EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

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

November 2022 Update

Country: Slovakia

FRANET contractor: Centre for the Research of Ethnicity and Culture

Author(s) name(s): Ivana Rapoš Božič

Table of Contents

1. Summary

*FRANET contractors are requested to highlight in 1 page **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 snapshot of the evolution during the reporting period (mid-2016 until third quarter of 2022). It should mention:*

> *the most significant legislative reform/s that took place or are taking place and highlight the key aspect/s of the reform, focusing on oversight and remedies.*
> *relevant oversight bodies' (expert bodies (including non-judicial bodies, where relevant), data protection authorities, parliamentary commissions) reports/statements about the national legal framework in the area of surveillance by intelligence services.*

List of the different relevant reports produced in the context of FRA's surveillance project to be taken into account

FRA 2017 Report:
Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update

FRANET data collection for the FRA 2017 Report:
Country studies for the project on National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies - Legal update

Country studies for the project on National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies - Monthly data collection on the current reform of intelligence legislation (BE, FI, FR, DE, NL and SE)

FRA 2015 Report:
Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – mapping Member States' legal framework

FRANET data collection for the FRA 2015 Report:
Country studies for the project on National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

*FRANET contractors are requested to highlight in 1 page **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 snapshot of the evolution during the reporting period (mid-2016 until third quarter of 2022). It should mention:*

> *the most significant legislative reform/s that took place or are taking place and highlight the key aspect/s of the reform, focusing on oversight and remedies.*
> *relevant oversight bodies' (expert bodies (including non-judicial bodies, where relevant), data protection authorities, parliamentary commissions) reports/statements about the national legal framework in the area of surveillance by intelligence services.*

Since mid-2016, there have been only few legal developments concerning the activities of Slovak intelligence services, including the Slovak Information Service, the Military Intelligence and the National Security Authority.

The most significant development concerns the draft of the Act on Military Intelligence that was prepared by the Ministry of Defence with the intention to replace the currently effective Act No.

198/1994 Coll. on Military Intelligence[1]. The draft of the new Act on Military Intelligence (LP/2022/385) entered the legislation process in May 2022 and is currently in the stage of governmental proceedings[2]. As the Ministry of Defence states in the explanatory memorandum, the aim of the new Act on Military Intelligence is to create a legislative framework that will enable the Military Intelligence to perform its tasks more efficiently and to carry out intelligence and security measures to an extent that corresponds to the requirements of the current security environment. The draft act thus mostly reacts to new types of threats, such as hybrid threats, cybernetic attacks, and disinformation, and strengthens the competencies of Military Intelligence when tackling them.

When it comes to oversight, the Articles 11-14 of the draft act specify the oversight competencies of the main oversight body, the National Council of the Slovak Republic. More specifically, the Articles 11-13 specify that the oversight is performed by the Special Commission of the National Council of the Slovak Republic to Control the Activities of the Military Intelligence. The Article 11 specifies the procedural aspects of the oversight performed by this commission, including the processes surrounding the nomination and replacement of its members and the frequency of its meetings. The Article 12 details the requirements for an annual report and other documents that should be submitted to this commission on an annual basis. The Article 13 details the competencies and obligations of the members of this commission. What is more, the Article 14 specifies that the oversight of the use of information-technical means by the Military Intelligence is carried out by the National Council of the Slovak Republic in accordance with the provisions of Act No. 166/2003 Coll. on the protection of privacy against unauthorized use of information-technical means[3], which in practice means that this type of oversight is carried out by a different commission, namely by the Special Commission of the National Council to Control the Use of Information-technological Tools.[4] All of this can be seen as an improvement, as the original Act No. 198/1994 Coll. on Military Intelligence does not detail the oversight competencies of the Special Commission of the National Council of the Slovak Republic to Control the Activities of the Military Intelligence nor does it specify the legal framework within which the oversight of the use of information-technical means should be performed. As of 11 November 2022, no public statements have been made by the experts, civil society actors, or media concerning the effects of the proposed provisions on fundamental rights.

