EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

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

November 2022 Update

Country: Portugal

FRANET contractor: Centre for Social Studies

Author(s) name(s): Diana Barros, João Paulo Dias

Table of Contents

1. Summary

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

the most significant legislative reform/s that took place or are taking place and highlight the key aspect/s of the reform, focusing on oversight and remedies.

relevant oversight bodies' (expert bodies (including non-judicial bodies, where relevant), data protection authorities, parliamentary commissions) reports/statements about the national legal framework in the area of surveillance by intelligence services.

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

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

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

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

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

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

As a preliminary remark, it should be noted that, in Portugal, the Intelligence System of the Portuguese Republic (*Sistema de Informações da República Portuguesa*) (SIRP), is a public body, that reports directly to the Prime Minister, and responsible for providing support to the political decision-maker by anticipating and assessing the different threats to Portugal and its interests regarding internal and external security, independence, and the integrity of the State's unity[1].Moreover, is within the structure of SIRP that the surveillance services are integrated[2]. The Security Intelligence Service (*Serviço de Informações de Segurança*) (SIS), safeguards internal security by preventing sabotage, terrorism, espionage, organised crime, proliferation and cyber threats and the Strategic Defence Intelligence Service (*Serviço de Informações Estratégicas de Defesa*) (SIED), a service that operates without geographical limitation, is responsible for producing strategic defence intelligence to safeguard national independence, national interests and external security of the Portuguese State, by anticipating situations of political, social and economic instability or transnational threats that may affect Portugal's external interests and the security of Portuguese

[1] For more information, see the website of the Intelligence System of the Portuguese Republic.
[2] Portugal, Lei 30/84, que estabelece a Lei-Quadro do Sistema de Informações da República Portuguesa (Law 30/84, which establishes the Portuguese Republic Intelligence System Framework Law), 5 September 1984.

communities. Within this context, it is important to note that, although SIS and SIED work together and share information, these services have distinct competences and organizational autonomy.

In matters of surveillance, **between mid-2016 and the third quarter of 2022**, there have been some legal changes. However, only a few changes aren't mainly related with the oversight of the surveillance services or with the right to information for persons subjected to surveillance services. According to the **Portuguese Republic Intelligence System Framework Law**[3] and **Law 50/2014**[4], the responsibility of intelligence services is to ensure the production of the necessary information for the preservation of internal and external security, as well as national independence and interests and the unity and integrity of the State. This means that they cannot execute criminal investigations, which, in turn, means that they cannot carry out target surveillance measures, since the **Portuguese Constitution**[5] only allows these to be carried out in the context of a criminal investigation. Therefore, we have selected the most relevant chances in order to show how intelligence services do relate with other entities and collect data. Some changes were also made regarding the nomination of members of the surveillance services.

Within the context of the **National Anti-Terrorism Strategy**[6], it was established the regime applicable to the organisation and functioning of the Anti-Terrorism Coordination Unit (Unidade de Coordenação Antiterrorismo)[7]. This Unit is a body created for the coordination and sharing of information, in the context of the threat and fight against terrorism. This Unit is composed, among others, by the Secretary-General of the Internal Security System, the Secretary-General of SIRP, the Director of SIED and the Director of SIS and operates within the Internal Security System, under the control and coordination of the Secretary-General of the Internal Security System.

Organic Law 4/2017[8] approved special procedures for access to telecommunications and internet data (also known as metadata), previously stored by electronic communications services providers, by intelligence officers of SIS and SEID. However, basic data and equipment location data can only be accessed for the purpose of producing information necessary to safeguarding national defence, internal security and to prevent acts of sabotage, espionage, terrorism, proliferation of weapons of mass destruction and highly organised crime and within its exclusive scope (Article 3). while, traffic data can only be accessed for the purposes of producing the necessary information to prevent acts of

[3] Portugal, Lei 30/84, que estabelece a Lei-Quadro do Sistema de Informações da República Portuguesa (Law 30/84, which establishes the Framework Law of the Portuguese Republic Intelligence System), 5 September 1984.

[4] Portugal, Lei 50/2014, que procede à primeira alteração à Lei n.º 9/2007, de 19 de fevereiro, que estabelece a orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa (SIED) e do Serviço de Informações de Segurança (SIS) e revoga os Decretos-Leis n.os 225/85, de 4 de julho e 254/95, de 30 de setembro (Law 50/2014, which makes the first amendment to Law no. 9/2007, of 19 February, establishing the organic structure of the Secretary-General of the Intelligence System of the Portuguese Republic, the Strategic Defence Intelligence Service (SIED) and the Security Intelligence Service (SIS) and revoking Decree-Laws no. 225/85, of 4 July and 254/95, of 30 September), 13 August 2014.

[5] Portugal, Constituição da República Portuguesa (Constitution of the Portuguese Republic), 10 April 1976.

[6] Portugal, Resolução do Conselho de Ministros 7-A/2015, que aprova a Estratégia Nacional de Combate ao Terrorismo (Resolution of the Council of Ministers 7-A/2015, which approves the National Counter-Terrorism Strategy), 8 August 2015.

[7] Portugal, Decreto Regulamentar 2/2016, que estabelece o regime aplicável à organização e funcionamento da Unidade de Coordenação Antiterrorismo (Regulatory Decree 2/2016, which establishes the regime applicable to the organisation and functioning of the Anti-Terrorism Coordination Unit), 23 August 2016.

[8] Portugal, Lei Orgânica 4/2017, que aprova e regula o procedimento especial de acesso a dados de telecomunicações e Internet pelos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa e procede à segunda alteração à Lei 62/2013, de 26 de agosto (Lei da Organização do Sistema Judiciário) (Organic Law 4/2017, that approves and regulates the special procedure for access to telecommunications and Internet data by intelligence officers of the Security Intelligence Service and the Defence Strategic Intelligence Service and makes the second amendment to Law 62/2013 of 26 August [Law on the Organisation of the Judiciary System]), 25 August 2017.

espionage and terrorism (Article 4). Furthermore, this law also established that access to metadata has to be subject to prior mandatory judicial authorisation (by a criminal section of the Supreme Court of Justice - *Supremo Tribunal de Justiça*)[9]/[10] and communicated to the Attorney General. Moreover, the Court can only access to this data when there is reason to believe that it is necessary, appropriate and proportionate to obtain information about a particular target or intermediary; or to obtain information that would be very difficult or impossible to obtain in any other way or in good time to respond to a situation of urgency. The decision is always communicated to the Attorney General, including decisions to cancel access and destroy data, for the purposes of exercising its legal powers of acting as a safeguard. These limitations mean that both the Court and the Attorney General act as a safeguard to the constitutional rights, freedoms and guarantees of the persons to whom the data belong. The Court has to make a decision based on the principles of necessity, adequacy, relevance and proportionality, while the Attorney General safeguards rights, freedoms and guarantees regarding cancelation of access and data destruction.

Real-time interconnection with the databases of telecommunications and internet operators for direct online access to the data requested is prohibited. This means that the surveillance services cannot conduct target surveillance measures, since this is an exclusive competence of criminal police authorities[11]. Therefore, SIS and SIED officers, according to this law can only access previously stored metadata for the purpose of producing information to pursue their competences. In terms of oversight, this law also established the Data Oversight Commission of the Information System of the Portuguese Republic (*Comissão de Fiscalização de Dados do Sistema de Informações da República Portuguesa*) is the competent authority overseeing compliance with the rules on the quality, confidentiality and security of the data obtained, whereby the Council for the Oversight of the Intelligence System of the Portuguese Republic (*Conselho de Fiscalização do Sistema de Informações da República Portuguesa*) also oversees the access procedures and the telecommunications and internet data obtained. This means that the oversight competences of these two authorities were extended to metadata.

In view of this law, in 2018, the Governmentdefined the technical and security conditions of electronic communication for the purpose of transmission of telecommunications and internet data by intelligence officers of SIS and SEID[12]. Thus it is established that all procedural steps shall be carried out via an internet-based computer service, specifically made available for this purpose, within the System for Access or Request of Data to Electronic Communication Service Providers (*Sistema de Acesso ou Pedido de Dados aos Prestadores de Serviços de Comunicações Eletrónicas*) (SAPDOC). This system is developed and managed by the Institute of Financial Management and Justice Equipment (*Instituto de Gestão Financeira e Equipamentos da Justiça*), of the Ministry of Justice (*Ministério da Justiça*), which shall also be responsible for managing the system and the respective access accreditation.

---

[9] This law amended Law 62/2013, that approved the Law on the Organisation of the Judiciary System, by establishing that there is a section at the Supreme Court of Justice, which supervises and gives prior authorisation for obtaining telecommunications and internet data within the framework of the activity of producing intelligence on espionage and terrorism of the Security Intelligence Service and the Defence Strategic Intelligence Service.

[10] Portugal, Lei 62/2013, que aprova a Lei da Organização do Sistema Judiciário (Law 62/2013, which approves the Law on the Organisation of the Judiciary System), 26 August 2013.

