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

November 2022 Update

Country: Cyprus

FRANET contractor: University of Nicosia and Symfiliosi

Author(s) name(s): Trimikliniotis N. and Demetriou C.

Table of Contents

1. Summary 3
2. Annexes- Table and Figures 7
2.1. Overview of security and intelligence services in the EU-27 7
2.2. EU Member States' legal framework on surveillance reformed since 2017 7
Figure 1: EU Member States' legal frameworks on surveillance reformed since October 2015 8
2.3. Intelligence services' accountability scheme 8
Figure 5: Intelligence services' accountability scheme 9
2.4. Parliamentary oversight of intelligence services in EU Member States 9
Figure 6: Parliamentary oversight of intelligence services in EU Member States 10
2.5. Expert bodies (excluding DPAs) overseeing intelligence services in the EU 10
Table 2: Expert bodies (excluding DPAs) overseeing intelligence services in the EU 10
2.6. DPAs' powers over national intelligence services, by member states 10
Figure 7: DPAs' powers over national intelligence services, by member states 11
2.7. DPAs' and expert bodies' powers over intelligence techniques, by EU Member State 11
Figure 8: DPAs' and expert bodies' powers over intelligence techniques, by EU Member State 12
2.8. Binding authorisation/approval of targeted surveillance measures in the EU 12
Table 4: Binding authorisation/approval of targeted surveillance measures in the EU-27 13
2.9. Approval/authorisation of general surveillance of communication 13
Table 5: Approval/authorisation of general surveillance of communication in France, Germany, the Netherlands and Sweden 13
2.10. Non-judicial bodies with remedial powers 13
Table 6: Non-judicial bodies with remedial powers in the context of surveillance, by EU Member State 13
2.11. Implementing effective remedies 13
Figure 9: Implementing effective remedies: challenges and solutions 14
2.12. Non-judicial bodies' remedial powers 14
Table 7: Non-judicial bodies' remedial powers in case of surveillance, by EU Member State 14
2.13. DPAs' remedial competences 15
Figure 10: DPAs' remedial competences over intelligence services 15

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 legislative change introduced in 2020

In 2020 the law regulating the waiving of the confidentiality of written private communications was revised to include the monitoring of private telephone communications for the purpose of combating serious crime (hereinafter referred to as the 2020 law).[1] The intelligence service's accountability scheme was only marginally affected by this reform. The mandate and powers of the oversight committee were specified in the 2020 law, however the reform mainly dealt with the procedure of obtaining judicial authorisation for surveillance of private communications:

- The Director is now under a duty to inform this committee about who can access the surveillance equipment and monitor private communications;[2]

[1] Cyprus, The Protection of Privacy of Private Communications (Interception of Conversations and Access to Recorded Content of Private Communications) Act of 1996 (92(I)/1996) [*Ο περί Προστασίας του Απόρρητου της Ιδιωτικής Επικοινωνίας (Παρακολούθηση Συνδιαλέξεων και Πρόσβαση σε Καταγεγραμμένο Περιεχόμενο Ιδιωτικής Επικοινωνίας) Νόμος του 1996 (92(I)/1996)*]

[2] Cyprus, The Protection of Privacy of Private Communications (Interception of Conversations and Access to Recorded Content of Private Communications) Act of 1996 (92(I)/1996) [*Ο περί Προστασίας του Απόρρητου της Ιδιωτικής Επικοινωνίας (Παρακολούθηση Συνδιαλέξεων και Πρόσβαση σε Καταγεγραμμένο Περιεχόμενο Ιδιωτικής Επικοινωνίας) Νόμος του 1996 (92(I)/1996)*], article 6A.

- The committee's oversight mandate now includes the monitoring of the implementation of the 2020 law and the procedure for waiving the confidentiality of communications in compliance with the court order authorising it;[3]
- In order to fulfil this mandate, the committee is now authorised to conduct both regular and irregular checks into installations, technical equipment, archives and data of the Central Intelligence Service, without prejudice to the monitoring powers of the DPA.
- The Committee is now authorised to collect information from the Central Intelligence Service and from actors in the public and private sector in order to further its mission and to call any representative of these services for a hearing.
- If it transpires that there is a possibility that a criminal offence or an offence under the 2020 law was committed, the Committee must inform the Attorney General or the DPA. The Committee submits to the President of the Republic, with notifications to the House of Parliament, the Attorney General, the Justice Minister, the Chief of Police and the Director of the Central Intelligence Service, regular activity reports which spell out its observations and recommendations for safeguarding the right to confidentiality.[4]

Initially, opposition MPs tried to introduce provisions into the law setting as preconditions for the surveillance court order, the presence of a 'serious reason' and 'necessity'. The Minister of Justice at the time objected to these restrictions, insisting that 'reasonable suspicion' should suffice and arguing that the proposed restrictions would render the law ineffective, for its purpose, which was the protection of the state and the combating of serious crime.[5] The law was adopted with a provision sanctioning surveillance where this is "necessary in the interest of the security of the Republic" or for the prevention, investigation or prosecution of serious offences as these are listed in Article 17 of the Constitution: Premeditated murder or manslaughter, trafficking in adults or minors and offences related to child pornography, trafficking, supply, cultivation or production of narcotic drugs, psychotropic substances or dangerous drugs, offences relating to the currency or banknotes of the Republic; and corruption offences which, upon conviction, shall be punishable by a term of imprisonment of five years or more.[6]

