Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU

Update 2023

Submission to the PEGA Committee, February 2023
Executive summary

This report presents a partial update of the 2017 FRA report on “Surveillance by intelligence services: safeguards and remedies in the European Union”. It was prepared in response to the request of the European Parliament, asking FRA to update its 2017 findings in order to support the work of its Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA).

The 2017 FRA report highlighted how fundamental rights related to the respect of private and family life (Article 7), the protection of personal data (Article 8) and the right to effective remedy and a fair trial (Article 47) of the Charter of Fundamental Rights of the European Union should be protected by setting up strong oversight systems and effective remedies open to individuals in the context of surveillance by intelligence services.

The present report updates relevant parts of the 2017 FRA report. Similar to the focus of the 2017 FRA report, this update focuses on the work of intelligence services and presents the developments since 2017 of intelligence laws in the EU. Significant developments that took place include the welcomed establishment of new oversight bodies following constitutional courts’ decisions and the impact of the 2016 European data protection reform on data protection authorities’ powers in the field of intelligence services’ activities. In 2023, 18 expert bodies oversee the work of intelligence services in the EU 27 (compared with 16 in the EU 28 in 2017). These developments are viewed in the light of minimum requirements shaped by the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR). In this context, the current report refers to a selection of relevant FRA Opinions drawn from the 16 FRA Opinions published in the Agency’s 2017 report, alongside key findings from this earlier report, and highlights relevant developments over time.

In particular, it provides, as per the European Parliament request, updated information on existing models of oversight mechanisms and remedies, illustrating them with examples from a select number of Member States. The report describes five distinct models of oversight frameworks, which encapsulate the diverse spectrum existing across EU Member States.

In 2017, FRA concluded that protecting the public from security threats while respecting fundamental rights can be achieved via strong oversight systems and effective remedies open to individuals. This conclusion remains valid in 2023.
Contents

Executive summary ....................................................................................................................... 2
Introduction .................................................................................................................................. 5
Surveillance legal frameworks reforms ..................................................................................... 7
Surveillance activities and national security: applicability of EU Law ........................................ 11
Requirements and conditions for lawful surveillance by intelligence services ....................... 14
Accountability .............................................................................................................................. 17
Relevant Updated Key Findings ............................................................................................... 17
Selected 2017 FRA Opinions .................................................................................................... 17
Intelligence services’ accountability scheme ............................................................................ 18
An imperative: internal control within intelligence services .................................................... 19
Stages of oversight and diversity of actors .............................................................................. 20
  Ex-ante authorisation ........................................................................................................... 20
  Ongoing and ex post oversight ............................................................................................ 24
Models of oversight framework of intelligence services based on different actors involved 36
Remedies ..................................................................................................................................... 43
  Relevant Updated Key Findings .......................................................................................... 43
  Selected 2017 FRA Opinions ............................................................................................ 44
Remedial powers of Data Protection Authorities ...................................................................... 48
Remedial powers of other non-judicial oversight bodies ........................................................ 51
Conclusions ................................................................................................................................. 53
Case law (post 2017) .................................................................................................................. 55
Annex 1 ........................................................................................................................................ 57
Annex 2 ........................................................................................................................................ 62

Table of Figures

Figure 1 – EU Member States’ legal frameworks on surveillance - reformed since mid-2017 ............. 8
Figure 2 – Applicability of EU Law in the context of intelligence services’ activities .............. 14
Figure 3 – Intelligence services’ accountability scheme ............................................................ 19
Figure 4 – Parliamentary oversight of intelligence services in EU Member States ............... 25
Table of Tables

Table 1 – Binding authorisation/approval of targeted surveillance measures in the EU-27 .................................................................21
Table 2 – Approval/authorisation of general surveillance of communications in EU Member States .................................................................23
Table 3 – Expert bodies (excluding DPAs) overseeing intelligence services in the EU ...27
Table 4 – Non-judicial bodies with remedial powers in the context of surveillance: different models by EU Member State.................................47
Table 5 – Overview of intelligence services in the 27 Member States .......................57
Introduction

This report provides a partial update of the 2015 and 2017 FRA reports on “Surveillance by intelligence services: safeguards and remedies in the European Union” (henceforth the 2017 FRA Report). The 2017 FRA Report was FRA’s response to a request by the European Parliament for in-depth research on the impact of surveillance on fundamental rights. Following the 2013 Snowden revelations, FRA focused on large scale technical collection of intelligence, referred to as general surveillance of communications and colloquially known as ‘mass surveillance’. In the context of surveillance by intelligence services, the 2017 FRA report highlighted how the respect for private and family life (Article 7), the protection of personal data (Article 8) and the right to an effective remedy and a fair trial (Article 47) of the Charter of Fundamental Rights of the European Union (the Charter) should be protected by setting up strong oversight systems and effective remedies open to individuals.

The European Parliament request

In the latter part of 2022, the European Parliament requested FRA to prepare this update to support the work of the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA Committee). In particular, FRA was asked to present different existing models of oversight mechanisms and to illustrate them with examples from a selected number of Member States. The PEGA Committee was asked to gather information on the extent to which Member States or third countries are using intrusive surveillance to the extent that it violates

---


the rights and freedoms enshrined in the Charter. In undertaking this task, the PEGA Committee held a significant number of hearings, published various studies and briefings, and undertook fact-finding missions.

The present update builds on the 2017 FRA report and the 16 FRA Opinions therein. This update refers to relevant FRA Opinions and key findings from the 2017 FRA report. The Agency’s multidisciplinary research network (FRANET) provided updated national data which formed the basis of this comparative analysis.

Similar to the focus of the 2017 FRA report, this update focuses on the work of intelligence services. It presents developments since 2017 of intelligence laws in the EU, and specifically addresses the work of intelligence services as listed in Table 5 (see Annex 1). Just as the 2017 FRA report did not address in detail the use of intelligence techniques such as spyware in the EU, or secret surveillance in the context of police work and criminal investigations, this update does not deal with these issues.

The legal frameworks on spyware are discussed in detail in the draft report prepared by the PEGA Committee, the proposed Recommendation of the European Parliament, as well as in reports prepared for the Committee’s work. The United Nations High Commissioner for Human Rights also dealt with the widespread abuse of intrusive hacking tools and the need for enhanced safeguards on their use. The

---

3 European Parliament (2022), Decision of 10 March 2022 on setting up a committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, and defining the subject of the inquiry, as well as the responsibilities, numerical strength and term of office of the committee, P9_TA(2022)0071, Thursday, 10 March 2022.

4 See the website of the PEGA Committee for more details at: <https://www.europarl.europa.eu/committees/en/pega/home/highlights>

5 The following report cover these areas: European Parliament (2022), The use of Pegasus and equivalent surveillance spyware. The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware, draft study, December 2022.

6 European Parliament (2022), DRAFT REPORT Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware, 8 November 2022


Council of Europe’s Parliamentary Assembly is also addressing the issue\textsuperscript{10} and the Commissioner for Human Rights issued a Comment.\textsuperscript{11}

This update focuses on two key aspects of intelligence services accountability: oversight and remedies. These two aspects should be enshrined in every secret surveillance framework to protect against abuse, as both the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) emphasise.

“In view of the risk that a system of secret surveillance set up to protect national security (and other essential national interests) may undermine or even destroy the proper functioning of democratic processes under the cloak of defending them, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on (...) the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law.”.

\textit{ECtHR, Big Brother Watch and Others v. the United Kingdom} [GC], Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021

\section*{Surveillance legal frameworks reforms}

Several key legal developments have taken place since the publication of the 2017 FRA report, including seminal judgements by the CJEU and ECtHR on the transatlantic flow of data and surveillance by intelligence services; the entry into force of the General Data Protection Regulation (GDPR) and the Law Enforcement Directive at EU level (the 2016 European data protection reform) and the adoption of the Modernised Convention for the protection of individuals with regard to the processing of personal data.

\textsuperscript{10} Council of Europe (2022), Committee on Legal Affairs and Human Rights, \textit{Pegasus and similar spyware and secret state surveillance}, 8 April 2022.

Data (Convention 108+) at Council of Europe level. Such legal developments have necessitated changes to national intelligence laws, thus resulting in the need for FRA to update its data collection to reflect such legal reforms.

*Figure 1* presents an overview of reforms of legal frameworks on surveillance that have taken place in the EU-27 since the 2017 FRA report. The majority (17) of EU Member States have reformed, or are in the process of reforming, their legal frameworks on intelligence services. Legal changes have been quite diverse, ranging from changes on organisational issues to the accountability regime of intelligence services and remedies against their actions.

*Figure 1 – EU Member States’ legal frameworks on surveillance - reformed since mid-2017*

Reforms were triggered for various reasons beyond legal developments at EU level needing to be transposed at EU Member States’ level. In Austria for example, findings

---

12 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).
of a parliamentary enquiry on serious misconduct and corruption by intelligence officials and the response to the terrorist attack in Vienna on 2 November 2020 lead to the creation of a new agency. A new specialised and independent oversight body was also established with the reforms.

Greece has also amended its legal framework several times since 2017. The changes involved various issues, such as the organisation of intelligence services, the authorisation of surveillance or the abolishment and the following re-introduction of notification of surveillance. The latest of these amendments followed complaints against the intelligence services for inappropriate monitoring communications of politicians and journalists, alongside allegations against the use of illegal spyware against politicians, journalists, and other public figures, as reported in the media.

FRA data suggest that spyware revelations since 2021 had almost no impact on national reforms to date, with the exception of Greece, where reforms in December 2022 addressed the regulation of spyware. In August 2022, the Prime Minister of

---


Spain announced plans for reforming the law on intelligence services. At the time of writing, no draft law was published, while the government’s 2023 plan does not include any reference to such a planned reform.

In some cases, the amendments of intelligence laws were necessitated by court judgments on successful constitutional or administrative law challenges against intelligence laws, such as in France, Germany and Portugal. In Germany for example, amongst other reforms, a new oversight body was set up in 2021.

Data protection reforms following the implementation of the 2016 European data protection reform also led to restrictions or exclusions in the powers of national Data Protection Authorities to exercise oversight over intelligence services in some countries, such as Bulgaria, Croatia, Greece and Lithuania. In others, such as in

---

19 Spain, Pedro Sánchez announces a reform of the legal control regulation of the National Intelligence Centre (CNI) to strengthen its guarantees, La Moncloa, press release, 26 May 2022.


21 French Council of State (Conseil d’État), French Data Network and others, Decision No 393099, 21 April 2021.

22 Germany, Federal Constitutional Court, (Bundesverfassungsgericht, BVerfG), Judgment of the First Senate, 1 BvR 2835/17, 19 May 2020 and Federal Constitutional Court (Bundesverfassungsgericht) (2022), 1 BvR 2354/13, 28 September 2022.


24 Germany, Act to Change the Federal Intelligence Service Act to Implement the Guidelines of the Federal Constitutional Court and the Federal Administrative Court (Gesetz zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts), 19 April 2021, setting up – the Independent Supervisory Council (Unabhängiger Kontrollrat).

25 Bulgaria, Amendments and Supplements to the Personal Data Protection Act (Закон за изменение и допълнение на Закона за защита на личните данни), 26 February 2019; State Intelligence Agency Act (Закон за Държавна агенция „Разузнаване”), 13 October 2015, last amended 4 August 2020, Arts. 27 and 28; Military Intelligence Act (Закон за военното разузнаване), 13 November 2015, last amended 26 March 2021, Art. 78; State Agency for National Security Act (Закон за Държавна агенция „Национална сигурност”), 13 October 2015, last amended 5 June 2020, Art. 37.

26 Croatia, General Regulation on Data Protection Act (Zakon o provedbi Opće uredbe o zaštiti podataka), 25 May 2018.


28 Lithuania, aw on Legal Protection of Personal Data Processed for the Purposes of Prevention, Investigation, Detection, or Prosecution of Criminal Acts, Execution of Sentences, or National Security and Defence (Asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas), No. XIII-1435, 30 June 2018. Article 39(3).
Hungary, changes do not appear to have substantially strengthened the data protection authorities.\textsuperscript{29} In some States, such as Luxembourg and Cyprus, reforms appear to have reinforced the role of national data protection authorities (see below Expert bodies and Data Protection Authorities).