The second legal development concerns the Act No. 312/2020 Coll. on the execution of a decision on the seizure of property and the administration of seized property and amending and supplementing certain laws.[5] This Act changed the formulation of the Article 115 of the Act No. 301/2005 Coll. the Criminal Procedure Code,[6] which specifies the conditions under which a court can issue an approval for the use of information-technical means as well as the conditions under which the evidence obtained via such means can be used in a criminal case. In line with this amendment, evidence obtained via information-technical means can be used also in other criminal cases than the criminal case for which the court order was originally issued as long as there is a subject matter of the proceedings in the form of an exhaustively specified criminal offences listed in the provisions of Article 115, Section 1 of the Criminal Procedure Code[7]. The Article 115, Section 1 specifies that "criminal proceedings concerning crime, corruption, the crime of extremism, the crime of abuse of authority of a public official, the crime of laundering the proceeds of crime pursuant to Articles 233 and 234 of the Criminal Code, or for any other intentional criminal offence which is subject to an international treaty, a warrant may be issued

[1] Slovakia, Act of the National Council of the Slovak Republic No. 198/1994 Coll. on Military Intelligence (*Zákon o vojenskom spravodajstve*), 30 June 1994.
[2] Slovakia, draft Act no. LP/2022/385 on Military Intelligence (*Zákon o Vojenskom spravodajstve*).
[3] Slovakia, Act No. 166/2003 Coll. on the protection of privacy against unauthorised use of information-technological tools that amends certain laws *(Zákon č. 166/2003 Z.z. o ochrane pred odpočúvaním)*, 24 April 2003.
[4] Slovakia, draft Act no. LP/2022/385 on Military Intelligence (*Zákon o Vojenskom spravodajstve*), Articles 11-14.
[5] Slovakia, Act No. 312/2020 Coll. on the execution of a decision on the seizure of property and the administration of seized property and amending and supplementing certain laws *(Zákon č. 312/2020 Z.z. o výkone rozhodnutia o zaistení majetku a správe zaisteného majetku a o zmene a doplnení niektorých zákonov)*, 21 October 2020.
[6] Slovakia, Act No. 301/2005 Coll. Code of Criminal Procedure (*Zákon č. 301/2005 Z.z. Trestný poriadok*), 24 May 2005.
[7] Slovakia, Act No. 301/2005 Coll. Code of Criminal Procedure (*Zákon č. 301/2005 Z.z. Trestný poriadok*), 24 May 2005, Article 115, Section 7.

for the interception and recording of telecommunication traffic if it can be reasonably assumed that facts relevant to the criminal proceedings will be ascertained".[8] Prior to this amendment, the conditions under which (and if at all) the evidence obtained via information-technical means could be used for other criminal cases were not clear[9].

There have been no legal developments with respect to the Act No. 46/1993 Coll. on the Slovak Information Service[10] that provides the main legal framework for the operation of this intelligence service. This act has been lately subjected to severe criticism from the experts, civil society actors, and media who repeatedly pointed out that it is outdated. The main grounds for critique concern insufficient legal basis for control and oversight of the activities of the Slovak Information Service, particularly when it comes to the use of information-technical means[11]. Some of the deficiencies of the oversight of the use of information-technical means by the Slovak Information Service attracted public attention as a part of a highly medialized case of interception, that took place in 2005 and 2006 under the code name "Gorilla". The Slovak Information Service obtained a court warrant to install an interception device to a flat owned by a crime suspect. However, the interception device recorded conversations of several other persons whose interception was not substantiated by a warrant. The recording from the interception was retained by the Slovak Information Service and it later leaked to the public. One of the people affected by the interception later turned to The European Court of Human Rights with the application to examine the legality of the interception by the Slovak Information Service. On June 23, 2022, The European Court of Human Rights issued a judgement, holding that "there has been a violation of Article 8 of the Convention on account of the implementation of the two warrants and the retention by the SIS of the derivative material from their implementation ".[12]

What is more, even though the Act No. 404/2015 Coll[13] that amended and supplemented the Act No. 166/2003 Coll.[14] on the protection of privacy against unauthorised use of information-technological tools set the legal framework for creation of a new oversight body - Special Commission of the National Council to Control the Use of Information-technological Tools[15] in relation to both the Military Intelligence and the Slovak Information Service – as of 11 November 2022, this special commission has not yet been created and still does not perform its oversight function. The governmental body responsible for the creation of this special commission is the National Council of the Slovak Republic.

Based on the information made available by media, all up to date attempts to create the Special Commission of the National Council to Control the Use of Information-technological Tools failed on the lack of political agreement on the selection of its members from among the representatives of the governmental and oppositional political parties. According to the information made available by the media, the concerns were related mainly to the trustworthiness of the nominated candidates and their