The reform was not initiated in the context of the PEGASUS revelations, nor is there any reform under way as a result of the PEGASUS revelations.[7]

The 2020 law essentially specified the procedure for surveillance of private communications and the mandate of the three-member oversight committee set up under the 2016 law, which had purported to regulate the operation of the Central Intelligence Service (hereinafter, the 2016 law).[8] Under the 2020 law, where there is reasonable suspicion that a suspect has committed, is committing or will commit a crime, or that the security of the Republic is at risk, the Director of the Central Intelligence Service may apply to the Attorney General who, in turn, may submit an ex parte application to the court in order

---

[3] Cyprus, The Protection of Privacy of Private Communications (Interception of Conversations and Access to Recorded Content of Private Communications) Act of 1996 (92(I)/1996) [*Ο περί Προστασίας του Απόρρητου της Ιδιωτικής Επικοινωνίας (Παρακολούθηση Συνδιαλέξεων και Πρόσβαση σε Καταγεγραμμένο Περιεχόμενο Ιδιωτικής Επικοινωνίας) Νόμος του 1996 (92(I)/1996)*], article 17A.

[4] Cyprus, The Protection of Privacy of Private Communications (Interception of Conversations and Access to Recorded Content of Private Communications) Act of 1996 (92(I)/1996) [*Ο περί Προστασίας του Απόρρητου της Ιδιωτικής Επικοινωνίας (Παρακολούθηση Συνδιαλέξεων και Πρόσβαση σε Καταγεγραμμένο Περιεχόμενο Ιδιωτικής Επικοινωνίας) Νόμος του 1996 (92(I)/1996)*], article 17A.

[5] Cyprus Ministry of Justice and Public Order (2020), 'Statements by the Minister of Justice and Public Order Mr. George Savvidis after the extraordinary session of the Legal Affairs Committee of the House of Representatives, on the referral of the bill on telephone interception' (*Δηλώσεις του Υπουργού Δικαιοσύνης και Δημοσίας Τάξεως κ. ΧΧΧ μετά από την έκτακτη συνεδρία της Επιτροπή Νομικών Βουλής, για την αναπομπή του νομοσχεδίου για τις παρακολουθήσεις τηλεφωνικών συνδιαλέξεων*), Press release, 21 April 2020.

[6] Cyprus, Constitution of the Republic of Cyprus (*Σύνταγμα της Κυπριακής Δημοκρατίας*), article 17.

[7] FRANET in-person interview with the Director of the Central Intelligence Service, 9 November 2022.

[8] Cyprus, The Cyprus Intelligence Service (CIS) Law of 2016 [*Ο περί της Κυπριακής Υπηρεσίας Πληροφοριών (ΚΥΠ) Νόμος του 2016*],

authorise the surveillance of private communication.[9] For this purpose, the Director of the Central Intelligence Service may authorise members of the intelligence service or persons providing services to the intelligence service to access surveillance systems and monitor private communications for a period of two years, renewable for an additional term of two years. A prison sentence of up to five years and/or a fine of up to €50,000 is foreseen in the law for the person authorised to monitor private communications who infringes the terms of the judicial order.[10] In addition to the monitoring of telephone of communications, the court may authorise the Central Intelligence Office to enter into premises and to install or remove surveillance equipment.[11] The surveillance authorisation granted by the court cannot exceed 30 days, although renewals can be granted upon request. A provision in the 2016 law enabling the Attorney General to authorise private communication surveillance before a court order is issued was deleted from the final version of the 2020 law.

Under the 2020 law, the court may instruct the Director of the Central Intelligence Service to submit regular reports to the Attorney General on the progress made regarding the surveillance activities authorised and the need to continue.[12] The private communication content recorded is at the disposal of the Attorney General who issues instructions on its safe keeping and can only be destroyed upon instructions from the Attorney General.

Changes on the ground triggered by the legislative change of 2020

Shortly after the adoption of the 2020 law, the Council of Ministers finally appointed the members of the two three-member committees, as foreseen under the 2016 law:

- The committee to oversee the activities of the Central Intelligence Service, foreseen under the 2016 law and whose mandate was further specified by the 2020 law; and
- The committee mandated with submitting non-binding recommendations to the Director of the Central Intelligence Service regarding the declassification of documents. This committee is responsible not only for the documents of the intelligence service but for the entire state archive.

No remuneration is foreseen for the members of the oversight committee and although not lacking in expertise, the committee undoubtedly lacks the resources. The members are appointed by the Council of Ministers, after a recommendation from the President of the Republic. There is no information as to whether the committee has full access to the intelligence service's archives. There is no legal provision obliging the intelligence service to provide full access.