### Surveillance activities and national security: applicability of EU Law

According to Article 4(2) of the TEU, activities of States protecting national security do not fall under EU competence. The ‘national security’ exemption is also reflected in the GDPR and the e-privacy Directive.\textsuperscript{30} Nonetheless, the 2017 FRA report discussed this exemption and highlighted examples of intelligence services activities that do fall within the scope of EU law and therefore are subject to EU law protections of fundamental rights, in addition to guarantees available for the same rights under national constitutional provisions and international human rights treaties. The report suggested that the protection offered by the GDPR could well apply to the transfer of communication data by service providers to intelligence services for national security purposes.\textsuperscript{31} The 2017 FRA report concluded that: “the ‘national security’ exemption thus cannot be seen as entirely excluding the applicability of EU law.”\textsuperscript{32} This was concurred by a report requested by the PEGA Committee.\textsuperscript{33}

The CJEU has since confirmed this conclusion stating that invoking national security cannot act as a blanket exception to avoid EU law, including scrutiny under the Charter.\textsuperscript{34} The Court clarified this in relation to general data retention and access, and

---

\textsuperscript{29} Hungary, \textit{Act 112 of 2011 on the right to informational self-determination and information freedom}, Art. 51/A, amendment entered into force on 26 July 2018, introduced by \textit{Amending Act 38 of 2018}, Art. 20.

\textsuperscript{30} Arts. 2(2), 23(1)(a), GDPR; Arts. 1(3), 15(1), Directive 2002/58/EC.

\textsuperscript{31} FRA (2017), p. 22.


\textsuperscript{33} European Parliament (2022), \textit{The impact of Pegasus on fundamental rights and democratic processes}, Study, December 2022.

\textsuperscript{34} CJEU, Joined Cases C-793/19 and C-794/19, \textit{SpaceNet AG} [GC], 20 September 2022, para. 66; Joined Cases C-511/18, C-512/18 and C-520/18, \textit{La Quadrature du Net and Others} [GC], 6 October 2020, para. 99; Case C-623/17, \textit{Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others} [GC], 6 October 2020, para. 44.
real-time access to communications data when protecting national security.\(^{35}\) The Court also defined ‘national security’ as the ‘protection of the essential functions of the State and the fundamental interests of society’ against actions ‘destabilising the fundamental structures of a country’ and threatening the population.\(^{36}\) Moreover, it specified that protecting public security and combating serious crime cannot be treated in the same way.\(^{37}\) By defining ‘national security’, the Court tried to rule out the possibility of invoking it as a pretext for other purposes.

“.. the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law”

“(…) national security (…) corresponds to the primary interest [of Member States] in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.”

CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others [GC], 6 October 2020, paras. 99 and 135

\(^{35}\) CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* [GC], 6 October 2020, paras. 56-79; Case C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [GC], 6 October 2020, paras. 19-29, 30, 50.

\(^{36}\) CJEU, Joined Cases C-793/19 and C-794/19, *SpaceNet AG* [GC], 20 September 2022, para. 92; Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* [GC], 6 October 2020, para. 135; Case C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [GC], 6 October 2020, para. 74.

\(^{37}\) CJEU, Joined Cases C-793/19 and C-794/19, *SpaceNet AG* [GC], 20 September 2022, paras. 72, 93-4; Case C-140/20, *Commissioner of An Garda Síochána and Others* [GC], 5 April 2022, para. 58; Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* [GC], 6 October 2020, para. 136; Case C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [GC], 6 October 2020, para. 75.
In the field of surveillance for national security purposes, the CJEU found that retaining and providing access to communication data — real-time or not — is an activity that is always performed by private parties (i.e. service providers) on the request of State authorities based on law. It is not an activity performed directly by State organs. Retaining data and providing access to such data or transmitting those to State authorities for national security purposes is permitted by provisions which derogate from the principle of the confidentiality of communications established in the e-privacy Directive. Hence, data retention and access for national security purposes fall within the scope of EU law.\textsuperscript{38}

The CJEU case law also had a significant impact at national level. In France, for example, a CJEU ruling led to a decision of the Council of State (\textit{Conseil d’État}),\textsuperscript{39} which triggered an amendment of the intelligence law in relation to the binding character of the opinions of the French oversight body. In 2020, noting the pending case before the CJEU at the time, the German Federal Constitutional Court (\textit{Bundesverfassungsgericht}) ruled that surveillance by intelligence services on foreign communications violated fundamental rights of the German Basic law.\textsuperscript{40} One of the reasons was that the powers, organisational and institutional design of the competent bodies did not ensure an extensive independent and continuing oversight.\textsuperscript{41}

In a nutshell, some aspects of the work by intelligence services, namely surveillance of communications data, cannot be deemed to be completely excluded from the scope of EU law and the Charter of Fundamental Rights. The CJEU also underscored that secret surveillance techniques that lie outside the scope of EU law should comply with the corresponding requirements of the ECHR.\textsuperscript{42} Figure 2 summarises the applicability of EU law in the context of the national security exemption as defined by the CJEU case law to date.

\textsuperscript{38} Directive 2002/58/EC, Art. 15(1); CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, \textit{La Quadrature du Net and Others} [GC], 6 October 2020, para. 58 referring to joined cases C-203/15 and C-698/15, \textit{Tele2 Sverige and Watson and Others} [GC], 21 December 2016, and oper. part; Case C-623/17, \textit{Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others} [GC], 6 October 2020, paras. 38, 49 and oper. part.

\textsuperscript{39} French Council of State (Conseil d’État), \textit{French Data Network and others}, Decision No 393099, 21 April 2021.

\textsuperscript{40} Federal Constitutional Court, (\textit{Bundesverfassungsgericht}, BVerfG), \textit{Judgment of the First Senate, 1 BvR 2835/17}, 19 May 2020.

\textsuperscript{41} Federal Constitutional Court, (\textit{Bundesverfassungsgericht}, BVerfG), \textit{Judgment of the First Senate, 1 BvR 2835/17}, 19 May 2020, paras. 265 – 300, 324.

\textsuperscript{42} CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, \textit{La Quadrature du Net and Others} [GC], 6 October 2020, para. 103.
Requirements and conditions for lawful surveillance by intelligence services

The 2017 FRA report was structured along the lines of the ECtHR case-law requirements. The report focused on three key aspects:

- the legal framework on surveillance and the requirement of having clear, foreseeable and accessible laws regulating secret surveillance;
- the accountability of intelligence services focusing on existing oversight bodies with appropriate powers;
- the availability of effective remedies for individuals before remedial bodies with appropriate powers.

Since 2017, both European Courts further elaborated their case-law requirements on surveillance by intelligence services. With regard to oversight and remedies in particular, their requirements are essentially aligned. Some notable developments include the following:

The CJEU held that:
Intelligence services can apply secret surveillance when it genuinely pursues the protection of national security based on the Court’s definition.43

Only a “genuine and present or foreseeable” serious threat to national security justifies measures that apply indiscriminately to all users of communications systems.44

Both European courts stressed the main key aspects of accountability for surveillance of communications by intelligence services:

- Secret surveillance should be subject to clear and publicly accessible legal rules, which include the necessary safeguards against abuses from surveillance techniques carried out for “national security” purposes.45

- Independent authorities and the courts should exercise review and supervision over the relevant rules and conditions during the authorisation and implementation of surveillance measures by intelligence services.46

- Individuals under surveillance should have recourse to remedies that are effective in practice for reviewing the lawfulness and proportionality of any surveillance against them and redressing any violations of their rights.47

---

43 CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* [GC], 6 October 2020, paras. 135-7; Case C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [GC], 6 October 2020, paras. 74-5, 77; Joined Cases C-793/19 and C-794/19, *SpaceNet AG* [GC], 20 September 2022, paras. 72, 131 and oper. part; Case C-140/20, *Commissioner of An Garda Síochána and Others* [GC], 5 April 2022, para. 58.

44 CJEU, Joined Cases C-793/19 and C-794/19, *SpaceNet AG* [GC], 20 September 2022, paras. 72, 131 and oper. part; Case C-140/20, *Commissioner of An Garda Síochána and Others* [GC], 5 April 2022, para. 58; Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* [GC], 6 October 2020, paras. 137, 177.


47 ECtHR, *Big Brother Watch and Others v. the United Kingdom* [GC], Nos. 58170/13, 62322/14 and 24969/15 [GC], 25 May 2021, paras. 337, 357; *Centrum för rättvisa v. Sweden* [GC], No. 35252/08, 25 May 2021, paras. 249, 251, 253, 271, 372; *Ekimdzhiiev and Others v. Bulgaria*, No. 70078/12, 11 January 2022, paras. 264-275, 354, 418, 419(f).
The ECtHR emphasised that remedial bodies should possess guarantees of “objectivity and thoroughness” to ensure against any conflicts of interest with the body that authorised and supervised the surveillance.\textsuperscript{48}

The ECtHR further clarified that notification of surveillance that is required as soon as the purpose of surveillance is not jeopardised, cannot depend on a national security exception.\textsuperscript{49} Unless remedies depend on it, notification may be omitted when affected individuals can request and receive relevant information through a competent independent authority.\textsuperscript{50}

Both Courts confirmed that the above main requirements apply to targeted surveillance of content data, bulk interception of communications data, as well as the retention of communication data by service providers and its subsequent access, real-time or not, by authorities.\textsuperscript{51} What may differ is the treatment of different types of data once obtained.\textsuperscript{52}

Recent European case-law has elaborated on the requirements applicable to the life cycle of surveillance activities by intelligence services. \textit{Figure 13} (in Annex 2) summarises the requirements as developed by the ECtHR and the CJEU.

This update is structured as follows: Part 1 focuses on accountability through oversight of intelligence services, while Part 2 deals with available remedies at EU Member States’ level.

\textsuperscript{48} ECtHR, \textit{Centrum för rättvisa v. Sweden} [GC], No. 35252/08, 25 May 2021, para. 359, 372.

\textsuperscript{49} ECtHR, \textit{Centrum för rättvisa v. Sweden} [GC], No. 35252/08, 25 May 2021, para. 272.

\textsuperscript{50} ECtHR, \textit{Marie Ringler v. Austria} (dec.), No. 2309/10, 12 May 2020, paras. 73, 79.

\textsuperscript{51} CJEU, Joined Cases C-140/20, \textit{Commissioner of An Garda Síochána and Others} [GC], 5 April 2022, para. 45; Joined Cases C-511/18, C-512/18 and C-520/18, \textit{La Quadrature du Net and Others} [GC], 6 October 2020, paras. 117-8; Case C-623/17, \textit{Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others} [GC], 6 October 2020, paras. 71-2; ECtHR, \textit{Big Brother Watch and Others v. the United Kingdom} [GC], Nos. 58170/13, 62322/14 and 24969/15 [GC], 25 May 2021, paras. 363-4, 416, 425; \textit{Centrum för rättvisa v. Sweden} [GC], No. 35252/08, 25 May 2021, paras. 164, 261-275; \textit{Ekimdzhiev and Others v. Bulgaria}, No. 70078/12, 11 January 2022, paras. 394-5.

\textsuperscript{52} E.g., ECtHR, \textit{Big Brother Watch and Others v. the United Kingdom} [GC], Nos. 58170/13, 62322/14 and 24969/15 [GC], 25 May 2021, paras. 364, 416, 421, 423.
Accountability

Relevant Updated Key Findings

Oversight bodies have diverse roles, including overseeing the legality of the intelligence services’ functioning, their efficiency, and policies.

Oversight of surveillance is normally undertaken either by the judiciary and/or an expert body. Currently, in 18 Member States out of all the 27 Member States which are covered by this report (compared to the 28 that were covered in the 2017 report) expert bodies are part of the oversight system. In 19 Member States (not necessarily the same), judicial authorities are authorising targeted surveillance measures.

In 25 Member States, parliaments are involved in oversight. In 22 Member States, one or two specialised parliamentary committees are involved in overseeing the intelligence services. In the other three EU Member States, a non-specialised committee is responsible for this task.

In five Member States, Data Protection Authorities (DPAs) have the same powers over intelligence services as over all other data controllers. In 15 Member States, DPAs have no powers over intelligence services. In seven Member States, their powers are limited. Following the coming into force of the 2016 European data protection reform, seven Member States have restricted or excluded DPAs from exercising supervision over data processing by intelligence services.

