

Short Thematic Report

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

Legal update

Country: Slovenia

Version of 29 June 2016

FRANET contractor: Institute of Criminology at the Faculty of Law

Author(s) name(s): Primož Gorkič, Aleš Završnik

DISCLAIMER: This document was commissioned under a specific contract as background material for the project on [National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies](#). The information and views contained in the document do not necessarily reflect the views or the official position of the EU Agency for Fundamental Rights. The document is made publicly available for transparency and information purposes only and does not constitute legal advice or legal opinion.

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.

In Slovenia, during the reporting period, no legislative changes have been made concerning powers of Slovenia's intelligence services, Slovene Intelligence and Security Agency (*Slovenska obveščevalno-varnostna agencija*, SOVA) or Intelligence and Security Service at the Ministry of Defence of the Republic of Slovenia (*Obveščevalno-varnostna služba Ministrstva Republike Slovenije za obrambo*, OVS MORS). Similarly, no relevant judicial decisions have been issued and no special commissions have been put to work after the so-called Snowden revelations. In the reporting period, Slovenian DPA, the Information Commissioner (*Informacijski pooblaščenec*, IP RS), published two annual reports (2014¹, 2015²), but does not report on issues related to Slovenian intelligence services and surveillance practices that would fall into the reporting period. On 23 April 2015 Slovenian Parliamentary Commission for the Supervision of the Intelligence and Security Services (*Komisija za nadzor obveščevalnih in varnostnih služb*) issued the annual report for 2014.³ The non-classified summary of the report does not refer to issues related to so-called Snowden revelation. In 2014, both SOVA and OVS MO were under the supervision of the Commission, the last inspection at SOVA headquarters took place 26 May 2014. The non-classified summary of the report contains the following points: (i) recommendation that the National Assembly, along with other competent bodies, closely follows any signs of extremism (point 1 of the summary); (ii) conclusion that events and (violent) demonstration in 2012/2013 were a form of organised extremist activities, rebutting statements that these groups were trained by members of Slovenian Army (point 2 of the summary); (iii)

- 1 Slovenia, The Information Commissioner of the Republic of Slovenia (*Informacijski pooblaščenec* RS, IP RS) (2015), Annual Report of the Information Commissioner for 2014 (*Letno poročilo Informacijskega pooblaščenca za leto 2014*), May 2015, available at: www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_IP_2014.pdf. All hyperlinks were accessed on 12 May 2016.
- 2 Slovenia, The Information Commissioner of the Republic of Slovenia (*Informacijski pooblaščenec* RS, IP RS) (2016), Annual Report of the Information Commissioner for 2015 (*Letno poročilo Informacijskega pooblaščenca za leto 2015*), May 2016, available at: www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2015_web.pdf.
- 3 Slovenia, Slovenian Parliamentary Commission for the Supervision of the Intelligence and Security Services (*Komisija za nadzor obveščevalnih in varnostnih služb*) (2015), Report on the Work of The Parliamentary Commission for the Supervision of the Intelligence and Security Services in 2014 (*Poročilo o delu Komisije za nadzor obveščevalnih in varnostnih služb v letu 2014*), 23 April 2015, available at: www.dz-rs.si/wps/portal/Home/deloDZ/zakonodaja/izbranZakonAkt?uid=C1257A70003EE749C1257E31004F3BA0&db=kon_akt&mandat=VII&tip=doc.

conclusion that provisions of Articles 153 and 154 of the Criminal Procedure Act (*Zakon o kazenskem postopku*),⁴ governing the handling of materials collected by police surveillance measures, were not followed, lacking in effective ex post and ex ante judicial supervision; (point 3 of the summary); (iv) suspecting, in individual cases, that police surveillance measures or search of premises is authorised without reasonable grounds for suspicion (point 4 of the summary); (v) finding that Commission for the Prevention of Corruption (*Komisija za preprečevanje korupcije*) in selected cases required the police or the state prosecutor's office to hand over sensitive documents that might jeopardise an on-going criminal investigation (point 5 of the summary); (vi) recommendation that the National Assembly be more active in passing the relevant missing legislation in the field of electronic communication, in particular by calling upon communication service providers to enact "security measure plans" as required by the Electronic Communications Act (*Zakon o elektronskih komunikacijah*).⁵

The report for 2015 is not yet available.

However, the National Assembly did, upon proposal by the Ministry of Justice, amend the Criminal Code (*Kazenski zakonik*)⁶ in order to (partially) decriminalise disclosure of classified information. Disclosure of classified information is, and remains, generally, a criminal offence (Article 260 of the Criminal Code). After amendments⁷ have entered into force on 18 October 2015, additional provision has been introduced, Article 260, § 3 of the Criminal Code. According to the amendment, even when classified information is disclosed contrary to rules stipulated under Classified Information Act (*Zakon o tajnih podatkih*),⁸ such disclosure is not punishable, if the disclosed classified information refers to (i) a violation of human rights, or (ii) grievous abuse of power or (iii) other grievous irregularities in the exercise of public office, powers or services - on condition that disclosure is (a) not motivated by gaining a pecuniary advantage, and (b) does not jeopardise life or limb and (c) does not result in grievous or irreparable damage to the security or legally protected interests of the Republic of Slovenia.

The amendment is a direct result of so-called Snowden revelations⁹ and complements the provisions of Classified Information Act. The Classified Information Act in Article 6 stipulates that information, even if labelled as classified, does not enjoy such protection, if designation is intended to cover up a criminal offence, abuse of power or other illegal acts (*mala fide*). The amendment to the Criminal Code also applies to disclosure of information that has been classified *bona fide* and seeks to broaden freedom of speech protections and protection of whistle-blowers.

4 Slovenia, Criminal Procedure Act (*Zakon o kazenskem postopku*), 13 Oct 1994, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362.

5 Slovenia, Electronic Communications Act (*Zakon o elektronskih komunikacijah*), 31 December 2012, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6405.

6 Slovenia, Criminal Code (*Kazenski zakonik*, KZ-1), 20 May 2008, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5050.

7 Slovenia, Act Amending the Criminal Code KZ-1C (*Zakon o spremembah in dopolnitvah Kazenskega zakonika, KZ-1C*), 9 July 2015, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6928.

8 Slovenia, Classified Information Act (*Zakon o tajnih podatkih, ZTP*), 25 October 2001, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO2133.

9 Slovenia, The Government of the Republic of Slovenia (*Vlada Republike Slovenije*) (2015), Proposal for the Act Amending the Criminal Code KZ-1C (*Predlog Zakona o spremembah in dopolnitvah Kazenskega zakonika KZ-1C*), 21 May 2015.

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 Wills, A. (2015), *Making international intelligence cooperation accountable*, Geneva, DCAF.¹⁰

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 (eg. internal guidance, ministerial directives etc.) and whether or not such documents are classified or publicly available.
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.