The adoption of the 2020 law also triggered the creation of a new employment regime for the members of the Central Intelligence Service. Whilst up until now the members of the intelligence service were seconded by the police force and the army, a set of regulations is now compiled and is under consideration by parliament to enable the Intelligence Service to recruit its own permanent staff. This is seen by the Director as an important development as it paves the way for better control of the intelligence service staff members by the respective director.[13]

---

[9] Cyprus, The Protection of Privacy of Private Communications (Interception of Conversations and Access to Recorded Content of Private Communications) Act of 1996 (92(I)/1996) [*Ο περί Προστασίας του Απόρρητου της Ιδιωτικής Επικοινωνίας (Παρακολούθηση Συνδιαλέξεων και Πρόσβαση σε Καταγεγραμμένο Περιεχόμενο Ιδιωτικής Επικοινωνίας) Νόμος του 1996 (92(I)/1996)*], article 6.

[10] Cyprus, The Protection of Privacy of Private Communications (Interception of Conversations and Access to Recorded Content of Private Communications) Act of 1996 (92(I)/1996) [*Ο περί Προστασίας του Απόρρητου της Ιδιωτικής Επικοινωνίας (Παρακολούθηση Συνδιαλέξεων και Πρόσβαση σε Καταγεγραμμένο Περιεχόμενο Ιδιωτικής Επικοινωνίας) Νόμος του 1996 (92(I)/1996)*], article 6A(4).

[11] Cyprus, The Protection of Privacy of Private Communications (Interception of Conversations and Access to Recorded Content of Private Communications) Act of 1996 (92(I)/1996) [*Ο περί Προστασίας του Απόρρητου της Ιδιωτικής Επικοινωνίας (Παρακολούθηση Συνδιαλέξεων και Πρόσβαση σε Καταγεγραμμένο Περιεχόμενο Ιδιωτικής Επικοινωνίας) Νόμος του 1996 (92(I)/1996)*], article 8(4).

[12] Cyprus, The Protection of Privacy of Private Communications (Interception of Conversations and Access to Recorded Content of Private Communications) Act of 1996 (92(I)/1996) [*Ο περί Προστασίας του Απόρρητου της Ιδιωτικής Επικοινωνίας (Παρακολούθηση Συνδιαλέξεων και Πρόσβαση σε Καταγεγραμμένο Περιεχόμενο Ιδιωτικής Επικοινωνίας) Νόμος του 1996 (92(I)/1996)*], article 12.

[13] FRANET in-person interview with the Director of the Central Intelligence Service, 9 November 2022.

Collaborations and oversight

As a matter of standard practice, the Central Intelligence Service maintains an institutional collaboration for exchange of information with the army, the national Anti-Cover-Up Offences Unit which deals with money laundering and financing of terrorism, as well as private actors. The DPA continues to have the same limited powers of check over the intelligence service which, however, maintains a close collaboration with the DPA and regularly consults the DPA on compliance with the data protection framework. The intelligence service can be subject to parliamentary scrutiny in a non-specialised parliamentary committee, if and when invited to attend. [14]

The institutional framework on oversight was amended by the 2020 law which introduced the procedure of applying for judicial authorisation to lift the confidentiality of private communications, as described above; this was not triggered by the Pegasus revelations and there is no indication at this stage that the Pegasus revelations will trigger any changes to the oversight framework of the intelligence service. Based on the information currently in the public sphere, the involvement of Cyprus in the PEGASUS affair relates to the licensing of the spyware companies and the monitoring of their activities by the competent governmental body, rather than the activities of the intelligence services.

The oversight mechanism was further developed with the specific duties afforded to the three-member committee by the 2020 law, although the final decision on authorising or approving surveillance measures rests with the court. The DPA continues to be the only non-judicial body with remedial powers: it has the right to issue binding decisions and to impose fines,[15] even though it has never conducted an investigation into the activities of the intelligence service. Its head is appointed by the Council of Ministers upon recommendation from the President of the Republic without independent evaluation of applicants. By contrast, the three-member committee can only refer a matter to the Attorney General to decide on prosecutions and cannot initiate prosecutions itself.

The Pega inquiry

There is abundant evidence of the manufacture and operation of surveillance equipment in Cyprus, which is also reportedly in the possession of the authorities and was used against citizens. Following its mission to Cyprus, the European Parliament's Committee of Inquiry into the use of surveillance software (PEGA) reported its will to look deeper into the Cyprus case, because of evidence that Cyprus is an important export hub and that there has been surveillance of citizens with such software both in Cyprus and in other countries.[16] A member of parliament told the press that spyware companies choose Cyprus as the basis of their operations because there is no check or control of their activities, adding that everyone is potentially under surveillance, including political parties.[17]

In accordance with a study conducted for the European Parliament, as of 2013 Cyprus permitted the registration and operation of companies leading to an Israeli businessman and former detective in the Israeli police's drug enforcement, selling electronic equipment and spyware to public services including the police and the drug enforcement authorities. The equipment sold by these companies is advertised as having the capacity to infiltrate smart mobile phones and comes in a portable form; the President of the Republic is reported to have carried surveillance equipment with him in a briefcase, during the 2017 negotiations for the Cyprus problem in Crans Montana. In 2022 a national court ruled that the company had illegally collected personal data of more than 600 citizens through access points at Cyprus' largest

[14] FRANET in-person interview with the Director of the Central Intelligence Service, 9 November 2022.
[15] Cyprus, Law on the protection of individuals with regard to the processing of personal data and the free circulation of personal data of 2018 (*Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018*) N. 125(I)/2018, article 32.
[16] Kathimerini (2022), 'PEGA: Θα πρέπει να εξετάσουμε πολύ περισσότερο την Κύπρο', 8 November 2022.
[17] Dialogos (2022), 'Κωστής Ευσταθίου στο InsideStory – Παρακολουθήσεις: «Γι' αυτό έρχονται, επειδή δεν τους ελέγχει κανείς»', 23 April 2022.