[8] Slovakia, Act No. 301/2005 Coll. Code of Criminal Procedure (*Zákon č. 301/2005 Z.z. Trestný poriadok*), 24 May 2005, Article 115, Section 1,
[9] Marr, S. (2021), "Aktuálne zmeny právnej úpravy odpočúvania v trestnom konaní a pár kritických poznámok k zákonu o ochrane pred odpočúvaním". Published on 24 April 2021.
[10] Slovakia, Act of the National Council of the Slovak Republic No. 46/1993 Coll., on the Slovak Information Service (*Zákon č. 46/1993 Z.z. o Slovenskej informačnej službe*), 21 January 1993.
[11] Valček, A. (2022), "SIS chýba kontrola a nie je to v poriadku, znie opäť z medzinárodného súdu", published on 24 June 2022.
[12] European Court of Human Rights (ECtHR), *HAŠČÁK v. SLOVAKIA*, No. 58359/12, 23 June 2022.
[13] Slovakia, Act No. 404/2015 Coll. amending and supplementing the 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*), 19 December 2015.
[14] Slovakia, Act No. 166/2003 Coll. on the protection of privacy against unauthorised use of information-technological tools that amends certain laws (*Zákon č. 166/2003 Z.z. o ochrane pred odpočúvaním*), 21 May 2003.
[15] For detailed discussion about the intended role and competencies of the Comission see the National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies - Legal update for Slovakia, pp. 3-4.

ability to keep the information classified.[16] There are no publicly available information about the selection of the two politically independent experts who should also be part of this special commission and it is, consequently, not clear whether they have already been selected or not. The National Council of the Slovak Republic is currently not able to provide any details concerning the expected time frame of the creation of the Special Commission of the National Council to Control the Use of Information-technological Tools or to further specify its competences[17].

There is no publicly available information concerning the reactions of the Slovak government to the revelations connected to the Pegasus spyware. None of the public officials has issued any public statement on the issue, nor there have been any measures officially announced by the government. We further requested information from the National Council of the Slovak Republic, which is responsible for the oversight over intelligence services, the Office of the Government of the Slovak Republic, Ministry of Interior, and the Ministry of Justice. The National Council of the Slovak Republic stated that it has "not yet received the final version of the final report of the European Parliament's Committee of Inquiry into the use of Pegasus and equivalent surveillance spyware (established by the European Parliament's decision of 10 March 2022)" and that it "does not have the investigative powers to respond to any findings of the Committee of Inquiry at this stage"[18]. The Office of the Government of the Slovak Republic stated that it did not adopt any actions[19]. Similarly, the Ministry of Interior and the Ministry of Justice also replied to the information request by stating they have not taken any actions[20] [21].

2. Annexes- Table and Figures

2.1. Overview of security and intelligence services in the EU-27

FRANET contractors are requested to check the accuracy of the table below (see Annex pp. 93 - 95 of the FRA 2015 report) and correct or add in track changes any missing information concerning security and intelligence services in their Member State (incl. translation and abbreviation in the original language). Please provide the full reference in a footnote to the relevant national law substantiating all the corrections and/or additions made in the table.

The table below accurately represents the situation in Slovakia as of 11.11.2022.

	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)

[16] Press Agency of the Slovak Republic (TASR) (2021), "Niektorí môžu vynášať utajované informácie, zloženie komisie na kontrolu odposluchov sa má menit", published on 23 October 2021.
[17] Information provided on request by the National Council of the Slovak Republic (*Národná rada SR*) on 10 November 2022.
[18] Information provided on request by the National Council of the Slovak Republic (*Národná rada SR*) on 10 November 2022.
[19] Information provided on request by the Office of the Government of the Slovak Republic (*Úrad vlády SR*) on 24 November 2022.
[20] Information provided on request by the Ministry of Interior of the Slovak Republic (*Ministerstvo vnútra SR*) on 22 November 2022.
[21] Information provided on request by the Ministry of Justice of the Slovak Republic (*Ministerstvo spravodlivosti SR*) on 24 November 2022.

2.2. EU Member States' legal framework on surveillance reformed since 2017

In order to update the map below (Figure 1 (p. 20) of the FRA 2017 report), FRANET contractors are requested to state:

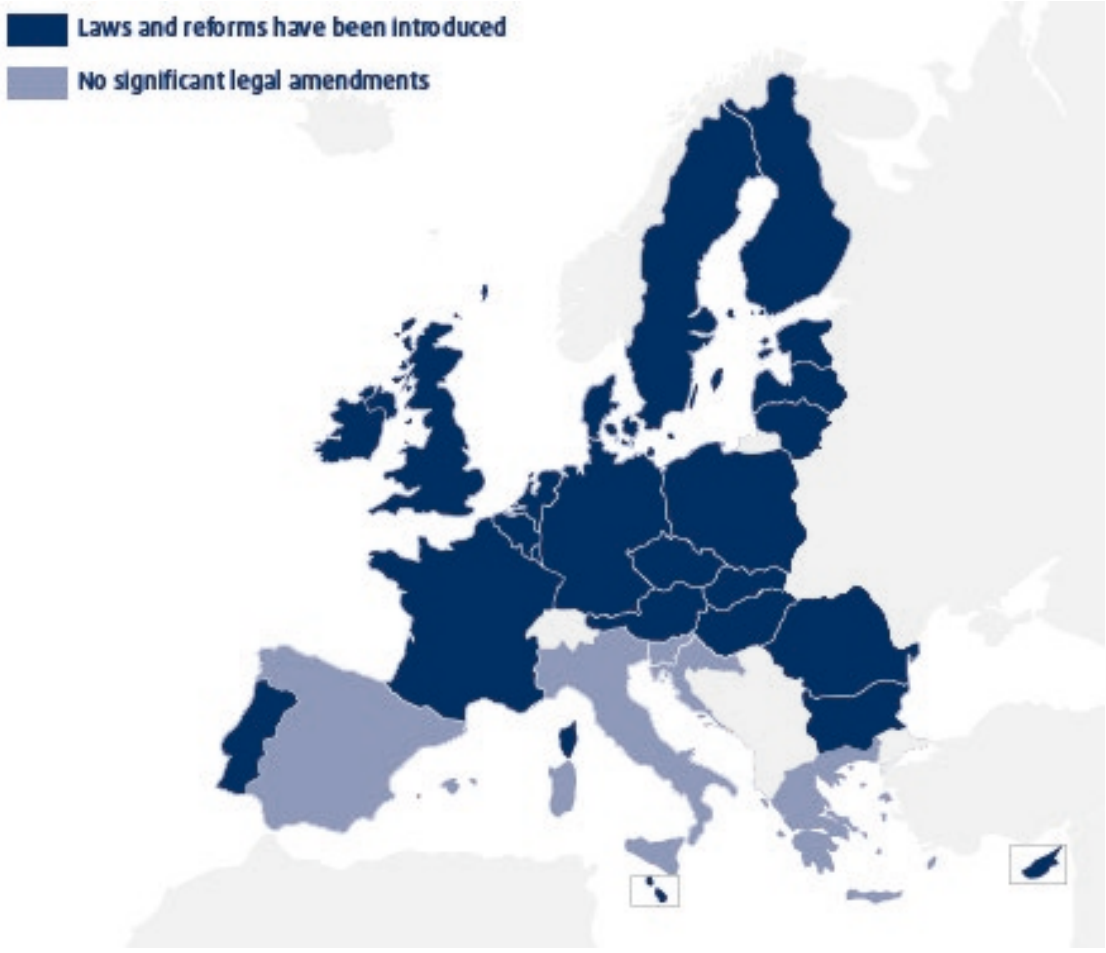
1. *Whether their legal framework on surveillance has been reformed or is in the process of being reformed since **mid-2017** – see the Index of the FRA 2017 report, pp. 148 - 151. Please do not to describe this new legislation but only provide a full reference.*

The map below (Figure 1 (p. 20) of the FRA 2017 report) accurately represents the situation in Slovakia as of 11 November 2022. The draft of the new Act on Military Intelligence (LP/2022/385) entered the legislation process in May 2022 and is currently in the stage of governmental proceedings[22].

2. *whether the reform was initiated in the context of the PEGASUS revelations.*

The draft of the new Act on Military Intelligence was not designed in response to the Pegasus revelations. According to the publicly available information, there have not been any legal developments in response to the Pegasus revelations in Slovakia as of 11 November 2022.

Figure 1: EU Member States' legal frameworks on surveillance reformed since October 2015