Five Member States have detailed provisions on general surveillance of communications. Out of these Member States, three provide for the binding involvement of an independent body in the authorisation of these measures. In the other two Member States, the opinions of the oversight body are not binding.

The oversight framework is characterised by a great diversity in the EU Member States. Five models of oversight frameworks based on the different actors overseeing the services illustrate this diversity.

Selected 2017 FRA Opinions

FRA opinion 2: Ensuring broad consultation and openness during the legislative process
EU Member States should undertake broad public consultations with a full range of stakeholders, ensure transparency of the legislative process, and incorporate relevant international and European standards and safeguards when introducing reforms to their legislation on surveillance.

**FRA opinion 3: Providing independent intelligence oversight with sufficient powers and competences**

EU Member States should establish a robust oversight framework adequate to the powers and capacities that intelligence services have. The independence of oversight bodies should be enshrined in law and applied in practice. EU Member States should grant oversight bodies adequate financial and human resources, including diverse and technically-qualified professionals. Member States should also grant oversight bodies the power to initiate their own investigations as well as permanent, complete and direct access to necessary information and documents for fulfilling their mandate. Member States should ensure that the oversight bodies’ decisions are binding.

**FRA opinion 4: Bolstering oversight with sufficient technical expertise**

EU Member State laws should ensure that oversight bodies have staff with the required technical expertise to assess independently the intelligence services’ often highly technical work.

**FRA opinion 5: Ensuring oversight bodies’ openness to public scrutiny**

EU Member States should ensure that oversight bodies’ mandates include public reporting to enhance transparency. The oversight bodies’ reports should be in the public domain and contain detailed overviews of the oversight systems and related activities (e.g. authorisations of surveillance measures, on-going control measures, ex-post investigations and complaints handling)

**FRA opinion 6: Fostering continuity of oversight**

EU Member States should ensure that the oversight bodies’ mandates complement each other, so that, overall, they provide continuous control and ensure proper safeguards. Such complementarity can be achieved with informal cooperation between oversight bodies or statutory means.

*Source: FRA, 2017*

---

**Intelligence services’ accountability scheme**

In preparing this update, FRA confirmed the accuracy of the intelligence services accountability scheme as presented in the 2017 FRA report. This update will focus on oversight entities during the different stages of surveillance, while recognising the
important role played by watchdogs (such as the media, whistleblowers or civil society organisations). The Pegasus revelations provided us with yet another example of the essential role played by civil society organisations and the media. Figure 3, first published in the 2017 FRA report, illustrates the main actors who contribute to the oversight of intelligence services and their accountability.

**Figure 3 – Intelligence services’ accountability scheme**

![Diagram showing the accountability scheme for intelligence services](Source: FRA, 2023)

An imperative: internal control within intelligence services

The 2017 FRA report emphasised that a crucial precondition of an effective oversight of intelligence services activity lies in the proper internal control of the services themselves.\(^{53}\) FRA did not collect updated data on the control exercised by intelligence services or the executive. A clear understanding of the legal obligations facilitates effective supervision over intelligence services. For example, the French oversight body justifies the low number of negative opinions on requested surveillance techniques because the intelligence services have a well understood notion of

---

Enhanced awareness can also be helped through a Memorandum of Understandings, as it is the case in Italy between the DPA and the Coordinator of the intelligence services (Department Security Intelligence – DIS).

Stages of oversight and diversity of actors

Ex-ante authorisation

Notes on terminology

**General surveillance of communications**

Intelligence can be collected with technical means and on a large scale. This surveillance technique is referred to in different ways, including ‘signals intelligence’, ‘strategic surveillance’, ‘bulk investigatory powers’, ‘mass digital surveillance’ and ‘storage of data on a generalised basis’. Whenever possible, FRA uses the national laws’ terminology, but also uses – as a generic encompassing term – ‘general surveillance of communications’.

**Targeted and untargeted surveillance**

Based on whether or not a target exists, surveillance measures can be divided into targeted and untargeted surveillance. ‘Targeted surveillance’ presupposes the existence of prior suspicion of a targeted individual or organisation. ‘Untargeted surveillance’ starts without prior suspicion or a specific target.

Source, FRA, 2017

As the 2017 FRA report stressed, effective oversight of surveillance operations requires, among others, that independent oversight be present at the stage when the surveillance measures are first ordered. Both European Courts underline that any measure of secret surveillance should be subject to a prior authorisation preferably by a court, or another independent authority. The authorising authority should ensure

---

54 France, CNCTR (2022), Annual report 2021, p. 67.


57 CJEU, Joined Cases C-793/19 and C-794/19, SpaceNet AG [GC], 20 September 2022, paras. 72, 131 and oper. part; Case C-140/20, Commissioner of An Garda Síochána and Others [GC], 5 April 2022, para. 58; Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others [GC], 6 October 2020, paras. 139, 179 and
that any requested measures are proportionate and necessary in practice to protect national security.  

Table 1 shows the different bodies that have a binding/final decision in the authorisation or approval processes of different types of targeted surveillance measures. The information provided for an individual Member State covers all potential actors with a binding decision-making power in allowing targeted surveillance measures. Pegasus and the other spyware subject to the PEGA Committee’s work fall within the category of targeted surveillance. Several Member States have two or more bodies authorising the surveillance technique. As stated in the 2017 FRA report, the modalities and details of this authorisation process vary considerably amongst Member States and depending on the different types of surveillance measures involved.

Table 1 – Binding authorisation/approval of targeted surveillance measures in the EU-27

<table>
<thead>
<tr>
<th></th>
<th>Judicial</th>
<th>Executive</th>
<th>Expert bodies</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BE</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>BG</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CY</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CZ</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DK</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EE</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EL</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


58 CJEU, Joined Cases C-793/19 and C-794/19, SpaceNet AG [GC], 20 September 2022, paras. 72, 131 and oper. part; Case C-140/20, Commissioner of An Garda Síochána and Others [GC], 5 April 2022, para. 58; Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others [GC], 6 October 2020, para. 139; ECtHR, Centrum för rättvisa v. Sweden [GC], No. 35252/08, 25 May 2021, paras. 266, 268, 270, 275, 298-302, 368; Ekimdzhiev and Others v. Bulgaria, No. 70078/12, 11 January 2022, paras. 292, 307, 318, 321, 419(a).

59 European Parliament (2022), Pegasus and surveillance spyware, In-Depth Analysis, May 2022, p. 4.
<table>
<thead>
<tr>
<th></th>
<th>Judicial</th>
<th>Executive</th>
<th>Expert bodies</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>ES</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FI</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FR</td>
<td>✓*</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HR</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HU</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>IE</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LT</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LU</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>LV</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MT</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NL</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>PL</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>PT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RO</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SE</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SI</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>SK</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*In France when the expert body issues a negative opinion on the use of a surveillance technique, if the Prime Minister wishes to disregard the opinion, the expert body takes immediately the matter before the Conseil d’État, which issues a final binding decision.


One notable example is the 2021 reform in France, which strengthened the decision-making power of the expert body. If the Prime Minister decides not to follow a negative opinion delivered by the National Commission for Control of Intelligence Techniques (*Commission nationale de contrôle des techniques de renseignement*, CNCTR), the CNCTR must then refer immediately the case to the Council of State (*Conseil d’État*), which takes the final decision.\(^{60}\) While a negative opinion used to be

non-binding, it now became “blocking”. The Netherlands provides another example with the establishment of a new body in 2017 - the Investigatory Powers Commission (*Toetsingscommissie inzet bevoegdheden*, TIB) – that became operational in May 2018. Its task is to assess in advance the legality of the authorisation by the government to the intelligence agencies for employing surveillance techniques. If it deems the authorisation unlawful, surveillance cannot proceed.

Five EU Member States have detailed laws on general surveillance of communications. As anticipated in the 2017 FRA report, since 2017, Finland completed its wide-reaching intelligence law reform, which included new legislation that details the use of general surveillance of communications by its services. Table 2 presents the bodies that have a final authorisation power on general surveillance of communications measures in the Member States that implement such surveillance techniques.

**Table 2 – Approval/authorisation of general surveillance of communications in EU Member States**

<table>
<thead>
<tr>
<th></th>
<th>Judicial</th>
<th>Parliamentary</th>
<th>Executive</th>
<th>Expert</th>
</tr>
</thead>
<tbody>
<tr>
<td>DE</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>FI</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FR</td>
<td>✓*</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>NL</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SE</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

*In France when the expert body issues a negative opinion on the use of a surveillance technique, if the Prime Minister wishes to disregard the opinion, the expert body takes immediately the matter before the Conseil d’État, which issues a final binding decision.*


The 2021 reform in Germany specified the threshold for general surveillance of foreign communication and tasked its new expert body - the Independent Supervisory Council (*Unabhängiger Kontrollrat*, UKRat) - with approving general surveillance of foreign

---


62 The Netherlands, Intelligence and Security Services Act 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*).

63 The Netherlands, Intelligence and Security Services Act 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*), Arts. 32-37.


communications ordered by the Federal Intelligence Service (*Bundesnachrichtendienst*, BND).\(^\text{66}\) In the Netherlands, the Investigatory Powers Commission (*Toetsingscommissie inzet bevoegdheden*, TIB) assesses the legality of the ministerial authorisation to intelligence services to acquire real-time and fully automated access to databases or large-scale monitoring of internet traffic.\(^\text{67}\) In Finland, the 2019 laws provided intelligence services with general surveillance of communications techniques; albeit under strict conditions and court authorisation.\(^\text{68}\) Intelligence services can acquire communications data based on the automated segregation of data traffic and the processing of acquired data concerning transborder data traffic.\(^\text{69}\) Network traffic is selected based on objective criteria (“search terms”) subjected to court authorisation.\(^\text{70}\) For granting authorisation, the intelligence service must justify that it is necessary to screen specific traffic during a specific period.\(^\text{71}\) Such data should provide information about activities that pose a serious threat to national security that is otherwise unattainable.\(^\text{72}\)

## Ongoing and ex post oversight

Parliaments

National parliaments are responsible for holding the executive accountable for its actions. The findings of the 2017 FRA report are still relevant to date: the vast majority

---

\(^{\text{66}}\) Germany, Act amending the BND Act to implement the requirements of the Federal Constitutional Court and the Federal Administrative Court (*Gesetz zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts*), 19 April 2021, Art. 1(21) amending §§ 23 and 42 of the BND Act

\(^{\text{67}}\) The Netherlands, Intelligence and Security Services Act 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*), Articles 32-37.

\(^{\text{68}}\) Finland, Act on the Use of Network Traffic Intelligence in Civilian Intelligence (*laki tietoliikennetiedustelusta siviiltiedustelussa/lag om civil underrättelseinhämtning avseende datatrafik*), Act No. 582/2019, 18 January 2019, section 7; Finland, Act on Military Intelligence (*laki sotilastiedustelusta/lag om militär underrättelseverksamhet*), Act No. 590/2019, 26 April 2019.

\(^{\text{69}}\) Finland, Act on the Use of Network Traffic Intelligence in Civilian Intelligence (*laki tietoliikennetiedustelusta siviiltiedustelussa/lag om civil underrättelseinhämtning avseende datatrafik*), Act No. 582/2019, 18 January 2019, section 2(1).

\(^{\text{70}}\) Finland, Act on the Use of Network Traffic Intelligence in Civilian Intelligence (*laki tietoliikennetiedustelusta siviiltiedustelussa/lag om civil underrättelseinhämtning avseende datatrafik*), Act No. 582/2019, 18 January 2019, section 5.

\(^{\text{71}}\) Finland, Ministry of Interior (*sisäministeriö/inrikeministeriet*), ‘Civilian intelligence protects Finland’s national security’, internet page, accessed on 1 December 2022.

\(^{\text{72}}\) Finland, Act on the Use of Network Traffic Intelligence in Civilian Intelligence (*laki tietoliikennetiedustelusta siviiltiedustelussa/lag om civil underrättelseinhämtning avseende datatrafik*), Act No. 582/2019, 18 January 2019, section 4.
of EU Member States provide for parliamentary oversight through specialised or non-specialised parliamentary committees (see Figure 4). The only two exceptions are Ireland and Malta, which are the only Member States not providing for some sort of parliamentary oversight of intelligence services. In three Member States – Sweden, Poland and Cyprus – this task is assigned to a non-specialised committee. In the other 22 Member States, parliamentary oversight is exercised by specialised parliamentary committees.

