Short Thematic Report

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

Legal update

Country: POLAND

Version of 8 July 2016

FRANET contractor: Helsinki Foundation for Human Rights

Author(s) name(s): Barbara Grabowska-Moroz

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.*

Definition of "intelligence services" (FRA report, p. 13) applies in Poland to the Internal Security Agency (*Agencja Bezpieczeństwa Wewnętrznego*) and Intelligence Agency (*Agencja Wywiadu*). However, the definition of the so-called "special services" (civil ones) also includes the Central Anti-corruption Bureau, which aims mostly at fighting the crimes of corruption[1]. Statutory tasks of the Internal Security Agency cover e.g. prevention and combating crimes[2], fighting national security threats, protection of classified information. Whereas the tasks of the Intelligence Agency (e.g. analysing foreign threats to security) can be run only outside the territory of Poland[3]. In case of a need to conduct surveillance in Poland, the Intelligence Agency is obliged to conduct it through the Internal Security Agency[4].

The Internal Security Agency is entitled to conduct "operational control" (i.e. wire-tapping) only when fighting crimes listed in Article 5.1. point 2 of the Act on the Internal Security Agency. Moreover, the Agency is competent to access metadata (telecommunication, internet and postal data) in order to complete the tasks mentioned in Article 5.1., which also includes general fight with national security threats[5].

It is worth to mention that according to Article 27.15 after conducting "operational control," the Agency shall transfer gathered material to the prosecutor's office if there is evidence of committing a crime[6]. According to statistical data gathered by the Institute of Justice Administration (*Instytut Wymiaru Sprawiedliwości*) – a governmental think tank – the number of cases where gathered information was transferred to the prosecutor and allowed for criminal investigation amounts to approx. 5% of all cases where operational control was conducted[7]. It rises doubts whether operational control (targeted surveillance) run by the Internal Security Agency really aims only at combating crimes.

---

1 Poland, Act on Anti-corruption Buraeu (*Ustawa z 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym*), 9 June 2006.

2 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu)*, 24 May 2002, Article 5.1 point 2.

3 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu)*, 24 May 2002, Article 6.2.

4 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu)*, 24 May 2002, Article 6.3.

5 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu)*, 24 May 2002, Article 28.1.

6 Poland, Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu)*, 24 May 2002

7 Poland, D. Szumiło-Kulczycka, Use of information gathered at operational stage by courts of first instance in the crimnal proceedings (*Korzystanie w postępowaniu karnym przez sądy pierwszej instancji z informacji zebranych operacyjnie*), available at: http://www.iws.org.pl/pliki/files/IWS_Szumi%C5%82o-Kulczycka%20D._%28._.%29%20z%20inf.%20zebranych%20%20%20%20%20operacyjnie.pdf (accessed on 15 June 2016), 2014, p. 40-42.

These competences (analogous to the competences of law enforcement services) were subject to constitutional judicial review in 2014. In its judgement of 30 July 2014 the Constitutional Tribunal[8] ruled that provisions on access of law enforcement and special services to telecommunication data retained by the operators are incompatible with the Constitution due to lack of independent oversight[9]. The Tribunal stated that there is a constitutional requirement to establish a procedure that would guarantee a protection of the seal of confessional and professional secrets (e.g. of attorneys in law and journalists). The Tribunal ruled that the previous regulations should become invalid 18 months after the publication of the judgement, i.e. on 7 February 2016.

The first draft of law implementing this judgement was proposed by the Senate and sent to the Sejm as an official legislative initiative in July 2015. Due to the end of the Parliament's tenure, the draft was not adopted. On 23 December 2015, a group of MPs submitted a new draft. On 15 January 2016, the Sejm passed the Act and on 29 January 2016, the Senat adopted legislation in which it submitted no amendments to the Act. On 3 February 2016, the President of the Republic of Poland signed the Act[10] that became law on 7 February 2016.

The Act of 15 January 2016 amended the Act on Police and other acts (including the Act on the Internal Security Agency and Intelligence Agency). It created a mechanism of oversight of access to telecommunication and internet data based on the *ex-post* supervision conducted by the regional court (*sąd okręgowy*) on the basis of a semi-annual statistical report prepared by the law enforcement and security services[11]. The collection of telecommunications data by law enforcement agencies shall not be subject to any *ex ante* external supervision. Moreover, after conducting supervisory activities, the court will only be able to inform the supervised law enforcement service about the results, but will not be able to order destruction of collected data.

The scope of competence to access telecommunication and Internet data is extremely broad. In case of Police, it covers "preventing or discovering crimes" as well as "protection of human life or health, or supporting search and rescue activities." Access to telecommunications, postal and Internet data is justified by any actions taken by the Police in order to prevent or discover any crimes, and not the most serious ones. Internal Security Agency is competent to access these data in order to complete the Agency's statutory tasks[12]. Under current legislation, collecting telecommunications, postal or Internet data would not be subject to the principle of subsidiarity, i.e. there is no requirement that the access to the telecommunication data is possible only if and when less burdensome means turnout (or may turn out) not useful (ineffective).

Furthermore, the new regulation expands the ways of access to Internet data. According to Article 28.2 of Act on Internal Security Agency, a telecommunications enterprise, postal operator, or Internet service provider (ISP) shall make available free of charge the data via a telecommunications network to an Agency's officer in possession of written authorization[13].

The Act of 15 January 2016 provides that the confidential materials containing defence secrets or seal of confessional shall be destroyed. When it comes to attorneys' or journalists' professional secrets, such materials gathered by the Internal Security Agency (e.g. during wire-tapping) shall be obligatorily

8 Poland, Constitutional Tribunal, judgement of 30 July 2014, case no. K 23/11, available [in English] at: http://trybunal.gov.pl/en/hearings/judgments/art/7004-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani/ (accessed on 12 May 2016).

9 Podkowik J., (2015) Privacy in the digital era – Polish electronic surveillance law declared partially unconstitutional. Judgment of the Constitutional Tribunal of Poland of 30 July 2014, K 23/11, European Constitutional Law Review, pp. 577-595.

10 Poland, Act amending Act on Police and other acts [*Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw*], 15 January 2016. English translation of the Act is available at: http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2016)036-e.

11 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu)*, 24 May 2002, Article 28a.

12 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu)*, 24 May 2002, Article 28.1.

13 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu)*, 24 May 2002

conveyed to the prosecutor who, however, shall not be able to verify such information and order their destruction, but will have to automatically convey them to the court. In turn, the court shall rule on their admissibility in a criminal proceeding "if such is necessary for the interests of justice and the circumstances may not be established pursuant to other evidence." The court shall also rule on the destruction of inadmissible materials[14]. The Venice Commission found that such a procedure is insufficient and that the law should prohibit surveillance of communications which are on the face covered by a lawyer-client privilege and should describe the circumstances in which privileged professional communications could be secretly recorded and then introduced as evidence[15].

Transitional regulations of the Act of 15 January 2016 also engender serious reservations. The regulations provide for the possibility of continued use of hitherto applicable regulations despite the fact that these have been deemed unconstitutional by the Tribunal[16].