2.3. Intelligence services' accountability scheme

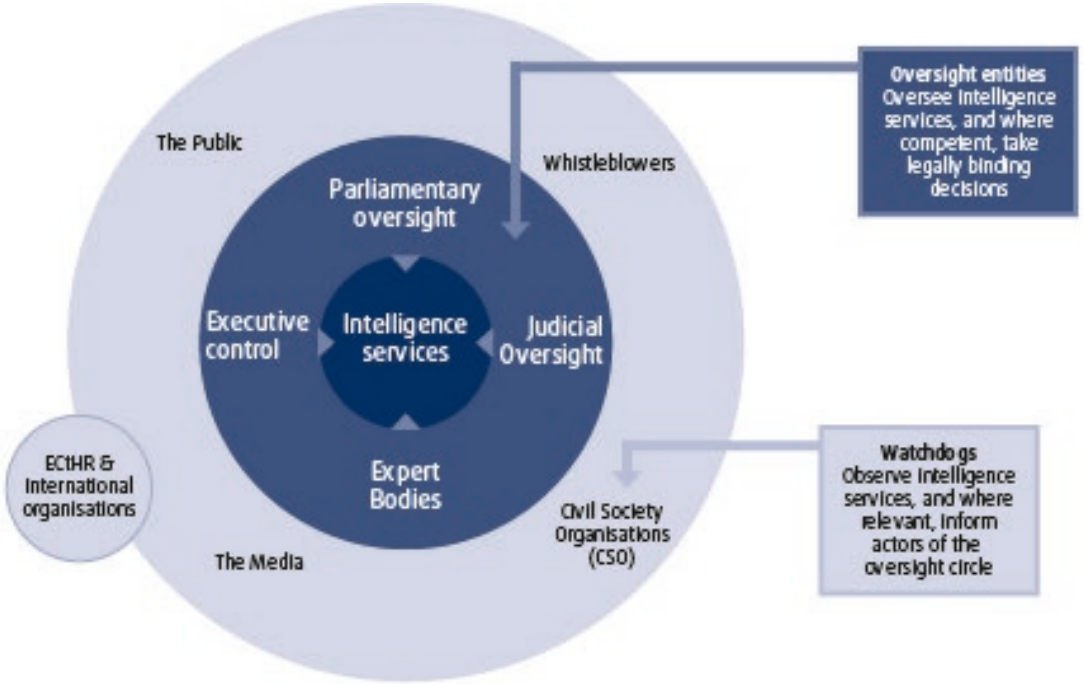
FRANET contractors are requested to confirm whether the diagram below (Figure 5 (p. 65) of the FRA 2017 report) illustrates the situation in your Member State in an accurate manner. If it is not the case,

[22] Slovakia, draft Act no. LP/2022/385 on Military Intelligence (*Zákon o Vojenskom spravodajstve*).

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

The diagram below (Figure 5 (p. 65) of the FRA 2017 report) does not accurately represent the situation in Slovakia as there are no expert bodies responsible for oversight or control of intelligence services.