international airport. Both the court[18] and the DPA[19] fined the company, however charges against the businessman personally were withdrawn, upon instructions from the Attorney General.[20] The report cites interviews with MPs and an official from the Cypriot security authorities stating that there is no regulatory framework in Cyprus either for the manufacture or for the use of software, which enabled the activities of these companies in Cyprus and the use of the spyware, including the Predator, Pegasus and another applications, as well as the use of the spyware briefcases. The report describes the Cypriot authorities as reacting belatedly and only after the event.[21]

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
CY	~~Central Intelligence Service/ *Κεντρική Υπηρεσία Πληροφορικών* (ΚΥΠ)~~		*[The Director of the Central Intelligence Service considers that it is both internal and external]* Central Intelligence Service/ *Κεντρική Υπηρεσία Πληροφορικών* (ΚΥΠ)	*[The Director of the Central Intelligence Service considers that it is also military]* Central Intelligence Service/ *Κεντρική Υπηρεσία Πληροφορικών* (ΚΥΠ)

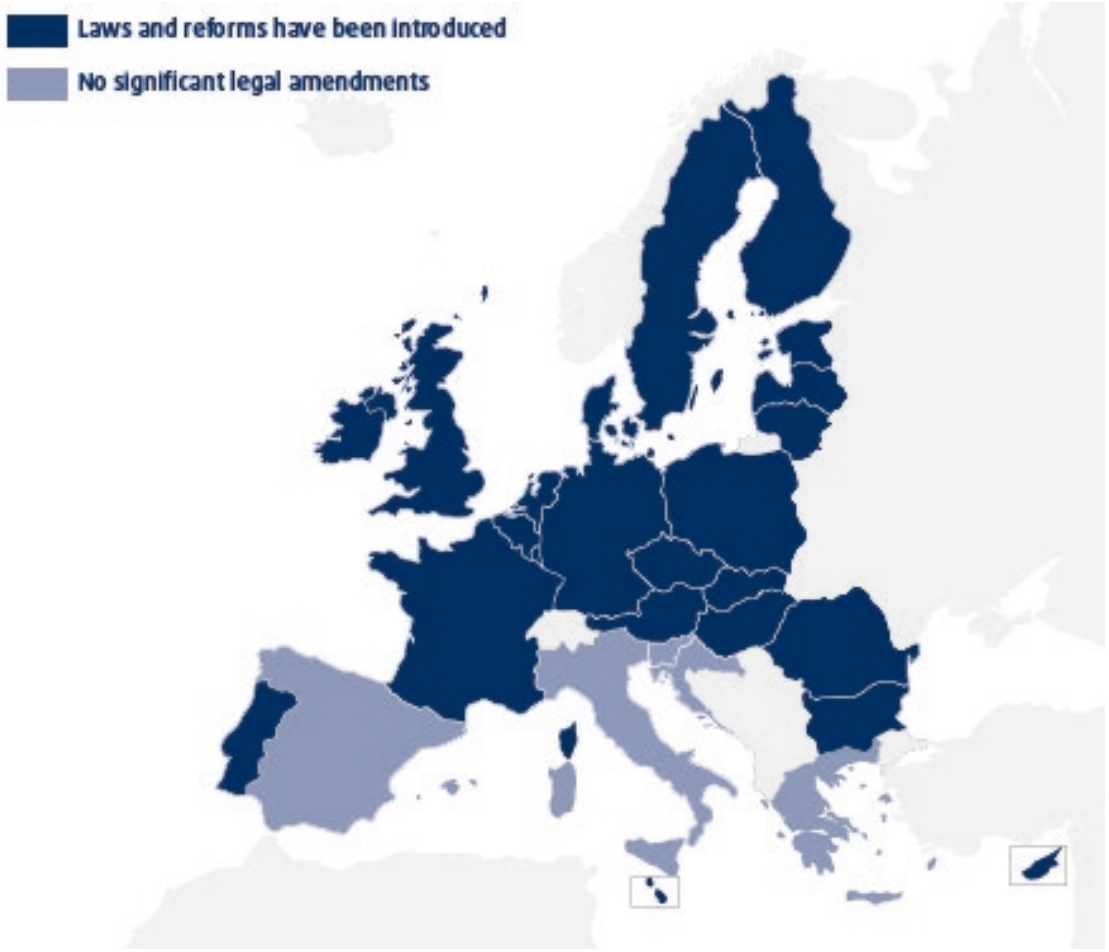
2.2. EU Member States' legal framework on surveillance reformed since 2017

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.*

[18] Cyprus, Assizes Court of Larnaca/Famagusta, *The Republic v. Ws Wispear Systems Limited*, Case No. 6839/21, ECLI:CY:KDLAR:2022:1, 22 February 2022.
[19] Cyprus, Commissioner for the protection of personal data (2021), 'Επιβολή διοικητικού προστίμου ύψους €925.000 στην εταιρεία WS WiSpear Systems Ltd', Press release, 12 Νοεμβρίου 2021.
[20] Financial Mirror (2021), Anger after 'spy van' charges dropped, 17 November 2021.
[21] European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs (2022), 'Briefing for the PEGA mission to Cyprus and Greece - 1-4 November 2022', 15 November 2022.