The Act of 15 January 2016 was a subject of the Venice Commission opinion[17] adopted in June 2016. It focused on "regular law enforcement action" regulated by the Act. As the Venice Commission stated, all amended acts (including the Act on the Internal Security Agency) employ basically the same model of surveillance, thus the Commission's comments on the Act on the Police may serve "as an illustration of regulations concerning other agencies"[18]. The Commission recommended to supplement the existing system of judicial pre-authorisation of classical surveillance with additional procedural safeguards, such as "privacy advocate", complaints mechanism, a system of *ex-post* automatic oversight by independent body. In respect to metadata collection, the Venice Commission recommended providing an effective mechanism of oversight of specific operations by an independent body that would have adequate investigative powers and expertise[19].

Since the Internal Security Agency, while conducting "operational control," gathers evidence of crimes, relevant amendment of the Code of Criminal Proceedings was introduced in March 2016[20]. It introduced a provision which states that evidence cannot be considered inadmissible solely on the grounds that it was obtained in violation of the rules of procedure or by means of an offence, unless the evidence has been obtained in connection with the performance by a public official duties as a result of murder, wilful causing of bodily injury or imprisonment[21]. Moreover, the amendment deleted the so-called "ex-post consent procedure" (*kontrola następcza*) conducted by the court. According to the previous law, if operational surveillance provided an evidence of a different crime or committed by a different person, the decision of the court was required. Act of 11 March 2016 deleted this procedure and provided that only a consent of prosecutor is required[22].

In March 2016, a new Law on the Prosecutor's Office entered into force[23]. According to the new law, the office of the Prosecutor General is held by the Minister of Justice[24]. It raises doubts concerning the

14 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu)*, 24 May 2002, Article 27.15h-15l.

15 Council of Europe, Venice Commission, Opinion on the Act of 15 January 2016 amending the Police Act and certains other acts, CDL-AD(2016)012, 13 June 2016, § 85.

16 Poland, Act amending Act on Police and other acts [*Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw*], 15 January 2016, Article 13, 15-16.

17 Council of Europe, Venice Commission, Opinion on the Act of 15 January 2016 amending the Police Act and certains other acts, CDL-AD(2016)012, 13 June 2016.

18 Council of Europe, Venice Commission, Opinion on the Act of 15 January 2016 amending the Police Act and certains other acts, CDL-AD(2016)012, 13 June 2016, § 7.

19 Council of Europe, Venice Commission, Opinion on the Act of 15 January 2016 amending the Police Act and certains other acts, CDL-AD(2016)012, 13 June 2016, § 133.

20 Poland, Act amending Code of Criminal Procedure and other acts (*Ustawa z dnia 11 marca 2016 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw*), 11 March 2016.

21 Poland, Act amending Code of Criminal Procedure and other acts (*Ustawa z dnia 11 marca 2016 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw*), 11 March 2016, Article 168a

22 Poland, Act amending Code of Criminal Procedure and other acts (*Ustawa z dnia 11 marca 2016 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw*), 11 March 2016, Article 168b.

23 Poland, Law on Prosecutor Office (*Prawo o prokuraturze*), 28 January 2016.

independence of prosecutors, since the Prosecutor General is entitled to influence every investigation (e.g. Prosecutor General may give instructions concerning the ongoing investigation[25]). It is particularly relevant when it comes to effectiveness of oversight over special services, conducted by the prosecutor's office. Such an oversight covers access to classified files containing information gathered during surveillance[26]. Details of the oversight shall be regulated by the Minister of Justice[27]. Moreover, the new law allows the Prosecutor General to order the competent authorities to conduct operational surveillance (*czynności operacyjno-rozpoznawcze*), if it is related to the ongoing investigation[28]. The Prosecutor General presents annual statistical data on "operational control" to Sejm and Senat[29].

On 10 June 2016, the Sejm adopted the Anti-terrorism Law[30]. It broadens the competences of the Internal Security Agency. According to the new law, the Chief of the Internal Security Agency will be entitled to order 3-months wire-tapping of a foreigner, without a judicial order, if there is a risk that he/she is involved in terrorist activities[31]. The Minister of Internal Affairs will define a catalogue of situations that might be considered as "terrorists events" (*katalog incydentów o charakterze terrorystycznym*)[32]. A draft of such catalogue contains e.g. establishing a Muslim academia or a visit of an Islamic cleric in prison[33]. The competences of the Internal Security Agency will be broadened to create a wide access to all public registers. The Act entered into force on 2 July 2016.

In November 2015, the Sejm amended the internal Rules of the Sejm,[34] regulating the number of members of the Committee on Special Services which conducts control of special services actions.

2. the important (higher) court decisions in the area of surveillance

On 28 April 2016 the Supreme Administrative Court ruled the case initiated by the Helsinki Foundation for Human Rights against the Internal Security Agency. Case dealt with motion on access to public information concerning Snowden revelations, including aspects of international intelligence cooperation (i.e. whether Internal Security Agency was involved in mass surveillance programs) and what means were used within such cooperation (i.e. XKeyscore programme)[35]. The Court found that information on surveillance methods used by the Agency should remain secret. Moreover, the Court ruled that there is an absolute prohibition of making this information available to the public. The interpretation of the Court was based e.g. on Article 39.3 of the Act on the Internal Security Agency[36] and on the Act on the protection of classified information[37]. However, according to the Court, it does not imply that all future motions concerning access

---

24 Poland, Law on Prosecutor Office (*Prawo o prokuraturze*), 28 January 2016, Article 1.2.
25 Poland, Law on Prosecutor Office (*Prawo o prokuraturze*), 28 January 2016, Article 8.2-3.
26 Poland, Law on Prosecutor Office (*Prawo o prokuraturze*), 28 January 2016, Article 57.2.
27 Poland, Law on Prosecutor Office (*Prawo o prokuraturze*), 28 January 2016, Article 36.4.
28 Poland, Law on Prosecutor Office (*Prawo o prokuraturze*), 28 January 2016, Article 57.3.
29 Poland, Law on Prosecutor Office (*Prawo o prokuraturze*), 28 January 2016,Article 11
30 Poland, Act on anti-terrorist actions (*Ustawa o działaniach antyterrorystycznych*), 10 June 2016.
31 Poland, Act on anti-terrorist actions (*Ustawa o działaniach antyterrorystycznych*), 10 June 2016, Article 9.
32 Poland, Act on anti-terrorist actions (*Ustawa o działaniach antyterrorystycznych*), 10 June 2016, Article 5.2.
33 Poland, Draft of Regulation of Minister of Internal Affairs and Administration on catalogue of terrorist events (Projekt Rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie katalogu zdarzeń o charakterze terrorystycznym), available at: http://orka.sejm.gov.pl/Druki8ka.nsf/0/9CCA65458151278AC1257FB50049D701/%24File/516.pdf (accessed on 14 June 2016), version of 16 May 2016.
34 Poland, Resolution of Sejm amending Rules of Sejm (*Uchwała Sejmu Rzeczypospolitej Polskiej w sprawie zmiany Regulaminu Sejmu Rzeczypospolitej Polskiej*), 13 November 2015.
35 Poland, Supreme Administrative Court, judgement, no. I OSK 2620/14, 28 April 2016.
36 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu)*, 24 May 2002.
37 Poland, Act on protection of classified information (*Ustawa o ochronie informacji niejawnych*), 5 August 2010.

to such information will be denied. The Court stated: "The fact that people who violate the law do not have knowledge about the methods of surveillance is preventive in its nature and hinders criminal activity". The Court also made a comment that the social control of special services should not relate to concrete surveillance methods employed by the special services. When it comes to the questions of international cooperation, the Court ruled that the Internal Security Agency should justify its decision (denying access to requested information) in a more detailed way. The Court emphasized that the Court does not have specialized knowledge in this respect.