Figure 5: Intelligence services' accountability scheme

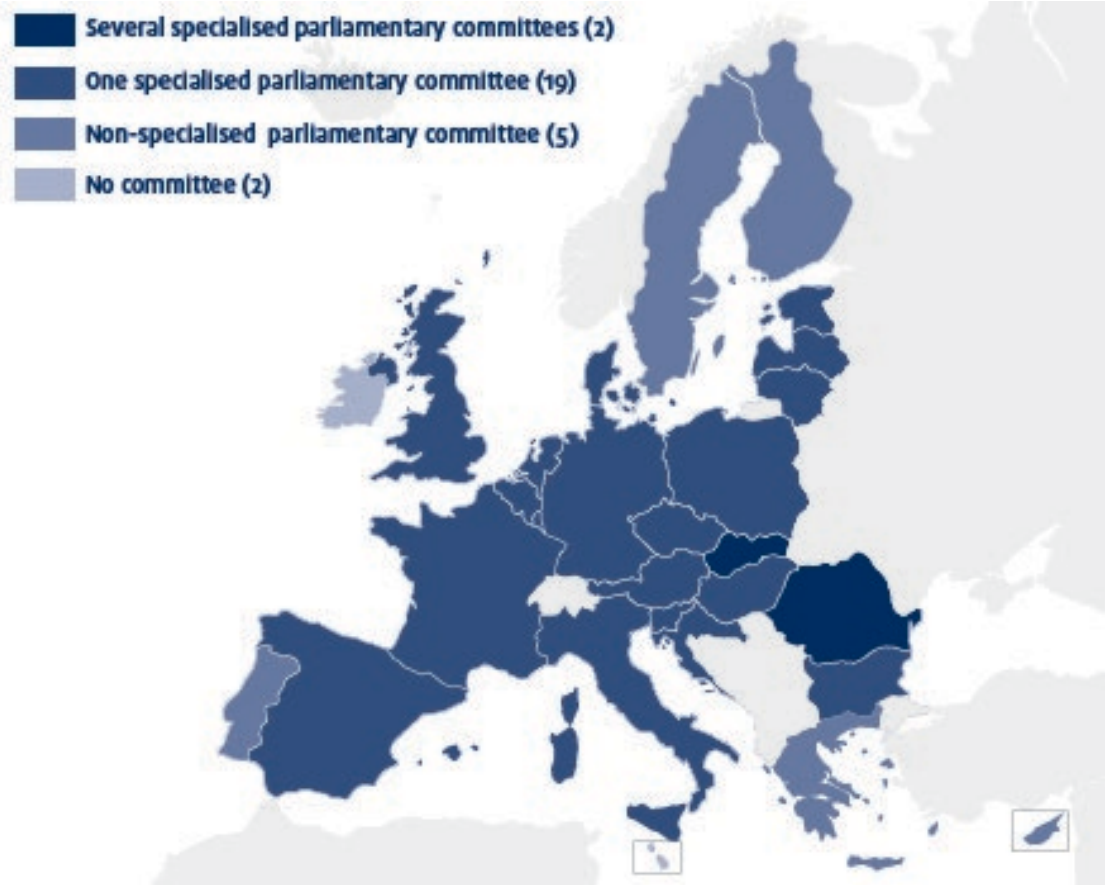


2.4. Parliamentary oversight of intelligence services in EU Member States

FRANET contractors are requested to confirm that the map below (Figure 6 (p. 66) of the FRA 2017 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.

The map below (Figure 6 (p. 66) of the FRA 2017 report) accurately represents the situation in Slovakia as of 11 November 2022.

Figure 6: Parliamentary oversight of intelligence services in EU Member States



2.5. Expert bodies (excluding DPAs) overseeing intelligence services in the EU

FRANET contractors are requested to check the accuracy of the table below (Table 2 (p. 68) of the FRA 2017 report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

The table below (Table 2 (p. 68) of the FRA 2017 report) accurately represents the situation in Slovakia as of 11 November 2022.

Table 2: Expert bodies (excluding DPAs) overseeing intelligence services in the EU

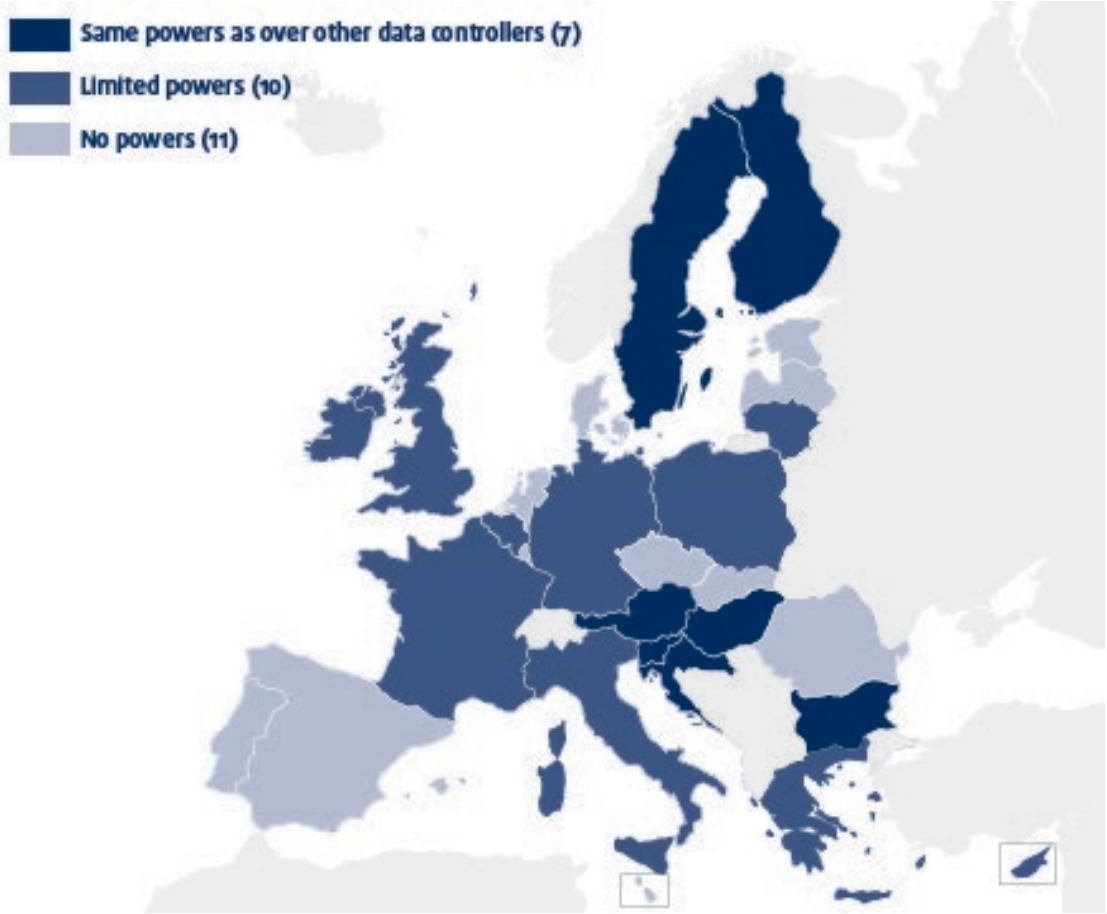
EU Member State	Expert Bodies
SK	N.A.

