

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

November 2022 Update

Country: Czechia

FRANET contractor: Institute of Sociology of the Czech  
Academy of Sciences

Author(s) name(s): Petr Agha, Tereza Stöckelová

**DISCLAIMER:** This document was commissioned under contract as background material for comparative analysis by the European Union Agency for Fundamental Rights (FRA) for the project '*National intelligence authorities and surveillance in the EU*'. The information and views contained in the document do not necessarily reflect the views or the official position of the FRA. The document is made publicly available for transparency and information purposes only and does not constitute legal advice or legal opinion.

## Table of Contents

1. Summary .....	3
2. Annexes- Table and Figures .....	6
2.1. Overview of security and intelligence services in the EU-27 .....	6
2.2. EU Member States' legal framework on surveillance reformed since 2017 .....	6
Figure 1: EU Member States' legal frameworks on surveillance reformed since October 2015.....	7
2.3. Intelligence services' accountability scheme .....	7
Figure 5: Intelligence services' accountability scheme .....	8
2.4. Parliamentary oversight of intelligence services in EU Member States .....	8
Figure 6: Parliamentary oversight of intelligence services in EU Member States .....	9
2.5. Expert bodies (excluding DPAs) overseeing intelligence services in the EU .....	9
Table 2: Expert bodies (excluding DPAs) overseeing intelligence services in the EU .....	9
2.6. DPAs' powers over national intelligence services, by member states .....	9
Figure 7: DPAs' powers over national intelligence services, by member states .....	10
2.7. DPAs' and expert bodies' powers over intelligence techniques, by EU Member State ...	10
Figure 8: DPAs' and expert bodies' powers over intelligence techniques, by EU Member State .....	11
2.8. Binding authorisation/approval of targeted surveillance measures in the EU.....	11
Table 4: Binding authorisation/approval of targeted surveillance measures in the EU-27.....	11
2.9. Approval/authorisation of general surveillance of communication.....	11
Table 5: Approval/authorisation of general surveillance of communication in France, Germany, the Netherlands and Sweden.....	12
2.10. Non-judicial bodies with remedial powers .....	12
Table 6: Non-judicial bodies with remedial powers in the context of surveillance, by EU Member State.....	12
2.11. Implementing effective remedies.....	12
Figure 9: Implementing effective remedies: challenges and solutions.....	13
2.12. Non-judicial bodies' remedial powers .....	13
Table 7: Non-judicial bodies' remedial powers in case of surveillance, by EU Member State.....	13
2.13. DPAs' remedial competences .....	13
Figure 10: DPAs' remedial competences over intelligence services.....	14

# 1. Summary

FRANET contractors are requested to highlight in 1 page **maximum** the key developments in the area of surveillance by intelligence services in their Member State. This introductory summary should enable the reader to have a snapshot of the evolution during the reporting period (mid-2016 until third quarter of 2022). It should mention:

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

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

### **FRA 2017 Report:**

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

### **FRANET data collection for the FRA 2017 Report:**

Country studies for the project on National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies - Legal update

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

### **FRA 2015 Report:**

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

### **FRANET data collection for the FRA 2015 Report:**

Country studies for the project on National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

The Czech Republic has three intelligence services: the Security Information Service, the Military Intelligence Service and the Office for Foreign Relations and Information. At present a debate is taking place amongst political representatives and experts on introducing new more comprehensive legal regulation of the status and activities of the intelligence services of the Czech Republic, on modernising the already long-standing legal regulations, and on some new roles and functions that should be entrusted to the intelligence services.<sup>1</sup> The most important topics under consideration<sup>2</sup> in the period under review have been: (1) the extension of external oversight of intelligence services and the possible evidentiary admissibility of information originating from intelligence services in judicial proceedings;

<sup>1</sup> See the Explanatory Memorandum to Act No. 325/2017 Coll., amending the Act on the Intelligence Services of the Czech Republic, pp. 1, 2, or the [Programme Statement of the Government of the Czech Republic](#) (approved on 12 February 2014), or the [National Security Audit](#) (approved by Government Resolution No. 1125 on 14 December 2016). Also see Pokorný, L. (2016). 'Current issues of the status and competences of the intelligence services of the Czech Republic.' In: Vegrichtová, B. et al. Security Threats of Today. Prague: PA Czech Republic in Prague.