2. *the reports and inquiry by oversight bodies (parliamentary committees, specialised expert bodies and data protection authorities) in relation to the Snowden revelations*

There was no investigation concerning information revealed by Edward Snowden.

3. *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.*

There was no parliamentary or expert investigation concerning information revealed by Snowden.

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.*[38]

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.*

According to Article 8 of the Act on the Internal Security Agency and the Intelligence Agency[39], the chief of the Agency is entitled to undertake cooperation (*podejmować współdziałanie*) with organs and services of other states in order to perform the statutory tasks of the Agency. Undertaking such cooperation requires the previous consent of the Prime Minister. The analogous regulation applies to the chief of the Central Anti-Corruption Bureau[40]. The statute does not regulate what kind of data can be exchanged. It does not provide how detailed the agreements concerning cooperation shall be either.

According to the Regulation of the Prime Minister concerning the tasks of so-called Minister-Coordinator[41], it is the role of the Minister-Coordinator to set goals and directions of development of international cooperation of special services and evaluating the effects of this cooperation. He is also responsible for cooperation with foreign and international bodies competent to control and oversee special services. The Regulation does not contain further provisions on details of cooperation.

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.*

38 http://www.dcaf.ch/Publications/Making-International-Intelligence-Cooperation-Accountable

39 Poland, Act on the Internal Security Agency and the Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*), 24 May 2002.

40 Poland, Act on Central Anti-Corruption Bureau (*Ustawa o Centralnym Biurze Antykorupcyjnym)*, 9 June 2006.

41 Poland, Regulation of Prime Minister on detailed scope of actions of Minister-Member of Council of Ministers Mariusz Kamiński (*Rozporządzenie Prezesa Rady Ministrów z dnia 18 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra – Członka Rady Ministrów Mariusza Kamińskiego – Koordynatora Służb Specjalnych*), 18 November 2015.

Information concerning international cooperation is covered with the highest clearance (the level of clearance depends on the kind and level of harm that might be caused if a document becomes public). Moreover, according to Article 7.1 point 3 of Act on protection of classified information, information received from a foreign state or international organisation are protected regardless of time that passed, if such was a condition of receiving the information[42]. Even members of the Parliamentary Committee must obtain such a special clearance. Meetings of the Committee are held in camera. Usually, the topics of their meetings deal with general issues, including international cooperation. The case of so-called "CIA black sites" was discussed by the Committee, but no further investigation was held by the Committee. It is worth to mention that the parliamentary Committee on Special Services is not entitled to run such an investigation on its own.

Within the government, there is a Collegium on Special Services, an advisory body in the field of programming, oversight and coordination of special services[43]. It is the Collegium's statutory task to present opinions concerning issues of international cooperation. However, the schedules of meetings and their agenda depend on the Prime Minister and the Secretary of the Collegium.

Judgements of the European Court of Human Rights[44] show how challenging is the oversight of international cooperation between security and intelligence services. Moreover, the Court identified more general doubts whether the oversight of special services in Poland is effective. The Court stated: "*The protection of human rights guaranteed by the Convention, especially in Articles 2 and 3, requires not only an effective investigation of alleged human rights abuses but also appropriate safeguards – both in law and in practice – against intelligence services violating Convention rights, notably in the pursuit of their covert operations. The circumstances of the instant case may raise concerns as to whether the Polish legal order fulfils this requirement*"[45].

The case concerning secret CIA detention in Poland shows also shortcomings of conducting – by prosecutor office – effective investigation concerning international intelligence cooperation. The issue is even more challenging bearing in mind that since 4 March 2016 the office of Prosecutor General is held by Minister of Justice, which might seriously undermine the independence of prosecutors and investigations. The Prosecutor General is also entitled to change the secrecy clause (*klauzula tajności*) of classified information or even declassify it. It might be particularly important in the case of investigating international intelligence cooperation (i.e. investigation concerning secret CIA detention site in Poland)[46].

Oversight of international cooperation causes a set of problems also at the international level of such oversight. The Committee of Ministers of the Council of Europe, which oversees the execution of the ECHR judgements on CIA secret rendition (Al Nashiri v. Poland), has noted serious obstacles of Poland with guaranteeing the rights of the applicants[47]. During its last meeting in June 2016, the Committee decided "in the absence of information convincingly addressing the root causes of the other violations, called on the authorities to reflect not only on the oversight of the daily operational work of the intelligence services, but also to scrutinise high-level decision making in this area"[48].

42 Poland, Act on protection of classified information (*Ustawa o ochronie informacji niejawnych*), 5 August 2010.

43 Poland, Act on the Internal Security Agency and the Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*), 24 May 2002

44 European Court of Human Rights, Al Nashiri v. Poland, No. 28761/11, judgement, 24 July 2014; European Court of Human Rights, Abu Zubaydah v. Poland, No. 7511/13, 24 July 2014.

45 European Court of Human Rights, Al Nashiri v. Poland, No. 28761/11, judgement, 24 July 2014, § 498

46 Poland, Law on Prosecutor Office (*Prawo o prokuraturze*), 28 January 2016, Article 57.5.

47 Helsinki Foundation for Human Rights, Council of Europe concerned with no progress in Polish CIA secret prisons inquiry, available at: http://www.hfhr.pl/en/council-of-europe-concerned-with-no-progress-in-polish-cia-secret-prisons-inquiry/, 18 March 2016.

48 Decision of Commitee of Ministers of Council of Europe, available at: https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168065c7b4, 7-8 June 2016.

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)[49] (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?*

According to the Act on Access to Public Information[50], such an access can be limited on the basis of rules concerning protection of classified information[51] and other secrets established by law.

According to the Act on the Internal Security Agency and the Intelligence Agency, the Head of the Agency is obliged to protect the means, forms and methods (*środki, formy, metody*) of realization of the Agency's tasks, including e.g. gathered information and data of the officers[52]. Such forms and methods are regulated by internal ordinance by the Head of Agency[53]. Access to such information is also limited for the court and prosecutor. In case the Chief of Internal Security Agency refused such access, the decision whether to grant access to such information is given by the President of the Supreme Court[54].

According to the case-law of the administrative courts, the refusal of access to such information (requested by the individual) is allowed, but as a legal basis the Agency needs to indicate the Act on Access to Public Information, and not solely the obligation to protect the forms and methods of operational work established in Article 35.1 of the Act on the Internal Security Agency and Intelligence Agency. The judgement of the Supreme Administrative Court of April 2016 – described in the Summary – strengthened this interpretation by stating that there is an absolute prohibition of making information on surveillance methods available to the public.