[11] Portugal, Lei 30/84, que estabelece a Lei-Quadro do Sistema de Informações da República Portuguesa (Law 30/84, which establishes the Framework Law of the Portuguese Republic Intelligence System), 5 September 1984.

[12] Portugal, Portaria 237-A/2018, que define as condições técnicas e de segurança da comunicação eletrónica para efeito de transmissão diferida dos dados de telecomunicações e Internet pelos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa (Order 237-A/2018, defining the technical and security conditions of electronic communication for the purpose of deferred transmission of telecommunications and internet data by the intelligence officers of the Security Intelligence Service and the Defence Strategic Intelligence Service), 28 August 2018.

It should be noted that, **Organic Law 4/2017**[13] was the subject of considerable discussion, especially after its approval. On January 2018, only a few months after the approval, 35 members of the Parliament (MPs) - members of 3 political parties - announced that they would request the Constitutional Court to conduct a review of the constitutionality of Articles 3 and 4, since, in their view, both articles violated Article 34(4) of the Portuguese Constitution[14], which expressly states that any interference by public authorities in correspondence, telecommunications and other means of communication is prohibited, except in cases provided for by law in relation to criminal proceedings[15].

Even before the Constitutional Court issued a decision, and in view of the approval of the technical and security conditions for the transmission of metadata by intelligence officers of SIS and SEID[16], an official of one of the 3 political parties that had requested the intervention of the Constitutional Court, criticised this approval, arguing that the Constitutional Court could invalidate not only this regulation as well the organic law that originated it. However, this official recognised that the organic law in question showed a concern to defend the law, by establishing control mechanisms, but simultaneously pointed out that the Constitution was very clear in relation to limiting the access to metadata in the context of criminal investigation, and that allowing access to intelligence services would be a violation, since intelligence services do not intervene in criminal investigations[17].

In May 2019, the Council for the Oversight of the Intelligence System of the Portuguese Republic, issued a report[18] which, among other issues, highlighted the importance of the intelligence services having access to metadata. The report also noted the positive design, construction and application of the system, as well as its unquestionable and unequivocal need (with no available substitute), which enabled Portugal to remedy a serious gap. However, at the same time, the report also considered that "specific clarifications and improvements" could be made to the system, namely: in the distinction between access to basic data and equipment location data, on the one hand, and access to traffic data, on the other; in the object of the data to be made available by the operators; in the obligation of data storage by the operators; in the communication of the information collected for the purposes of criminal proceedings; and in the relationship with foreign intelligence services having as its object the same type of telecommunications and internet data.

---

[13] Portugal, Lei Orgânica 4/2017, que aprova e regula o procedimento especial de acesso a dados de telecomunicações e Internet pelos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa e procede à segunda alteração à Lei 62/2013, de 26 de agosto (Lei da Organização do Sistema Judiciário) (Organic Law 4/2017, that approves and regulates the special procedure for access to telecommunications and Internet data by intelligence officers of the Security Intelligence Service and the Defence Strategic Intelligence Service and makes the second amendment to Law 62/2013 of 26 August [Law on the Organisation of the Judiciary System]), 25 August 2017.

[14] Portugal, Constituição da República Portuguesa (Constitution of the Portuguese Republic), 10 April 1976.

[15] Renascença (2018), "PCP, Bloco e PEV pedem inconstitucionalidade de acesso aos metadados" (PCP, Bloco and PEV call for unconstitutionality of access to metadata), 11 January 2018.

[16] Portugal, Portaria 237-A/2018, que define as condições técnicas e de segurança da comunicação eletrónica para efeito de transmissão diferida dos dados de telecomunicações e Internet pelos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa (Order 237-A/2018, defining the technical and security conditions of electronic communication for the purpose of deferred transmission of telecommunications and internet data by the intelligence officers of the Security Intelligence Service and the Defence Strategic Intelligence Service), 28 August 2018.

[17] Diário de Notícias (2018), "Metadados: "Seria sensato não ter aprovado ainda o regulamento", diz PCP" (Metadata: "It would be wise not to have approved the regulation yet", says PCP), 4 September 2018.

[18] Council for the Oversight of the Intelligence System of the Portuguese Republic (2019), *Parecer Anual de 2018 do Conselho de Fiscalização do Sistema de Informações da República Portuguesa* (2018 Annual Opinion of the Oversight Board of the Intelligence System of the Portuguese Republic), Lisbon, Council for the Oversight of the Intelligence System of the Portuguese Republic.

In October 2019, the Constitutional Court, in Judgement 464/2019[19], declared Article 3 unconstitutional, with mandatory general force, in the part that allowed access by intelligence officers regarding basic data and equipment location data, when this data wasn't regarding a concrete communication (for example, having access to the location of all cell phones in a city), for the purpose of producing information necessary to safeguarding national defence and internal security, as it was in violation of Articles 26 (right to private life) and 35 (right to data) of the Portuguese Constitution[20]. It also declared the unconstitutionality, with general binding force, of Article 4, for being in violation of the provisions of Article 34 (4), of the Portuguese Constitution, with regard to access to traffic data involving intersubjective communication - communications involving a finite number of interlocutors, usually determined by the sender of the communication, via email or other type of message (for instance, whatsapp, skype, etc.), and for violation of the provisions of Articles 26 and 35 of the Portuguese Constitution[21], in conjunction with Article 18(2) (principle of proportionality) of the same law, with regard to access to traffic data not involving intersubjective communication. In other words, the Constitutional Court understood that there were insufficient guarantees that interference in citizens' privacy was limited to the minimum necessary and was proportionate. However, the ruling also admitted that exceptions could be made, for instance in suspected cases of serious crimes like terrorism or espionage.

In view of this outcome, it was expected that this law would be amended or even revoked and a new draft law presented to comply with the decision of the Constitutional Court. However, no amendment or new draft has been presented to date. According to media reports[22], in February of 2022, a Socialist Party MP noted that this is a problem that remains to be solved, since due to the pandemic it wasn't possible to discuss the issue properly, and added that this issue could be taken up again after the summer of 2022. However, there is no sign that such discussions are taking place. Meanwhile, because Articles 3 and 4 were declared unconstitutional, SIS and SIED officers don't have access to metadata previously stored by electronic communications services providers.

Furthermore, as regards to data held by electronic communications service providers, it should also be noted that although the **Metadata Law**[23] allows access to private data by criminal police authorities, excluding intelligence services, these can indirectly have access to this data. This happens due to the fact that the **Organisation of the Intelligence Services Act**[24] establishes that criminal police authorities can share collected data with the SIRP and SIS and SIED services, when the data is considered to be relevant. In August 2019, the Ombudsman requested the Constitutional Court to provide a ruling on the constitutionality of Articles 4 (list of data to be retained), 6 (obligation to retain traffic and location data of all electronic communications for one year) and 9 (data

[19] Portugal, Decisão do Tribunal Constitucional – Acórdão 464/2019 (Decision of the Constitucional Court – Judgement 464/2019), 21 October 2019.
[20] Portugal, Constituição da República Portuguesa (Constitution of the Portuguese Republic), 10 April 1976.
[21] Portugal, Constituição da República Portuguesa (Constitution of the Portuguese Republic), 10 April 1976.
[22] Expresso (2022), "PS volta a colocar como possibilidade acesso das secretas a metadados" (PS again poses possibility of access to metadata by secret services), 15 February 2022.
[23] Portugal, Lei 32/2008, que transpõe para a ordem jurídica interna a Directiva 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações (Law 32/2008, which transposes into national law Directive 2006/24/EC, of the European Parliament and of the Council, of 15 March, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks), 17 July 2008.
[24] Portugal, Lei 9/2007, que estabelece a orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa e do Serviço de Informações de Segurança e revoga os Decretos-Leis 225/85, de 4 de Julho, e 254/95, de 30 de Setembro (Law 9/2007, which establishes the organic law of the Secretary-General of the Portuguese Republic's Intelligence System, the Defence Strategic Intelligence Service and the Security Intelligence Service, and revokes Decree-Laws 225/85, of 4 July and 254/95, of 30 September), 19 February 2007.

transmission) of the **Metadata Law**[25]. The Constitutional Court issued a ruling[26] on 19 April 2022, declaring these articles unconstitutional as they violated the right to inviolability of communications (Articles 34 of the Portuguese Constitution[27]). In this ruling, the Court considered that by keeping all the location and traffic data of all subscribers, the electronic communications of nearly the entire population were covered, without any differentiation, which, in turn, means that the data collected in the context of this law could also be extended to communications between people who are not connected to any criminal proceedings. Therefore, the Court considered that this law was a disproportionate restriction to the right to inviolability of communication, by determining the generalized conservation of traffic data generated by communications between persons (or its attempt), even within the scope of matters relating to criminal proceedings. Still regarding data protection, **Law 58/2019**[28], which ensured the implementation of the General Data Protection Regulation into national law, also established that the rules foreseen in this law exempted the processing of personal data by the SIRP. This also meant that National Commission for Data Protection (*Comissão Nacional de Proteção de Dados*) does not have power over SIRP. As mentioned before, the Data Oversight Commission of the Information System of the Portuguese Republic is the competent authority to oversee the respect and compliance with the rules concerning the quality and safeguarding of confidentiality and security of the data obtained by any service of SIRP, whereby the Council for the Oversight of the Intelligence System of the Portuguese Republic also oversees the access procedures and the telecommunications and internet data obtained.