1. Legal basis and conditions applicable to **international cooperation** of intelligence services

The international cooperation of Slovenian intelligence services, Slovene Intelligence and Security Agency Act (SOVA) and Intelligence and Security Service of the Ministry of Defence (OVS MORS), is based on (i) international treaties and (ii) laws adopted by the Slovenian National Assembly. Given that both services are a part of the state administration, their organisation, competences and performance of their duties must be governed by law (Article 120 of the Constitution (*Ustava Republike Slovenije*)¹¹. Actions of state authorities (including intelligence services) must be based on laws or other regulations adopted pursuant to law (Article 153, § 3 of the Constitution). Laws must be in conformity with generally accepted principles of international law and with valid treaties ratified by the National Assembly, whereas regulations and other general acts must also be in conformity with other ratified treaties (Article 153, § 1 of the Constitution).

Same requirements apply to any international cooperation that intelligence services – as state authorities - undertake.

The basis (competences) for international cooperation of SOVA are governed by:

- Article 2 of the Slovene Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji, ZSOVA*),¹² stipulating that (SOVA) is competent to collect, analyse and provide information obtained from abroad, in order to further security, political and economic interests of the state;
- Article 7 of ZSOVA, authorising the director of SOVA to determine, when/if the agency may cooperate or exchange information with foreign intelligence and security services, in the course of exercising its competences under Article 2;
- Article 12, §11 of the ZSOVA, requiring that SOVA – in the course of providing personal data to foreign intelligence and security services – obtain assurances that the recipient state

¹⁰ www.dcaf.ch/Publications/Making-International-Intelligence-Cooperation-Accountable

¹¹ Slovenia, Constitution of the Republic of Slovenia (*Ustava Republike Slovenije*, U RS), 23 December 1991, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=USTA1.

¹² Slovenia, Slovene Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji, ZSOVA*), 7 April 1999, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1884.

regulates the protection of personal data and that the recipient service will use the data only for purposes stipulated by Act.

The basis (competences) for international cooperation of OVS MORS are governed by:

- Article 32, § 1 of the Defence Act (*Zakon o obrambi, ZObr*),¹³ authorising OVS MORS (i) to determine and analyse military and political security situations and military capabilities abroad, that are of particular importance to the security of the state; and (ii) to collect and analyse data related to situations in the areas where members of the Slovenian army operate;

- Article 33, §5 of the Act, authorising OVS MORS to exchange intelligence with foreign military intelligence and security services, with prior consent of the minister of defence.

- Executive Regulation on Intelligence and Security Service of the Ministry of Defence (*Uredba o obveščevalno-varnostni službi Ministrstva za obrambo*),¹⁴ adopted by the Government of the Republic of Slovenia, in particular Article 3 of the Regulation that specifies the competences of OVS MORS intelligence tasks as collecting, documenting and analysing information and data on foreign states, that are of interest to defence interests of the state, specifically allowing for an exchange of intelligence with other similar services, in accordance with international treaties and international obligations of the state.

Additionally, provisions on exchange and protection of classified information must be observed, as regulated by Classified Information Act (*Zakon o tajnih podatkih*).¹⁵ Access to classified data of foreign state or international organisation must be based on laws or regulations adopted on the basis of laws, or in accordance with international treaties (Article 9 of the Act). Exchange of classified data with other states or international organisations, based on international treaties, must provide for a comparable level of protection of classified information (Article 20 of the Act).

The statutory framework is focused on providing legal basis for information sharing as a form of cooperation between intelligence services. Conditions for information sharing are both (i) formal, i.e. consent of the head of the service (director of SOVA or the minister of defence), and (ii) substantive, i.e. ensuring that data protection framework exists in the recipient state. No specific domestic provisions on other forms of international cooperation (covert operational cooperation, hosting facilities and equipment, training and capacity building, providing hardware and software) exist. Article 7 of ZSOVA does provide a basis for “cooperation” with foreign intelligence and security services (other than exchange of data), but does not specify the nature of such cooperation.

There are, however, a number of bi-lateral international treaties in the field of security and military affairs that provide for mutual assistance between Slovenia and other Member States.

It should be noted, that in response to our queries,¹⁶ the two agencies, SOVA and OVS MORS, did not mention international treaties as a basis for their cooperation with foreign

13 Slovenia, Defence Act (*Zakon o obrambi, ZObr*), 20 December 1994, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO532.

14 Slovenia, Executive Regulation on Intelligence and Security Service of the Ministry of Defence (*Uredba o obveščevalno-varnostni službi Ministrstva za obrambo*), 29 July 1997, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=URED699.

15 Slovenia, Classified Information Act (*Zakon o tajnih podatkih, ZTP*), 25 October 2001, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO2133.

16 Slovene Intelligence and Security Agency (*Slovenska obveščevalno-varnostna agencija, SOVA*), reply to our e-mail query, 9 May 2016; Intelligence and Security Service at the Ministry of

agencies and referred only to Slovene Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji*).¹⁷

International treaties that facilitate or form a basis for cooperation of intelligence services, are typically bilateral. In order to be valid, they must be published in the Official gazette of the Republic of Slovenia (Article 154 of the Constitution).¹⁸ Bi-lateral treaties typically refer to: (i) exchange and protection of classified data; (ii) cooperation in military matters, and (iii) cooperation in the matters of security.¹⁹ Given that no additional information has been provided by relevant intelligence services, the scope of their actual application and interpretation in the field of international cooperation of intelligence services remains unknown. To clarify, the treaties are published; whether or how they are applied in the field of international cooperation of intelligence services, is not. As said, the services contacted (see previous paragraph) do not cite international treaties as a basis for international cooperation.

The most common are treaties concerning mutual exchange and protection of classified information. Slovenia has signed treaties in this area with, for example: Austria,²⁰ Bulgaria,²¹ Croatia,²² Estonia,²³ France,²⁴ Germany,²⁵ and Spain.²⁶

-
- Defence of the Republic of Slovenia (*Obveščevalno-varnostna služba Ministrstva Republike Slovenije za obrambo*, OVS MORS), reply to our e-mail query, 6 May 2016.
- 17 Slovenia, Slovene Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji*, ZSOVA), 7 April 1999, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1884.
- 18 Slovenia, Constitution of the Republic of Slovenia (*Ustava Republike Slovenije*, U RS), 23 December 1991, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=USTA1.
- 19 A list of bilateral treaties is available at: www.uvtp.gov.si/si/zakonodaja_in_dokumenti/mednarodni_bilateralni_sporazumi/. Bilateral treaties on military and security affairs are available on: www.mzz.gov.si/si/zunanja_politika_in_mednarodno_pravo/mednarodno_pravo/mednarodne_pogodbe/sklenjene_mednarodne_pogodbe/.
- 20 Slovenia, Act ratifying the Agreement between the Government of the Republic of Slovenia and the Austrian Federal Government on the Exchange and Mutual Protection of Classified Information (*Zakon o ratifikaciji Sporazuma med Vlado Republike Slovenije in Avstrijsko zvezno vlado o izmenjavi in medsebojnem varovanju tajnih podatkov*), 18 May 2009, available at: www.uradni-list.si/1/objava.jsp?sop=2009-02-0041.
- 21 Slovenia, Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Bulgaria on the Exchange and Mutual Protection of Classified Information (*Zakon o ratifikaciji Sporazuma med Vlado Republike Slovenije in Vlado Republike Bolgarije o izmenjavi in medsebojnem varovanju tajnih podatkov*), 29 December 2012, available at: www.uradni-list.si/1/objava.jsp?sop=2012-02-0108.
- 22 Slovenia, Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Croatia on Mutual Protection of Classified Information (*Zakon o ratifikaciji Sporazuma med Vlado Republike Slovenije in Vlado Republike Hrvaške o medsebojnem varovanju tajnih podatkov*), 22 August 2011, available at: www.uradni-list.si/1/objava.jsp?sop=2011-02-0051.
- 23 Slovenia, Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Estonia on the Exchange and Mutual Protection of Classified Information (*Zakon o ratifikaciji Sporazuma med Vlado Republike Slovenije in Vlado Republike Estonije o izmenjavi in medsebojnem varovanju tajnih podatkov*), 13 April 2010, available at: www.uradni-list.si/1/objava.jsp?sop=2010-02-0035.
- 24 Slovenia, Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the French Republic on the Exchange and Mutual Protection of Classified Information (*Zakon o ratifikaciji Sporazuma med Vlado Republike Slovenije in Vlado Francoske republike o izmenjavi in medsebojnem varovanju tajnih podatkov*), 3 May 2010, available at: www.uradni-list.si/1/objava.jsp?sop=2010-02-0043.