In 2014, the Constitutional Tribunal ruled that "*it is necessary to introduce a legal obligation to disclose to the public compiled statistical data on the number and types of operational and investigative activities that are carried out and which interfere in constitutional rights and freedoms of the individual*"[55].

2. *Do individuals have the right to access information on whether they are subject to surveillance?*

The Act on Police states that a person subject to surveillance shall not have access to information gather during the operational control[56]. Such provision was not included in the Act on the Internal Security Agency and Intelligence Agency, but it is interpreted in a similar way. It does not create an obligation of notification of such surveillance.

Act on access to public information does not regulate the issue of access to information about being subject to surveillance. The Regional Administrative Court ruled in June 2015 a case of a former judge who filed a motion for information whether she was subject to surveillance. The Court found that

---

49 http://www.right2info.org/exceptions-to-access/national-security/global-principles#section-10
50 Poland, Act on Access to public information (*Ustawa o dostępie do informacji publicznej*), 6 September 2001.
51 Poland, Act on Access to public information (*Ustawa o dostępie do informacji publicznej*), 6 September 2001, Article 5.1.
52 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu*), 24 May 2002, Article 35.1.
53 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu*), 24 May 2002, Article 19.3.
54 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu*), 24 May 2002, Article 39.6.
55 Poland, Constitutional Tribunal (*Trybunał Konstytucyjny*), judgement, case no. K 23/11, 30 July 2014.
56 Poland, Act on the Police (*Ustawa o policji*), 6 September 1990, Article 19.16.

denial of access to such information was poorly reasoned by the prosecutor's office and that the law does not prohibit access to such information. The judgement is not final[57].

The person is entitled to access such information during the pre-trial stage of prosecutor investigation. If no investigation was initiated, the person will not be notified about the surveillance. The Constitutional Tribunal ruled in 2006 that there is a constitutional obligation to introduce a procedure of notifying a person subject to surveillance after it was completed[58]. The decision of 2006 related directly to the Act on Police, but in the judgement of 2014, the Constitutional Tribunal ruled that *"it is not ruled out that differentiation may be introduced with regard to the intensity of the protection of privacy, informational self-determination as well as the privacy of communication, depending on whether data on given persons are obtained by intelligence services and state security services or whether they are gathered by police forces"*[59]. In the light of above, the decision of Constitutional Tribunal of 2006 may cover gathering information by intelligence services as well.

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.*

   N/A

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

   N/A

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

   None.

1 Intelligence services and surveillance laws

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

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

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

1.1 Intelligence services

57 Poland, Regional Administrative Court in Warsaw (Wojewódzki Sąd Administracyjny w Warszawie), case no. II SA/Wa 140/15, 3 June 2015.
58 Poland, Constitutional Tribunal (*Trybunał Konstytucyjny*), judgement, case no. S 2/06, 25 January 2006.
59 Poland, Constitutional Tribunal (*Trybunał Konstytutcyjny*), judgement, case no. K. 23/11, 30 July 2014.

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
   Correct: In some Member States, such as France, Germany, Italy, Romania and Poland, civil intelligence services are further divided into two separate services, mandated with a domestic or foreign scope. Moreover, some Member States grant intelligence-like means to units specialised in a defined threat, such as organised crime in Spain, corruption in Poland or the fight against terrorism in Hungary.

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

   The Act on the Internal Security Agency and the Intelligence Agency was amended in January 2016 but it did not change the nature or number of special services in Poland. There are five special services in Poland. The Intelligence Agency is not entitled to conduct wire-tapping on the territory of Poland, thus such operations are conducted through the Internal Security Agency[60].

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.*

   N/A

1.2 Surveillance measures

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

   In 2014, the Constitutional Tribunal ruled that "*it is desirable to specify by statute the types of measures used for the secret obtaining of information, as well as the types of information obtained with particular measures*"[61]. The case concerned the previous wording of e.g. Act on Police which stated that "*Operational surveillance shall be carried out in secret and shall consist in: (…) applying technical measures that make it possible to secretly obtain information and evidence as well as to record them, including the content of telephone conversations and other information transferred via telecommunications networks*". The Tribunal found that such provisions is specified enough and does not violate the Constitution. However, it ruled that the provision should be interpreted in a way that "*a competent authority ordering operational surveillance is obliged to indicate the type of a technical measure prescribed by law for obtaining information and evidence as well as for recording them*".

   However, the law concerning the operational surveillance was amended in January 2016 and it provides that operation surveillance is based on:

   1) collecting and recording the contents of conversations conducted using technical means including via telecommunications networks;
   2) collecting and recording images or sounds of persons from indoors, means of transport or locations other than public places;
   3) collecting and recording the contents of correspondence including correspondence conducted via electronic means of communication;
   4) collecting and recording data contained in data carriers, telecommunications terminal devices, information technology and tele-information systems;
   5) collecting access to and review of the contents of posted mail.

60 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu*), 24 May 2002, Article 6.3.
61 Poland, Constitutional Tribunal's rulling no. K 23/11, 30 July 2014

Operational control (tradition targeted surveillance) is regulated in almost the same way for both – law enforcement and special services (Internal Security Agency, Intelligence Agency and Central Anti-corruption Bureau).

Moreover, the Act on Internal Security Agency and Intelligence Agency provides that one of the tasks of Intelligence Agency is to conduct "electronic intelligence" (*prowadzenie wywiadu elektronicznego*)[62]. Since this competence is not regulated in law (it is just mentioned once in the Act on the Internal Security Agency and Intelligence Agency), it is difficult to precisely describe the nature of such surveillance. Most probably, it is an example of untargeted surveillance.

Detailed regulations in the Act on the Internal Security Agency and Intelligence Agency relate to targeted surveillance (so called operational control)[63] and untargeted surveillance which covers access to metadata (telecommunication, internet and postal data)[64].

What is important, amendments of January 2016 broadened the ways of access the internet data held by the ISPs. According to law, it is possible for Internal Security Agency to access such information via a telecommunications network to a police officer in possession of written authorization (if certain technical requirement are met)[65].

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.*

Correct: Page 24, footnote 157, reference to judgement of the Constitutional Court.

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

N/A

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

The Internal Security Agency is entitled to conduct "operational control" (i.e. wire-tapping) only when fighting crimes listed in Article 5.1. point 2 of the Act on the Internal Security Agency. Moreover, the Agency is competent to access metadata (telecommunication and internet data) in order to complete tasks mentioned in Article 5.1 which also includes general fight with national security threats.

It is doubtful whether law regulating the access to telecommunication and internet data is precise enough. The Internal Security Agency is entitled to collect telecommunication, postal and internet data (which does not constitute the contents of, respectively, telecommunications messages, posted mail or messages through services provided in electronic format) in order to complete its tasks[66].

---

62 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu*), 24 May 2002, Article 6.1 point 8.

63 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu*), 24 May 2002, Article 27.

64 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu*), 24 May 2002, Article 28.

65 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu*), 24 May 2002, Article 27.