Law 83/2017[29], which established measures to combat money laundering and terrorist financing, established that entities with operational competences in the field of preventing and combating money laundering and terrorist financing (which includes SIRP, SIS and SIED)should cooperate with each other and exchange all essential or relevant information in this field, on their own initiative or whenever so requested in a reasonable manner, even where such information is subject to a duty of secrecy imposed by law, regulation or contract. In terms of oversight, it was also establishes that the Committee for the Coordination of Policies for Prevention and Combating Money Laundering and Terrorist Financing (*Comissão de Coordenação das Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo*) promoted the signing of cooperation protocols between entities with operational competences to prevent and combat money laundering and terrorist financing, in which, at least, the type of information to be spontaneously shared between the

[25] Portugal, Lei 32/2008, que transpõe para a ordem jurídica interna a Directiva 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações (Law 32/2008, which transposes into national law Directive 2006/24/EC, of the European Parliament and of the Council, of 15 March, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks), 17 July 2008.

[26] Portugal, Decisão do Tribunal Constitucional – Acórdão 268/2022 (Decision of the Constitucional Court – Judgement 268/2022), 19 April 2022.

[27] Portugal, Constituição da República Portuguesa (Constitution of the Portuguese Republic), 10 April 1976.

[28] Portugal, Lei 58/2019, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Law 58/2019, ensuring the implementation in national law of Regulation (EU) 2016/679 of the Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), 8 August 2019.

[29] Portugal, Lei 83/2017, que estabelece medidas de combate ao branqueamento de capitais e ao financiamento do terrorismo, transpõe parcialmente as Diretivas 2015/849/UE, do Parlamento Europeu e do Conselho, de 20 de maio de 2015, e 2016/2258/UE, do Conselho, de 6 de dezembro de 2016, altera o Código Penal e o Código da Propriedade Industrial e revoga a Lei n.º 25/2008, de 5 de junho, e o Decreto-Lei n.º 125/2008, de 21 de julho (Law 83/2017, which establishes measures to combat money laundering and terrorist financing, and partially transposes Directives 2015/849/EU, of the European Parliament and of the Council, of 20 May 2015, and 2016/2258/EU, of the Council, of 6 December 2016, amending the Criminal Code and the Industrial Property Code and revoking Law 25/2008, of 5 June, and Decree-Law 125/2008, of 21 July), 18 August 2017.

entities, the terms under which such information is provided, the protection mechanisms for information deemed sensitive and the designation of the persons within each of the entities responsible for the communications would be foreseen.

Resolution of the Council of Ministers 188/2017[30], adopted the regulations for the Defence Strategic Intelligence Service Data Centre (*Centro de Dados do Serviço de Informações Estratégicas de Defesa*) and for the Security Intelligence Service Data Centre (*Centro de Dados do Serviço de Informações de Segurança*). Thus, this regulation establishes, within the scope of SIRP, the operating rules, criteria, technical standards, measures and procedures aimed at ensuring the security of the information processed in the data centres of SIS and SIED, in accordance with applicable national and international security standards, as well as with the guidelines set by its own bodies at political level. Therefore, this regulation defines the data centres as the set of data and information collected within the scope of the activities of SIED and SIS, concerning their legally established institutional tasks, processed and kept in digital files or other type of files. However, it should be referred that each data centres operates autonomously and there can be no connection of any kind between them.

Regarding the collection of personal data for automated processing, this law also establishes that this collection is limited to what is necessary to produce information that may contribute to the performance of the institutional tasks of SIED and SIS. Such data shall be adequate, pertinent and not excessive in relation to the purpose for which they were collected, as well as accurate and up-to-date, and shall be kept only for the period of time strictly necessary. Furthermore, the data centres' directors are responsible for the processing of personal data under the terms of the law.

As to oversight mechanisms, this law also foresees that the director of each data centre shall be responsible for ensuring: respect for the applicable constitutional, legal and regulatory provisions in the processing, storage and access to data and information collected by SIED and/or SIS, within the scope of their respective activities; the supervision of compliance with the rules governing access by officials to data held in the respective Data Centre, as well as with other rules regarding the security of information processed and the technical standards and criteria of its operation; and the preparation of the monthly reports, or whenever exceptional circumstances so require, to the Secretary-General of SIRP, the Data Oversight Committee of SIRP and the respective SIED or SIS Directors on the control activities for the automated processing of information. Finally, it is also established that the Secretary-General of SIRP is responsible for directing the activity of the data centres, in conjunction with the directors of SIED and SIS.

Law 46/2018[31] introduced measures for a high common level of security of network and information systems across the EU, establishing a legal framework for cyberspace security. This law also created the Higher Council for Cyberspace Security (*Conselho Superior de Segurança do Ciberespaço*), a specific body to advise the Prime Minister on matters relating to cyberspace security, of which, are members the Secretary General of SIS, the Secretary General of the SIRP, the Director of SIS and the Director of SIED. This law isn't applicable to networks and information systems processing classified information. Therefore,the rules foreseen aren't applicable to the classified information that the intelligence services process.

---

[30] Portugal, Resolução do Conselho de Ministros 188/2017, que aprova o Regulamento do Centro de Dados do Serviço de Informações Estratégicas de Defesa e do Centro de Dados do Serviço de Informações de Segurança (Resolution of the Council of Ministers 188/2017, approving the Regulation of the Data Centre of the Defence Strategic Intelligence Service and the Data Centre of the Security Intelligence Service), 5 December 2017.

[31] Portugal, Lei 46/2018, que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (Law 46/2018, which establishes the legal framework for cyberspace security, transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of network and information systems across the Union), 13 August 2018.

The **National Strategy for Cyberspace Security 2019-2023**[32] established in its first axis, regarding cybersecurity issues, the goal of strengthening the cybersecurity structure by, among other measures: reinforcing and consolidating the Higher Council for Cyberspace Security as an advisory body to the Prime Minister, with representatives of all stakeholders, that guarantees a transversal and inclusive approach to the policies and initiatives developed by the various entities with responsibilities in this area; establishing the National Cybersecurity Centre (*Centro Nacional de Cibersegurança*), as the single national contact point for the purposes of international cooperation in cyber-security matters, without prejudice to the legal attributions entrusted to other entities, such as to the Secretary-General of SIRP regarding the production of national security information ; and to strengthen the intelligence services (SIS and SIED), within the scope of their exclusive competences, so that the respective human and technical resources for research and analysis may have a clear picture of the capabilities and intentions of the threats identified at any given moment, while reinforcing international cooperation and consolidating proximity to national actors in this area. Moreover, it should be noted that recently, on 2 November 2022, a new National Cyber Defence Strategy[33] was approved. This strategy establishes, in point 3, that to cope with situations of crisis or exception, it will be important to strengthen the existing information sharing and incident classification systems, promoting, in coordination with the Secretary-General of the Internal Security System, technical and functional interoperability between the Cyber Defence Operations Command (*Comando das Operações de Ciberdefesa*), the National Cybersecurity Centre, the Criminal Police (*Polícia Judiciária*) and the SIRP, without prejudice on the use of other channels deemed necessary for this sharing.

Decree-Law 19/2022[34], that established the Organic Law of the Military Headquarters of the Armed Forces (*Estado-Maior-General das Forças Armadas*) envisaged how the Armed Forces communicate with the intelligence system. Thus, this law establishes two bodies within the structure of Military Headquarters of the Armed Forces that are in direct contact with the intelligence system, and are responsible, among other functions, for liaison with the intelligence services of SIRP. These bodies are: the Joint Command for Military Operations (*Comando Conjunto para as Operações Militares*) responsible for the operational command of the forces and resources of the operational component of the force system, in all types of situations and for the missions of the Armed Forces, with the exception of air and sea search missions and rescue services; and the Military Information and Security Centre (*Centro de Informações e Segurança Militares*), the military intelligence and security body of the Armed Forces, responsible for producing the necessary intelligence for the fulfilment of the Armed Forces' missions and to guarantee military security . It should be noted that the provisions of the **Portuguese Republic Intelligence System Framework Law**[35]are also applicable to the Military Information and Security Centre.

Regarding oversight of the surveillance services, **the Rules of Procedure of the Parliament 1/2020**[36], established that, from a decision of the President of the Parliament or from a resolution of the parliamentary committee responsible for the matter, the Parliament should hold a prior hearing of

---

[32] Portugal, Resolução do Conselho de Ministros 92/2019, que aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (Resolution of the Council of Ministers 92/2019, approving the National Strategy for Cyberspace Security 2019-2023), 5 June 2019.

[33] Portugal, Resolução do Conselho de Ministros 106/2022, que aprova a Estratégia Nacional de Ciberdefesa (Resolution of the Council of Ministers 106/2022, approving the National Cyber Defence Strategy), 2 November 2022.