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



- In 2016 a law was adopted to regulate the operation of the intelligence service: The Cyprus Intelligence Service (CIS) Law of 2016 [*Ο περί της Κυπριακής Υπηρεσίας Πληροφοριών (ΚΥΠ) Νόμος του 2016*]

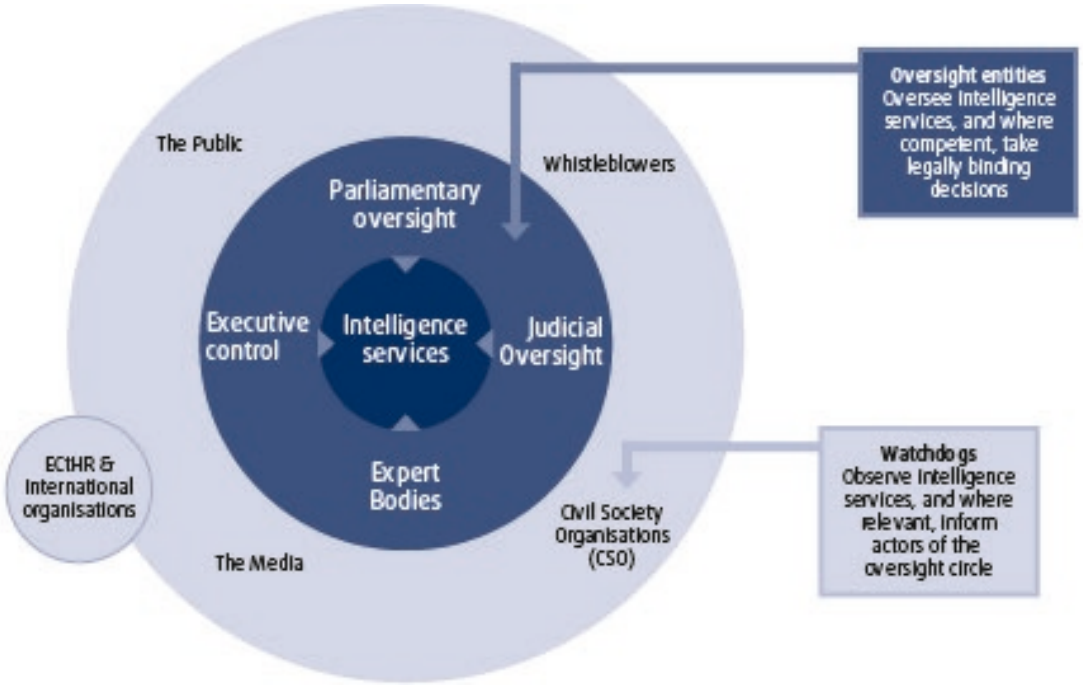
- In 2018 a new data protection law was adopted to bring the national framework in line with the GDPR: Law on the protection of individuals with regard to the processing of personal data and the free circulation of personal data of 2018 (*Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018*) N. 125(I)/2018.

- In 2020 a new law was adopted to regulate the surveillance of private communications: The Protection of Privacy of Private Communications (Interception of Conversations and Access to Recorded Content of Private Communications) Act of 1996 (92(I)/1996) [*Ο περί Προστασίας του Απόρρητου της Ιδιωτικής Επικοινωνίας (Παρακολούθηση Συνδιαλέξεων και Πρόσβαση σε Καταγεγραμμένο Περιεχόμενο Ιδιωτικής Επικοινωνίας) Νόμος του 1996 (92(I)/1996)*]

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.