<sup>2</sup> See the [Programme Statement of the Government of the Czech Republic](#) (approved on 12 February 2014).

(2) the lack of a specific law governing the Office for Foreign Relations and Information, which concerns so-called umbrella legislation on intelligence services.<sup>3</sup>

An Independent Intelligence Review Authority was established<sup>4</sup> at the beginning of 2018 in order to expand the external oversight of the intelligence services. The aim was to increase the credibility of intelligence services by checking the legality of their activities, and, in turn, to reduce political influences and pressures. Oversight will be exercised by a special independent body to be set up by the Chamber of Deputies, whose members must not be MPs. Thus, a 'two-tier' system of intelligence control has been introduced. In addition to the already established special oversight bodies (first level) of the Chamber of Deputies of the Parliament of the Czech Republic, an expert non-executive control body (second level) is established, and it oversees all three existing intelligence services of the Czech Republic. Its task is to carry out, at its own initiative, reviews of the legality of the activities of the intelligence services, including respect for fundamental rights and freedoms. The five members of the independent body are responsible for the independent oversight of the activities of the Security Information Service (civilian counterintelligence), the Office of Foreign Relations and Information (civilian intelligence), and the Military Intelligence Service. However, the Authority can only act at the initiative of one of the Intelligence Review Committees. Candidates are elected by the Chamber of Deputies for a five-year term upon recommendation by the government. Due to the high requirements for its members, its positions have not yet been filled, as members must have, among other things, top secret clearance, have no connection to the intelligence services, and be over the age of 40. The original idea was that the officials would have a legal background and would preferably be former judges with experience authorising intelligence activities. This requirement has proved difficult to meet and the prerequisite of a legal education was therefore removed by the amendment, effective 2022,<sup>5</sup> and the overall procedure for their selection will be simplified.

The 2019 amendment to the Intelligence Services Act<sup>6</sup> mainly responded to the situation where certain interpretative ambiguities had arisen in the application of already existing legislation, which stemmed from the vagueness of the general terms used in the applicable laws. The number of amendments and the change in security risks led to certain interpretative uncertainties with the existing legislation. The Intelligence Services Act has been amended several times since 1994 to reflect developments in technology and society. However, based on experience there was a need to better define the remit of the intelligence services. For example, according to the new wording of the law, the BIS should not provide information on 'activities threatening the state and state secrets' but on 'intentions and activities threatening the protection of classified information'. The new law will also add the requirement that information be obtained on the 'intention' to engage in activities that may threaten the security or significant economic interests of the Czech Republic. Another reason for the amendment was the need to introduce a requirement to authorise the intelligence services to obtain certain data that are supplementary in nature to the data that the intelligence services are already authorised to obtain.<sup>7</sup> The

---

<sup>3</sup> The amendment to the Intelligence Services Act, adopted by Act No. 325/2017 Coll., was intended to adjust the scope and method of oversight by intelligence services and to strengthen the monitoring applied to all three intelligence services of the Czech Republic by making all intelligence services of the Czech Republic subject to parliamentary oversight.

<sup>4</sup> The establishment of the body was stipulated by Act No. 325/2017 Coll., effective from 1 January 2018, which amended Act No. 153/1994 Coll., on the Intelligence Services of the Czech Republic. Later it was amended by Act No. 150/2021 Coll. Act amending Act No. 289/2005 Coll., on Military Intelligence, as amended, and some other acts.

<sup>5</sup> Act No. 150/2021 Coll., amending Act No. 289/2005 Coll. on Military Intelligence, as amended, and some other acts.

<sup>6</sup> Act No. 205/2019 Coll., amending Act No. 153/1994 Coll. on the Intelligence Services of the Czech Republic, as amended; Act No. 154/1994 Coll. on the Security Information Service, as amended; and Act No. 289/2005 Coll. on Military Intelligence, as amended.

<sup>7</sup> Explanatory memorandum to the Act No. 205/2019 Coll. Act amending Act No. 153/1994 Coll., on the Intelligence Services of the Czech Republic, as amended, Act No. 154/1994 Coll., on the Security Information Service, as amended, and Act No. 289/2005 Coll., on Military Intelligence, as amended.

lack of a specific law governing the Office for Foreign Relations and Information was not addressed this time.