[34] Portugal, Decreto-Lei 19/2022, que estabelece a Lei Orgânica do Estado-Maior-General das Forças Armadas e altera as Leis Orgânicas dos três ramos das Forças Armadas (Decree-Law 19/2022, which establishes the Organic Law of the Military Headquarters of the Armed Forces and amends the Organic Laws of the three branches of the Armed Forces), 24 Janeiro 2022.

[35] Portugal, Lei 30/84, que estabelece a Lei-Quadro do Sistema de Informações da República Portuguesa (Law 30/84, which establishes the Portuguese Republic Intelligence System Framework Law), 5 September 1984.

[36] Portugal, Regimento da Assembleia da República 1/2020, que aprova o Regimento da Assembleia da República (Rules of Procedure of the Parliament 1/2020, which approves the Rules of Procedure of the Assembly of the Republic), 31 August 2020.

candidates for certain posts outside the Parliament. Within the list of posts foreseen are the members of the Council for the Oversight of the Intelligence System of the Portuguese Republic.

Finally, it should be highlighted that **Parliamentary Decree 17/XV**[37], that amended the **Internal Security Law**[38], established a change in Article 25 of the **Law of Internal Security**, in which the heads of the security forces and services, which includes SIS, has to be preceded by a hearing with the Secretary-General of the Internal Security System. This means that the appointment of the Director of SIS - which is currently the Prime Minister's responsibility, after hearing the Secretary-General of SIRP would be made by hearing not only the Secretary-General of SIRP, but also the Secretary-General of the Internal Security System. Even during the discussion of this Parliamentary Decree, the Council for the Oversight of the Intelligence System of the Portuguese Republic issued an opinion[39], on 12 October 2022, in which it considered that the proposal in discussion lacked reflection. The opinion pointed out that it would create a system in which the two directors (the Director of SIS and the Director of SIED), who are part of the same system (SIRP), would be subject to different appointment processes; that it wouldn't make sense to include the Secretary-General of the Internal Security System in this process, since this figure has no institutional role in the SIRP; and that this obligation would introduce an entropy in the system, in the sense that, if the opinions of the Secretary-General of SIRP and of the Secretary-General of the Internal Security System clashed, it wasn't clear which one would be given precedence by the Prime Minister. Therefore, the Council for the Oversight of the Intelligence System of the Portuguese Republic issued the opinion arguing that this part of the proposal should be excluded.

The proposal was approved on October 2022 by the Parliament. However, when sent for promulgation by the President of the Republic, the last step for a law to be fully approved, the President decided to request the Constitutional Court to conduct a preventive constitutional review of this Parliamentary Decree, for possible violation of the principle of separation of powers[40]. This request is mainly focused on the changes regarding the INTERPOL and EUROPOL national units, but it will also review Article 25 of the of the **Law of Internal Security**. Therefore, there is the possibility of the Court to declare the changes to Article 25 unconstitutional.

Regarding reports or statements on the national legal framework in the area of surveillance by intelligence services, it should be noted that the Council for the Oversight of the Intelligence System of the Portuguese Republic, issues two reports[41] every year - one about the first semester of the year and one annual – which can include suggestions or opinions on legislation. The relevant information has been described above.

---

[37] Portugal, Decreto da Assembleia da República 17/XV, que reestrutura o Ponto Único de Contacto para a Cooperação Policial Internacional, alterando a Lei n.º 49/2008, de 27 de agosto, que aprova a Lei de Organização da Investigação Criminal, e a Lei n.º 53/2008, de 29 de agosto, que aprova a Lei de Segurança Interna (Parliamentary Decree 17/XV, restructuring the Single Point of Contact for International Police Cooperation, amending Law 49/2008 of 27 August, which approves the Law on the Organisation of Criminal Investigation, and Law 53/2008 of 29 August, which approves the Internal Security Law), 10 November 2022.

[38] Portugal, Lei 53/2008, que aprova Lei de Segurança Interna (Law 53/2008, which approves the Law of Internal Security), 29 August 2008.

[39] Council for the Oversight of the Intelligence System of the Portuguese Republic (2022), Parecer sobre a Proposta de Lei 28/XV (Reestruturação do Ponto Único de Contacto para a Cooperação Policial Internacional; Alteração à Lei de Segurança Interna) (Opinion on Draft Law 28/XV (Restructuring the Single Point of Contact for International Police Cooperation; Amendment to the Internal Security Act)), Lisbon, Council for the Oversight of the Intelligence System of the Portuguese Republic.

[40] The request for a preventive constitutional review can be found in the website of the Parliament.

[41] The reports can be found on the website of the Council for the Oversight of the Intelligence System of the Portuguese Republic.

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.

	Civil (internal)	**Civil (external)**	**Civil (internal and external)**	**Military**
PT			Security Intelligence Service/ *Serviço de Informações de Segurança* (SIS)	Strategic Defence Intelligence Service/ *Serviço de Informações Estratégicas e de Defesa* (SIED)

The above table is accurate. According to the **Framework Law of the Portuguese Republic Intelligence System**[42], the Security Intelligence Service (*Serviço de Informações de Segurança*) (SIS)and the Strategic Defence Intelligence Service (*Serviço de Informações Estratégicas de Defesa*) (SIED), are integrated in the structure of SIRP.

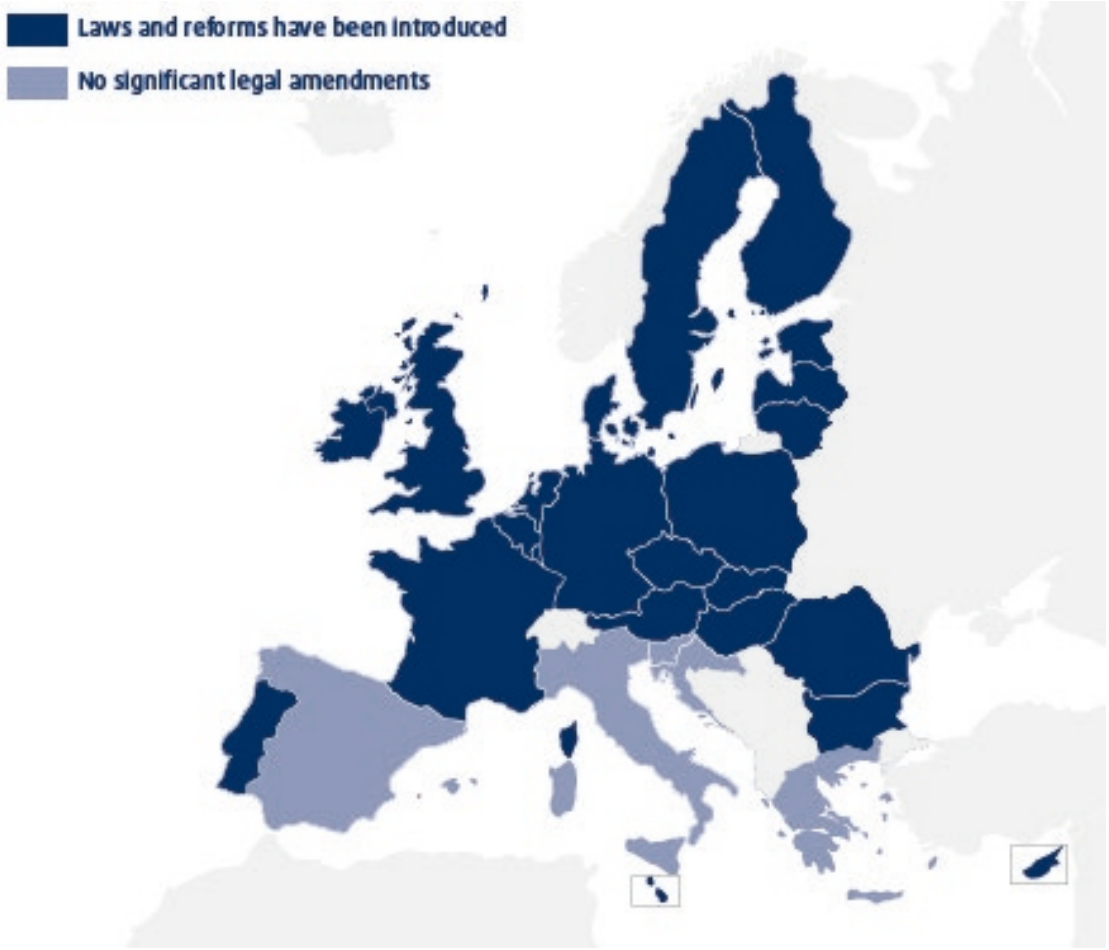
2.2. EU Member States' legal framework on surveillance reformed since 2017

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

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

[42] Portugal, Lei 30/84, que estabelece a Lei-Quadro do Sistema de Informações da República Portuguesa (Law 30/84, which establishes the Framework Law of the Portuguese Republic Intelligence System), 5 September 1984.