Figure 4 – Parliamentary oversight of intelligence services in EU Member States

By way of example, in Finland, the newly established Intelligence oversight committee (Tiedusteluvalvontavalioikeus, TiVi) performs the following oversight tasks: It oversees the proper implementation and appropriateness of intelligence operations; monitors and evaluates the focus areas of intelligence operations; monitors and promotes the effective exercise of fundamental and human rights in intelligence operations;
provisionally considers reports by the Intelligence Ombudsman (before a discussion in plenary); and processes the supervisory findings of the Intelligence Ombudsman.\textsuperscript{73}

In France also, the responsible parliamentary committee for intelligence services (\textit{Délégation parlementaire au renseignement}, DPR) has been reinforced.\textsuperscript{74} Amongst others, it can now request any document, information and assessment consideration needed to carry out its duties and can hold hearings of persons exercising management duties within the intelligence services. The scope of the DPR has been extended to include the monitoring of current issues and future challenges to public intelligence policy. It is in this context that the DPR addressed Pegasus in its latest report.\textsuperscript{75}

The role of parliamentary oversight on intelligence services can be crucial for the overall functioning of intelligence services. In Austria, for example, the abolishment and replacement of the intelligence service in 2021 is mainly attributed to the findings of a parliamentary enquiry committee which established serious shortcomings in the intelligence service.\textsuperscript{76} The effectiveness of parliamentary oversight must be assessed in practice, as required by case-law. In the case of \textit{Zoltan Varga v. Slovakja}, the ECtHR underlined some shortcomings in relation to parliamentary oversight.\textsuperscript{77} Shortcomings were further detailed in the case of \textit{Ekimdzhiev and Others v. Bulgaria}: First, the Court noted that the committee members do not need to have legal qualifications or experience and, secondly, the committee “has no power to order remedial measures in concrete cases.”\textsuperscript{78}

**Expert bodies and Data Protection Authorities**

The 2017 FRA report presented the various expert oversight bodies established in the Member States and analysed the oversight framework, alongside the features and

\textsuperscript{73} Finland, \textit{Parliament’s Rules of Procedure (eduskunnan työjärjestys/riksdagens arbetsordning)}, Act No. 40/2000, Chapter 3, section 31 b. For the English translation of the tasks provided in section 31 b of the Act, see the website of the Committee: [‘Intelligence Oversight Committee’](https://www.ly sek.fi/)

\textsuperscript{74} France, Order No. 58-1100 on the functioning of parliamentary assemblies (\textit{Ordonnance n° 58-1100 relative au fonctionnement des assemblées parlementaires}), 17 November 1958, Article 6 ninth.


\textsuperscript{76} Austrian Parliament, Website on the parliamentary enquiry committee concerning the Federal Agency for State Protection and Counter Terrorism (\textit{BVT-Untersuchungsausschuss}); Commission of Inquiry into the Terrorist Attack of November 2nd, 2020 (\textit{Untersuchungskommission}), Final report (\textit{Abschlussbericht}), 10 February 2021

\textsuperscript{77} ECtHR, \textit{Zoltán Varga v. Slovakja}, 20 July 2021, Nos. 58361/12, 25592/16 and 27176/16, paras. 135 and 159

\textsuperscript{78} ECtHR, \textit{Ekimdzhiev and Others v. Bulgaria}, No. 70078/12, 11 January 2022, para. 414.
competences of these bodies. Namely, these bodies should have “two essential qualities: be independent and have sufficient powers to carry out continuous control that is subject to public scrutiny”. These powers relate, on the one hand, to the appropriate review of the measures and, on the other, to the oversight bodies’ ability to ensure that effective action is taken in case they find irregularities.

Since 2017, six Member States – Czechia, Finland, Germany, Lithuania, Luxembourg and the Netherlands - have set up new (or replaced old) expert bodies dedicated to intelligence service oversight. In Czechia, the establishment of a new oversight body is regulated by a 2018 law. This body has not become operational yet because of the high requirements imposed on its members. They should hold among other things, top secret clearance, have no connection to the intelligence services, and be over the age of 40. Additional requirements were removed in 2022 to facilitate the nomination procedure. Table 3 provides an updated list of these bodies specialised in intelligence oversight, excluding DPAs. For the purpose of this report, DPAs are considered to be expert bodies, but since they are not specialised in intelligence oversight (with the exception of Belgium) they are dealt with separately.

Table 3 – Expert bodies (excluding DPAs) overseeing intelligence services in the EU

<table>
<thead>
<tr>
<th>EU Member State</th>
<th>Expert Bodies</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT</td>
<td>Legal Protection Commissioner at the Ministry of Interior (Rechtsschutzbeauftragter beim Bundesminister für Inneres) and Independent Control Commission for Protection of the Constitution (Unabhängige Kontrollkommission Verfassungsschutz)</td>
</tr>
<tr>
<td>BE</td>
<td>Standing Intelligence Agencies Review Committee – Standing Committee I (Vast Comité van Toezicht op de inlichtingen - en veiligheidsdiensten/Comité permanent de Contrôle des services de renseignement et de sécurité)* Administrative Commission (Bestuurlijke Commissie/Commission Administrative)</td>
</tr>
</tbody>
</table>

---

79 FRA (2017), p. 73

80 FRA (2017), p. 75

<table>
<thead>
<tr>
<th>EU Member State</th>
<th>Expert Bodies</th>
</tr>
</thead>
<tbody>
<tr>
<td>BG</td>
<td>National Bureau for Control over Special Intelligence Means (Національно бюро за контрол на спеціальні резонансні средства)</td>
</tr>
<tr>
<td>CY</td>
<td>Three-Member Committee (Τριμελής Επιτροπή)</td>
</tr>
<tr>
<td>CZ</td>
<td>Independent Control Body of the Intelligence Services (Orgán nezávislé kontroly zpravodajských služeb České republiky)</td>
</tr>
<tr>
<td>DE</td>
<td>G 10 Commission (G 10-Kommission) Independent Supervisory Council (Unabhängiger Kontrollrat)</td>
</tr>
<tr>
<td>DK</td>
<td>The Danish Intelligence Oversight Board (Tilsynet med Efterretningstjenesterne)</td>
</tr>
<tr>
<td>EE</td>
<td>N.A.</td>
</tr>
<tr>
<td>EL</td>
<td>Hellenic Authority for Communication Security and Privacy (Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών)</td>
</tr>
<tr>
<td>ES</td>
<td>N.A.</td>
</tr>
<tr>
<td>FI</td>
<td>Intelligence Ombudsman (Tiedusteluvalvontavaltuutettu/ Underrättelsetillsynsombudsman)</td>
</tr>
<tr>
<td>FR</td>
<td>National Commission for Control of Intelligence Techniques (Commission nationale de contrôle des techniques de renseignement) Specialised Formation of the Council of State (formation spécialisée du Conseil d’État)</td>
</tr>
<tr>
<td>HR</td>
<td>Office of the National Security Council (Ured Vijeća za nacionalnu sigurnost) Council for Civilian Oversight of Security and Intelligence Services (Vijeće za građanski nadzor sigurnosno-obavještajnih agencija)</td>
</tr>
<tr>
<td>HU</td>
<td>N.A.</td>
</tr>
<tr>
<td>IE</td>
<td>A designated judge of the High Court oversees interception of communications and data retention, while a separate designated judge of the High Court oversees the use of surveillance devices such as audio bugs and location tracking devices.</td>
</tr>
<tr>
<td>IT</td>
<td>N.A.</td>
</tr>
<tr>
<td>LT</td>
<td>Intelligence Ombudsman (Žvalgybos kontrolierius)</td>
</tr>
<tr>
<td>LU</td>
<td>Special Commission (Commission Spéciale)</td>
</tr>
<tr>
<td>EU Member State</td>
<td>Expert Bodies</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>LV</td>
<td>N.A.</td>
</tr>
</tbody>
</table>
| MT             | Commissioner of the Security Service *(Kummissarju tas-Servizz ta’ Sigurtà)*  
Security Committee *(Kumitat ta’ Sigurtà)* |
| NL             | The Review Committee on the Intelligence and Security Services *(Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, CTIVD)*  
Investigatory Powers Commission *(Toetsingscommissie Inzet Bevoegdheden, TIB)* |
| PL             | N.A.         |
| PT             | Council for the Oversight of the Intelligence System of the Portuguese Republic *(Conselho de Fiscalização do Sistema de Informações da República Portuguesa)* |
| RO             | N.A.         |
| SE             | Swedish Foreign Intelligence Inspectorate *(Statens inspektion för försvarsunderrättelseverksamheten)*  
Commission on Security and Integrity Protection *(Säkerhets- och integritetsskyddsnämnden)*  
Foreign Intelligence Court *(Försvarsunderrättelsedomstolen)* |
| SI             | N.A.         |
| SK             | N.A.         |

N.A: Not applicable

* The 2018 data protection reform in Belgium established the Standing Committee I as the supervisory authority in the area of data protection.

Source: FRA, 2023

Austria reformed its oversight framework and established a new expert body in 2021: the Independent Control Commission on the Protection for the Constitution *(Unabhängige Kontrollkommission Verfassungsschutz).* This body identifies systemic deficiencies and ways to improve the intelligence services. It acts either on its own

---

initiative or at the request of the Minister of the Interior or the parliamentary committee on intelligence oversight. In addition, it serves as contact point for whistle-blowers.\textsuperscript{83} This new expert body consists of five independent persons appointed by the National Council with a two-thirds majority. These members must possess legal qualifications and experience and undergo a trustworthiness test before appointment.\textsuperscript{84} In order to safeguard its independence, this body has separate office premises from the intelligence agency. This body does not deal with matters in the area of competence of the Legal Protection Commissioner at the Federal Ministry of Interior or any other legal protection authority.

Another example of a new oversight body is the Finnish Intelligence Ombudsman (\textit{tiedusteluvalvontavaltuutettu / underrätelsetillsynombudsmannen}), set up in 2019, which oversees both the civilian intelligence and military intelligence authorities. This is an independent body with investigative powers and an extensive right to access information. It can order the suspension or cessation of surveillance if it considers that the intelligence authority has acted unlawfully. It can also temporarily stop a surveillance technique authorised by a court and refer the matter to the authorising court. It also receives investigation requests and complaints by individuals and acts upon them.\textsuperscript{85}

Similarly, in Lithuania, a new expert body – the Intelligence Ombudsman (\textit{Žvalgybos kontrolierius, LRT}) – was set up with a 2021 law that came into effect on 1 January 2022.\textsuperscript{86} This body was established after the national DPA was excluded from exercising any control over data processing by national institutions for the purposes of national security and defence.\textsuperscript{87} It is composed of two Ombudspersons who are appointed by

\begin{itemize}
\item \textsuperscript{83} Austria, Explanatory notes to the Federal Act amending the Act concerning Police State Protection Act of the State, the Security Police Act, the Criminal Code, the Code of Criminal Procedure 1975 and the Expungement Redemption Act 1972 (\textit{Eräuterungen zum Bundesgesetz, mit dem das Polizeiliche Staatsschutzgesetz, das Sicherheitspolizeigesetz, das Strafgesetzbuch, die Strafprozeßordnung 1975 und das Tilgungsgesetz 1972 geändert werden}).
\item \textsuperscript{85} Finland, Act on the Oversight of Intelligence Gathering (\textit{laki tiedustelutoiminnan valvonnasta / lag om övervakning av underrättelseverksamheten}), Act No. 121/2019, 18 January 2019, Sections 11-14.
\item \textsuperscript{86} Lithuania, Law on Intelligence Ombudsmen (\textit{Žvalgybos kontrolierių įstatymas}), No. XIV-868, 23 December 2021
\item \textsuperscript{87} Lithuania, aw on Legal Protection of Personal Data Processed for the Purposes of Prevention, Investigation, Detection, or Prosecution of Criminal Acts, Execution of Sentences, or National Security and Defence (\textit{Asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas}), No. XIII-1435, 30 June 2018. Article 39(3).
the Parliament for a five-year term. This body has its own staff and budget and is headed by one of the two Ombudspersons. It is independent and accountable to Parliament only, to which it submits an annual report. It carries out supervision of intelligence services and their compliance with human rights standards and data protection. It also carries out legality assessments of the intelligence services activities and methods. It can investigate intelligence services’ activities and personal data processing and may access their collected data. It can initiate investigations on its own initiative, or based on complaints received from individuals, parliamentarians, and other public institutions.