Figure 5: Intelligence services' accountability scheme

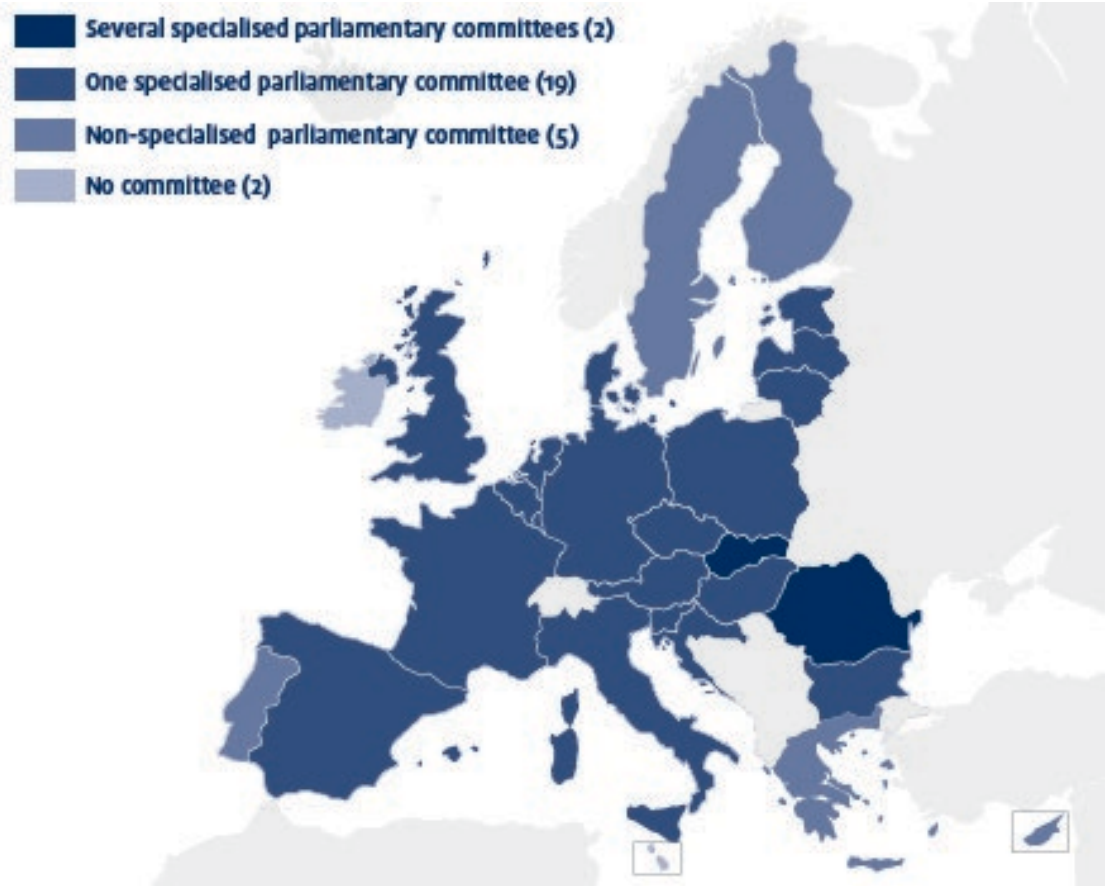


The oversight three-member committee does not have competence to make legally binding decisions; it can only refer issues to the Attorney General. There are no civil society organisations active in the field of personal data protection.

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 classification is correct: The intelligence service may be called upon by a non-specialised parliamentary committee to attend a session for the purposes of parliamentary scrutiny. The parliamentary committee however does not have any specific oversight mandate nor is it empowered to make binding decisions in relation to specific surveillance activities of the intelligence service.[22]

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 three-member committee foreseen in the 2016 legislation has now been appointed, albeit without remuneration.[23] No the information is not in the public sphere; neither are the names of the persons appointed.

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

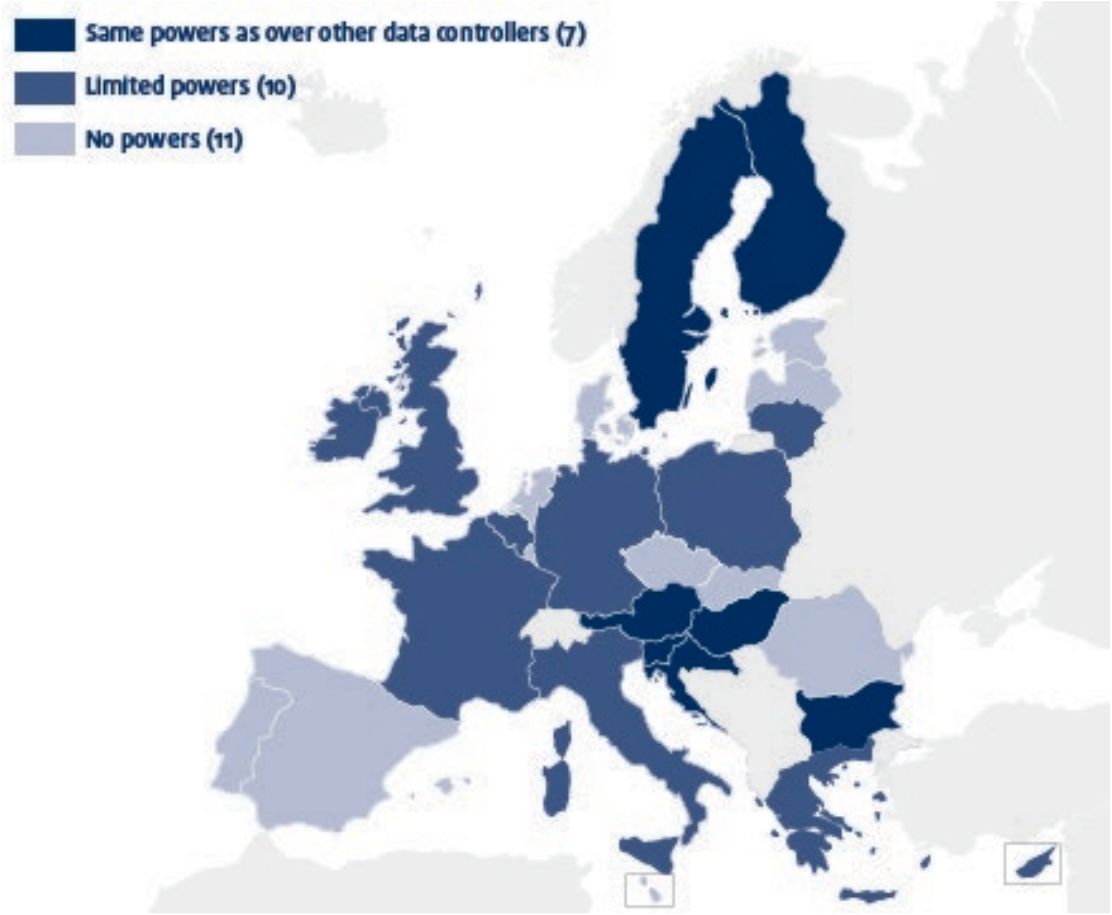
EU Member State	Expert Bodies
CY	Three-Member Committee (*Τριμελής Επιτροπή*) ~~[Not yet in place]~~