Typically, these treaties include not only provisions on protection of classified data exchanged between competent state bodies, but also during visits to signatory states. For example, the treaty with Germany in Article 7 of the Treaty (cited above) provides that access to classified information or institutions handling classified information during visits is subject to prior authorisation of competent bodies and prior security check. The treaties are general in nature and not specifically tailored to cooperation of intelligence services. They do, however, apply, given the classified nature of their activities.

Treaties relating to military matters, have been signed with, for example: Bulgaria,²⁷ Croatia,²⁸ Estonia,²⁹ France³⁰, Germany,³¹ and Italy.³²

Most of these treaties do not mention cooperation of military intelligence as an area of cooperation. At the same time, they do not contain an exhaustive list of areas of cooperation (for example, Article 2 of the treaty with Bulgaria). Only treaty with Croatia (Article 2, cited above) specifically mentions exchange of intelligence information as an area of cooperation between military intelligence services. As a form of cooperation, visits and exchange of information are typically envisaged (for example, Article 3 of the treaty with France, cited above).

-
- 25 Slovenia, Act ratifying the agreement between the Government of the Republic of Slovenia and the Government of the federal Republic of Germany on mutual protection of confidential information (*Zakon o ratifikaciji Sporazuma med Vlado Republike Slovenije in Vlado Zvezne republike Nemčije o vzajemnem varovanju zaupnih podatkov*), 15 January 2004, available at: www.uradni-list.si/1/objava.jsp?sop=2004-02-0004.
 - 26 Slovenia, Act ratifying the Agreement between the Republic of Slovenia and the Kingdom of Spain on the Exchange and Mutual Protection of Classified Information (*Zakon o ratifikaciji Sporazuma med Republiko Slovenijo in Kraljevino Španijo o izmenjavi in medsebojnem varovanju tajnih podatkov*), 3 July 2015, available at: www.uradni-list.si/1/objava.jsp?sop=2015-02-0044.
 - 27 Slovenia, Agreement on co-operation between the Ministry of Defence of the Republic of Slovenia and the Ministry of Defence of the Republic of Bulgaria (*Zakon o ratifikaciji Sporazuma o sodelovanju med Ministrstvom za obrambo Republike Slovenije in Ministrstvom za obrambo Republike Bolgarije*), 10 March 2000, available at: www.uradni-list.si/1/objava.jsp?sop=2000-02-0023.
 - 28 Slovenia, Act ratifying the agreement between the Government of the Republic of Slovenia and the Government of the Republic of Croatia on defence co-operation (*Zakon o ratifikaciji Sporazuma med Vlado Republike Slovenije in Vlado Republike Hrvaške o obrambnem sodelovanju*), 15 January 2004, available at: www.uradni-list.si/1/objava.jsp?sop=2004-02-0005.
 - 29 Slovenia, Agreement between the Ministry of Defence of the Republic of Slovenia and the Ministry of Defence of the Republic of Estonia on Co-operation in the field of defence (*Zakon o ratifikaciji Sporazuma med Ministrstvom za obrambo Republike Slovenije in Ministrstvom za obrambo Republike Estonije o sodelovanju na obrambnem področju*), 6 June 2000, available at: www.uradni-list.si/1/objava.jsp?sop=2000-02-0070.
 - 30 Slovenia, Act ratifying an agreement between the Government of the Republic of Slovenia and the Government of the French Republic on defence cooperation (*Zakon o ratifikaciji Sporazuma med Vlado Republike Slovenije in Vlado Francoske republike o sodelovanju na obrambnem področju*), 28 June 2002, available at: www.uradni-list.si/1/objava.jsp?sop=2002-02-0053.
 - 31 Slovenia, Act ratifying the Agreement between the ministry of defence of the Republic of Slovenia and the Federal ministry of defence of the Federal Republic of Germany on military cooperation (*Zakon o ratifikaciji Sporazuma med Ministrstvom za obrambo Republike Slovenije in Zveznim ministrstvom za obrambo Zvezne republike Nemčije o sodelovanju na vojaškem področju*), 13 November 2003, available at: www.uradni-list.si/1/objava.jsp?sop=2003-02-0077.
 - 32 Slovenia, Act ratifying an agreement between the Government of the Republic of Slovenia and the Government of the Republic of Italy on defence cooperation (*Zakon o ratifikaciji Sporazuma o sodelovanju na obrambnem področju med Vlado Republike Slovenije in Vlado Republike Italije*), 201 March 1998, available at: www.uradni-list.si/1/objava.jsp?sop=1998-02-0014.

Treaties related to matters of security typically regulate cooperation in the field of fighting international organised crime and terrorism. Given the competence of SOVA in the field of terrorism and international organised crime (Article 24 of the Slovene Intelligence and Security Agency Act, *Zakon o Slovenski obveščevalno-varnostni agenciji*),³³ they may apply *ratione materiae*. However, some treaties typically designate competent state bodies of the signatories. On Slovenian side, this is Ministry of the Interior, for example, in the treaty with Austria,³⁴ Bulgaria,³⁵ Croatia,³⁶ and Sweden.³⁷ Some treaties do not specify the competent bodies of signatory states but allow for subsequent designation of such bodies (for example, treaty with Estonia³⁸ and France³⁹).