Germany established the Independent Supervisory Council (*Unabhängiger Kontrollrat*) in 2021. This Council acts as a quasi-judicial oversight body tasked with prior authorisation of surveillance measures, and as an administrative oversight body for *ex post* oversight. Its members are six judges of the Federal Supreme Court and/or the Federal Administrative Court, who are elected by the Parliamentary Control Panel (*Parlamentarisches Kontrollgremium*) for twelve years. Cooperation among the different German intelligence oversight bodies is provided for by an amendment of the Parliamentary Control Panel Act, according to which the Control Panel was authorised to request information from the G10 Commission, the Federal Data Protection Commissioner and the Independent Supervisory Council, if deemed necessary for investigations of the Control Panel. 88

In the Netherlands, the Investigatory Powers Commission (TIB) assesses the legality of the prior authorisation granted by the responsible ministers to intelligence services to perform surveillance activities. This body supplements the main oversight body, the Review Committee on the Intelligence and Security Services (*Commissie Van Toezicht op de Inlichtingen- en Veiligheidsdiensten*, CTIVD), which is tasked with ongoing supervision of surveillance activities by intelligence services after authorisation. 89

The 2016 European data protection reform also led to important changes in intelligence oversight. FRA research indicates that national data protection laws passed after 2016 led mostly to broader restrictions or even exclusions of data protection authorities from exercising oversight and review of data processing activities of intelligence services (see *Figure 5*), such as in Bulgaria, Croatia or Greece. These changes concerned not only the oversight functions of data protection authorities over intelligence activities, but also impacted on data protection authorities’ remedial


89 The Netherlands, Intelligence and Security Services Act 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*), Articles 32-37.
powers, as described in the separate section on remedies (see p. 4848 below). In some States however, such as France, Italy or Slovenia, no important changes affected the general oversight structure. In Slovenia, under the 2022 data protection reform, the Director of the intelligence service can delay inspections of the DPA in very limited circumstances.\(^{90}\) In some countries, such as in Lithuania or Belgium, the exclusion of DPAs from exercising oversight on intelligence services was accompanied by supervisory powers in the area of data protection given to the oversight bodies.

**Figure 5 – DPAs’ oversight powers over national intelligence services, by Member State**

Personal Data Protection (Комисия за защита на личните данни, CPDP). This change was accompanied by corresponding amendments to the laws governing the different intelligence services, excluding the State Intelligence Agency from CPDP’s oversight, but retaining limited oversight on the Military Intelligence Service and the State Agency for National Security. A similar change was passed in Greece in 2019. The Greek Data Protection Authority was excluded from supervising processing operations of classified personal data carried out for activities concerning national security with the new data protection law. A similar change also occurred in Croatia. The new data protection laws excluded data processing for national security by bodies of the security-intelligence system and, hence, exempt them from any oversight by its data protection authority.

While it established a new oversight body in 2021, Lithuania – by enacting the European data protection reform in 2018 – had specifically removed the Data Protection Authority’s competencies over data processing by intelligence services for the purposes of national security and defence. In Belgium, the 2018 data protection reform designated the Standing Committee I (Le Comité permanent de contrôle des services de renseignement, Comité permanent R) as supervisory authority for all data

---

91 Bulgaria, Amendments and Supplements to the Personal Data Protection Act (Закон за изменение и допълнение на Закона за защита на личните данни), 26 February 2019.

92 Bulgaria, State Intelligence Agency Act (Закон за Държавна агенция „Разузнаване”), 13 October 2015, last amended 4 August 2020, Arts. 27 and 28; Military Intelligence Act (Закон за военното разузнаване), 13 November 2015, last amended 26 March 2021, Art. 78; State Agency for National Security Act (Закон за Държавна агенция „Национална сигурност”), 13 October 2015, last amended 5 June 2020, Art. 37.

93 Greece, Law No. 4624, Government Gazette Issue A’ 137/29.08.2019, “Personal Data Protection Authority [...]and other provisions.”, Art. 10 para 5.

94 Croatia, Implementation of the General Regulation on Data Protection Act (Закон о provedbi Opće uredbe o zaštiti podataka) Official Gazette (Narodne novine) No. 42/18, Art.1(2); Act on the Protection of Natural Persons in Connection with the Processing and Exchange of Personal Data for the Purposes of Prevention, Research, Detection or Prosecution of Criminal Offenses or Execution of Criminal Sanctions (Закон о заштити фizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe spriječavanja, istraživanja, otkrivanja ili progona kaznenih diela ili izvršavanja kaznenih sankcija), Official Gazette (Narodne novine) No. 68/18, Art. 3(2); Personal Data Protection Agency (Agencija za zaštitu osobnih podataka), Insight into the files of school employees by employees of the Security and Intelligence Agency (Uvid u dosje zaposlenika škole od strane zaposlenika Sigurnosno-obavještajne agencije).

95 Lithuania, Law on Legal Protection of Personal Data Processed for the Purposes of Prevention, Investigation, Detection, or Prosecution of Criminal Acts, Execution of Sentences, or National Security and Defence (Asmens duomeny, tvarkomu nusikalstamų veiku prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, baudsmų vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas), No. XIII-1435, 30 June 2018. Article 39(3).
processing activities of intelligence services linked to national security. The Belgian Data protection Authority (L’Autorité de protection des données (APD)) is excluded from performing any oversight on data processing by the intelligence service. However, cooperation between the various sectorial supervisory authorities is called for by law. Accordingly, a Protocol for cooperation was adopted in 2020. It clarifies the division of tasks and the scope of competencies of the data protection supervisory authorities in Belgium. Since 2018, the Standing Committee I reports annually on its activities as a supervisory authority in the area of data protection.

Other data protection reforms were enacted in other Member States. In Germany, for example, the data protection reform revised the framework for data processing in the field of national security. New provisions on the specific role and oversight of the Federal Data Protection Commissioner (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, BfDI) were included in the laws of the three federal intelligence services thus transferring the supervisory powers from the old Federal Data Protection Act to intelligence legislation. In particular, with regard to the Federal Intelligence Service (Bundesnachrichtendienst, BND), the BfDI’s power to issue ad hoc opinions on critical issues to the parliament and the general public was limited in that the BfDI may inform other oversight bodies on a confidential basis only.


97 Belgium, L’Autorité de protection des données (APD), l’Organe de contrôle de l’information policière (COC), le Comité permanent de contrôle des services de renseignement (CPR) et le Comité permanent de contrôle des services de police (CPP), Protocol for cooperation between the Belgian federal supervisory authorities in the field of data protection agreement between the data protection authority, the police information supervisory body, the permanent committee for the control of the intelligence services and the permanent committee control of police services (Protocole de coopération entre les autorités de contrôle fédérales belges en matière de protection des données convention entre l’autorité de protection des données, l’organe de contrôle de l’information policière, le comité permanent de contrôle des services de renseignement et le comité permanent de contrôle des services de police), 20 November 2020.


100 Germany, After further legal changes, Federal Act on the Protection oft he Constitution (Bundesverfassungsschutzgesetz), Sections 27 and 28; Federal Intelligence Agency Act (Bundesnachrichtendienstgesetz), Sections 63 and 64; Military Counter Intelligence Act (Gesetz über den Militärischen Abschirmdienst), Sections 13 and 13a.

101 Germany, Act to Change the Federal Intelligence Service Act to Implement the Guidelines of the Federal Constitutional Court and the Federal Administrative Court (Gesetz zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts), 19 April 2021.
The oversight powers of Data Protection Authorities appear to have been reinforced since 2017 only in a few countries. For example, in Luxembourg, based on the data protection reform of 2018, the National Commission for Data Protection (Commission Nationale pour la Protection des Données, CNPD) is responsible for monitoring and verifying legal compliance of the processing of personal data by the State Intelligence Service. In this regard, the CNPD enjoys significant investigative, corrective, authorisation and advisory powers. It also hears complaints and provides for remedies, subject to judicial appeal. In Cyprus, following the 2018 reforms, the Data Protection Authority has access to all personal data and information necessary for the performance of its mandate, without any form of confidentiality, unless it is covered by legal professional privilege. Past restrictions on accessing records, which were kept for national security purposes, were abolished. In Sweden, the Authority for Privacy Protection (Integritetskyddsmyndigheten) can on its own initiative now issue warning orders, but also injunctions for requiring the intelligence services to take measures to secure the lawfulness of data processing.

In Hungary, the implementation of the GDPR allowed the National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság, NAIH) which exerts oversight on intelligence services - to start investigations on its own initiative (ex officio), which was relied on in reviewing Pegasus-related allegations. However, the ECtHR recently found a violation with respect to the

---

102 Luxembourg, Act of 1 August 2018 on the organisation of the National Commission for Data Protection and the general data protection regime etc (Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d’avancement des fonctionnaires de l’État), Arts. 8, 44,45.

103 Cyprus, Law on the protection of individuals with regard to the processing of personal data and the free circulation of personal data of 2018 (Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018) N. 125(I)/2018, article 25(a).


limited powers of the NAIH which can perform its tasks by sending its fact-finding requests to the overseeing Minister and rely on her or his findings.  

**Figure 6** Figure 6 summarises the current situation with regard to oversight of intelligence services by expert bodies and data protection authorities across EU Member States.

**Figure 6 – Oversight of surveillance by intelligence services by expert bodies and DPAs**

![Diagram showing models of oversight framework of intelligence services based on different actors involved](image)

* As over other data controllers

_Source: FRA, 2023_

**Models of oversight framework of intelligence services based on different actors involved**

As highlighted in the 2017 FRA report and considering the recent development in the framework of oversight bodies as described in previous sections, the oversight of intelligence services is organised differently across EU Member States. The

---

106 ECtHR, _Hüttl v. Hungary_, No. 58032/16, 29 September 2022, para. 18.
jurisprudence of both European Courts has set minimum standards, but leaves States with significant leeway to organise the oversight of the activities of their own intelligence services. This section specifically responds to the request of the European Parliament, which asked to see which oversight models were prevalent in the EU. FRA’s research identified 18 different oversight frameworks in the EU. Out of these, the following section describes five models covering most EU Member States. When assessing the efficiency of an oversight framework, two key elements should be highlighted: 1) the oversight framework should reflect the powers of the intelligence services (see FRA Opinion 3 above) and 2) the oversight structure, including through collaboration of different entities should cover the full surveillance cycle - the ECtHR refers to a ‘continuous control’ (see FRA Opinion 6 above). The models below focus on expert bodies exercising oversight on intelligence services during and also after secret surveillance measures. They do not describe nor extend to ex post judicial control of surveillance measures at the stage of remedies. This choice does not disregard the important role that courts play in the overall oversight framework of intelligence services, especially at the remedial stage.

The Member States that are not covered by the five models are Ireland and Malta because they do not rely on any arrangement of parliamentary oversight.

The multitude of models across the EU is due to the diversity of actors contributing to the oversight framework. Several Member States place emphasis on the role of Parliament in the oversight structure. This forms the first model identified by FRA. It mainly relies on two actors: an authority authorising the surveillance measure in advance and a parliamentary committee exercising subsequent oversight. Figure 7 illustrates this model. It is present in Estonia, Latvia, Romania, Slovakia and Spain. Poland has features of this model but instead of the judge authorising the surveillance measure, it is the executive or the services (depending on the surveillance measure) that approve the surveillance technique.

As noted above, the majority of EU Member States has set up specialised expert bodies overseeing the work of intelligence services. In this second model, the specialised expert body focuses its work on ex post oversight alongside a parliamentary committee. A judicial authority authorises the surveillance measure. 