The existence of new phenomena emerging in the area of security threats was reflected in an amendment to the 2021 Military Intelligence Amendment Bill dealing with cyber defence.<sup>8</sup> The National Cyber Operations Centre is responsible for defending the state against hackers. The law defines three areas of activity. The first is the detection of all cyber attacks originating abroad. The second activity is the analysis of all such attacks, threats, and impacts. And the third area of activity involves all measures taken to counter detected cyber attacks. The detection and assessment of cyber attacks has not been the responsibility of any government agency yet. If Military Intelligence detects a specific threat of a cyber attack, it will pass the detected information on to the relevant administrative authority, or to a specific legal entity, or it will take action itself. However, the latter option is conceived as an exception and is subject to strict conditions. First of all, the threat to important national interests must be of a significant scale and the attack must be ongoing or imminent. Intervention is possible only with the approval of the Minister of Defence.<sup>9</sup>

The law is based on the requirements of the strategy developed by the National Cyber and Information Security Bureau (NCISB) and approved by the Government. It reflects the requirements stemming from membership in the North Atlantic Treaty Organization (NATO), which recognised cyberspace as an operational domain in 2016. It also provides for the creation of a Cyber Defence Inspector. The Cyber Defence Inspector is a member of the Military Intelligence Service but reports directly to the Minister of Defence. The nomination is discussed in the Defence and Security Committees and then submitted to the Government. Upon appointment, the Cyber Defence Inspector formally becomes a member of the Military Intelligence Service, reporting directly to the Minister of Defence. The main tasks of the Inspector include reviewing the correctness of procedures and activities related to the handling of data and information obtained in the framework of ensuring national defence in cyberspace. The Inspector is also tasked to cooperate with operators and service providers, where the Military Intelligence Department places so-called detection tools, and to handle any complaints from them.

The Office for Personal Data Protection (Úřad pro ochranu osobních údajů - ÚOOÚ)<sup>10</sup> was transformed into the Data Protection Authority in 2019.<sup>11</sup> It is part of the executive branch and operates in conformity with administrative law, primarily by issuing authoritative administrative acts.<sup>12,13</sup> Administrative, internal, and state oversight are the three forms of oversight exercised]. ÚOOÚ most often carries out inspections on the basis of a suggestion or complaint received (sometimes also on the basis of information from the media).<sup>14</sup> It also draws up an inspection plan each year that focuses on specific areas. The competence of the ÚOOÚ excludes the supervision of intelligence services, which was the practice under previous regulations. This exemption is due to the special nature of the intelligence services, which operate on the principle of secrecy.<sup>15</sup>

---

<sup>8</sup> Act No. 150/2021 Coll., amending Act No. 289/2005 Coll. on Military Intelligence, as amended.

<sup>9</sup> Parliament of the Czech Republic (2020) [Sněmovní tisk 800/0 – Novela z. o Vojenském zpravodajství](#) (Parliamentary paper 800/0 – Amendment of the Act on Military Intelligence).

<sup>10</sup> Established by Act No. 101/2000 Coll. on the Protection of Personal Data and on Amendments to Certain Acts.

<sup>11</sup> Transformed by Act No. 110/2019 Coll. on the Processing of Personal Data (ZZOÚ).

<sup>12</sup> This is governed by Act No. 255/2012 Coll. on Control (Control Regulations).

<sup>13</sup> The tasks can be summarised in the following groups: a) monitoring the application of the GDPR in practice; b) awareness-raising and advisory activities; c) oversight in a narrower sense (mainly monitoring and assigning corrective measures and sanctions); d) international cooperation; e) tasks related to specific institutes or processes; and f) other tasks.

<sup>14</sup> Areas concerned include: the processing of personal data via recordings from cameras on unmanned aircraft; the publication of personal data in the media; the use of electronic cards; the processing of personal data by e-shops; personal data processing in the context of the clinical testing of drugs and other medical substances; and the publication of personal data on the internet.

<sup>15</sup> Act No. 110/2019 Coll. on the Processing of Personal Data, § 54 para 4.

## 2. Annexes- Table and Figures

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

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

The table is accurate.