2.6. DPAs' powers over national intelligence services, by member states

FRANET contractors are requested to confirm that the map below (Figure 7 (p. 81) of the FRA 2017 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.

The map below (Figure 7 (p. 81) of the FRA 2017 report) accurately represents the situation in Slovakia as of 11 November 2022.

Figure 7: DPAs' powers over national intelligence services, by member states

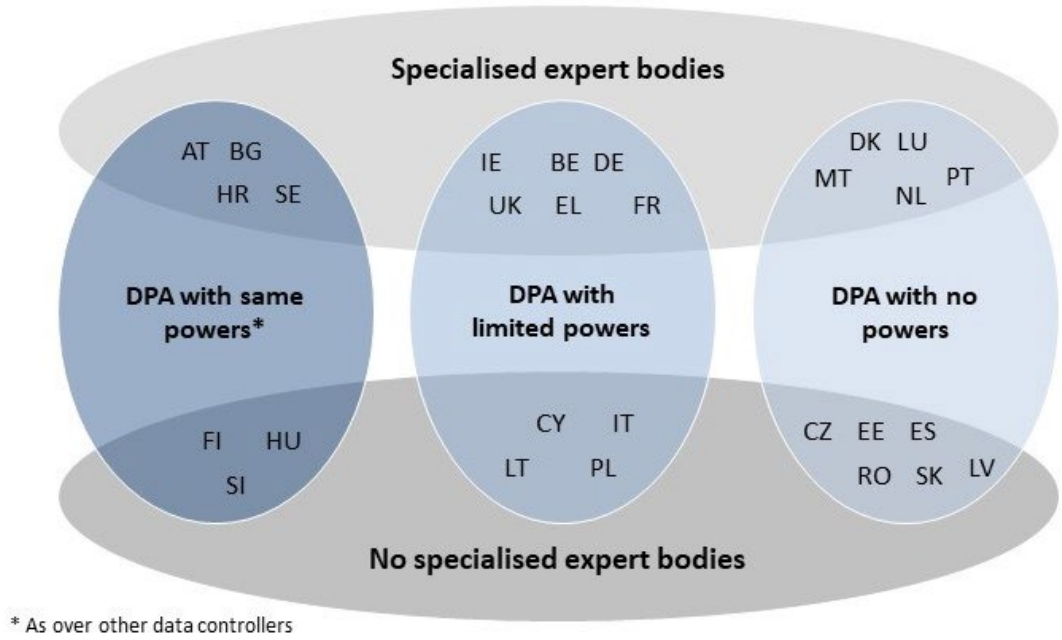


2.7. DPAs' and expert bodies' powers over intelligence techniques, by EU Member State

FRANET contractors are required to check the accuracy of the figure below (Figure 8 (p. 82) of the FRA 2017 report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

The figure below (Figure 8 (p. 82) of the FRA 2017 report) accurately represents the situation in Slovakia as of 11 November 2022.

Figure 8: DPAs' and expert bodies' powers over intelligence techniques, by EU Member State



2.8. Binding authorisation/approval of targeted surveillance measures in the EU

FRANET contractors are required to check the accuracy of table below (Table 4 (p. 95) of the FRA 2017 report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

The table below (Table 4 (p. 95) of the FRA 2017 report) accurately represents the situation in Slovakia as of 11 November 2022.

Table 4: Binding authorisation/approval of targeted surveillance measures in the EU-27

	Judicial	Executive	Expert bodies	Services
SK	✓			

2.9. Approval/authorisation of general surveillance of communication

All FRANET contractors are requested to check the accuracy of the table below (Table 5 (p. 97) of the FRA 2017 report), and to update/include information as it applies to their Member State (if not previously referred to). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework, in particular where - since 2017 - your Member State regulates these type of surveillance methods (for a definition of general surveillance, see FRA 2017 Report, p. 19).

The table below 5 (Table 5 (p. 97) of the FRA 2017 report) is not applicable to the situation in Slovakia. The legal amedments that came into effect on 1 January 2006 made the blanket data retention illegal (for details see p. 2 of the Short Thematic Report "National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies. Legal update" for Slovakia.

Table 5: Approval/authorisation of general surveillance of communication in France, Germany, the Netherlands and Sweden

	Judicial	Parliamentary	Executive	Expert
DE		✓		✓
FR			✓	
NL	✓		✓	✓
SE				✓

2.10. Non-judicial bodies with remedial powers

FRANET contractors are requested to check the accuracy of table below (Table 6 (p. 112) of the FRA 2017 report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

The table below (Table 6 (p. 112) of the FRA 2017 report) accurately represents the situation in Slovakia as of 11 November 2022.