*Figure 8* illustrates the role played by the expert body, which is not competent at the authorisation stage. This model has been adopted in Croatia, Czechia, Denmark, Greece and Lithuania. The Belgium and Dutch systems also resemble this model. In the Netherlands however the authorisation can be given by a judicial authority, the executive or the expert body, depending on the surveillance measure at stake, while in Belgium, the authorisation is given by the executive, the expert body or the services, depending on the surveillance measure at stake.
A significant number of Member States rely not only on specialised expert bodies to oversee intelligence services activities, but also include data protection authorities in their oversight framework. In most cases, the DPA has limited power compared with that of the specialised expert body, which leads the *ex post* oversight of intelligence services activities. In this third model, a parliamentary committee also contributes to the oversight function. Luxembourg provides an example of this model as illustrated in Figure 9. Germany also largely adheres to this model - the only difference being that the parliamentary committee approves certain surveillance measures. France also follows the same model, but with the executive having the binding approval power when authorising a surveillance technique. This model also largely fits with the Bulgarian oversight framework, but in Bulgaria the authorisation can only be given by a judge. In exceptional cases, the DPA holds the same powers towards the intelligence service activities as for any other data controller. This is the case in Austria and Finland.
Figure 9 – Model of oversight framework No. 3 – ex post oversight by expert body, DPA and parliament.

Source: FRA, 2023

The fourth model relies on the DPA and the parliamentary committee to conduct the oversight of intelligence services, without a separate oversight body with a mandate wider than data protection. In Hungary, Italy and Slovenia, where this model is applied, there is no specialised expert body. The DPA has either limited power (Hungary and Italy) or the same power as for any other data controllers (Slovenia). Figure Figure 10 below illustrates the Hungarian model. In Italy, authorisations of intelligence measures are always given by a judge.
The fifth and last model is characterised by a non-specialised parliamentary committee at the *ex post* oversight stage. This model is present in Sweden, where the expert body is working with a DPA with the same powers over intelligence services activities as any other data controllers, while a judge is authorising the use of surveillance. *Figure 11* is illustrating this model. Non-specialised parliamentary committees are also present in Cyprus and Portugal. In Cyprus, the executive authorises surveillance with an expert body and a DPA performing the expert oversight. In Portugal, a judge authorises the use of surveillance, while an expert body performs the oversight.

*Source: FRA, 2023*
Figure 11 – Model of oversight framework No. 5 – ex post oversight by expert body and non-specialised parliament committee

Source: FRA, 2023
Remedies

Relevant Updated Key Findings

The 2017 FRA report highlighted the challenges for accessing effective remedies when it comes to surveillance: on the one hand, the need for secrecy that is inherent to the intelligence field impedes effective access to classified information, and on the other hand, the lack of expertise of the staff of remedial bodies may create specific issues. To these specific issues, classic challenges averting effective remedies also apply: judicial avenues are often costly, slow, and entail complex procedural rules. In this context, non-judicial avenues may provide individuals with important complementary remedial avenues.

In 2017, FRA’s research showed that, overall, in the context of surveillance, only few individuals seek remedy. The average of 10 to 20 per year in 2017 stayed stable in more recent years.

FRA highlighted the necessity to ensure minimum requirements for remedies to be effective. Non-judicial bodies must be independent. They must tackle the following challenges: awareness of surveillance measures by individuals (either through notification or through any other possibility to obtain information about interceptions), access to classified information for remedial bodies, appropriate redress (destruction of the data collected, monetary relief), and proper expertise of remedial bodies.

In 2023, the situation appears quite similar to 2017. However, the 2016 European data protection reform impacted six DPAs, which lost their remedial powers in this area.

In most EU Member States, non-judicial bodies can offer individuals remedies. Only three Member States do not offer non-judicial remedial avenues to lodge a complaint related to activities of intelligence services. In this regard, the situation remains unchanged since 2017.

In 12 Member States, individuals may lodge a complaint with only one single non-judicial body with remedial powers (in 2017 this was the case in 10 Member States out of the 28 EU Member States). In the remaining 12 Member States (out of a total of 24 that do offer non-judicial remedies), two or more such bodies have remedial powers.

Since 2017, the situation with regards to the scope of remedial powers of expert bodies has remained largely unchanged. Basically, compared to other non-judicial bodies with remedial powers, expert bodies still enjoy the broader powers: in nine of the 14 Member States that have expert bodies, these bodies have the strongest...
powers to offer an effective remedy. However, the following changes should be noted. In the three Member States where new expert bodies were established, two were granted large remedial powers (to take binding decisions, to fully access collected data, and to communicate that a control was performed to the complainant), while the other one only granted the new expert body with full access to the data, including classified information.

Remedial bodies’ effectiveness depends foremost on their binding decision-making powers. In 15 Member States, remedial bodies can issue binding decisions. Most of them are expert bodies and Data Protection Authorities. While in 2017 six Member States had not empowered any of their non-judicial bodies with the ability to take binding decisions, this is now the case in seven Member States.

**Selected 2017 FRA Opinions**

**Opinion 12: Providing for effective remedies before independent bodies with remedial powers**

EU Member States should ensure that judicial and non-judicial bodies with remedial powers have the powers and competences to effectively assess and decide on individuals’ complaints related to surveillance.

**Opinion 13: Ensuring availability of nonjudicial bodies with remedial powers**

EU Member States should ensure that both judicial and non-judicial remedial bodies are accessible to individuals. Notably, Member States should identify what potential gaps prevent individuals from having their complaints effectively reviewed, and ensure that non-judicial expert bodies can complement the remedial landscape where needed.

**Opinion 14: Allowing for awareness of completed surveillance measures**

EU Member States should ensure that the legitimate aim and proportionality tests are conducted by intelligence services before limiting access to information based on national security. A competent authority should assess the confidentiality level. Alternatively, controls should be carried out by oversight bodies in the name of complainants when notification or disclosure are not possible.

**Opinion 15: Ensuring a high level of expertise among remedial bodies**

EU Member States should ensure that where judicial or non-judicial remedial bodies lack relevant expertise to effectively assess individuals’ complaints, specific systems are established to address these gaps. Cooperation with expert oversight bodies, technical experts or members of the intelligence services can support effective remedial systems.
In line with the well-established European case law, any individual may claim to be a victim of an interference with their privacy rights based on the existence of intelligence laws prescribing secret surveillance.\(^{108}\) Individuals shall have recourse to remedies that are effective in law and practice for reviewing the lawfulness and proportionality of any surveillance against them and redressing any violations of their rights. While such remedies do not need to be of a judicial nature, they need to be effective.

The courts have an important role to play in reviewing surveillance ex post at the remedial stage, either when directly handling complaints against intelligence services or when examining appeals against the decisions of a non-judicial oversight body.\(^{109}\) While in principle all Member States provide the opportunity to complain about privacy and other rights violations before a judge, as the 2017 FRA report highlighted, judicial avenues are not necessarily effective. Recourse to courts may be hindered by strict procedural rules on evidence and legal standing. The common ineffectiveness of judicial recourse is acknowledged by the ECtHR and has resulted in affording a much broader meaning to notion of ‘victim’ based on the ECHR, not requiring the prior exhaustion of domestic judicial remedies in a number of cases regarding surveillance by intelligence services.\(^{110}\) At the same time, recourse to non-judicial bodies raises issues of powers, independence as well as expertise.\(^{111}\)

In this regard, the ECtHR has repeatedly found the notification of surveillance measures, or, at least, an adequate possibility of requesting and obtaining information about interceptions from the authorities, to be a relevant factor in assessing the effectiveness of remedies and hence the existence of effective safeguards against the abuse of surveillance powers.\(^{112}\)

“As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is a relevant factor in assessing the

---


109 CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others [GC]*, 6 October 2020, para. 190; ECtHR, *Centrum för rättvisa v. Sweden* [GC], No. 35252/08, 25 May 2021, paras. 166-7, 249, 251, 271, 273, 275, 362; *Big Brother Watch and Others v. the United Kingdom [GC]*, Nos. 58170/13, 62322/14 and 24969/15 [GC], 25 May 2021, paras. 413, 415, 425;


112 ECtHR, *Centrum för rättvisa v. Sweden* [GC], No. 35252/08, 25 May 2021, para. 271.
effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of surveillance powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspects that he or she has been subject to surveillance can apply to courts, whose jurisdiction does not depend on notification to the surveillance subject of the measures taken.”

ECtHR, **Centrum för rättvisa v. Sweden [GC]**, No. 35252/08, 25 May 2021, para. 251

Providing individuals with the necessary information, although crucial, is not sufficient and is only a pre-condition for an effective access to remedies. Excessive formal requirements (e.g. short-time limitations to bring a complaint) would severely undermine the effectiveness of any available remedies. In **Centrum för rättvisa v. Sweden**, the ECtHR stressed the need for guarantees that exclude any conflict of interests of remedial bodies with the body authorising the surveillance or exercising regular oversight on intelligence services. In **Ekimdzhiev and Others v. Bulgaria** also, the Court highlighted other challenges for the effectiveness of remedies, and notably the ability for any remedial body to take binding decisions, including on the destruction of collected information.

“(…) several shortcomings undermine its [the special parliamentary committee] effectiveness. First, its members need not be persons with legal qualifications or experience. Secondly, it has no power to order remedial measures in concrete cases, such as the destruction of retained or accessed communications data; it can only give instructions designed to improve the relevant procedures. If it detects irregularities, it can only bring the matter to the attention of the prosecuting authorities, or inform the heads of the relevant access-requesting authorities

---

113 ECtHR, **Ekimdzhiev and Others v. Bulgaria**, No. 70078/12, 11 January 2022, paras. 264-275, 354-5, 356(h), 380-382; **Marie Ringler v. Austria** (Dec.), No. 2309/10, 12 May 2020, para. 73.

114 ECtHR, **Centrum för rättvisa v. Sweden [GC]**, No. 35252/08, 25 May 2021, para. 359, 372.
and communications service providers. In view of the shortcomings outlined above, the system of overseeing the retention of communications data and its subsequent accessing by the authorities in Bulgaria, as currently organised, does not appear capable of providing effective guarantees against abusive practices in this respect.”


As Table 4 shows, in most EU Member States, different models exist in terms of non-judicial bodies such as DPAs, expert bodies, executive bodies, parliamentary committees, and ombuds institutions that can offer remedies. There are only three Member States (Czechia, Latvia and Poland) that do not offer non-judicial remedial avenues but only provide individuals with judicial avenues to lodge a complaint. In these Member States, neither data protection authorities nor any other oversight bodies have remedial powers over intelligence services. In this regard, the situation remains unchanged compared to 2017.

**Table 4 – Non-judicial bodies with remedial powers in the context of surveillance: different models by EU Member State**

<table>
<thead>
<tr>
<th></th>
<th>Executive (ministry)</th>
<th>Expert body(ies)</th>
<th>DPA</th>
<th>Parliamentary committee(s)</th>
<th>Ombuds institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>BE</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>BG</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CY</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CZ</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>DK</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>EL</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>FI</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
Remedial powers of Data Protection Authorities

In relation to Data Protection Authorities’ remedial powers over intelligence services, the situation has evolved in seven Member States since 2017. In Belgium, Bulgaria, Croatia, Greece and Lithuania, with national data protection reforms, DPAs no longer have competency to control matters linked to national security. They have consequently lost their power to investigate complaints lodged by individuals in the context of intelligence services’ activities. These modifications were introduced by the Member States while implementing the 2016 EU Data Protection reform. In Bulgaria, for example, the 2019 legislative reform excluded surveillance activities from the
overall scope of application of the Personal Data Protection Act. The explanatory report accompanying the amendments referred to EU Data protection reform to justify the amendments. Similarly, in Croatia, the act adopted in 2018 to implement the GDPR prescribes that the law does not apply to the processing of personal data carried out by competent authorities for the purpose of, among others, protecting against threats to public security and their prevention, including in the areas of national security and defence. In Lithuania, both the DPA and the ombudsperson have lost their remedial powers through the adoption of two legislative reforms: in 2018, the Law transposing the EU Law Enforcement Directive precludes the Lithuanian DPA from exercising any control over data processing by national institutions for the purposes of national security and defence, and in 2022, amendments to the Law on Seimas Ombudsmen precludes the Ombudsmen from investigating activities of intelligence institutions. Simultaneously to the 2022 reform, a new expert body, the Intelligence Ombudsman, has been set up and it was given remedial powers concerning intelligence services’ personal data processing and other activities. In Belgium, the remedial powers were expressively shifted from the Data Protection Authority to the expert oversight body in the 2018 law implementing the 2016 European data protection reform.

