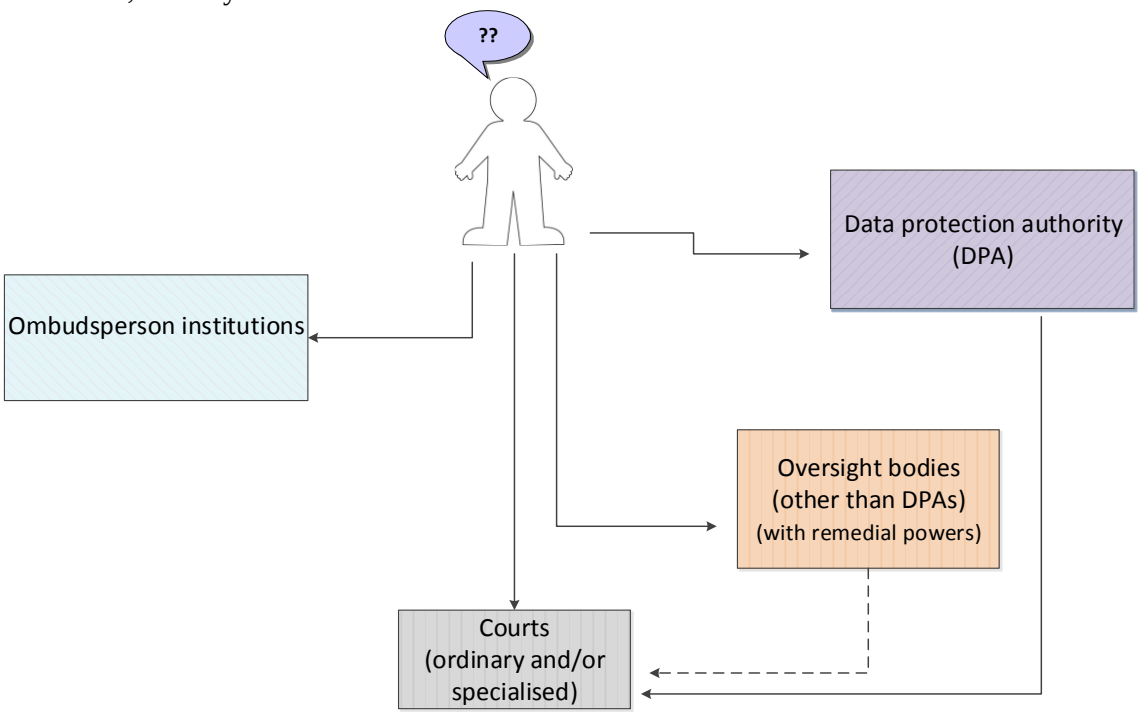
EU Member State	Judicial	Parliamentary	Executive	Expert
FR			X	
DE		X (telco relations)		X (selectors)

NL			X (selectors)	
SE				X
UK			X	

1.5.11 Figure 5: Remedial avenues at the national level

Please confirm that Figure 5 below (p. 60 of the FRA Report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

In Slovakia, the only remedial avenue is the court.



1.5.12 Figure 6: Types of national oversight bodies with powers to hear individual complaints in the context of surveillance, by EU Member States

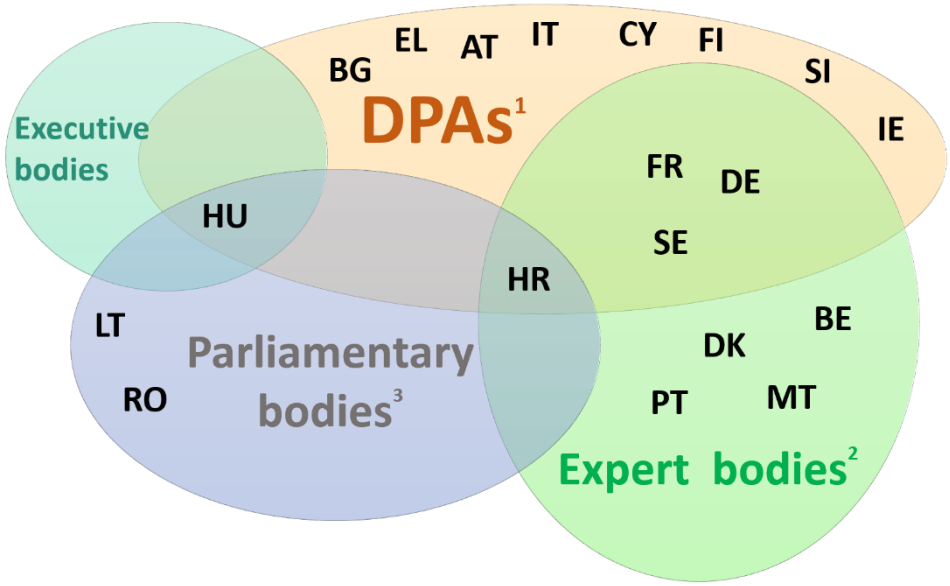
Please check the accuracy of Figure 6 (p. 73 of the FRA Report) below. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