2. Oversight of international cooperation agreements, data exchange and joint surveillance agreements

- 33 Slovenia, Slovene Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji*, ZSOVA), 7 April 1999, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1884.
- 34 Slovenia, Act Ratifying the Agreement between the Ministry of the Interior of the Republic of Slovenia and the Federal Minister of the Interior of the Republic of Austria on the cooperation in the suppression of international organised crime, international illicit drug traffic and international terrorism (*Zakon o ratifikaciji Dogovora med Ministrstvom za notranje zadeve Republike Slovenije in zveznim ministrom za notranje zadeve Republike Avstrije o sodelovanju pri zatiranju mednarodno organiziranega kriminala, mednarodnega ilegalnega trgovanja z mamili in mednarodnega terorizma*), 29 March 1996, available at: www.uradni-list.si/1/objava.jsp?sop=1996-02-0017.
- 35 Slovenia, Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Bulgaria on Co-operation in the fight against organised crime, illicit drugs, psychotropic substances and precursors trafficking, terrorism and other serious crimes (*Zakon o ratifikaciji Sporazuma med Vlado Republike Slovenije in Vlado Republike Bolgarije o sodelovanju v boju proti organiziranemu kriminalu, nezakoniti trgovini s prepovedanimi drogami, psihotropnimi snovmi in predhodnimi sestavinami, terorizmu in drugim hujšim kaznivim dejanjem*), 22 March 2002, available at: www.uradni-list.si/1/objava.jsp?sop=2002-02-0024.
- 36 Slovenia, Act Ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Croatia on the cooperation in combating terrorism, illicit traffic in and abuse of drugs as well as against organised crime (*Zakon o ratifikaciji pogodbe o sodelovanju med Vlado Republike Slovenije in Vlado Republike Hrvaške v boju proti terorizmu, tihotapljenju in zlorabi mamil, kot tudi proti organiziranemu kriminalu*), 28 Februar 1994, available at: www.uradni-list.si/1/objava.jsp?sop=1994-02-0022.
- 37 Slovenia, Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Kingdom of Sweden on Cooperation in the Fight against Organised Crime, Illicit Drug Trafficking in Drugs and Precursors, Terrorism and other Serious Crimes (*Zakon o ratifikaciji Sporazuma med Vlado Republike Slovenije in Vlado Kraljevine Švedske o sodelovanju v boju proti organiziranemu kriminalu, nezakoniti trgovini s prepovedanimi drogami in predhodnimi sestavinami, terorizmu in drugim hujšim kaznivim dejanjem*), 18 July 2005, available at: www.uradni-list.si/1/objava.jsp?sop=2005-02-0034.
- 38 Slovenia, Act ratifying the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Estonia on co-operation in the fight against organised crime, illicit drugs, psychotropic substances and precursors trafficking and terrorism (*Zakon o ratifikaciji Sporazuma med Vlado Republike Slovenije in Vlado Republike Estonije o sodelovanju v boju proti organiziranemu kriminalu, nezakoniti trgovini s prepovedanimi drogami, psihotropnimi snovmi in predhodnimi sestavinami in terorizmu*), 15 January 2004, available at: www.uradni-list.si/1/objava.jsp?sop=2004-02-0006.
- 39 Slovenia, Act Ratifying the Agreement on Cooperation in the Field of Internal Security between the Government of the Republic of Slovenia and the Government of the French Republic (*Zakon o ratifikaciji Sporazuma o sodelovanju na področju notranje varnosti med Vlado Republike Slovenije in Vlado Francoske republike*), 25 March 2008, available at: www.uradni-list.si/1/objava.jsp?sop=2008-02-0037.

There are no specific rules applicable to oversight of international cooperation of Slovenian intelligence services. The applicable statutes do not specifically mention international cooperation activities. The following rules apply:

- parliamentary oversight under The Parliamentary Supervision of the Intelligence and Security Services Act (*Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb, ZPNOVS*)⁴⁰ extends to any statutory defined activities of intelligence services (Article 4, § 4 of the ZPNOVS), therefore including international cooperation insofar as it is subject to laws; the non-classified report summary⁴¹ of the 2014 Slovenian Parliamentary Commission for the Supervision of the Intelligence and Security Services (*Komisija za nadzor obveščevalnih in varnostnih služb*) does not mention oversight of international cooperation;

- government (executive) oversight: under Article 4 of ZSOVA, concerning oversight by the Government, and Articles 5 and 18 of the Government of the Republic of Slovenia Act (*Zakon o Vladi Republike Slovenije, ZVRS*),⁴² concerning oversight of OVS MORS by the minister of defence and the Government, applies to oversight of any activities in the competence of government services or other state bodies, therefore including international cooperation of intelligence services;

- oversight by the Information Commissioner, under Article 2 of the Information Commissioner Act (*Zakon o Informacijskem pooblaščenju, ZInfP*)⁴³ encompasses oversight of any transfer of personal data originating in the Republic of Slovenia and any form of personal data processing;

- observance of the provisions of Classified Information Act (ZTP) is ensured by internal oversight by heads of authorities (Article 41 of the Act) and by external oversight, by the Inspectorate for Interior Affairs, the Defence Inspectorate of the Republic of Slovenia (Article 42a of the Act) and The Government Office for the Protection of Classified Information (Articles 43 et seq. of the Act).

Some forms of oversight apply to all forms of cooperation (parliamentary, government), while others apply specifically to information exchange (Information Commissioner and the oversight under the Classified Information Act).

40 Slovenia, The Parliamentary Supervision of the Intelligence and Security Services Act (*Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb, ZPNOVS*), 6 February 2003, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3455.

41 Slovenia, Slovenian Parliamentary Commission for the Supervision of the Intelligence and Security Services (*Komisija za nadzor obveščevalnih in varnostnih služb*) (2015), Report on the work of the Parliamentary Commission for the Supervision of the Intelligence and Security Services in 2014 (*Poročilo o delu Komisije za nadzor obveščevalnih in varnostnih služb v letu 2014*), 23 April 2015, available at: www.dz-rs.si/wps/portal/Home/deloDZ/zakonodaja/izbranZakonAkt?uid=C1257A70003EE749C1257E310048B591&db=kon_akt&mandat=VII.

42 Slovenia, Government of the Republic of Slovenia Act (*Zakon o Vladi Republike Slovenije, ZVRS*), 12 January 1993, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO242.

43 Slovenia, Information Commissioner Act (*Zakon o Informacijskem pooblaščenju, ZInfP*), 30 November 2005, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4498.

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)*⁴⁴ (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?

Access to information and surveillance of the Slovenian intelligence services, i.e. Slovene Intelligence and Security Agency (*Slovenska obveščevalno-varnostna služba*, SOVA) and Intelligence and Security Service of the Ministry of Defence (*Obveščevalno-varnostna služba Ministrstva Republike Slovenije za obrambo*, OVS MORS), is based on (1) general laws governing personal data protection and access to information, (2) laws governing both intelligence services and (3) laws on supervision of the intelligence services.

1. The **general** legal framework in Slovenia in relation to **access** to information and surveillance is governed by the Constitution of the Republic of Slovenia (*Ustava Republike Slovenije*, U RS),⁴⁵ which stipulates in the Article 38 “Protection of Personal Data” that everyone has the right of access to the collected personal data that relates to him and the right to judicial protection in the event of any abuse of such data.

Personal Data Protection Act (*Zakon o varstvu osebnih podatkov*, ZVOP-1)⁴⁶ further operationalises the constitutional right. Articles 19, 30, 31, 32, 34, 36 of the Act define the following safeguards: obligatory notification of the individual about the processing of personal data (Article 19), the right of the individual to information (Article 30), detailed procedure for logging the request (Article 31), the right to supplement, correct, block, erase and to object (Article 32), procedure of supplementing, correction, blocking, deletion and objection (Article 33), judicial protection of the rights of the individual (Article 34).

However, the rights of individuals may exceptionally be restricted (Article 36) by statute for several reasons, e.g. for protection of national sovereignty and national defence, protection of national security and the constitutional order of the state, security, political and economic interests of the state. Such restrictions may only be provided to the extent necessary for achieving the purpose of the restriction.