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



In matters of surveillance, **since mid-2017** there have been some legal changes, as described above. The following are the references to those legal changes, in chronological order:

- Portugal, Lei 83/2017, que estabelece medidas de combate ao branqueamento de capitais e ao financiamento do terrorismo, transpõe parcialmente as Diretivas 2015/849/UE, do Parlamento Europeu e do Conselho, de 20 de maio de 2015, e 2016/2258/UE, do Conselho, de 6 de dezembro de 2016, altera o Código Penal e o Código da Propriedade Industrial e revoga a Lei n.º 25/2008, de 5 de junho, e o Decreto-Lei n.º 125/2008, de 21 de julho (Law 83/2017, which establishes measures to combat money laundering and terrorist financing, and partially transposes Directives 2015/849/EU, of the European Parliament and of the Council, of 20 May 2015, and 2016/2258/EU, of the Council, of 6 December 2016, amending the Criminal Code and the Industrial Property Code and revoking Law 25/2008, of 5 June, and Decree-Law 125/2008, of 21 July), 18 August 2017.
- Portugal, Lei 97/2017, que regula a aplicação e a execução de medidas restritivas aprovadas pela Organização das Nações Unidas ou pela União Europeia e estabelece o regime sancionatório aplicável à violação destas medidas (Law 97/2017, which regulates the application and enforcement of restrictive measures approved by the United Nations or the European Union and establishes the penalty regime applicable to the violation of these measures), 23 August 2017.

- Portugal, Lei Orgânica 4/2017, que aprova e regula o procedimento especial de acesso a dados de telecomunicações e Internet pelos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa e procede à segunda alteração à Lei 62/2013, de 26 de agosto (Lei da Organização do Sistema Judiciário) (Organic Law 4/2017, which approves and regulates the special procedure for access to telecommunications and internet data by intelligence officers of the Security Intelligence Service and the Defence Strategic Intelligence Service and makes the second amendment to Law 62/2013 of 26 August [Law on the Organisation of the Judiciary System]), 25 August 2017.
- Portugal, Resolução do Conselho de Ministros 188/2017, que aprova o Regulamento do Centro de Dados do Serviço de Informações Estratégicas de Defesa e do Centro de Dados do Serviço de Informações de Segurança (Resolution of the Council of Ministers 188/2017, which approves the Regulation of the Data Centre of the Strategic Defence Intelligence Service and the Data Centre of the Security Intelligence Service), 5 December 2017.
- Portugal, Lei 46/2018, que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (Law 46/2018, which establishes the legal framework for cyberspace security, transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of network and information systems across the Union), 13 August 2018.
- Portugal, Portaria 237-A/2018, que define as condições técnicas e de segurança da comunicação eletrónica para efeito de transmissão diferida dos dados de telecomunicações e Internet pelos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa (Order 237-A/2018, defining the technical and security conditions of electronic communication for the purpose of deferred transmission of telecommunications and internet data by the intelligence officers of the Security Intelligence Service and the Defence Strategic Intelligence Service), 28 August 2018.
- Portugal, Resolução do Conselho de Ministros 92/2019, que aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (Resolution of the Council of Ministers 92/2019, approving the National Strategy for Cyberspace Security 2019-2023), 5 June 2019.
- Portugal, Lei 58/2019, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Law 58/2019, ensuring the implementation in national law of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), 8 August 2019.
- Portugal, Decreto-Lei 142/2019, que aprova o Programa Nacional de Segurança da Aviação Civil (Decree-Law 142/2019, which approves the National Programme for Civil Aviation Security), 19 September 2019.
- Portugal, Regimento da Assembleia da República 1/2020, que aprova o Regimento da Assembleia da República (Rules of Procedure of the Parliament 1/2020, which approves the Rules of Procedure of the Parliament), 31 August 2020.
- Portugal, Decreto-Lei 19/2022, que estabelece a Lei Orgânica do Estado-Maior-General das Forças Armadas e altera as Leis Orgânicas dos três ramos das Forças Armadas (Decree-Law 19/2022, which establishes the Organic Law of the Military Headquarters of the Armed Forces and amends the Organic Laws of the three branches of the Armed Forces), 24 Janeiro 2022.

- Portugal, Lei 16/2022, que aprova a Lei das Comunicações Eletrónicas, transpondo as Diretivas 98/84/CE, 2002/77/CE e (UE) 2018/1972, alterando as Leis n.os 41/2004, de 18 de agosto, e 99/2009, de 4 de setembro, e os Decretos-Leis n.os 151-A/2000, de 20 de julho, e 24/2014, de 14 de fevereiro, e revogando a Lei n.º 5/2004, de 10 de fevereiro, e a Portaria n.º 791/98, de 22 de setembro (Law 16/2022, which approves the Electronic Communications Law, transposing Directives 98/84/EC, 2002/77/EC and (EU) 2018/1972, amending Laws 41/2004, of 18 August, and 99/2009, of 4 September, and Decree-Laws 151-A/2000, of 20 July, and 24/2014, of 14 February, and revoking Law 5/2004, of 10 February, and Ordinance 791/98, of 22 September), 16 August 2022.
- Portugal, Resolução do Conselho de Ministros 106/2022, que aprova a Estratégia Nacional de Ciberdefesa (Resolution of the Council of Ministers 106/2022, approving the National Cyber Defence Strategy), 2 November 2022.
- Portugal, Decreto da Assembleia da República 17/XV, que reestrutura o Ponto Único de Contacto para a Cooperação Policial Internacional, alterando a Lei n.º 49/2008, de 27 de agosto, que aprova a Lei de Organização da Investigação Criminal, e a Lei n.º 53/2008, de 29 de agosto, que aprova a Lei de Segurança Interna (Parliamentary Decree 17/XV, restructuring the Single Point of Contact for International Police Cooperation, amending Law 49/2008 of 27 August, which approves the Law on the Organisation of Criminal Investigation, and Law 53/2008 of 29 August, which approves the Internal Security Law), 10 November 2022.

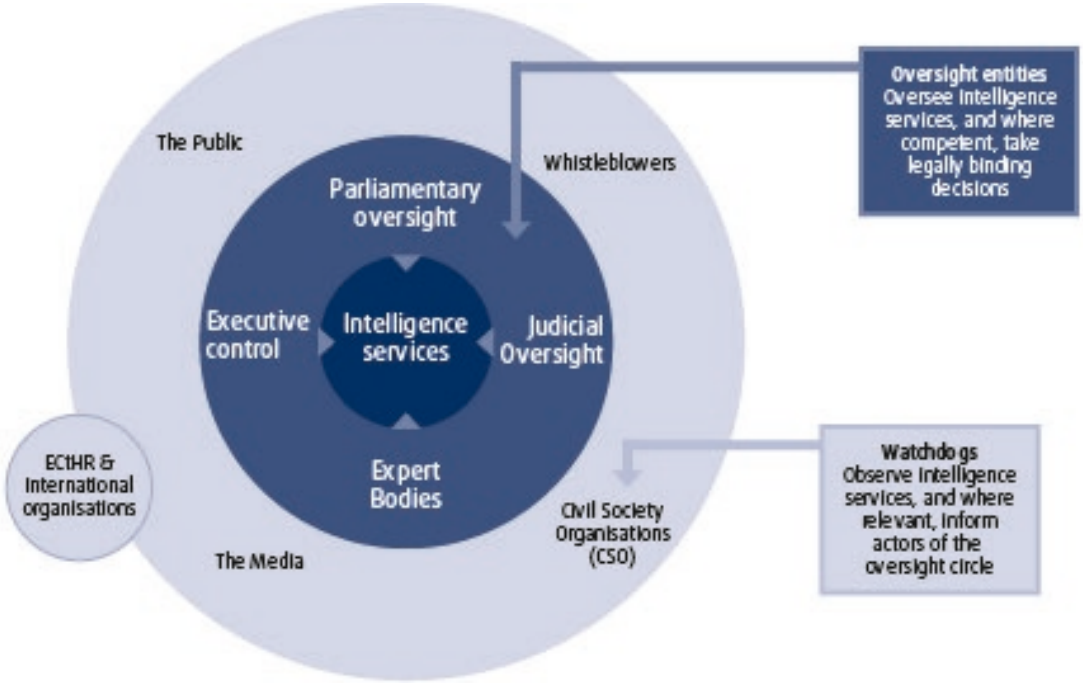
It should be pointed out that none of these changes was initiated in the context of the PEGASUS revelations, since there are no allegations of the use of this software in Portugal. In fact, and although not directly related with the surveillance system, but with criminal authorities, on May 2022, when questioned by Members of Parliament on whether Portugal had already acquired or was considering using the Israeli electronic spying system, the Minister for Internal Affairs assured MPs that PEGASUS "will not be used by the national security services"[43]. However, in 2021, it was reported that a company called "Hacking Team" tried to sell the software to the Criminal Police in 2015. The attempted sale was made public after an email exchange was published on the Wikileaks website. However, the Criminal Police stressed that it had never used that system or any other NSO Group software[44].

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.

[43] Jornal de Notícias (2022), "Portugal não usa nem vai usar sistema Pegasus" (Portugal does not and will not use the Pegasus system), 6 May 2022.
[44] Jornal de Negócios (2021), "Empresa tentou vender software de espionagem Pegasus à PJ em 2015" (Company tried to sell Pegasus spy software to PJ in 2015), 23 July 2021.