66 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu*), 24 May 2002, Article 28.

Moreover, one of the tasks of the Internal Security Agency is to investigate, prevent and detect crimes "harming the economic foundations of the state". In 2014, the Constitutional Tribunal ruled that such task that allows for conducting operational surveillance is not precise enough and violates the Constitution. Amendments adopted in January 2016 introduced more precise rules on operational surveillance but did not amended the provision regulating task dealing with crimes "harming the economic foundations of the state". Such a broad task is still a legal basis for access the telecommunication and internet data.

Anti-terrorism law gives broad powers to the Internal Security Agency. The use of new surveillance competences are based on a broad definition of "offence of a terrorist nature" which is a "prohibited act, subject to imprisonment with the upper limit of at least five years, committed in order to: 1) seriously intimidate many persons; 2) to compel the public authority of the Republic of Poland or of the other state or of the international organisation to undertake or abandon specific actions; 3) cause serious disturbance to the constitutional system or to the economy of the Republic of Poland, of the other state or international organisation and a threat to commit such an act".[67].

FRA key findings

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

   N/A

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

   N/A

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.*

   Intelligence services in Poland are described as "special services", which covers the Internal Security Agency, Intelligence Agency and Central Anti-corruption Bureau. The last one is in fact a law enforcement entitled to conduct surveillance within the scope of its mandate (combating corruption).

   The Internal Security Agency deals with threats to national security, protects classified information and prevents and combats crimes listed in Article 5.1 point 2. of the Act on the Internal Security Agency and Intelligence Agency. Types of surveillance – targeted wire-tapping (so-called operational control) and untargeted (access to telecommunication, internet and postal data) are regulated in a similar way in all acts regulating special services and law enforcement. Especially the second type of surveillance is very broad – in case of the Internal Security Agency it relates to the obligation to "complete its statutory tasks", which covers both – fighting crimes and preventing general threats to the internal security of the state.

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.*

   Correct. Page 31: Poland employs an "agent for the control of personal data processing" within the Central Anti-Corruption Bureau.

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

   "Agent for the control of personal data processing" publishes annual reports. Verifications of personal data conducted by the agent are: periodical (every 5 years), current (by each agent)

67 Poland, Criminal Code (*Ustawa z dnia 6 czerwca 1997 r. Kodeks karny*), 6 June 1997**;** Poland, Draft of Act on anti-terrorism actions, 9 May 2016.

and special (by applying special procedures provided by law)[68]. Since the function is conducted by one person it is difficult to state to what extent the verification conducted by the Agent is effective. HFHR has requested the reports of the last 3 years.

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.*
N/A

2.1 Executive control

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

Correct*:* In Poland, the Prime Minister appoints and dismisses the heads of the Polish intelligence services. She/he is in charge of approving their intelligence objectives and has the most far-reaching competences in terms of oversight of the intelligence services within the country. However, the Supreme Audit Office found that his/her oversight lacks efficacy, since she/he does not have access to the internal procedures of the intelligence services. The information given by the services both as to the content and the means by which intelligence is collected cannot therefore be verified.

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

Tasks of the Prime Minister with respect to oversight of special services were transferred to so-called Minister-Coordinator of Special Services. It was transferred by the resolution of the Prime Minister and not by the statute, thus it raises questions concerning legality of such decision[69]. One of the previous regulations was challenged before the Constitutional Tribunal as unconstitutional, but since it was derogated and was not binding any more, the Tribunal discontinued the case[70].

The Prosecutor General conducts certain competences related to the oversight of surveillance. His consent is required in the procedure of ordering "operational surveillance". New position of Prosecutor General, who is member of government, results that his/her oversight shall be recognised as an "executive control". New anti-terrorism law broadens his/her competences in this respect.

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.*
N/A

2.2 Parliamentary oversight

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
Footnote 236 (referring to the powers of the Committee): Poland, Resolution of the Polish Sejm on the Polish Sejm's Rules of Procedure (*Uchwała Sejmu Rzeczypospolitej Polskiej Regulamin Sejmu Rzeczypospolitej Polskiej*), 30 July 1992, Art. 140.
Correct

2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
N/A

68 Poland, Protection of personal data in Central Anti-Corruption Buraeu, [presentation], available at: http://www.giodo.gov.pl/plik/id_p/9972/j/pl/ .

69 Poland, Regulation of Prime Minister on detailed scope of actions of Minister-Member of Council of Ministers Mariusz Kamiński (*Rozporządzenie Prezesa Rady Ministrów z dnia 18 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra – Członka Rady Ministrów Mariusza Kamińskiego – Koordynatora Służb Specjalnych*), 18 November 2015

70 Poland, Constitutional Tribunal, decision no. U 3/12, 20 March 2013.

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.*
N/A

2.2.1 Mandate

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
Correct: page 36

2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
N/A

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

In 2012, the group of MPs submitted a draft of law which aimed at broadening the mandate of the parliamentary Committee on Special Services (*Komisja ds. Służb Specjalnych*). It proposed that the Committee could conduct their own investigations. Currently, such parliamentary investigations might be conducted only if special "investigative commission" is established. Thus existing Committees, including Committee on Special Services, do not have competence to run their own investigations. The draft was not however adopted by the end of the Parliament's tenure.

2.2.2 Composition

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

Page 40: "Vetting, that is to say, assessing parliamentarians' backgrounds to identify any risks involved in providing the MPs with security clearance, is one way of ensuring the protection of classified information. It is required in the parliamentary oversight committees of Estonia, Hungary, Latvia, Lithuania, and Poland".

Correct

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

In November 2015, the Sejm amended the internal Rules of Sejm[71]. It limited the number of members of Committee on Special Services. According to new law, the Committee consists of up to 7 members (previously is was composed up to 9 members)[72]. Currently, four members of the Committee are affiliated with the government majority, which might seriously undermine the efficiency of parliamentary control of special services. The Rules of the Sejm provide that the Sejm decides on the number of members of the Committee. Candidatures for the members shall be submitted by a group of at least 35 MPs[73] and the Sejm votes jointly on all candidatures.
Moreover, the resolution adopted in November deleted the provision which stated that the function of President of the Committee and Vice-President of the Committee is held by 6 months be each member of the Committee.

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.*

71 Poland, Resolution of Sejm amending the Rules of the Sejm (*Uchwała Sejmu Rzeczypospolitej Polskiej w sprawie zmiany Regulaminu Sejmu Rzeczypospolitej Polskiej*), 13 November 2015.
72 Poland, Rules of Sejm (*Regulamin Sejmu*), Article 137.1.
73 Poland, Rules of Sejm (Regulamin Sejmu), 30 July 1992, Article 137.3.

N/A

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.*

N/A

2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
N/A

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.*
According to the Rules of Sejm, access to classified data with "secret" and "top secret" clause, is regulated by Act on protection of classified information[74]. Then the MPs and Senators need to be verified under "expanded checking procedure" (*poszerzone postępowanie sprawdzające*)[75].