In Cyprus and Sweden, on the other hand, the implementation of GDPR at national level resulted in providing Data Protection Authorities with new powers which strengthen their ability to provide an effective remedy. In Cyprus, following the adoption of the 2018 law implementing the GDPR, the DPA was provided with the legal

115 Bulgaria, Amendments and Supplements to the Personal Data Protection Act (Закон за изменение и допълнение на Закона за защита на личните данни), 26 February 2019.


117 Croatia, Act on the Protection of Natural Persons in Connection with the Processing and Exchange of Personal Data for the Purposes of Prevention, Research, Detection or Prosecution of Criminal Offenses or Execution of Criminal Sanctions (Закон о заштити фizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili praga znanstvenih djela ili izvršavanja kaznenih sankcija), 4 August 2018.


120 Lithuania, Law on Intelligence Ombudsmen (Žvalgybos kontrolierių įstatymas), No. XIV-868, 23 December 2021. Art. 3.
basis to access data held by the intelligence services and take binding decisions.\textsuperscript{121} Similarly, in Sweden, the DPA was granted access to all personal data processed by intelligence services, including safety and protective measures. In addition, the DPA may order the Swedish Security Service to stop processing or destroy personal data (but not order the Swedish Armed Forces nor the National Defence Radio Establishment). Finally, decisions taken by the DPA may be reviewed by a court.

\textit{Figure 12} illustrates the diversity of DPAs’ remedial competences over intelligence services across the EU.

**Figure 12 – DPAs’ remedial competences over intelligence services compared to powers over other data controllers**

\textsuperscript{121} Cyprus, Law on the protection of individuals with regard to the processing of personal data and the free circulation of personal data of 2018 (\textit{Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018}) N. 125(I)/2018,
Remedial powers of other non-judicial oversight bodies

In 2023, the situation remained largely unchanged regarding the remedial powers of non-judicial oversight bodies other than Data Protection Authorities. A few developments are, however, worth noting.

In few Member States (including Croatia, Denmark and Finland), the oversight bodies have gained certain aspects of remedial powers over the intelligence authorities. In Finland, the Intelligence Ombudsman may fully access data collected by intelligence services and may take binding decisions. So far, the Intelligence Ombudsman did not receive any complaints. When an investigation has been carried out, the Intelligence Ombudsman may inform individuals, but only stating that an investigation has been carried out.\textsuperscript{122} In Denmark, according to the act on the Security and Intelligence Service and the act on the Danish Defence Intelligence Service that were consolidated in 2017,\textsuperscript{123} a natural or legal person living in Denmark may file a complaint and request the oversight body (TET) to investigate whether the intelligence service has illegally processed information about them. The TET can only inform the individual that the service does not illegally process information regarding them, without providing any further information. Where it is established in the course of an examination that intelligence services processed information illegally, TET has the power to issue binding decisions requesting the services to delete the data. If special circumstances so warrant, TET has the power to instruct intelligence services to give whole or partial access specifying which information were processed concerning the complainant. However, the TET highlighted in 2021 that in practice, these provisions have limited application, as few individuals have so far requested TET to investigate whether an intelligence service has illegally processed information about them.\textsuperscript{124} In Croatia, the Civilian Oversight Council of Security Intelligence Agencies, re-established in 2018 after several years of inactivity, may now access data collected by intelligence services, and may inform complainants once it performs an investigation based on their complaints.

As it was shown in 2017, only very few individuals alleged unlawful activities by intelligence services before oversight bodies.\textsuperscript{125} The following examples confirm 2017 findings. In 2021, the Belgian Standing Committee I received 72 complaints (compared

\textsuperscript{122} Finland, \textit{Act on the Oversight of Intelligence Gathering (laki tiedustelutoiminnan valvonnasta/lagom övervakning av underrättelseverksamheten)}, Act No. 121/2019, 18 January 2019, Chapter 2, section 3.

\textsuperscript{123} Denmark, \textit{Consolidated act no. 231 of 7 March 2017 on Danish Security and Intelligence Service (Bekendtgørelse af lov om Politiets Efterretningstjeneste (PET)).}

\textsuperscript{124} Denmark, TET, \textit{Annual report on PET (2021)}, p. 28; and TET, \textit{Annual report on FE (2021)}, p. 22.

\textsuperscript{125} FRA (2017), p. 118.
to 62 in 2020). In 2020, most of them were dismissed (55 out of 62).\footnote{Belgium, Standing Committee I (2021), \textit{Activity Report 2020}, p. 1.} By contrast, in 2021, 23 were rejected as manifestly ill-founded and 28 because the Standing Committee I was not competent. 14 of the remaining 24 were handled within 2021.\footnote{Belgium, Standing Committee I (2022), \textit{Rapport d’activités 2021}, p. 1.}

In France, the CNCTR received 48 complaints in 2021 (compared to 33 in 2020). A complaint is handled within two months. Once the individual has received the answer from the CNCTR, they can bring the case before the Specialised Formation of the Council of State (\textit{la formation spécialisée du Conseil d’État}). In 2021, like 2020, it received 8 applications.\footnote{France, CNCTR (2022), \textit{Sé rapport d’activité 2021}, p. 108.} The German G 10 Commission received four complaints in 2020, three of which were ill-founded.\footnote{Germany, Federal Parliament (2022), \textit{Report 1 January – 31 January 2020}, Doc. 20/4976, p. 7.} The Dutch CTIVD handled 23 complaints in 2021.\footnote{Netherlands, CTIVD (2022), \textit{Annual Report CTIVD 2021}, p. 19.}
Conclusions

This update presented developments in a field of law in continuous evolution: Intelligence laws need constantly to keep up the capacity of intelligence services with current threats and technical developments. At the same time, the CJEU case-law has made clear that secret surveillance impacts, among others, on the right to respect private and family life (Article 7), the protection of personal data (Article 8) and the right to an effective remedy and a fair trial (Article 47) of the Charter of Fundamental Rights of the European Union. It also makes clear that bodies exercising oversight on intelligence services should evolve in a similar fashion as intelligence law and capacities of intelligence services. Their power and technical abilities should match those of the services they oversee to fulfil the requirements set by the case-law of the CJEU and the ECtHR. The crucial concept of ‘continuous control’ developed by the ECtHR should be a reality in practice. In all EU Member States, several entities contribute to the oversight framework. Enhanced collaboration between relevant oversight authorities should ensure an oversight of the full surveillance cycle. The efficiency of the five oversight models presented in this report should be assessed based on two principles: matching powers and continuous control over the intelligence cycle.

The report also addresses the issue of remedies. As already highlighted by FRA in 2017, remedies in the field of surveillance by intelligence services need to overcome a number of challenges. In this area, individuals wishing to complain about alleged fundamental rights violations face a number of issues, including a challenge which undermines the right to a fair hearing, namely secrecy. The 2017 FRA report discussed how Member States addressed this key aspect. In this update, FRA found that the situation has not much evolved in 2023. Pursuing a claim against an alleged illegal surveillance measure places the individual in a situation where they need to trust the remedial body. The effectiveness of bodies dealing with remedies is the element on which such trust stems from. Furthermore, the 2016 EU data protection reform led to some Member States significantly reducing Data Protection Authorities’ remedial competencies in the field of national security, while in other Member States, DPAs powers were reinforced.

In 2023, as it was the case in 2017, a strong independent oversight structure offering effective remedies to individuals would “pave the way (...) to renewed trust among European citizens towards their intelligence services and, as a result, a more effective defence of national security.”\(^1\) Enhanced security measures should be enshrined in a

\(^1\) FRA (2017), p. 135.
strong fundamental rights framework, where the necessity and proportionality of surveillance measures are regularly assessed.
Case law (post 2017)

Court of Justice of the European Union

Joined Cases C-793/19 and C-794/19, SpaceNet AG [GC], 20 September 2022

Case C-140/20, Commissioner of An Garda Síochána and Others [GC], 5 April 2022,

Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others [GC], 6 October 2020

Case C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others [GC], 6 October 2020

European Court of Human Rights

Big Brother Watch and Others v. the United Kingdom [GC], Nos. 58170/13, 62322/14 and 24969/15 [GC], 25 May 2021

Centrum för rättvisa v. Sweden [GC], No. 35252/08, 25 May 2021

Hüttl v. Hungary, No. 58032/16, 29 September 2022

Haščák v. Slovakia, Nos. 58359/12 and 2 others, 23 June 2022

Ekimdzhiev and Others v. Bulgaria, No. 70078/12, 11 January 2022

Zoltán Varga v. Slovakia, Nos. 58361/12 and 2 others, 20 July 2021

Tretter and Others v. Austria, No. 3599/2010 (dec.), 29 September 2020

Marie Ringler v. Austria (dec.), No. 2309/10, 12 May 2020.

Breyer v. Germany, No. 50001/12, 30 January 2020.

National courts

France, Council of State (Conseil d'État), French Data Network and others, Decision No 393099, 21 April 2021.
Germany, Federal Constitutional Court, (Bundesverfassungsgericht, BVerfG), Judgment of the First Senate, 1 BvR 2835/17, 19 May 2020.

Germany, Federal Constitutional Court (Bundesverfassungsgericht) (2022), 1 BvR 2354/13, 28 September 2022.