Figure 5: Intelligence services' accountability scheme

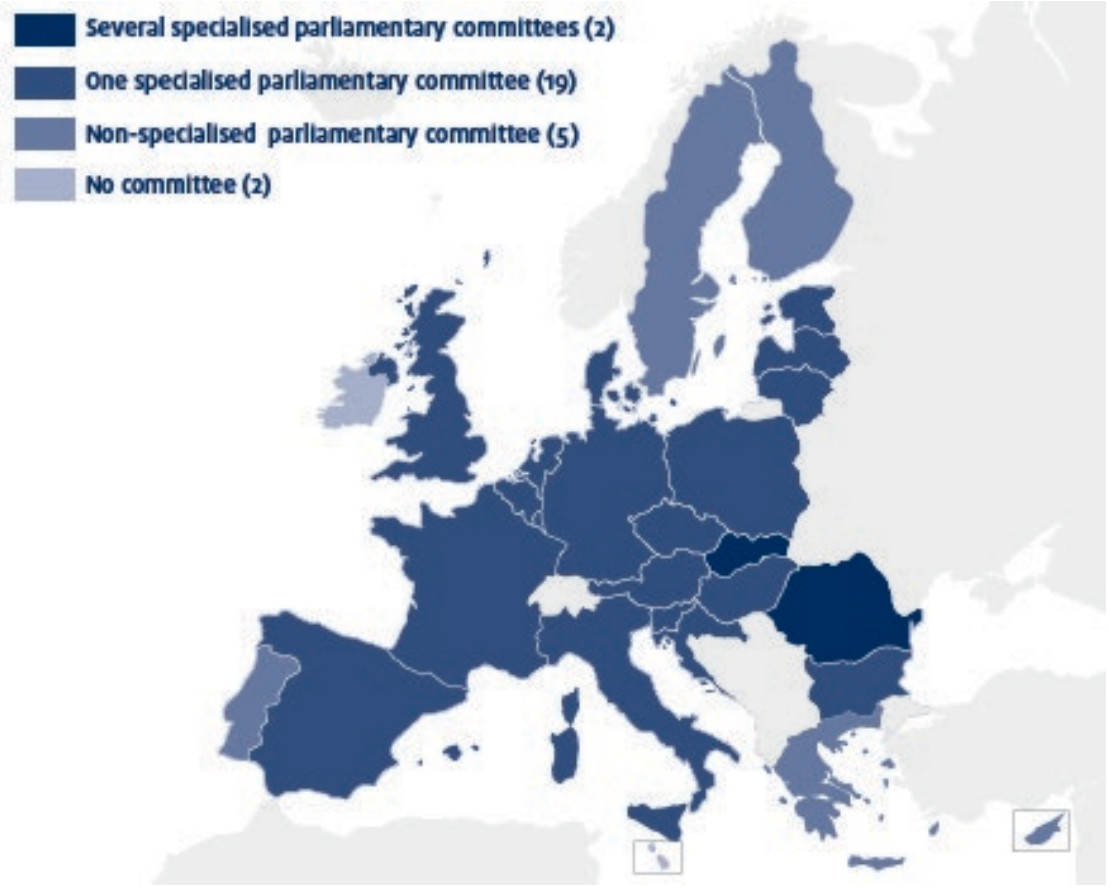


The diagram above is accurate, reflecting the current situation in Portugal.

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.

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



The map above is accurate. According to the **Portuguese Republic Intelligence System Framework Law**[45] and **The Rules of Procedure of the Parliament**[46], the election/nomination of the members of the Council for the Oversight of the Intelligence System of the Portuguese Republic, the General-Secretary of SIRP, and the Directors of SIS and SIED is preceded by a hearing before the Parliamentary Committee for Constitutional Affairs, Rights, Freedoms and Guarantees (*Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias*), which assesses not only their profile, but also the curricula of the candidates. This Committee can also verify impediments, as well as to recommend the dismissal of any member of the Council for the Oversight of the Intelligence System of the Portuguese Republic to the Parliament. Furthermore, and according to the **Portuguese Republic Intelligence System Framework Law**[47]**,** the Parliament can also request the presence of the Council for the Oversight of the Intelligence System of the Portuguese Republic with the purpose of obtaining clarifications on the exercise of its activity, as it can also issue opinions concerning the operation of SIRP and receives the twice-yearly Reports drawn up by the Supervisory Authority on the intelligence system's performance, through a parliamentary committee level (that may happen in the Parliamentary Committee for Constitutional Affairs, Rights, Freedoms and Guarantees).

[45] Portugal, Lei 30/84, que estabelece a Lei-Quadro do Sistema de Informações da República Portuguesa (Law 30/84, which establishes the Portuguese Republic Intelligence System Framework Law), 5 September 1984.
[46] Portugal, Regimento da Assembleia da República 1/2020, que aprova o Regimento da Assembleia da República (Rules of Procedure of the Parliament 1/2020, which approves the Rules of Procedure of the Assembly of the Republic), 31 August 2020.
[47] Portugal, Lei 30/84, que estabelece a Lei-Quadro do Sistema de Informações da República Portuguesa (Law 30/84, which establishes the Portuguese Republic Intelligence System Framework Law), 5 September 1984.

According to the **Portuguese Republic Intelligence System Framework Law**[48] and the **Regime of the State Secrets**[49], a person with knowledge of matters covered by state secrecy, called to testify or make statements before judicial authorities or parliamentary committees of enquiry, may not disclose them, in whole or in part. This means that even if the Parliament requests the presence of a representative of the Council for the Oversight of the Intelligence System of the Portuguese Republic, with the purpose of obtaining clarifications on the exercise of the activity of the surveillance services, this person cannot disclose matters/information classified as state secrets. However, if the Parliament considers the refusal to be unjustified, it may communicate the fact to the entity holding the confidentiality (in this matters, the SIRP), which shall justify whether or not the refusal should be maintained.

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.

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

EU Member State	Expert Bodies
PT	Council for the Oversight of the Intelligence System of the Portuguese Republic (*Conselho de Fiscalização do Sistema de Informações da República Portuguesa*)

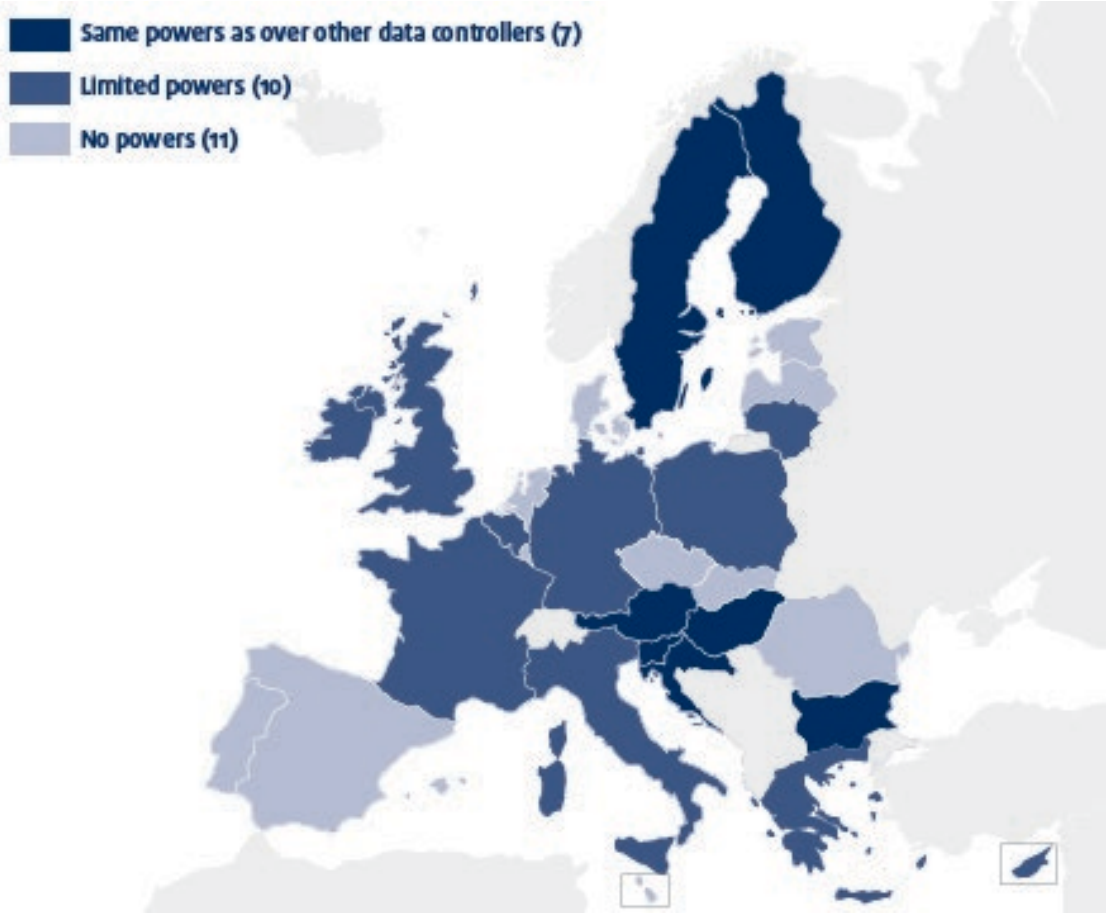
The table above is accurate. According to the **Portuguese Republic Intelligence System Framework Law**[50], the Council for the Oversight of the Intelligence System of the Portuguese Republic is the body that monitors and supervises the activity of the Secretary-General and the intelligence services, ensuring compliance with the Constitution and the law, with particular focus on the preservation of rights, freedoms and guarantees (Article 9).