Public Information Access Act (*Zakon o dostopu do informacij javnega značaja*, ZDIJZ)⁴⁷ codifies the free access principle to public information, equally for legal entities and natural persons (Article 5). Applicant has, at his/her request, the right to acquire information from a public body: by consulting it on the spot, or by acquiring a transcript, a copy or an electronic

44 <http://www.right2info.org/exceptions-to-access/national-security/global-principles#section-10>

45 Slovenia, Constitution of the Republic of Slovenia (*Ustava Republike Slovenije*, U RS), 23 December 1991, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=USTA1.

46 Slovenia, Personal Data Protection Act (*Zakon o varstvu osebnih podatkov*, ZVOP-1), 15 July 2004, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3906.

47 Slovenia, Public Information Access Act (*Zakon o dostopu do informacij javnega značaja*, ZDIJZ), 25 February 2003, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3336.

record of such information. However, the free access principle is limited and exceptions related to legal proceedings and protections of confidential source are set down in Article 5a ZDIJZ. The public body as defined in Article 1 can deny access to requested information, inter alia, if the source of information is classified. Furthermore, exception to the free access principle is set down in Article 6 which stipulates that the public body may, inter alia, deny access to requested information, if the request relates to information which, pursuant to the Classified Information Act (*Zakon o tajnih podatkih, ZTP*)⁴⁸ is designated as classified (Article 6, § 1, point 1).

These exceptions (defined in Article 6, § 1) are mitigated in Article 6, § 2. The access to the requested information is nevertheless *sustained*, if public interest for disclosure prevails over public interest or interest of other persons not to disclose the requested information. This balancing act is performed by several bodies, depending on the body liable to garner public information, i.e.: (a) government, (b) Supreme Court, (c) Council of local self-governing community, or (d) the body itself (Article 21, § 2). However, this balancing act is not permitted and *exceptions are valid*, if: (Article 6, § 2, the first and the second point): (1) the information, designated as classified enjoys one of the two top levels of protection; and (2) if information contains or was prepared by using classified information of another country or an international organization, with which the Republic of Slovenia signed an international agreement on the exchange or transmission of classified information.

2. The legal framework in Slovenia in relation **to access** to information and surveillance of **SOVA** encompasses:

SOVA is subject to supervision of the Information Commissioner (*Informacijski pooblaščenec, IP*)⁴⁹ responsible for issues of personal data protection, and the Parliamentary Commission for the Supervision of the Intelligence and Security Services (*Komisija za nadzor obveščevalnih in varnostnih služb*).⁵⁰

Slovene Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji, ZSOVA*)⁵¹ stipulates that SOVA, when collecting personal data, is not bound to inform the individual to whom the data refers and the individual does not have the right to access the personal data collected by the Agency (Article 17, § 1) - on condition, that informing or allowing the individual access to personal data would make the tasks of the Agency impossible or difficult to fulfil (Article 17, § 2). Same conditions apply to a request by the Director of SOVA that personal data controllers, which supplied the Agency with personal data, only inform the individual to whom the personal data refer after a period of five years (Article 17, § 3). The *exemption is thus not complete* and a balancing act is required in order to limit the right to access to information.⁵²

ZSOVA furthermore stipulates in Article 24, § 5 the right to be informed that person's private communication has been under surveillance, i.e. in a case of interception of

48 Slovenia, Classified Information Act (*Zakon o tajnih podatkih, ZTP*), 25 October 2001, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO2133.

49 Slovenia, Information Commissioner Act (*Zakon o informacijskem pooblaščenecu, ZInfP*), 13 November 2005, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4498.

50 Slovenia, Parliamentary Supervision of the Intelligence and Security Services Act (*Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb, ZPNOVS*), 26 February 2003, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3455.

51 Slovenia, Slovene Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji, ZSOVA*), 7 April 1999, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1884.

52 Information Commissioner (*Informacijski pooblaščenec*), e-mail correspondence from 4 May 2016.

telecommunications in the Republic of Slovenia. After the case has been closed, the Director of the Agency (SOVA) informs the person subject to interception of communications of his/her right to get acquainted with the collected material or with a summary of the collected material, if access to large amounts of materials would not be practical. However, the right can be limited if it is reasonable to conclude that the acquaintance with the material will endanger people's lives and health or the national security. In the latter case, the Director of the Agency may decide not to inform the person concerned of the content of the collected material (Article 24, § 5 ZSOVA).

The provision does not differentiate between suspicion-based surveillance and non-suspicion based large-scale surveillance, therefore it is applicable also in the case of the latter.

The Parliamentary Supervision of the Intelligence and Security Services Act (*Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb, ZPNOVS*)⁵³ defines conditions for parliamentary supervision of SOVA and OVS MORS. In Article 33, § 2 the act defines the right of an individual under surveillance to be informed by the parliamentary supervisory commission about *unlawful* surveillance conducted against the individual.

3. The legal framework in Slovenia in relation to access to information and surveillance of **OVS MORS** is defined by the Defence Act (*Zakon o obrambi, ZObr*),⁵⁴ Article 36, authorizing OVS MORS to keep filing systems of personal data related to the intelligence, counterintelligence and security tasks within its powers under the conditions and in the manner and to the extent prescribed for the police and SOVA. See Article 17 and Article 24, § 5 of ZSOVA. An exemption to the right to access to information is envisaged in Article 35, § 8 and 9 ZObr. When the intelligence and security service collects personal and other data, it is not obliged to inform the individual to whom the data relate, if this would prevent or hinder the execution of the tasks of intelligence and security services. In such a case, bodies and organizations with public powers may, at the request of the Minister of Defence, inform the person to whom the personal information relates about the data collection, only after the expiry of five years from the transmission of data to the intelligence and security service.

Data protection safeguards apply to all types of surveillance, suspicion-based and non-suspicion based large-scale surveillance, of SOVA and OVS MORS. The Information Commissioner (*Informacijski pooblaščenec, IP RS*) checks on a case-by-case basis whether data protection guarantees cannot be invoked due to these exceptions. The exceptions are therefore *not used blankly* in relation to all the activities of SOVA and OVS MORS, but only in relation to the specific data related to a particular case.⁵⁵

The Information Commissioner published two annual reports (2014⁵⁶, 2015⁵⁷) in the reporting period (last trimester of 2014 until mid-2016). Both of the reports refer to data protection and

53 Slovenia, The Parliamentary Supervision of the Intelligence and Security Services Act (*Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb, ZPNOVS*), 26 February 2003, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3455.

54 Slovenia, Defence Act (*Zakon o obrambi, ZObr*), available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO532.

55 Information Commissioner (*Informacijski pooblaščenec*), e-mail correspondence from 4 May 2016.

56 Slovenia, The Information Commissioner of the Republic of Slovenia (*Informacijski pooblaščenec RS, IP RS*) (2015), Annual Report of the Information Commissioner for 2014 (*Letno poročilo Informacijskega pooblaščenca za leto 2014*), May 2015, available at: <https://www.ip-rs.si/o-pooblastencu/informacije-javnega-znacaja/letna-porocila/>.

57 Slovenia, The Information Commissioner of the Republic of Slovenia (*Informacijski pooblaščenec RS, IP RS*) (2016), Annual Report of the Information Commissioner for 2015 (*Letno poročilo*

access to information, but there are no issues reported on data protection and access to information related solely to the intelligence activities.