## Annex 1

### Table 5 – Overview of intelligence services in the 27 Member States

<table>
<thead>
<tr>
<th>EU MS</th>
<th>Security/Intelligence Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT</td>
<td>Directorate State Protection and Intelligence Service / Direktion Staatsschutz und Nachrichtendienst (DSN)</td>
</tr>
<tr>
<td></td>
<td>Military Intelligence Service/Heeresnachrichtenamt (HNaA)</td>
</tr>
<tr>
<td></td>
<td>Military Defence Agency/Abwehramt (AbwA)</td>
</tr>
<tr>
<td>BE</td>
<td>State Security/ Veiligheid van de Staat /Sûreté de l'Etat (VSSE)</td>
</tr>
<tr>
<td></td>
<td>General Intelligence and Security Services of the Armed Forces / Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht / Service Général du Renseignement et de la Sécurité (ADIV/SGRS)</td>
</tr>
<tr>
<td>BG</td>
<td>State Intelligence Agency (SIA) /Nationalna Razuznavatelna Služba (NRS)</td>
</tr>
<tr>
<td></td>
<td>State Agency for National Security / Държавна Агенция &quot;Национална сигурност (SANS)</td>
</tr>
<tr>
<td></td>
<td>State agency “Technical operations” / Държавна агенция „Технически операции (SATO)</td>
</tr>
<tr>
<td></td>
<td>Military Information Service (MIS)/Sluzhba Voenna Informatcia (CBP)</td>
</tr>
<tr>
<td>CY</td>
<td>Cypriot Intelligence Service/Κυπριακή Υπηρεσία Πληροφοριών (ΚΥΠ)</td>
</tr>
<tr>
<td>CZ</td>
<td>Security Information Service/Bezpečnostní informační služba (BIS)</td>
</tr>
<tr>
<td></td>
<td>Office for Foreign Relations and Information/Úřad pro Zahraniční Styky a Informace (UZSI)</td>
</tr>
<tr>
<td></td>
<td>Military Intelligence/Vojenské Zpravodajství (VZ)</td>
</tr>
<tr>
<td>DE</td>
<td>Federal Office for the protection of the Constitution/ Bundesamt für Verfassungsschutz (BfV)</td>
</tr>
<tr>
<td></td>
<td>Federal Intelligence Service/Bundesnachrichtendienst (BND)</td>
</tr>
<tr>
<td></td>
<td>Federal Office for Military Counter-Intelligence Service/ Bundesamt für den Militärischen Abschirmdienst (BAMAD)</td>
</tr>
<tr>
<td></td>
<td>State Office for the Protection of the Constitution of Baden-Württemberg/ Landesamt für Verfassungsschutz Baden-Württemberg</td>
</tr>
<tr>
<td></td>
<td>Bavarian Office for Protection of the Constitution/ Bayerische Landesamt für Verfassungsschutz</td>
</tr>
<tr>
<td></td>
<td>Berlin Senate Administration for Home Affairs, Department of Protection of Constitution/Senatsverwaltung für Inneres, Abteilung Verfassungsschutz Berlin</td>
</tr>
<tr>
<td>EU MS</td>
<td>Security/Intelligence Service</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td></td>
<td>Brandenburg Ministry of Interior and Municipalities, Department of Protection of Constitution/Ministerium des Innern und für Kommunales, Abteilung Verfassungsschutz Brandenburg</td>
</tr>
<tr>
<td></td>
<td>Bremen State Office for the Protection of Constitution/Landesamt für Verfassungsschutz Bremen</td>
</tr>
<tr>
<td></td>
<td>State Office for the Protection of Constitution of the Free and Hanseatic City of Hamburg/Landesamt für Verfassungsschutz der Freien und Hansestadt Hamburg</td>
</tr>
<tr>
<td></td>
<td>Hessen State Office for the Protection of Constitution/Landesamt für Verfassungsschutz Hessen</td>
</tr>
<tr>
<td></td>
<td>Lower Saxony Ministry of Interior, Sport and Integration, Department 5/Ministerium für Inneres, Sport und Integration, Abteilung 5 Niedersachsen</td>
</tr>
<tr>
<td></td>
<td>Mecklenburg-Vorpommern Ministry of Interior, Department II 5/Mecklenburg-Vorpommern Innenministerium, Abteilung II 5</td>
</tr>
<tr>
<td></td>
<td>North Rhine-Westphalia Ministry of Interior and Municipalities, Department for the Protection of Constitution/Nordrhein-Westfalen Ministerium für Inneres und Kommunales, Abteilung Verfassungsschutz</td>
</tr>
<tr>
<td></td>
<td>Rhineland-Palatinate Ministry of Interior and Sport, Department for the Protection of Constitution/Rheinland-Pfalz Ministerium des Innern und für Sport, Abteilung Verfassungsschutz</td>
</tr>
<tr>
<td></td>
<td>Saarland State Office for the Protection of Constitution/Landesamt für Verfassungsschutz Saarland</td>
</tr>
<tr>
<td></td>
<td>Saxony State Office for the Protection of Constitution/Landesamt für Verfassungsschutz Sachsen</td>
</tr>
<tr>
<td></td>
<td>Saxony-Anhalt Ministry of Interior and Sport, Department for the Protection of Constitution/Sachsen-Anhalt Ministerium für Inneres und Sport, Abteilung Verfassungsschutz</td>
</tr>
<tr>
<td></td>
<td>Schleswig-Holstein Ministry of Interior, Department for the Protection of Constitution/Schleswig-Holstein Innenministerium, Abteilung Verfassungsschutz</td>
</tr>
<tr>
<td></td>
<td>Thüringen Ministry of Interior and Municipalities, Office for the Protection of Constitution /Thüringen Ministerium für Inneres und Kommunales, Amt für Verfassungsschutz</td>
</tr>
<tr>
<td>DK</td>
<td>Danish Defence Intelligence Service (DDIS)/Forsvarets Efterretningstjenst (FE)</td>
</tr>
<tr>
<td></td>
<td>Danish Security and Intelligence Service (DSIS)/Politiets Efterretningstjeneste (PET) (part of the police)</td>
</tr>
<tr>
<td>EE</td>
<td>Estonian Foreign Intelligence Service/ Välsluureame</td>
</tr>
<tr>
<td></td>
<td>Estonian Internal Security Service/ Kaitsepolitseiamet (KAPO)</td>
</tr>
<tr>
<td></td>
<td>Military Intelligence Branch of the Estonian Defence Forces/Kaitseväe peastaabi luureosakond</td>
</tr>
<tr>
<td>EU MS</td>
<td>Security/Intelligence Service</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>EL</td>
<td>National Intelligence Service/Εθνική Υπηρεσία Πληροφοριών (EYP)</td>
</tr>
<tr>
<td></td>
<td>Directorate of Military Intelligence of the National Defence General Staff/Διεύθυνση Στρατιωτικών Πληροφοριών του Γενικού Επιτελείου Εθνικής Άμυνας</td>
</tr>
<tr>
<td>ES</td>
<td>National Center for the Protection of Critical Infrastructures /Centro Nacional de Protección de Infraestructuras Críticas (CNPIC)</td>
</tr>
<tr>
<td></td>
<td>National Intelligence Centre/Centro Nacional de Inteligencia (CNI)</td>
</tr>
<tr>
<td></td>
<td>Intelligence Centre on Organised Crime and Terrorism/Centro de Inteligencia Contra el Terrorismo y el Crimen Organizado (CITCO)</td>
</tr>
<tr>
<td></td>
<td>Intelligence Centre of the Armed Forces/Centro de Inteligencia de las Fuerzas Armadas (CIFAS)</td>
</tr>
<tr>
<td>FI</td>
<td>Finnish Defence Intelligence Agency/Tiedustelulaitos (FDIA)</td>
</tr>
<tr>
<td></td>
<td>The Intelligence Division of the Defence Command (Pääesikunnan tiedusteluosasto/Huvudstabens underrättelseavdelning)</td>
</tr>
<tr>
<td></td>
<td>Finnish Security Intelligence Service/Suojelupoliisi/Skyddspolisen (SUPO) (service belonging to the police)</td>
</tr>
<tr>
<td>FR</td>
<td>Directorate General of External Security/Direction Générale de la Sécurité Extérieure (DGSE)</td>
</tr>
<tr>
<td></td>
<td>Directorate of Military Intelligence/Direction du renseignement militaire (DRM)</td>
</tr>
<tr>
<td></td>
<td>Directorate General of Interior Security/ Direction générale de la sécurité intérieure (DGSI)</td>
</tr>
<tr>
<td></td>
<td>National Directorate of customs intelligence and investigations/Direction nationale du renseignement et des enquêtes douanières (DNRED)</td>
</tr>
<tr>
<td></td>
<td>Service du traitement du renseignement et action contre les circuits financiers clandestins (Tracfin)</td>
</tr>
<tr>
<td>HR</td>
<td>Security Intelligence Agency/Sigurnosna-Obavjestanja Agencija (SOA)</td>
</tr>
<tr>
<td></td>
<td>Military /Vojna Sigurnosna-Obavjestanja Agencija (VSOA)</td>
</tr>
<tr>
<td></td>
<td>Information Office/ Informacjos Hivatal (IH)</td>
</tr>
<tr>
<td>HU</td>
<td>Constitution Protection Office/ Alkotmányvédelmi Hivatal (AH)</td>
</tr>
<tr>
<td></td>
<td>Special Service for National Security/ Nemzetbiztonsági Szakszolgálat (NBSZ)</td>
</tr>
<tr>
<td></td>
<td>Counter Terrorism Centre/ Terrorelhárítási Központ (TEK) (service belonging to the police)</td>
</tr>
<tr>
<td></td>
<td>Information Office / Információs Hivatal (IH)</td>
</tr>
<tr>
<td></td>
<td>Military National Security Service/Katonai Nemzetbiztonsági Szolgála (KNBSZ)</td>
</tr>
<tr>
<td>IE</td>
<td>Defence Forces/Óglaigh na hÉireann Directorate of Intelligence (G2)</td>
</tr>
<tr>
<td>EU MS</td>
<td>Security/Intelligence Service</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>EU</td>
<td>Garda Síochána National Surveillance Unit (NSU) (belonging to the police)</td>
</tr>
<tr>
<td>EU</td>
<td>Police/An Garda Síochána Crime and Security Branch</td>
</tr>
<tr>
<td>IT</td>
<td>Information and Internal Security Agency/ Agenzia informazioni e sicurezza interna (AISI)</td>
</tr>
<tr>
<td>IT</td>
<td>Information and External Security Agency/Agenzia Informazioni e Sicurezza Esterna (AISE)</td>
</tr>
<tr>
<td>IT</td>
<td>Department information and security/Reparto informazioni e sicurezza (RIS)</td>
</tr>
<tr>
<td>LT</td>
<td>State Security Department/ Valstybes Saugumo Departamentas (VSD)</td>
</tr>
<tr>
<td>LT</td>
<td>Second Investigation Department under the Ministry of National Defence/Antrais Departamentas Prie Krasto Apsaugos Ministerijos (AOTD prie KAM)</td>
</tr>
<tr>
<td>LU</td>
<td>State Intelligence Service/Service de Renseignements de l’État (SREL)</td>
</tr>
<tr>
<td>LV</td>
<td>Constitutional Protection Bureau/Satversmes Aizsardzības Birojs (SAB)</td>
</tr>
<tr>
<td>LV</td>
<td>Defence Intelligence and Security Service/ Militārās izlūkošanas un drošības dienests (MIDD)</td>
</tr>
<tr>
<td>LV</td>
<td>Security Police/ Drošības policija</td>
</tr>
<tr>
<td>MT</td>
<td>Security Service / Servizz tas-Sigurtà</td>
</tr>
<tr>
<td>NL</td>
<td>General Intelligence and Security Service/Algemene Inlichtingen- en Veiligheidsdienst (AIVD)</td>
</tr>
<tr>
<td>NL</td>
<td>Military Intelligence and Security Service/Militaire Inlichtingen- en Veiligheidsdienst (MIVD)</td>
</tr>
<tr>
<td>PL</td>
<td>Foreign Intelligence Authority/Agencja Wywiadu (AW)</td>
</tr>
<tr>
<td>PL</td>
<td>Military Counter-intelligence Service/Služba Wywiadu Wojskowego (SWW)</td>
</tr>
<tr>
<td>PL</td>
<td>Internal Security Agency/Agencja Bezpieczeństwa Wewnętrznego (ABW)</td>
</tr>
<tr>
<td>PL</td>
<td>Central Anti-Corruption Bureau/Centralne Biuro Antykorupcyjne (CBA)</td>
</tr>
<tr>
<td>PL</td>
<td>Military Intelligence Service/Ślużba Wywiadu Wojskowego (SWW)</td>
</tr>
<tr>
<td>PT</td>
<td>Strategic Intelligence and Defence Service/Serviço de Informações Estratégicas de Defesa (SIED)</td>
</tr>
<tr>
<td>PT</td>
<td>Service of Security Intelligence/ Serviço de Informações de Segurança (SIS)</td>
</tr>
<tr>
<td>RO</td>
<td>External Intelligence Service/Serviciul de Informatii Externe (SIE)</td>
</tr>
<tr>
<td>RO</td>
<td>Defence General Directorate for Information/Direcția Generală de Informații a Apărării (DGIA)</td>
</tr>
<tr>
<td>RO</td>
<td>Romanian Intelligence Service/ Serviciul Roman de Informatii (SRI)</td>
</tr>
<tr>
<td>EU MS</td>
<td>Security/Intelligence Service</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td></td>
<td>Department for Information and Internal Protection/ <em>Direcția Generală de Informații și Protecție Internă</em> (DGIP)</td>
</tr>
<tr>
<td>SE</td>
<td>National Defence Radio Establishment / <em>Försvarets radioanstalt</em> (FRA)</td>
</tr>
<tr>
<td></td>
<td>Military Intelligence and Security Service / <em>Militära underrättelse- och säkerhetstjänsten</em> (MUST)</td>
</tr>
<tr>
<td></td>
<td>Security Service/ <em>Säkerhetspolisen</em>, (SÄPO)</td>
</tr>
<tr>
<td>SI</td>
<td>Slovene Intelligence and Security Agency/ <em>Slovenska obveščevalno-varnostna agencija</em> (SOVA)</td>
</tr>
<tr>
<td></td>
<td>Intelligence and Security Service of the Ministry of Defence/ Obveščevalno-varnostna služba Ministrstva za obrambo (OVS)</td>
</tr>
<tr>
<td>SK</td>
<td>National Security Authority/ <em>Národný bezpečnostný úrad</em> (NBÚ)</td>
</tr>
<tr>
<td></td>
<td>Slovak Information Service/ <em>Slovenská informačná služba</em> (SIS)</td>
</tr>
<tr>
<td></td>
<td>Military Intelligence/ <em>Vojenské spravodajstvo</em> (VS)</td>
</tr>
</tbody>
</table>
Annex 2

Figure 13 – Oversight and review of surveillance: E CtHR and CJEU case-law main requirements

Source: FRA, 2023