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

[22] FRANET in-person interview with the Director of the Central Intelligence Service, 9 November 2022.
[23] FRANET in-person interview with the Director of the Central Intelligence Service, 9 November 2022.

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.

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



The classification 'limited powers' is correct. There was no change to the DPA's powers over the intelligence service since 2017.

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.

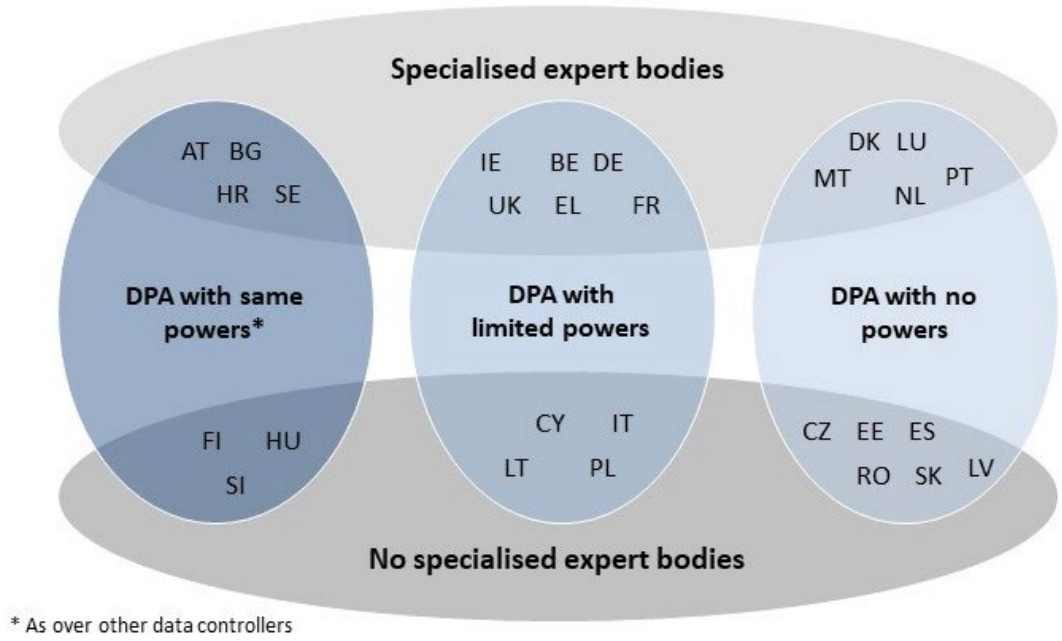
The new law adopted in 2018 to bring the national framework in line with the GDPR does not include the provisions of the old law, which foresaw restriction in the records kept for national security purposes and data revealing the identity of collaborators. Under the 2018 law, the DPA has access to all personal data and information necessary for the performance of its mandate, without any form of confidentiality, with the exception of legal professional privilege.[24] In light of this, perhaps the Cypriot DPA must be moved to the category 'same powers as over other data controllers'. The only differential treatment

[24] In 2018 a new data protection law was adopted to bring the national framework in line with the GDPR: Law on the protection of individuals with regard to the processing of personal data and the free circulation of personal data of 2018 (*Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018*) N. 125(I)/2018, article 25(a).

foreseen in the law between monitoring the work of the CIS as compared to the work of other controllers is a provision stating that the DPA may not examine or discontinue the examination of a complaint on grounds of public interest.[25]

The Director of the Central Intelligence Service suggests that the three-member committee may potentially be seen as a specialised expert body, although its members do not exclusively work on the intelligence service and are not remunerated for their work.[26]

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



The Cypriot DPA should be moved in the category "DPA with same powers" and Cyprus should be moved into the category of countries with specialised expert bodies.

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.

In the case of Cyprus, the column 'Judicial' must also be ticked. Under the 2020 law, judicial authorisation must be sought for targeted surveillance measures affecting specific data subjects.[27]

[25] In 2018 a new data protection law was adopted to bring the national framework in line with the GDPR: Law on the protection of individuals with regard to the processing of personal data and the free circulation of personal data of 2018 (*Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018*) N. 125(I)/2018, article 24(d).

[26] FRANET in-person interview with the Director of the Central Intelligence Service, 9 November 2022.

[27] Cyprus, The Protection of Privacy of Private Communications (Interception of Conversations and Access to Recorded Content of Private Communications) Act of 1996 (92(I)/1996) [*Ο περί Προστασίας του Απόρρητου της Ιδιωτικής Επικοινωνίας (Παρακολούθηση Συνδιαλέξεων και Πρόσβαση σε Καταγεγραμμένο Περιεχόμενο Ιδιωτικής Επικοινωνίας) Νόμος του 1996 (92(I)/1996)*], articles 6 and 8.