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 your Member State is mentioned, please update the data (new legislation, new report etc.)
3. If your 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. There is nothing to add to 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 your Member State is mentioned, please update the data (new legislation, new report etc.)
3. If your 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. There is nothing to add to 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 your Member State is mentioned, please update the data (new legislation, new report etc.)
3. If your 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. There is nothing to add to the analysis.

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 your Member State is mentioned, please update the data (new legislation, new report etc.)

3. If your 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. There is nothing to add to the analysis.

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 your Member State is mentioned, please update the data (new legislation, new report etc.)
3. If your 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. There is nothing to add to the analysis.

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 your Member State is mentioned, please update the data (new legislation, new report etc.)
3. If your 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. There is nothing to add to 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.
2. If your Member State is mentioned, please update the data (new legislation, new report etc.)
- If your 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. While there are no special provisions on whistle-blower protection within intelligence services, and the disclosure of classified information is a criminal offence under Article 260, §1, of the Criminal Code,⁵⁸ the Classified Information Act⁵⁹ in Article 6 stipulates that information labelled as classified, does not enjoy such protection, if designation is intended to cover up a criminal offence, abuse of power or other illegal acts. Disclosure of such information does not lead to prosecution. With Criminal Code amendments of 2015⁶⁰, additional provision has been added (Article 260, §3 of the Criminal Code). According to the amendment, even when classified information is disclosed contrary to rules stipulated under Classified Information Act (i.e. without recourse to Article 6 of the Act), such disclosure is not punishable, if the disclosed classified information refers to a violation of human rights, grievous abuse of power

58 Slovenia, Criminal Code (*Kazenski zakonik*, KZ-1), 20 May 2008, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5050

59 Slovenia, Classified Information Act (*Zakon o tajnih podatkih*, ZTP), 25 October 2001, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO2133..

60 Slovenia, Act Amending the Criminal Code (*Zakon o spremembah in dopolnitvah Kazenskega zakonika* KZ-1C), 9 July 2015, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6928.

or other grievous irregularities in the exercise of public office, powers or services - on conditions that disclosure is not motivated by gaining a pecuniary advantage, does not jeopardise life or limb and does not result in grievous or irreparable damage to the security or legally protected interests of the Republic of Slovenia.

2.1 Executive control

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.* While the reference on page 32 is accurate, it should be added that The Slovene Intelligence and Security Agency (*Slovenska obveščevalno-varnostna agencija*, SOVA) is an independent governmental service (Article 1 ZSOVA). It regularly informs the Primer Minister of its findings, as well as, in the matter concerned within their prerogatives, also the President of the Republic (*Predsednik republike*), the President of the National Assembly (*Državni zbor*) and competent ministers. The independent position of SOVA reflects its formal position of SOVA in the system of public administration. There are ministries, independent governmental services, agencies etc. SOVA is organised as “independent governmental office.” This means it is subordinated directly to the Government; and it is not part of any ministry. The Government sets its priorities based on the national security programme as defined in the Resolution on National Security Strategy of the Republic of Slovenia and adopted by the Parliament (Article 2, §3, of ZSOVA).
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.*

2.2 Parliamentary 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.* There is nothing to add to the analysis.

2.2.1 Mandate

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.* The reference on page 37 is accurate. However, the reference in table 1 on page 36 is not accurate. The Parliamentary Commission for the Supervision of the Intelligence and Security Services (*Komisija za nadzor obveščevalnih in varnostnih služb*) has the power to receive notifications and initiatives of individuals and organisations related to the prerogatives and tasks of the Parliamentary Commission for the Supervision of the Intelligence and Security Services according to the Article 13, §1(5) and Article 33 of the Parliamentary Supervision of the Intelligence and Security Services Act (*Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb*).⁶¹ Subsequently, The Parliamentary

61 Slovenia, The Parliamentary Supervision of the Intelligence and Security Act (*Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb*, ZPNOVS), 26 February 2003, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3455.

Commission has the power to investigate, i.e. inspect premises and equipment (Article 24 of the Parliamentary Supervision of the Intelligence and Security Services Act), and demand access to classified information (Article 25 of the Parliamentary Supervision of the Intelligence and Security Services Act).

2. If your Member State is mentioned, please update the data (new legislation, new report etc.)
3. If your 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.

2.2.2 Composition

1. If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference. The reference on page 40 is accurate.
2. If your Member State is mentioned, please update the data (new legislation, new report etc.)
3. If your 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.

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 your Member State is mentioned, please update the data (new legislation, new report etc.)
3. If your 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. There is nothing substantially to add to the analysis. The Slovenian Parliamentary Commission for the Supervision of the Intelligence and Security Services (*Komisija za nadzor obveščevalnih in varnostnih služb*) has powers similar to Luxembourg's Parliament Control Committee described on page 40, last paragraph (Article 25 para. 2 of the *Parliamentary Supervision of the Intelligence and Security Services Act*).⁶²

2.2.4 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 your Member State is mentioned, please update the data (new legislation, new report etc.)
3. If your 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 Slovenian Parliamentary Commission for the Supervision of the Intelligence and Security Services (*Komisija za nadzor obveščevalnih in varnostnih služb*) reports once a year to the parliament about its work and general supervision findings and proposes to parliament adoption of opinions and acceptance of resolutions.⁶³ However, the annual report must not

62 Slovenia, the Parliamentary Supervision of the Intelligence and Security Services Act (*Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb*, ZPNOVS), 26 February 2003, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3455.

63 Slovenia, the Parliamentary Supervision of the Intelligence and Security Services Act (*Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb*, ZPNOVS), 26 February 2003, Article 34, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3455.

encompass information about on-going activities that are of special interest for national security and information on individual cases of privacy limitations.⁶⁴ As noted above, the Slovenian Parliamentary Commission for the Supervision of the Intelligence and Security Services (*Komisija za nadzor obveščevalnih in varnostnih služb*) issued the annual report for 2014 on 23 April 2015. The non-classified summary of the report does not refer to issues related to Snowden revelations. It also does not mention any issues relevant to reporting to parliament. The report for 2015 is not yet available.

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 your Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If your 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. There is nothing to add to the analysis.*

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 your Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If your 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. There is nothing to add to the analysis.*

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. The reference on page 40 is accurate.*
2. *If your Member State is mentioned, please update the data (new legislation, new report etc.). There is no new data to add.*
3. *If your 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.*

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. A more exact formulation of the situation when court order is required on page 53, para. 2, would be that court orders are required for the “the interception of letters and other consignments, and the interception of telecommunications in the Republic of Slovenia”⁶⁵ and, additionally, for “the*

64 Slovenia, the Parliamentary Supervision of the Intelligence and Security Services Act (*Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb*, ZPONVS), 26 February 2003, Article 35, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3455

65 Slovenia, The Slovene Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji*, ZSOVA), 7 April 1999, Article 24, §1, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1884.

surveillance of telecommunications in the Republic of Slovenia by requiring the call related information”⁶⁶ (the so called “meta data”).

2. If your Member State is mentioned, please update the data (new legislation, new report etc.)
3. If your 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.