	<b>Civil (internal)</b>	<b>Civil (external)</b>	<b>Civil (internal and external)</b>	<b>Military</b>
<b>CZ</b>	Security Information Service / <i>Bezpečnostní informační služba</i> (BIS)	Office for Foreign Relations and Information / <i>Úřad pro zahraniční styky a informace</i> (ÚZSI)		Military Intelligence / <i>Vojenské zpravodajství</i> (VZ)

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

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

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

Act No. 325/2017 Coll., amending the Act on Intelligence Services of the Czech Republic

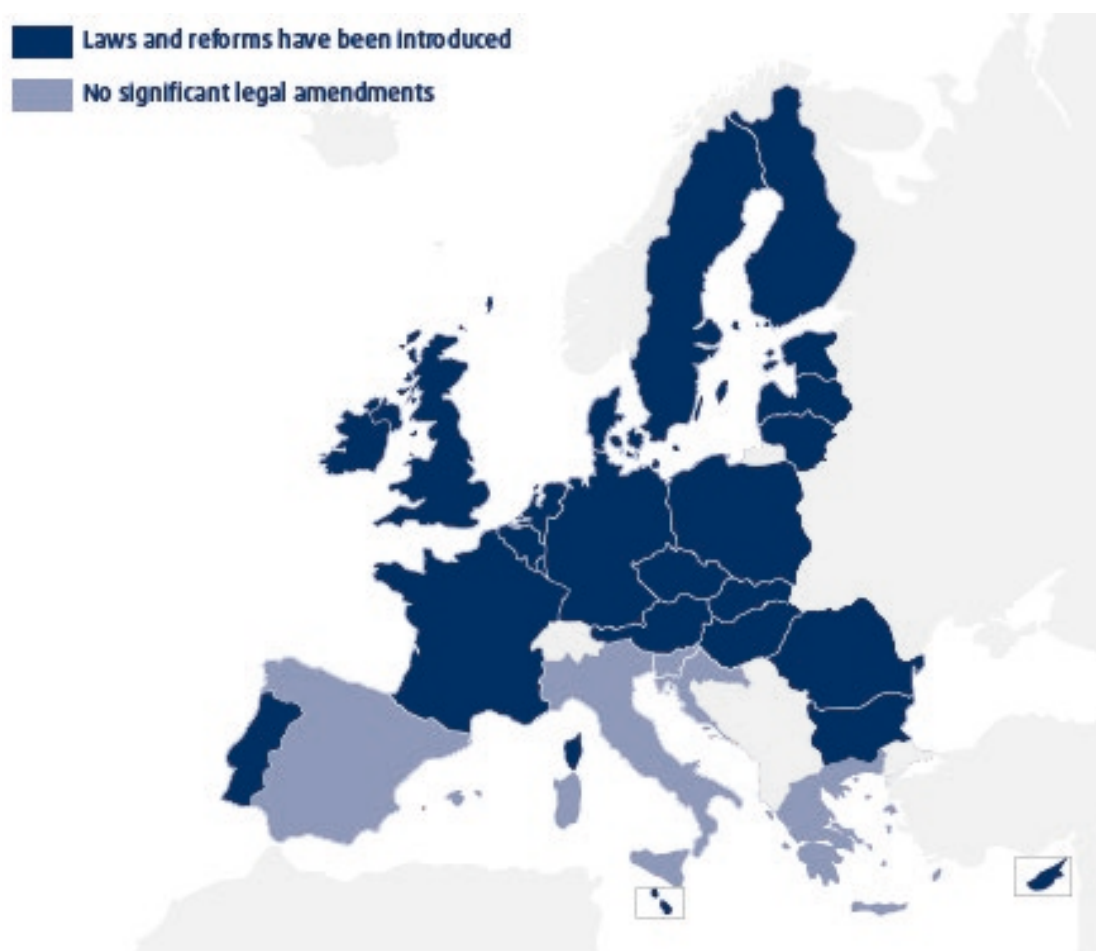
Act No. 150/2021 Coll., amending Act No. 289/2005 Coll. on Military Intelligence, as amended

Act No. 205/2019 Coll., amending Act No. 153/1994 Coll. on the Intelligence Services of the Czech Republic, as amended

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

No, it wasn't.