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.

[48] Portugal, Lei 30/84, que estabelece a Lei-Quadro do Sistema de Informações da República Portuguesa (Law 30/84, which establishes the Portuguese Republic Intelligence System Framework Law), 5 September 1984.
[49] Portugal, Lei Orgânica 2/2014, que aprova o Regime do Segredo de Estado, procede à vigésima primeira alteração ao Código de Processo Penal e à trigésima primeira alteração ao Código Penal e revoga a Lei 6/94, de 7 de abril (Organic Law 2/2014, which approves the State Secret Regime, makes the twenty-first amendment to the Code of Criminal Procedure and the thirty-first amendment to the Criminal Code and revokes Law 6/94, of 7 April), 6 August 2014.
[50] Portugal, Lei 30/84, que estabelece a Lei-Quadro do Sistema de Informações da República Portuguesa (Law 30/84, which establishes the Framework Law of the Portuguese Republic Intelligence System), 5 September 1984.

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



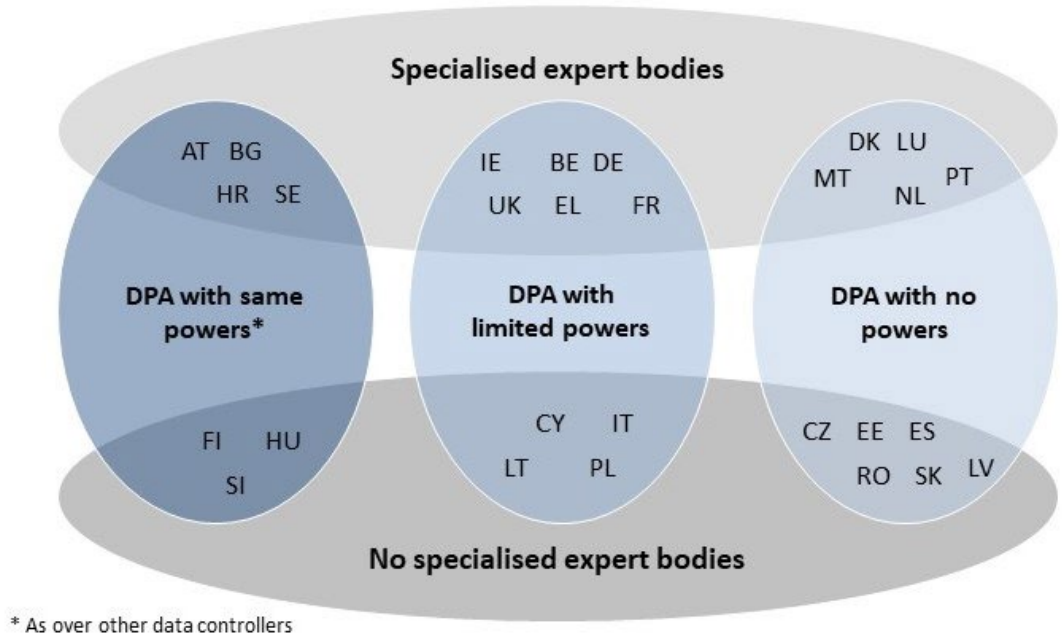
The above map is accurate. As mentioned before, Law 58/2019[51], that ensured the implementation of the General Data Protection Regulation, also establishes that the rules foreseen wouldn't apply to data files constituted and maintained under the responsibility of SIRP. This also meant that the National Commission for Data Protection does not have competences over SIRP.

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.

[51] Portugal, Lei 58/2019, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Law 58/2019, ensuring the implementation in national law of Regulation (EU) 2016/679 of the Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), 8 August 2019.

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



The above figure is accurate. As mentioned above, the National Commission for Data Protection does not have competences over the SIRP. Instead, as expressed in the **Portuguese Republic Intelligence System Framework Law**[52], it establishes the Council for the Oversight of the Intelligence System of the Portuguese Republic as the body that monitors and supervises the activity of the Secretary-General and the intelligence services, ensuring compliance with the Constitution and the law, with particular focus on the preservation of rights, freedoms and guarantees, and it shares its competences of oversight with the Data Oversight Commission of the Information System of the Portuguese Republic, when it comes to data related issues.

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
PT	N/A	N/A	N/A	N/A

[52] Portugal, Lei 30/84, que estabelece a Lei-Quadro do Sistema de Informações da República Portuguesa (Law 30/84, which establishes the Framework Law of the Portuguese Republic Intelligence System), 5 September 1984.

The table above isn't accurate, since the intelligence services have legal limitations on their activities. According to the **Portuguese Republic Intelligence System Framework Law** [53] and **Law 50/2014**[54]**,** the responsibility of intelligence services is to ensure the production of the necessary information for the preservation of internal and external security, as well as national independence and interests and the unity and integrity of the State. This means that they cannot execute criminal investigations, which, in turn, means that they cannot carry out target surveillance measures, since the **Portuguese Constitution**[55] only allows these measures to be carried out in the context of a criminal investigation. Even the **law** that approved special procedures for access to metadata by intelligence officers of SIS and SEID,[56] prohibits real-time interconnection with the databases of telecommunications and internet operators. The intelligence services can, however, as described above and under the terms of the law[57], collaborate with other public entities in order to access data considered relevant for the pursuit of its competences. The way this access is done is established by protocols. But when it comes to criminal police authorities, they are obliged to provide SIS, at its request, with any news and information of which they may have knowledge, directly or indirectly related to internal security and the prevention of sabotage, terrorism, espionage and the practice of acts which, by their nature, may alter or destroy the constitutional established rule of law. This means that criminal police authorities are obliged to provide news and information of which they may have knowledge. SIS cannot, in its turn, request these entities to start investigations in order to get any specific data. Therefore, we suggest reflecting this nuance of the Portuguese legal framework in the text of the report.

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).

---

[53] Portugal, Lei 30/84, que estabelece a Lei-Quadro do Sistema de Informações da República Portuguesa (Law 30/84, which establishes the Framework Law of the Portuguese Republic Intelligence System), 5 September 1984.

[54] Portugal, Lei 50/2014, que procede à primeira alteração à Lei n.º 9/2007, de 19 de fevereiro, que estabelece a orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa (SIED) e do Serviço de Informações de Segurança (SIS) e revoga os Decretos-Leis n.os 225/85, de 4 de julho e 254/95, de 30 de setembro (Law 50/2014, which makes the first amendment to Law no. 9/2007, of 19 February, establishing the organic structure of the Secretary-General of the Intelligence System of the Portuguese Republic, the Strategic Defence Intelligence Service (SIED) and the Security Intelligence Service (SIS) and revoking Decree-Laws no. 225/85, of 4 July and 254/95, of 30 September), 13 August 2014.

[55] Portugal, Constituição da República Portuguesa (Constitution of the Portuguese Republic), 10 April 1976.

[56] Portugal, Lei Orgânica 4/2017, que aprova e regula o procedimento especial de acesso a dados de telecomunicações e Internet pelos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa e procede à segunda alteração à Lei 62/2013, de 26 de agosto (Lei da Organização do Sistema Judiciário) (Organic Law 4/2017, that approves and regulates the special procedure for access to telecommunications and Internet data by intelligence officers of the Security Intelligence Service and the Defence Strategic Intelligence Service and makes the second amendment to Law 62/2013 of 26 August [Law on the Organisation of the Judiciary System]), 25 August 2017.

[57] Portugal, Lei 50/2014, que procede à primeira alteração à Lei n.º 9/2007, de 19 de fevereiro, que estabelece a orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa (SIED) e do Serviço de Informações de Segurança (SIS) e revoga os Decretos-Leis n.os 225/85, de 4 de julho e 254/95, de 30 de setembro (Law 50/2014, which makes the first amendment to Law no. 9/2007, of 19 February, establishing the organic structure of the Secretary-General of the Intelligence System of the Portuguese Republic, the Strategic Defence Intelligence Service (SIED) and the Security Intelligence Service (SIS) and revoking Decree-Laws no. 225/85, of 4 July and 254/95, of 30 September), 13 August 2014.

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

	Judicial	Parliamentary	Executive	Expert
PT	N/A	N/A	N/A	N/A

As stated above, and according to the **Portuguese Republic Intelligence System Framework Law**[58] and **Law 50/2014**[59], the responsibility of intelligence services is to ensure the production of information necessary for the preservation of internal and external security, as well as national independence and interests and the unity and integrity of the State. This means that they cannot execute criminal investigations, which, in turn, means that they cannot conduct general surveillance of communications, since, as referred before, the **Portuguese Constitution**[60] only allows these measures to be carried out in the context of a criminal investigation. Therefore, we suggest reflecting this nuance of the Portuguese legal framework in the text of the report.