2.2.3 Reporting to parliament

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

N/A

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

N/A

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.*

N/A

2.3 Expert oversight

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

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

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

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.*

Table: page 42 [**Correct**]

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

74 Poland, Rules of Sejm (*Regulamin Sejmu*), 30 July 1992, Article 137.4.
75 Poland, Act on protection of classified information (*Ustawa o ochronie informacji niejawnych*), 6 August 2010, Article 34.12.

N/A

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.*
N/A

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.*

Page 47: In nine Member States (Belgium, Cyprus, France, Germany, Greece, Ireland, Italy, Poland, Lithuania), DPAs have limited powers over intelligence services.
Correct

Footnote 365 - **Correct**

Page 48: Some DPAs lack the power to handle complaints of individuals related to data processing activities by intelligence services, or to issue binding decisions (Belgium, Poland).
Correct

Footnote 366 – **Correct**

Page 48: Investigatory powers, especially the powers to request and/or access data and premises, are also limited (France, Germany, Ireland and Poland).

Correct

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

In 2014, Senate Committee discussed a draft of law which aimed at broadening the competences of DPAs also on security services, but it was not adopted after all[76]

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.*

N/A

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.*

Page 54: Other countries, such as Poland and Romania, have a two-tiered system of judicial approval.
Correct

2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
Before March 2016, the requirement for the Prosecutor General's consent for operational surveillance was treated as independent from the government (however still independent court order was required). Now, the Prosecutor General is a member of the Government.

76 Poland, Draft of law amending rules on access to telecommunication data (*Projekt ustawy o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjnych*), available at:
http://www.senat.gov.pl/gfx/senat/userfiles/_public/k8/komisje/2015/kpcpp/materialy/bilingi/wniosek_nik_bilingi03120020140221095724.pdf, February 2014. Article 4 of the draft provided amendment of Article 43.2 of Data Protection Act (Ustawa o ochronie danych osobowych), 29 August 1997.

According to Law on Prosecutor, Prosecutor General is competent to order law enforcement and security services to initiate "operational actions" (*czynności operacyjno-rozpoznawcze*)[77]. The two-tired system of judicial approval applies to "operational control" (i.e. wire-tapping) which is the most invasive form of surveillance (detailed description of forms were described in 1.2 Surveillance measures). "Operation actions" is a broader term and covers also less intrusive forms such as observation or access to phone records without access to the content of communication.

Moreover, the draft of the Anti-terrorism law provides that the Prosecutor General will be the only oversight body of surveillance targeted at foreigners. According to the Anti-terrorism law, the same forms of operational control will be ordered by the Chief of the Internal Security Agency for 3 months without judicial approval. It is aimed at foreigners who might pose a terrorist threat. The Chief of the Agency will have to inform the Prosecutor General about this case and the Prosecutor General will by competent to order its termination. Judicial approval will be required after 3 months of such surveillance[78].

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.*

N/A

FRA key findings

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

2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
   N/A

3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*
   None.

3 Remedies

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

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

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

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.*

Page 62: The obligation to information and the right to access are not provided for in eight Member States (the Czech Republic, Ireland, Latvia, Lithuania, Poland, Slovakia, Spain and the United Kingdom).

Correct

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

77 Poland, Act on Prosecutor Office (*Prawo o prokuraturze*), 28 January 2016.

78 Poland, Act on anti-terrorist actions (*Ustawa o działaniach antyterrorystycznych*), 10 June 2016, Article 9.

Even though the obligation of notification is still not introduced, recently the individuals submitted motions to special services asking if they were under surveillance. They argue, that according to Article 51 of the Constitution they are entitled to know what information about them were gathered by the state institutions[79].

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.*
N/A

3.2 Judicial remedies

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

2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
N/A

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.*
N/A

3.2.1 Lack of specialisation and procedural obstacles

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

Page 68: This is why individuals may prefer to access justice via non-judicial avenues or through intermediaries, such as relevant civil society organisations. The latter may play a vital role in taking such complaints to court when class actions are allowed[506], as well as in bringing cases of a more general nature requesting access to specific information on the activities and investigative methods of intelligence authorities to contribute to greater transparency and accountability in this area.

The sentence refers to "class action" cases and footnote 506 refers to HFHR case on access to public information, which is not a class action case. This footnote should relate to the second part of the sentence ("as well as in bringing cases of a more general nature requesting access to specific information...").

2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
N/A

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.*
N/A

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.*
N/A

2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
N/A

79 Poland, E. Ivanova, *Obywatel nie dowie się, że był inwigilowany*, available at: http://prawo.gazetaprawna.pl/artykuly/925250,inwigilacja-obywatel-nie-dowie-sie-ze-byl-inwigilowany.html.

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 still no special procedure (or institution, e.g. special advocate) within the court administrative proceedings that would guarantee (for the applicant) at least a partial access to classified information that were legal basis for e.g. decision on expulsion from Poland due to causing danger for public security.

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.*

   N/A

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

   N/A

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.*

   N/A

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.*

   N/A

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

   N/A

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.*
   N/A

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.*

   N/A

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

   N/A

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.*

   N/A

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.*

Page 72: Additionally, several EU Member States have oversight bodies with no remedial powers. These include the Czech Republic, Estonia, Latvia, Luxembourg, Poland, Slovakia, Spain and the United Kingdom.

Correct

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

In 2014, Senate Committee discussed a draft of law which aimed at broadening the competences of DPAs also on security services (with respect to gathering telecommunication data by the services) but it was not adopted after all[80].

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.*

N/A

FRA key findings

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

N/A

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

N/A

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.*

N/A

Conclusions

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

N/A

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

N/A

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.*

N/A

80 Poland, Draft of law amending rules on access to telecommunication data (*Projekt ustawy o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjnych*), available at: http://www.senat.gov.pl/gfx/senat/userfiles/_public/k8/komisje/2015/kpcpp/materialy/bilingi/wniosek_nik_bilingi03120020140221095724.pdf, February 2014. Article 4 of the draft provided amendment of Article 43.2 of Data Protection Act (*Ustawa o ochronie danych osobowych*), 29 August 1997.

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.*

Correct

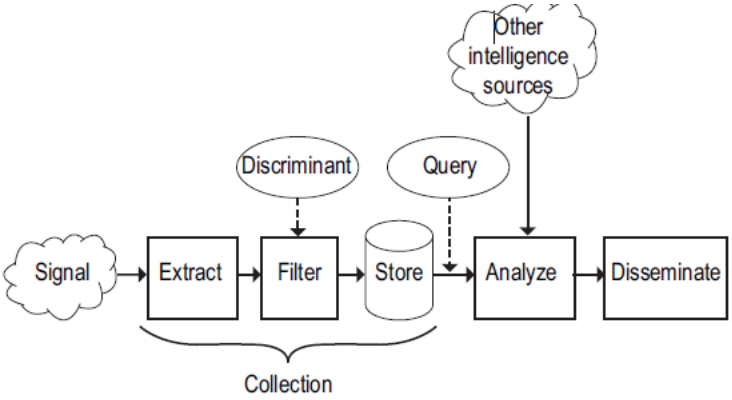
	Civil (internal)	**Civil (external)**	**Civil (internal and external)**	**Military**
PL	Internal Security Agency/*Agencja Bezpieczeństwa Wewnętrznego*- (ABW) Central Anti–Corruption Bureau/*Centralne Biuro Antykorupcyjne* (CBA)	Foreign Intelligence Agency /*Agencja Wywiadu* (AW)		Military Counter-intelligence Service/*Służba Kontrwywiadu Wojskowego* (SKW) Military Intelligence Service/*Służba Wywiadu Wojskowego* (SWW)