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

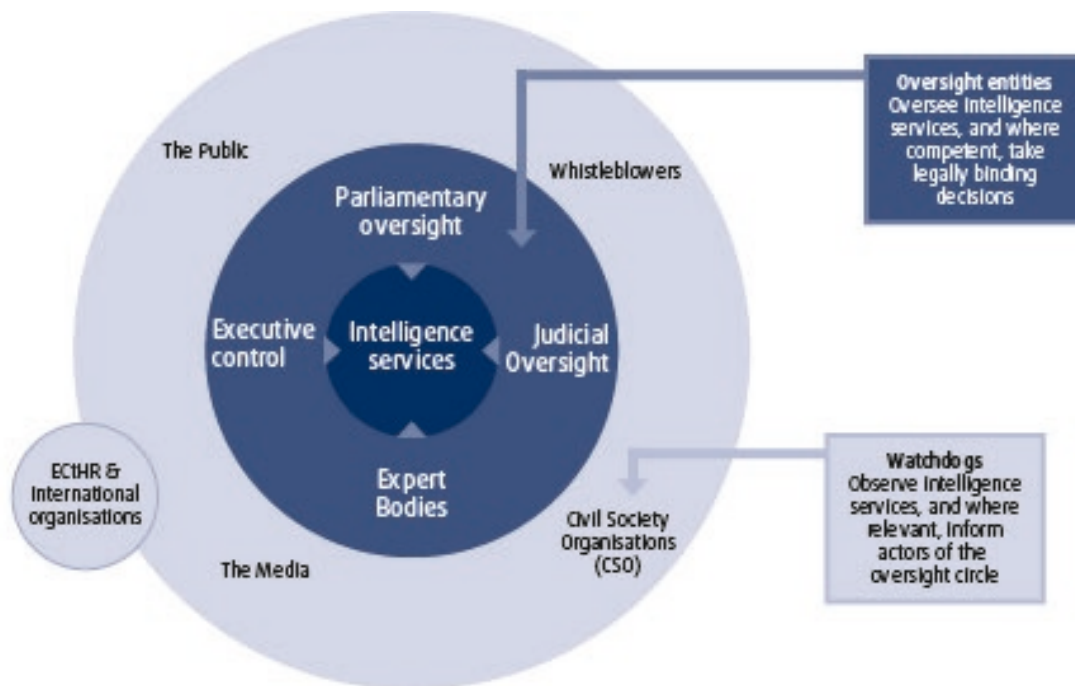


### **2.3. Intelligence services' accountability scheme**

*FRANET contractors are requested to confirm whether the diagram below (Figure 5 (p. 65) of the FRA 2017 report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.*

The following diagram is accurate

**Figure 5: Intelligence services' accountability scheme**



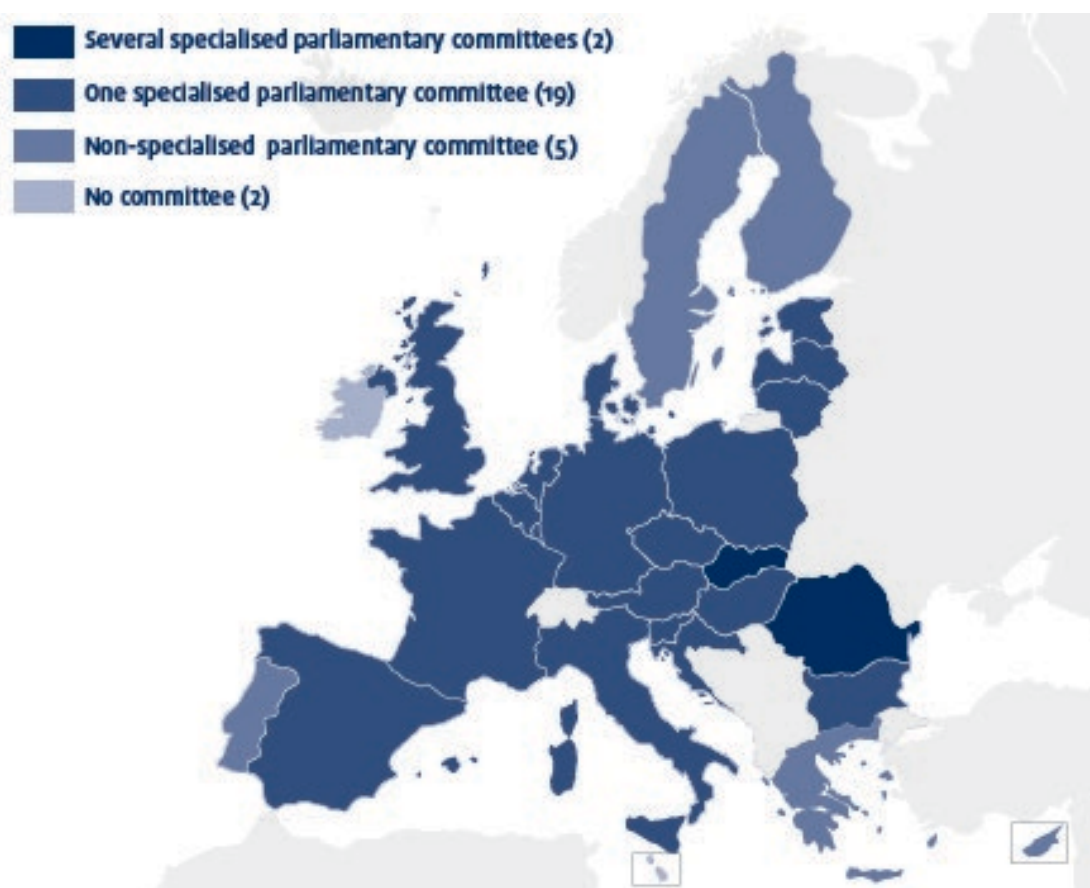
#### **2.4. Parliamentary oversight of intelligence services in EU Member States**