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 your Member State is mentioned, please update the data (new legislation, new report etc.)
3. If your 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. **There is nothing to add to 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 your Member State is mentioned, please update the data (new legislation, new report etc.)
3. If your 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. **There is nothing to add to the analysis.**

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. **The reference is accurate.**
2. If your Member State is mentioned, please update the data (new legislation, new report etc.) **There is nothing to add to the analysis.**
3. If your 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.

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 your Member State is mentioned, please update the data (new legislation, new report etc.)
3. If your 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. **There is nothing to add to the analysis.**

3.2.1 Lack of specialisation and procedural obstacles

66 Slovenia, The Slovene Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji, ZSOVA*), 7 April 1999, Article 24a, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1884.

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If your Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If your 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. There is nothing to add to the analysis.*

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 your Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If your 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. There is nothing to add to the analysis.*

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 your Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If your 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. There is nothing to add to the analysis.*

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 your Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If your 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. Given the exhaustive nature of the list of Member States where parliamentary bodies act as remedial bodies (p. 70), Slovenia should be added, due to Article 33 of the Parliamentary Supervision of the Intelligence and Security Services Act (*Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb*⁶⁷) which allows for an individual to file a complaint with the competent parliamentary commission. Figure 6 should be amended accordingly.*

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 your Member State is mentioned, please update the data (new legislation, new report etc.)*

67 Slovenia, Parliamentary Supervision of the Intelligence and Security Services Act (*Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb*, ZPNOVS), 6 February 2003, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3455.

3. *If your 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. There is nothing to add to the analysis.*

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. While the reference on page 74 is accurate, it should be added that the ombudsman under the Slovenian legislation is competent to file a constitutional complaint with the Constitutional Court of the Republic of Slovenia, given prior consent of the individual affected by a violation and provided prior effective legal remedies have been exhausted (Articles 50, §2, 51, §1, and 52, §2 of the Constitutional Court Act (*Zakon o Ustavnem sodišču*)).⁶⁸ While the ombudsman does not have the power to render legally binding decisions, it may facilitate further access to legal remedies.*
2. *If your Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *To expand further on the note on section 3.3.1.: The complaint filed with the Slovenian parliamentary commission on intelligence services oversight may result in an investigation of the alleged violation of his/her rights by the intelligence services. If the allegations are confirmed, he/she will be notified of the violation and may pursue other legal remedies. The commission does not have the power to render legally binding decisions.*
4. *If your 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.*

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 your Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If your 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. There is nothing to add to the analysis.*

Conclusions

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If your Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If your 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. There is nothing to add to the analysis.*

68 Slovenia, Constitutional Court Act (*Zakon o Ustavnem sodišču*, ZUstS), 18 March 1994, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO325.

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

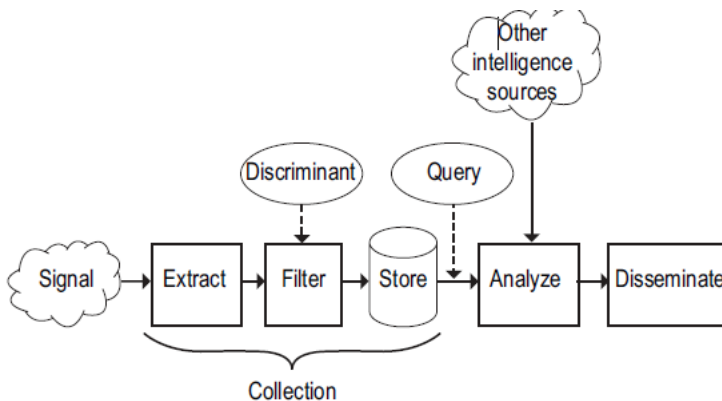
- Please, delete all lines not referring to your country in the table below (see Annex p. 93 of the FRA Report)
- Check accuracy of the data
- Add in track changes any missing information (incl. translation and abbreviation in the original language).
- Provide the reference to the national legal framework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

The table is accurate.

	Civil (internal)	Civil (external)	Civil (internal and external)	Military
SI			Slovene Intelligence and Security Agency/ Slovenska obveščevalno-varnostna agencija (SOVA)	Intelligence and Security Service of the Ministry of Defence/ Obveščevalno-varnostna služba Ministrstva Republike Slovenije za obrambo (OVS MORS)

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.
- The figure is accurate. No alternative description or conceptualisation of signal intelligence could be found.



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.

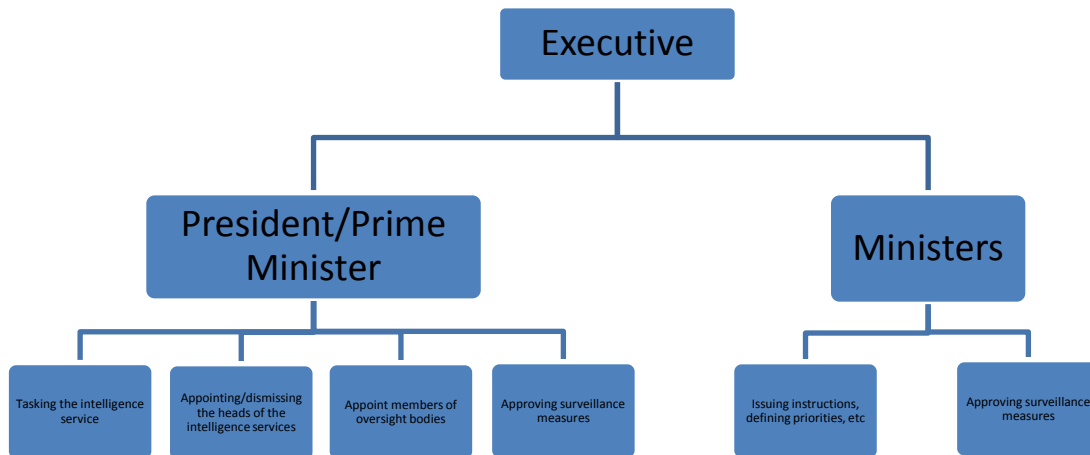
There are no expert bodies in Slovenia.



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.

This figure is appropriate.



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.

Member States	Essential powers	Enhanced powers
SI		X

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

According to the definition of “enhanced powers” in the FRA Report (p. 35) the Slovenian Parliamentary Commission for the Supervision of the Intelligence and Security Services (*Komisija za nadzor obveščevalnih in varnostnih služb*)⁶⁹ has enhanced power because it has the power to receive notifications and initiatives of individuals and organisations related to the prerogatives and tasks of the Parliamentary Commission according to the Article 13, para. 1, point 5 and Article 33 of the Parliamentary Supervision of the Intelligence and Security

69 The Parliamentary Supervision of the Intelligence and Security Services Act (*Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb, ZPNOVS*), 26 February 2003, available at: www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3455.

Services Act. Subsequently, The Parliamentary Commission has the power to investigate, i.e. inspect premises and equipment (Article 24 of the Act), and demand access to classified information (Article 25 of the Act). The Parliamentary Commission informs the Slovenian Parliament (*Državni zbor RS, DZ RS*) about its findings and proposes adoption of opinions and recommendations (Article 34 of ZPNOVS).

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.

EU Member State	Expert Bodies
SI	N.A.

The table is accurate.

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.