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.*

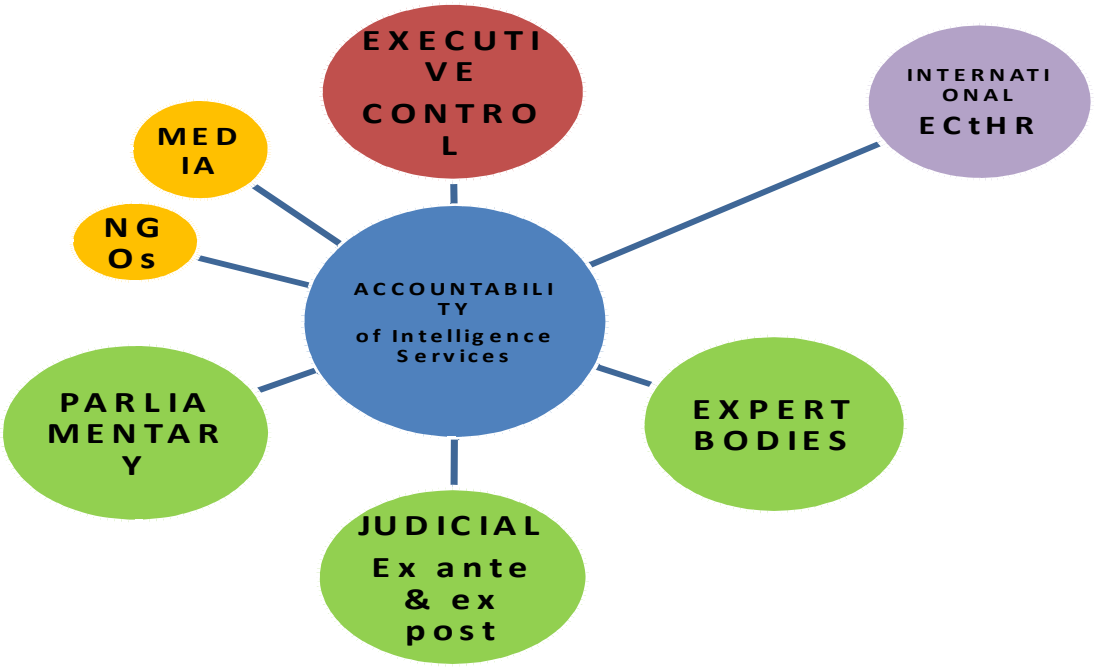
The same picture was published in *Bulk Collection of Signals Intelligence: Technical Options*[81]. An analogous figure relates to the so-called intelligence cycle[82]. However, a similar description of SIGINT was presented by the Venice Commission[83] and in literature[84].

81 Available at: http://www.nap.edu/catalog/19414/bulk-collection-of-signals-intelligence-technical-options, page. 5.
82 L. Johnson, Handbook of Intelligence Studies, Routledge 2009, p. 366, Appendix C.
83 Report on the Democratic Oversight of Signals Intelligence Agencies adopted by the Venice Commission at its 102nd Plenary Session (Venice, 20-21 March 2015), CDL-AD(2015)011-e, available at: http://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2015)011-e
84 M. Lowenthal, Intelligence. From Secrecy to Policy, SAGE 2015, p.118-127.



1.5.3 Figure 2: Intelligence services' accountability mechanisms

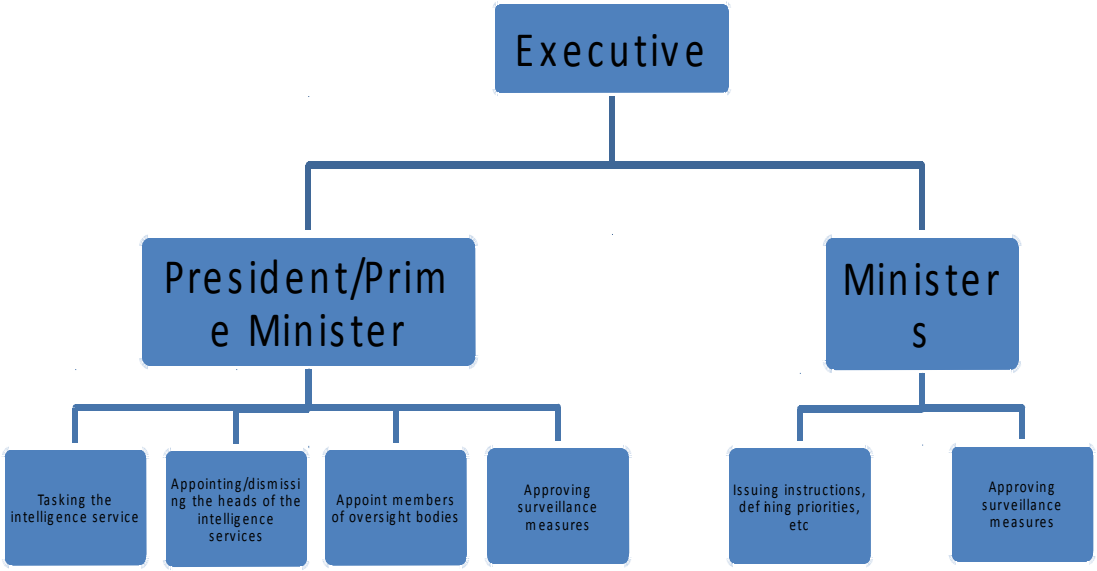
Please confirm that Figure 2 below (p. 31 of the FRA Report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.



Confirmed. However, it should be noticed that in Poland the only expert body is DPA with limited powers. There is no separate expert body dealing only with the intelligence.

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.



According to Polish law, the competences of the Prime Minister were transferred to a special Minister-Coordinator.

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
PL	X	

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

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

Please, delete all lines not referring to your country in the table below (p. 42 of the FRA Report). Please check the accuracy of the data. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

EU Member State	Expert Bodies
PL	N.A.