*FRANET contractors are requested to confirm that the map below (Figure 6 (p. 66) of the FRA 2017 report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.*

The following map accurately illustrates the situation in Czechia.



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



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

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

The Czech Republic has a special oversight body of the Chamber of Deputies of the Parliament of the Czech Republic. The table is accurate.

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

EU Member State	Expert Bodies
CZ	Independent Control Body of the Intelligence Services (Orgán nezávislé kontroly zpravodajských služeb České republiky)

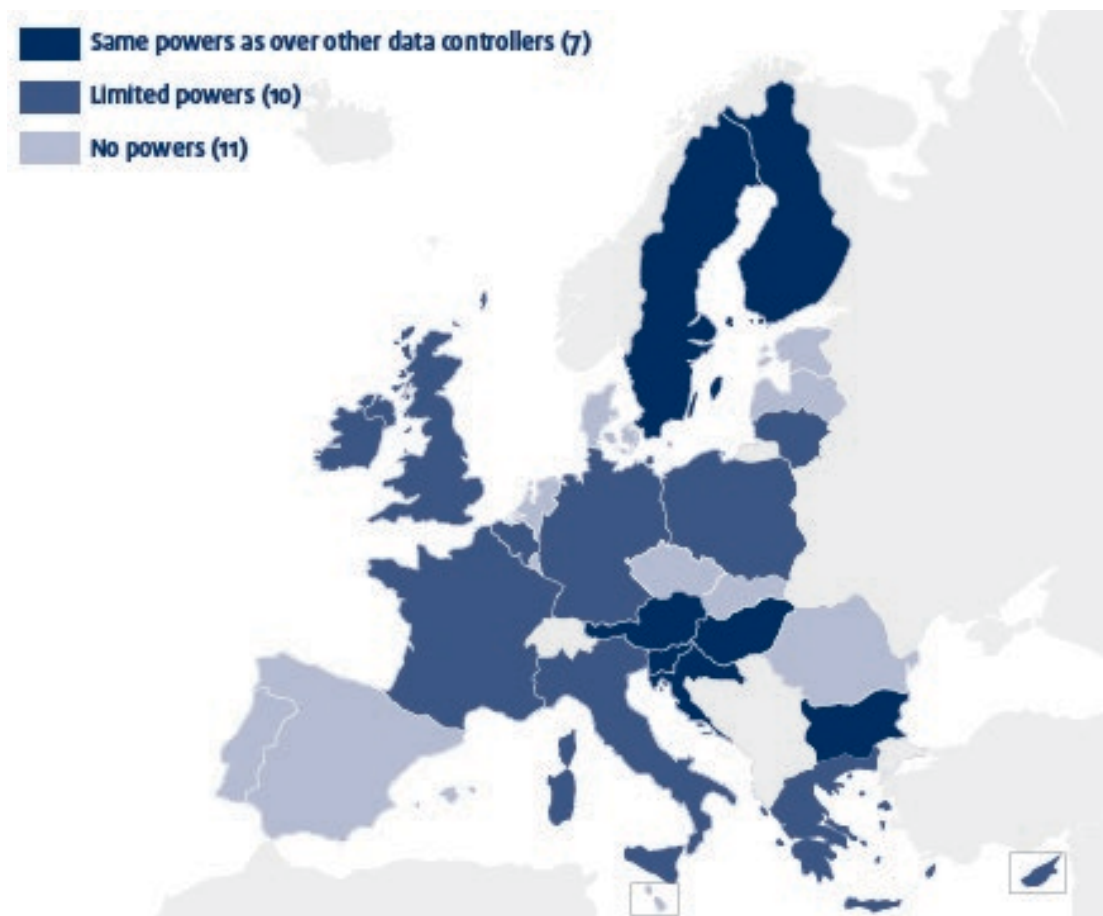
## 2.6. DPAs' powers over national intelligence services, by member states