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
PT		✓			✓

The above table is accurate. The non-judicial bodies with remedial competences in the context of surveillance are the Council for the Oversight of the Intelligence System of the Portuguese Republic and the Data Oversight Commission of the Information System of the Portuguese Republic, when it comes to issues related with surveillance[61]. According to this law, the Council for the Oversight of the Intelligence System of the Portuguese Republic can receive claims regarding data processing and the respect for rights, liberties and guarantees. If the Council finds that the data processing was unlawful, this must be deleted. Furthermore, it can also propose the undergoing of inquiries, investigation or sanctions, if the situation is serious and justifies further actions to the Government. The sanctions range from disciplinary to criminal procedures, in the case of a violation of special duties by the staff of the intelligence services. The complaints regarding data processing can also be lodged with the Data Oversight Commission of the Information System of the Portuguese Republic, that can order the elimination of incorrect or unlawful data and report the situation to the Council for the Oversight of the Intelligence System of the Portuguese Republic. Both entities conduct periodical inspections to the

[58] Portugal, Lei 30/84, que estabelece a Lei-Quadro do Sistema de Informações da República Portuguesa (Law 30/84, which establishes the Framework Law of the Portuguese Republic Intelligence System), 5 September 1984.

[59] Portugal, Lei 50/2014, que procede à primeira alteração à Lei n.º 9/2007, de 19 de fevereiro, que estabelece a orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa (SIED) e do Serviço de Informações de Segurança (SIS) e revoga os Decretos-Leis n.os 225/85, de 4 de julho e 254/95, de 30 de setembro (Law 50/2014, which makes the first amendment to Law no. 9/2007, of 19 February, establishing the organic structure of the Secretary-General of the Intelligence System of the Portuguese Republic, the Strategic Defence Intelligence Service (SIED) and the Security Intelligence Service (SIS) and revoking Decree-Laws no. 225/85, of 4 July and 254/95, of 30 September), 13 August 2014.

[60] Portugal, Constituição da República Portuguesa (Constitution of the Portuguese Republic), 10 April 1976.

[61] Portugal, Lei 30/84, que estabelece a Lei-Quadro do Sistema de Informações da República Portuguesa (Law 30/84, which establishes the Framework Law of the Portuguese Republic Intelligence System), 5 September 1984.

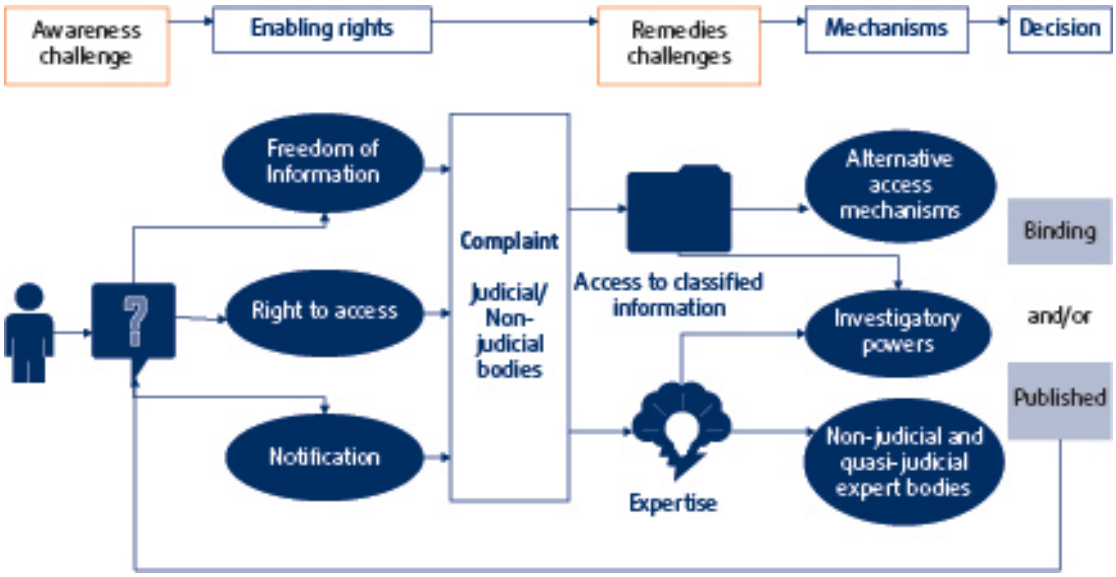
surveillance system, in order to ensure that the activities of the surveillance services and data centres (in the case of the Data Oversight Commission of the Information System of the Portuguese Republic) is lawful.

Furthermore, the Ombudsperson, as a person elected by the Parliament whose main duties is to defend and to promote the rights, freedoms, guarantees and legitimate interests of the citizens, can issue recommendations, opinions, promote public interventions and point out shortcomings in the legislation of any aspect that is linked with the scope of its activity. Within its competences and since intelligence services are public services, they fall under the scope of activity of the Ombudsperson. Therefore, the Ombudsperson can act if there is evidence of any violation of the citizens' rights, freedoms and guarantees[62]. Although these mechanisms are available to any person, they also imply that the person has knowledge that their data is being processed, which is something difficult to occur.

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.

Figure 9: Implementing effective remedies: challenges and solutions



The above diagram is accurate, reflecting the current situation in Portugal.

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.

[62] Portugal, Lei 9/91, que aprova o Estatuto da Provedoria de Justiça (Law 9/91, which approves the Statute of the Ombudsperson), 9 April 1991.

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

	Bodies with remedial competence	Decisions are binding	May fully access collected data	Control is communicated to complainant	Decision may be reviewed
PT	Council for the Oversight of the Intelligence				
	Data Oversight Commission of the Information System of the Portuguese Republic (regarding data issues)				
	Portuguese Ombudsman				

Note:

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

Source: FRA, 2017

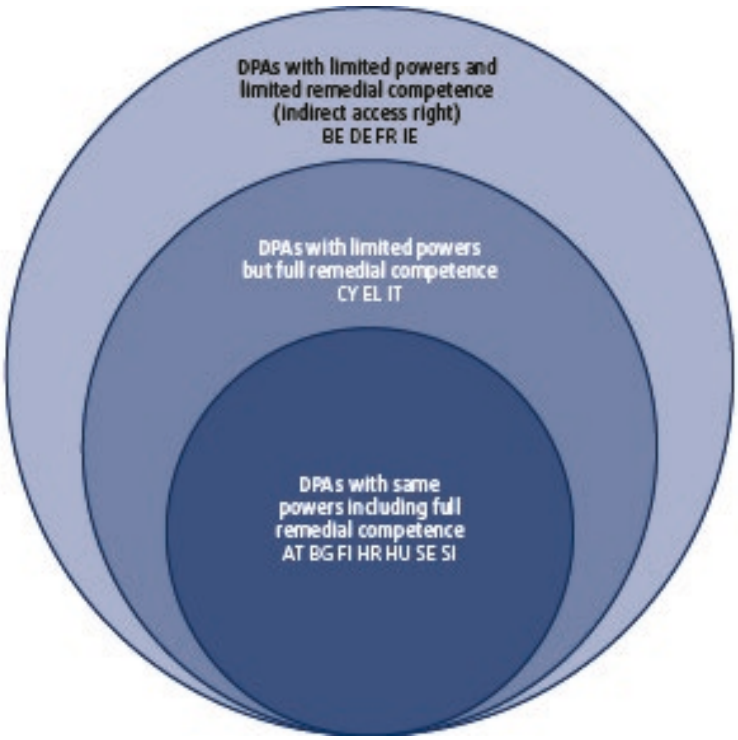
The above table is accurate. We suggest to include the Data Oversight Commission of the Information System of the Portuguese Republic, because this body has remedy competences when the situation pertains to data issues, under the terms of the **Portuguese Republic Intelligence System Framework Law**[63]. According to this law, an error in the imputation of data or information or irregularities in their processing are revealed that error has to reported to the Data Oversight Commission of the Information System of the Portuguese Republic. A person that has knowledge of data concerning them, considered to be erroneous, unlawfully obtained or in breach of their rights, freedoms and personal guarantees may also request to the Data Oversight Commission of the Information System of the Portuguese Republic to carry out the necessary verifications and to order the cancellation or rectification of any data. If an irregularity or violation is verified, the Data Oversight Commission of the Information System of the Portuguese Republic has to report the situation to the Council for the Oversight of the Intelligence System of the Portuguese Republic.

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.

[63] Portugal, Lei 30/84, que estabelece a Lei-Quadro do Sistema de Informações da República Portuguesa (Law 30/84, which establishes the Framework Law of the Portuguese Republic Intelligence System), 5 September 1984.

Figure 10: DPAs' remedial competences over intelligence services



The above figure is accurate in the sense that doesn't include Portugal. The Portuguese National Commission for Data Protection does not have competences over the SIRP, as described above.