The situation has changed in Slovakia since the new parliamentary Commission to Supervise the Use of Information-Technological Tools has the competence to receive individual complaints and issue recommendations. The commission has the power to deal with motions filed by individuals who suspect violations of their rights guaranteed by the Act no. 166/2003 Coll.[102]

[102]Slovakia, Act No. 166/2003 on the protection of privacy against unauthorised use of information-technological tools that amends certain laws (*Zákon č. 166/2003 Z.z. o ochrane súkromia pred neoprávneným použitím informačno technologických prostriedkov*), from 21 May 2003, Article 8a, Paragraph 6.

31

The commission has the power to inspect decisions to deploy information-technological tools and issue protocols on the results of such inspections[103]. The commission subsequently submits the inspection protocols along with the minutes of discussing them within the commission to the applicable parliamentary committee. If the committee finds out the facts that might indicate violations of Act no.166/2003 Coll., it informs the parliament's speaker and the attorney general about them. The commission is entitled to submit a report on its findings twice a year to be discussed by the National Council. This report shall contain information on every single case of violation of rights by using information-technological tools. Findings of the report may be published by the media however they may not reveal any confidential (classified) information[104]. The law also stipulates that submitting individual complaint to the commission does not limit in any way the aggrieved party's right to seek judicial remedy or other means of protection[105].



Notes: 1. The following should be noted regarding national data protection authorities: In Germany, the DPA may issue binding decisions only in cases that do not fall within the competence of the G 10 Commission. As for 'open-sky data', its competence in general, including its remedial power, is the subject of on-going discussions, including those of the NSA Committee of Inquiry of the German Federal Parliament

[103] Slovakia, Act No. 166/2003 on the protection of privacy against unauthorised use of information-technological tools that amends certain laws (*Zákon č. 166/2003 Z.z. o ochrane súkromia pred neoprávneným použitím informačno technologických prostriedkov*), from 21 May 2003, Article 8a, Paragraph 13.
[104] Slovakia, Act No. 166/2003 on the protection of privacy against unauthorised use of information-technological tools that amends certain laws (*Zákon č. 166/2003 Z.z. o ochrane súkromia pred neoprávneným použitím informačno technologických prostriedkov*), from 21 May 2003Article 9.
[105] Slovakia, Act No. 166/2003 on the protection of privacy against unauthorised use of information-technological tools that amends certain laws (*Zákon č. 166/2003 Z.z. o ochrane súkromia pred neoprávneným použitím informačno technologických prostriedkov*), from 21 May 2003, Article 8a, Paragraph 15.

32

2. *The following should be noted regarding national expert oversight bodies: In Croatia and Portugal, the expert bodies have the power to review individual complaints, but do not issue binding decisions. In France, the National Commission of Control of the Intelligence Techniques (CNCTR) also only adopts non-binding opinions. However, the CNCTR can bring the case to the Council of State upon a refusal to follow its opinion. In Belgium, there are two expert bodies, but only Standing Committee Ican review individual complaints and issue non-binding decisions. In Malta, the Commissioner for the Security Services is appointed by, and accountable only to, the prime minister. Its decisions cannot be appealed. In Sweden, seven members of the Swedish Defence Intelligence Commission are appointed by the government, and its chair and vice chair must be or have been judges. The remaining members are nominated by parliament.*
3. *The following should be noted regarding national parliamentary oversight bodies: only the decisions of the parliamentary body in Romania are of a binding nature.*