*FRANET contractors are requested to confirm that the map below (Figure 7 (p. 81) of the FRA 2017 report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.*

The Data Protection Authority has no direct powers over the intelligence services as explained in the summary above – therefore, there has been no change. Control[Oversight] is exercised by the Independent Control Body of the Intelligence Services of the Czech Republic.

The activities of the Independent Control Body of the Intelligence Services of the Czech Republic relate to monitoring the legality of the activities of the intelligence services within their field of competence on the territory of the Czech Republic, which includes monitoring compliance with fundamental rights and freedoms. The Authority carries out its monitoring activities at the request of one of the special control bodies, these bodies being the Parliamentary Standing Committees for the Control of the Activities of Individual Intelligence Services. Monitoring of the activities of an intelligence service by the Independent Control Body is always conducted with the knowledge of the director of the relevant intelligence service.

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

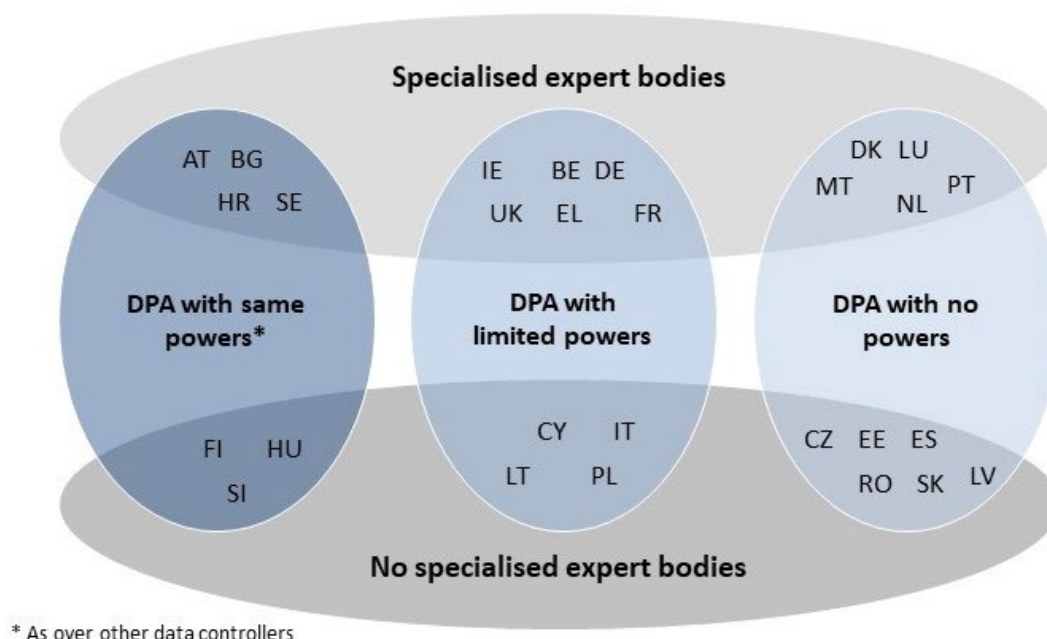


## **2.7. DPAs' and expert bodies' powers over intelligence techniques, by EU Member State**

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

CZ should now be moved to the top of the right egg (DPA with no powers) and with specialised expert bodies).