Table 6: Non-judicial bodies with remedial powers in the context of surveillance, by EU Member State

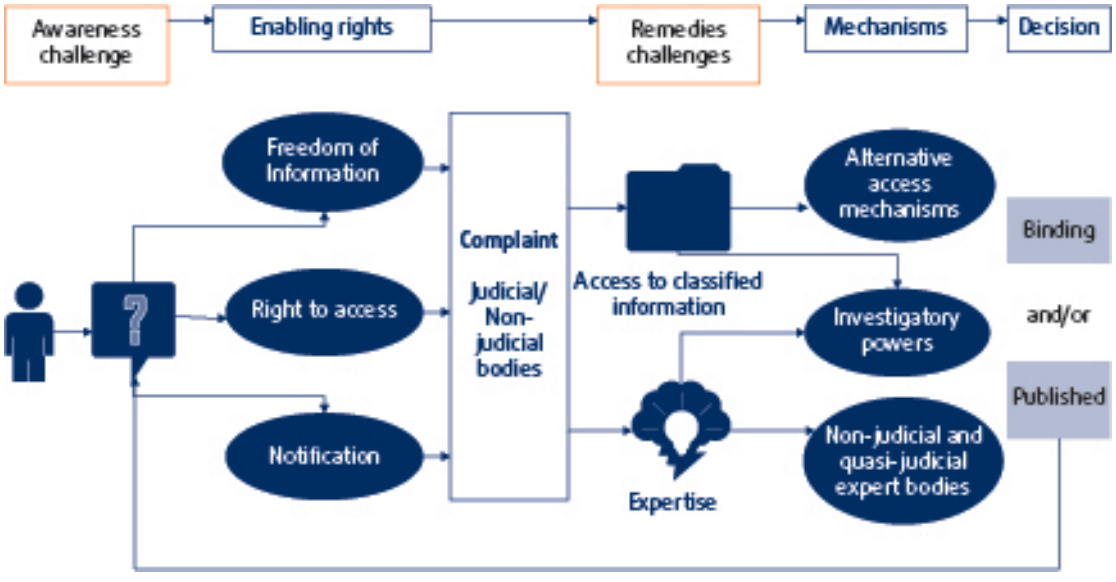
	Executive (ministry)	Expert body(ies)	DPA	Parliamentary committee(s)	Ombuds institution
SK				✓	

2.11. Implementing effective remedies

FRANET contractors are requested to confirm that the diagram below (Figure 9 (p. 114) of the FRA 2017 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.

The diagram below (Figure 9 (p. 114) of the FRA 2017 report) accurately represents the situation in Slovakia as of 11 November 2022.

Figure 9: Implementing effective remedies: challenges and solutions



2.12. Non-judicial bodies' remedial powers

FRANET contractors are required to check the accuracy of table below (Table 7 (pp. 115 - 116) of the FRA 2017 report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

It is not possible to assess the accuracy of the table below (Table 7 (pp. 115 - 116) of the FRA 2017 report) because, as of 11 November 2022, the Special Commission of the National Council to Control the Use of Information-technological Tools has not yet been made operational and its precise competences and procedures have not yet been laid down (see the introductory summary). The Act no. 404/2015 Coll. that amended and supplemented the Act no. 166/2003 Coll. on the protection of privacy against unauthorised use of information-technological tools (Act on protection against eavesdropping)[23] and created the legal frame for the establishment of the Special Commission does not specifc if and how complainants should be informed about the control.

Table 7: Non-judicial bodies' remedial powers in case of surveillance, by EU Member State

	Bodies with remedial competence	Decisions are binding	May fully access collected data	Control is communicated to complainant	Decision may be reviewed
SK	Special Commission of the National Council to Control the Use of Information-technological Tools				

Note:

= Expert body
= Ombuds institution
= Data protection authority
= Parliamentary Committee
= Executive

Source: FRA, 2017

2.13. DPAs' remedial competences

FRANET contractors are required to check the accuracy of the figure below (Figure 10 (p. 117) of the FRA 2017 report) with respect to the situation in your Member State. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

The figure below (Figure 10 (p. 117) of the FRA 2017 report) is not applicable to the situation in Slovakia as the Slovak DPA does not have any remedial competences over intelligence services.

[23] Slovakia, Act No. 166/2003 Coll. on the protection of privacy against unauthorised use of information-technological tools that amends certain laws *(Zákon č. 166/2003 Z.z. o ochrane pred odpočúvaním)*, 24 April 2003.

Figure 10: DPAs' remedial competences over intelligence services