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

	Judicial	Executive	Expert bodies	Services
CY		✓		

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).

There is no legislation in Cyprus sanctioning or regulating mass surveillance, although the CIS does have mass surveillance tools in its possession.[28] According to the director of the CIS, Cyprus follows the French model, where surveillance can be carried out with only executive approval.[29]

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

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

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.

Under the 2020 law, the three member committee can raise issues with the Attorney General who, however, retains absolute discretion to decide on prosecutions. The only non-judicial body with its own remedial powers remains the DPA.

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
CY			✓		

2.11. Implementing effective remedies

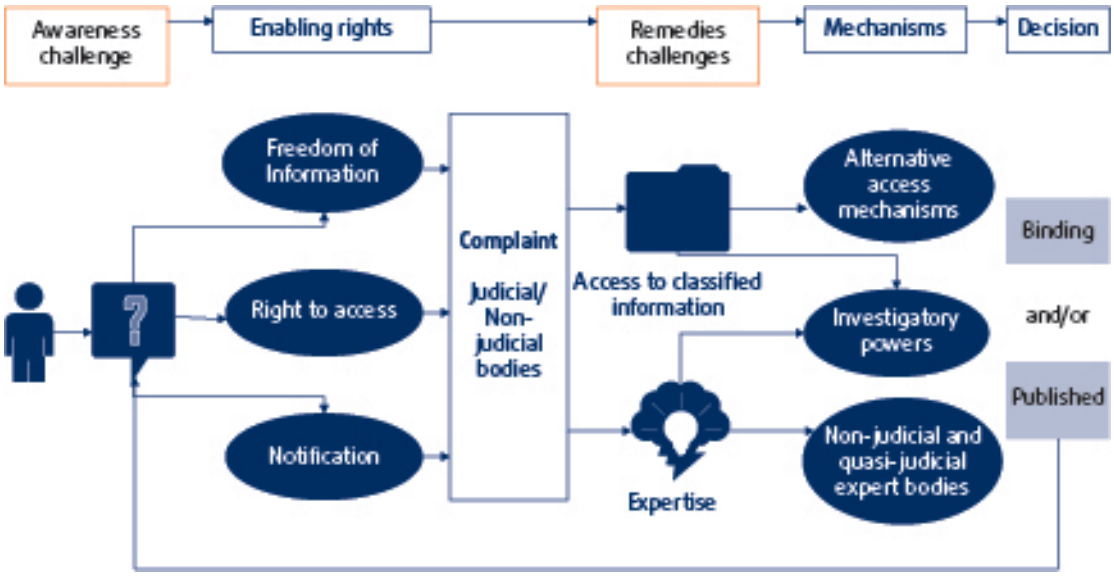
FRANET contractors are requested to confirm that the diagram below (Figure 9 (p. 114) of the FRA 2017 report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to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

Under the 2020 law, the Attorney General is obliged to inform the persons affected by judicial orders authorising the surveillance of their private telephone communications within a reasonable time not exceeding 90 days, or 30 days in the case of written content, from the issue of the judicial order where

[28] Makrides F. (2022), 'Παρακολουθήσεις: Απόρρητες συμβάσεις συνδέουν την ΚΥΠ', 24 October 2022.
[29] FRANET in-person interview with the Director of the Central Intelligence Service, 9 November 2022.

there is reasonable suspicion that the security of the Republic might be at risk. Upon an application from the Attorney General, the court can postpone the date of notification to the data subject if it considers it necessary in the interests of the security of the Republic or of constitutional order or of public safety or of public order or of public health or of public morals or of the protection of the rights or freedoms or of the reputation of others and in order to prevent the disclosure of information obtained in confidence or to prevent the disclosure of information obtained in confidence or to protect the rights or freedoms of others. If the court is convinced that notification may endanger the security of the Republic, then it can order that the notification is not communicated at all.[30] This means that the data subjects affected are not aware of the surveillance of their communications at the time that this takes place in order to take pre-emptive action.

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.

Under the 2018 law purporting to bring the national framework in line with the GDPR, the DPA has access to the data held by the CIS. The DPA's decisions are binding and can be reviewed in court.

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
CY	Commissioner for Personal Data Protection				

[30] Cyprus, The Protection of Privacy of Private Communications (Interception of Conversations and Access to Recorded Content of Private Communications) Act of 1996 (92(I)/1996) [*Ο περί Προστασίας του Απόρρητου της Ιδιωτικής Επικοινωνίας (Παρακολούθηση Συνδιαλέξεων και Πρόσβαση σε Καταγεγραμμένο Περιεχόμενο Ιδιωτικής Επικοινωνίας) Νόμος του 1996 (92(I)/1996)*], article 17.

Note:

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

Source: FRA, 2017

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.

The DPA has powers of accessing data and remedial competence, in the sense that it can issue binding decisions and impose fines which can be collected as a civil debt. It does not have the power to award compensation to victims. Cyprus should be moved in the category with 'DPAs with same powers including full remedial competence', although perhaps with a note that it cannot award compensation.

Figure 10: DPAs' remedial competences over intelligence services