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

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

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

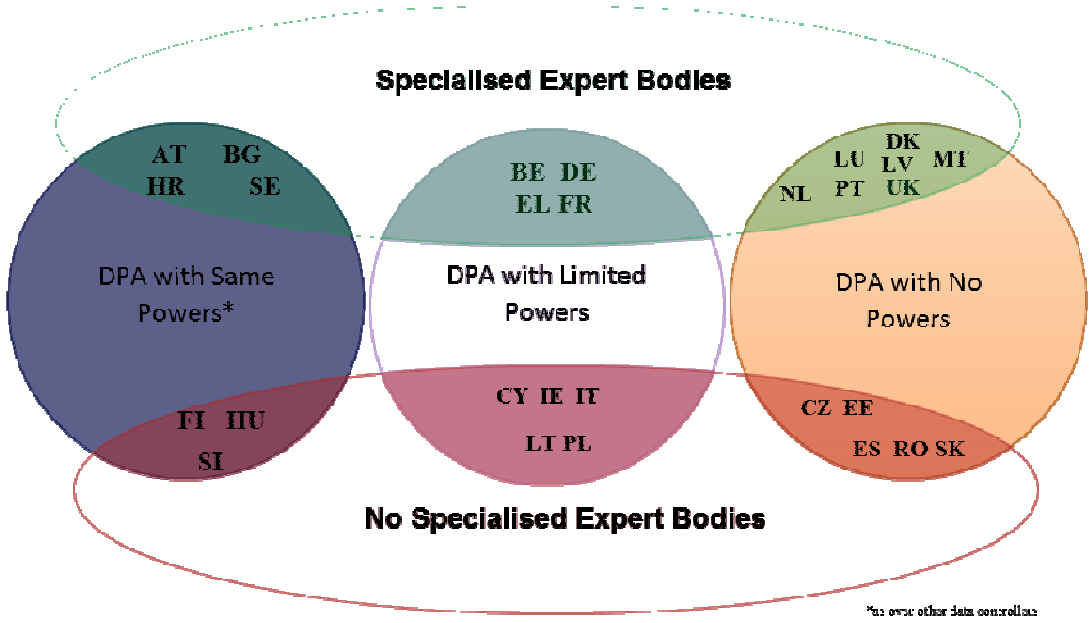
Notes: No powers: refers to DPAs that have no competence to supervise NIS.

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

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

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

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



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

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

Judicial approval is required under e.g. the Act on Internal Security Agency and Intelligence Agency[85] (before judicial decision, the prosecutor approval is needed as well; "two-tiered system of judicial approval", FRA report, p. 54). However, the Act on Anti-terrorist actions - that entered into force on 2 July 2016 - provides that in cases concerning terrorism threat, decision on conducting surveillance ("operational control") is made by the Chief of Internal Security Agency. Information about the decision is transmitted to the Minister-Coordinator and to the Prosecutor General. The Prosecutor General may decide to stop the surveillance.[86] Judicial approval is required after 3 months of such surveillance, if the Internal Security Agency wants to prolong it.

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.

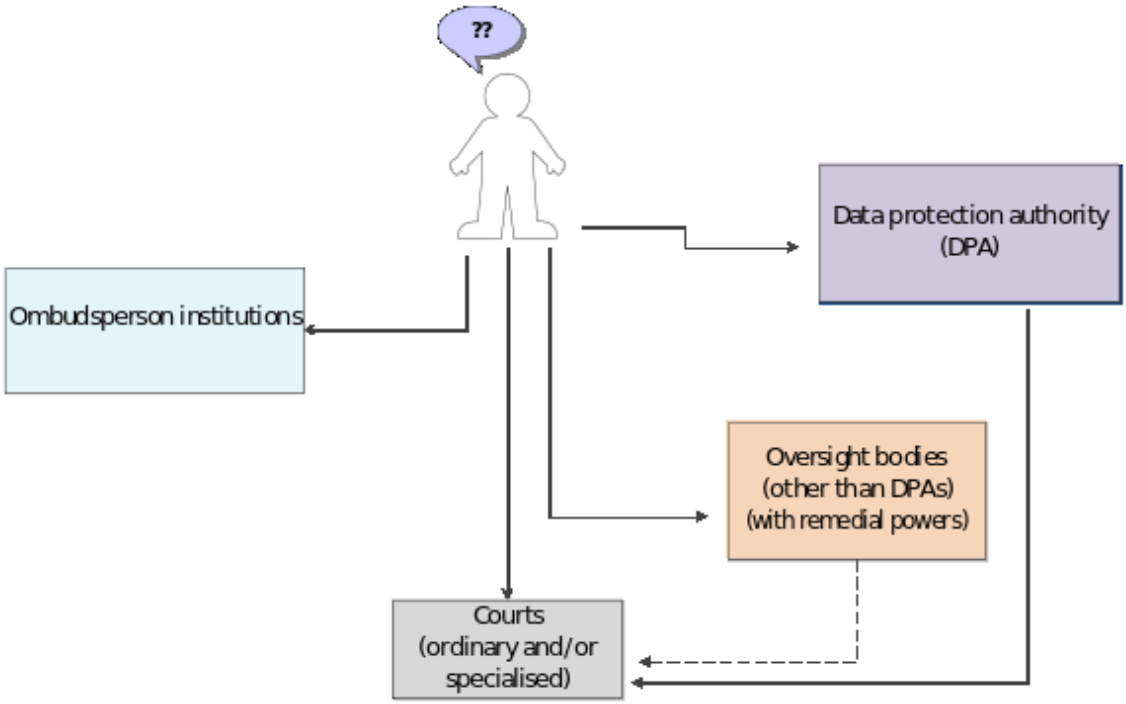
EU Member State	Judicial	Parliamentary	Executive	Expert
FR			X	
DE		X (telco relations)		X (selectors)
NL			X (selectors)	
SE				X
UK			X	

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.

85 Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu)*, 24 May 2002, Article 27.1.

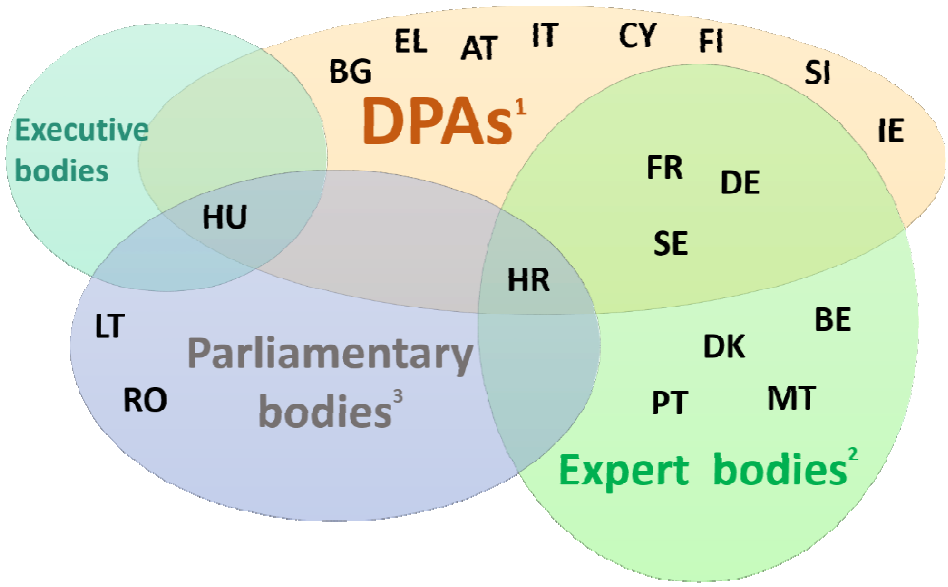
86 Poland, Act on anti-terrorist actions (*Ustawa o działaniach antyterrorystycznych*), 10 June 2016, Article 9.



In Poland, DPA and Ombudsperson do not have remedial competences towards intelligence services.

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.