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



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

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

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

	Judicial	Executive	Expert bodies	Services
CZ	✓			

Judicial oversight focuses mainly on the use of intelligence technology (warrants to use intelligence technology are issued by the Chairman of the Panel of Judges of the respective High Court - depending on where the official address of the Security Information Service is located). The judge is entitled to request information from the BIS in order to assess whether the reasons for the requested use of intelligence technology are still relevant.

## 2.9. Approval/authorisation of general surveillance of communication

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

*your Member State regulates these type of surveillance methods (for a definition of general surveillance, see FRA 2017 Report, p. 19).*

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

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

Czech legislation does not regulate in detail the general surveillance of communications.

## 2.10. Non-judicial bodies with remedial powers

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

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

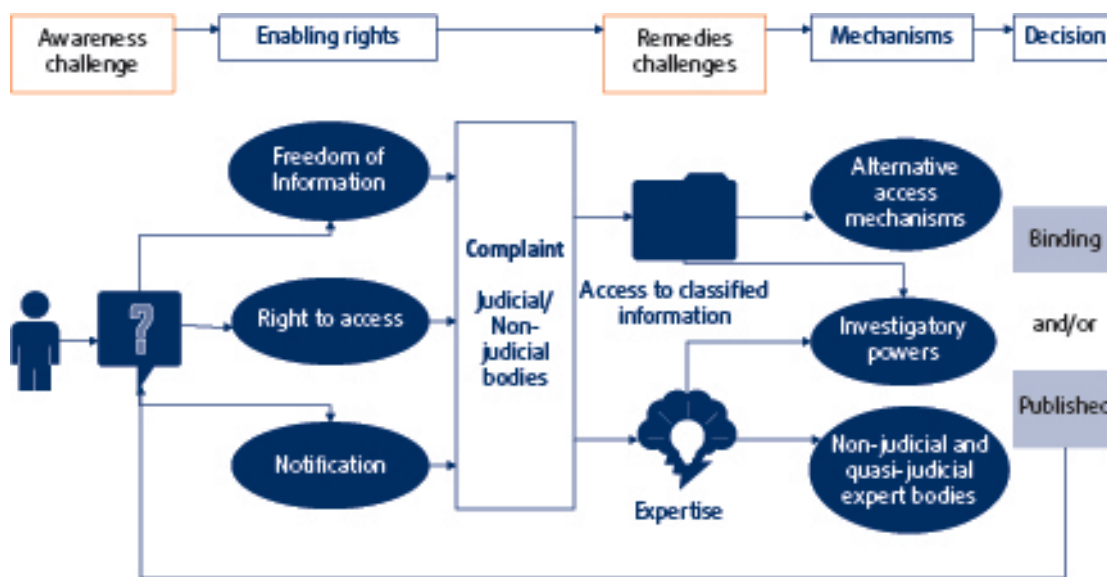
	Executive (ministry)	Expert body(ies)	DPA	Parliamentary committee(s)	Ombuds institution
CZ					

## 2.11. Implementing effective remedies

*FRANET contractors are requested to confirm that the diagram below (Figure 9 (p. 114) of the FRA 2017 report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.*

The following figure accurately illustrates the situation in the Czechia.

**Figure 9: Implementing effective remedies: challenges and solutions**



## 2.12. Non-judicial bodies' remedial powers

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

The figure accurately illustrates the situation in the Czech Republic. Individuals cannot access non-judicial bodies to lodge a complaint against the activities of the intelligence services.

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

## 2.13. DPAs' remedial competences

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

DPA in the Czech Republic has no direct remedial powers or authority over the intelligence services; however, the Independent Control Body of the Intelligence Services of the Czech Republic is tasked with monitoring the legality of their activities.

The figure below accurately reflects the situation in the Czech Republic.

The activities of the Independent Control Body of the Intelligence Services of the Czech Republic relate to the control of [relate to monitoring] the legality of the activities of the intelligence services within their field of competence on the territory of the Czech Republic, which includes monitoring compliance with fundamental rights and freedoms. The Authority carries out its monitoring activities on the basis of an initiative of one of the special control bodies, these bodies being the Parliamentary Standing Committees for the Control of the Activities of Individual Intelligence Services. The monitoring of the activities of an intelligence service by the Independent Control Body is always conducted with the knowledge of the director of the relevant intelligence service.

**Figure 10: DPAs' remedial competences over intelligence services**