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

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

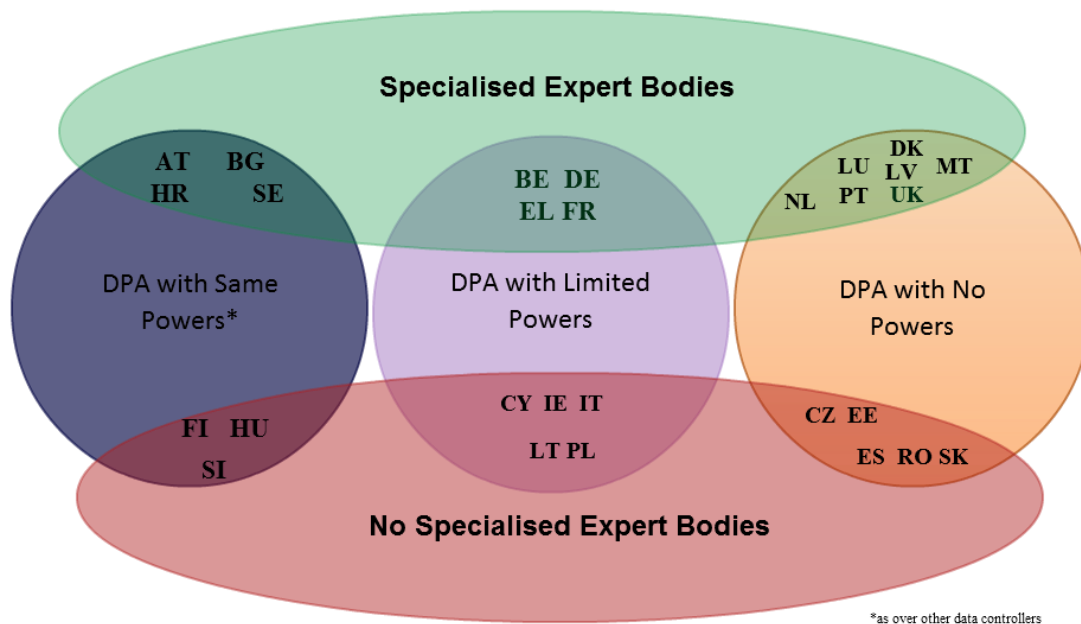
Same powers: refers to DPAs that have the exact same powers over NIS as over any other data controller.

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.

The table is accurate.

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 figure is accurate.

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.

EU Member State	Judicial	Parliamentary	Executive	Expert bodies	None
SI	X				X

The table is accurate.

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

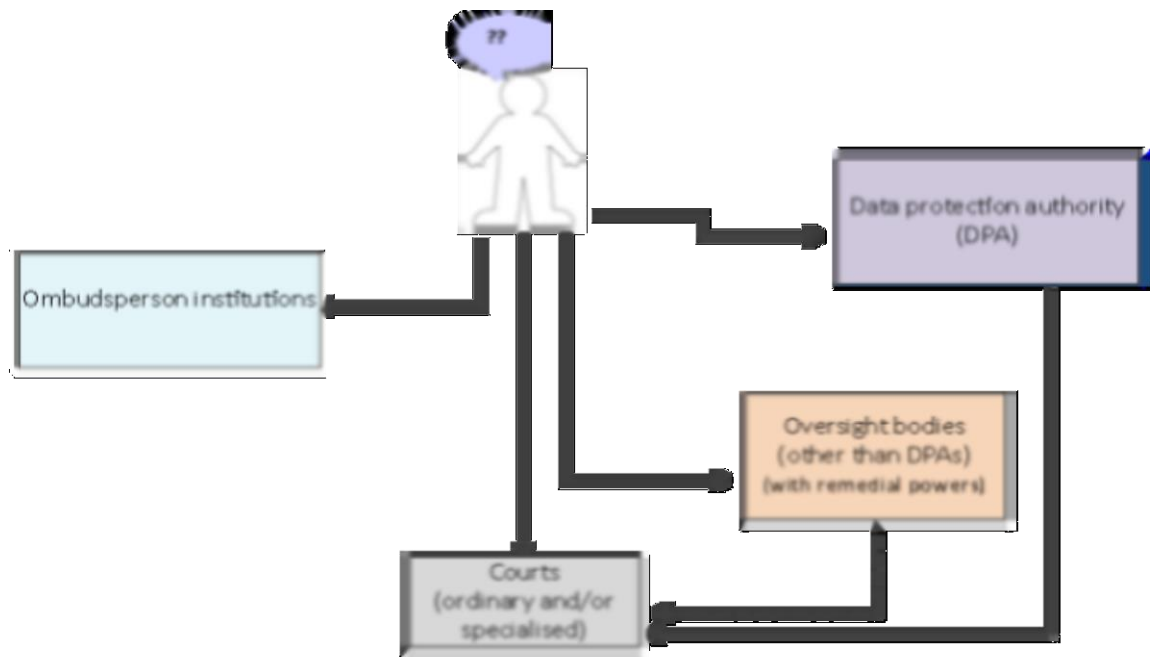
Please check the accuracy of Table 5 below (p. 55 of the FRA Report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

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

Not relevant.

1.5.11 Figure 5: Remedial avenues at the national level

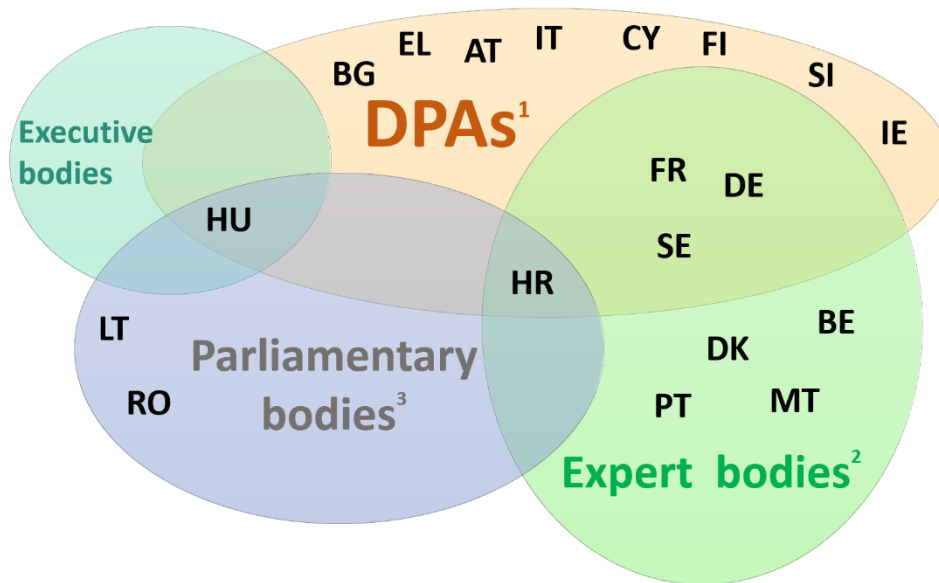
Please confirm that Figure 5 below (p. 60 of the FRA Report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.



The figure is accurate. Given that Slovenian Parliamentary Committee has the power to hear individual complaints, it should be added to the scheme.

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.



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

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 I can 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.

Given that parliamentary bodies, too, are competent to hear individual cases (without remedial powers), Slovenia should be positioned accordingly (i.e. both DPA and parliamentary bodies are competent to hear claims).