

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

November 2022 Update

Country: Estonia

FRANET contractor: Estonia Human Rights Centre

Author(s) name(s): Liina Laanpere

DISCLAIMER: This document was commissioned under contract as background material for comparative analysis by the European Union Agency for Fundamental Rights (FRA) for the project '*National intelligence authorities and surveillance in the EU*'. The information and views contained in the document do not necessarily reflect the views or the official position of the FRA. The document is made publicly available for transparency and information purposes only and does not constitute legal advice or legal opinion. FRA would like to express its appreciation for the comments on the draft report provided by Estonia that were channelled through the FRA National Liaison Officer.

Table of Contents

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

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](#)

In Estonia, surveillance by intelligence services is regulated in the Security Authorities Act (*Julgeolekuasutuste seadus*)¹. The act defines security authorities as the Estonian Internal Security Service (*Kaitsepolitseiamet*) and the Estonian Foreign Intelligence Service (*Välisluureamet*). In addition, the Estonian Defence Forces Organisation Act (*Kaitseväge korralduse seadus*)² also includes provisions on surveillance by the Defence Forces (*Kaitsevägi*).

Within the reporting period, the Security Authorities Act (*Julgeolekuasutuste seadus*) has been amended four times, though the amendments have been small-scale. In 2017, the Security Authorities Act was amended to ensure better legal clarity – the amendments mainly clarified the regulation of covert measures for collection of information. The amendments do not provide for increased means to collect information, but elaborate on rules for collecting information using undercover staff and recruitment of persons to secret co-operation. Also, the name of the authority “Information Agency” (*Teabeamet*) was replaced with the name “Foreign Intelligence Agency” (*Välisluureamet*) throughout the text of the law. According to the explanatory memorandum, the new name conveys the content of

¹ Estonia, Riigi Teataja, [Security Authorities Act](#) (*Julgeolekuasutuste seadus*), 20 December 2000.

² Estonia, Riigi Teataja, [Estonian Defence Forces Organisation Act](#) (*Kaitseväge korralduse seadus*), 19 June 2008.

the work of the agency better.³ In 2019, the Security Authorities Act was amended to bring it in line with GDPR. The amendments included general principles of data protection (e.g. the manner and scope of collection and processing of information may not excessively adversely affect the fundamental rights of a person compared to the objective pursued by the security authority), as well as a provision on which type of data security authorities process and which rights of data subjects may be restricted, as per GDPR.⁴ In 2022, changes were made concerning service regulations of security authorities officers (regarding probation period, holidays, salary etc.).⁵

In February 2019, the Parliament (*Riigikogu*) adopted a bill to amend the Estonian Defence Forces Organisation Act, which gave the Defence Forces the right, in order to identify and counter a serious threat in their security area, to covertly verify personal data from various databases and to conduct covert surveillance. The explanatory memorandum of the bill explained that currently the law does not provide the Defence Forces with the ability to identify circumstances that pose a threat to the security area of the Defence Forces and there is a lack of basic possibilities to check the personal data of persons involved in security incidents in the immediate vicinity of their territory.⁶ However, the President refused to promulgate the bill, finding parts of it unconstitutional. The President found that the Defence Forces do not have a precise and clear legal framework or legal guarantees for the restriction of fundamental rights in connection with covert processing of personal data.⁷ The Supreme Court (*Riigikohus*) agreed that the bill was unconstitutional, finding that in case of covert surveillance, there must be effective procedural guarantees provided for in the law which would prevent the person from being arbitrarily left uninformed about the processing of their data by the Defence Forces.⁸

The bill was changed according to the Supreme Court's opinion. The general provision which required the Defence Forces to notify a person whose fundamental rights are restricted unless it "endangers the aim of the restriction" was replaced with a provision outlining the exact conditions in which case it is justified not to notify the person of the restriction (e.g. if it endangers another person) and how long the non-notification is justified. During the adoption of the amended version of the bill, the Chancellor of Justice (*Õiguskantsler*) proposed to also amend the Security Authorities Act, as similar issues were present there – according to the Chancellor of Justice, the Security Authorities Act did not ensure sufficient oversight on whether the failure to inform a person about surveillance was justified.⁹ As a result, an amendment to the Security Authorities Act was included in the bill, specifying the provision on notifying persons of surveillance. The previous provision stated that a person whose right to the confidentiality of messages or whose right to the inviolability of home, and family or private life had been restricted must be notified by a security authority of the measures used and the circumstances relating to the restriction of fundamental rights if this does not endanger the aim of the restriction. The new provision provides more specific conditions in case of which the requirement of notification does not apply, similarly to the Defence Forces Organisation Act.¹⁰ In addition, the Chancellor of Justice Act (*Õiguskantsleri seadus*) was amended, adding that the Chancellor of Justice exercises supervision, at

³ Estonia, Parliament (*Riigikogu*), [Julgeolekuasutuste seaduse ja teiste seaduste muutmise seadus 383 SE, Seletuskiri julgeolekuasutuste seaduse ning teiste seaduste muutmise seaduse eelnõu juurde](#).

⁴ Estonia, Parliament (*Riigikogu*), [Isikuandmete kaitse seaduse rakendamise seadus 778 SE](#).

⁵ Estonia, Riigi Teataja, [Politsei ja piirivalve seaduse ning teiste seaduste muutmise seadus \(eriteenistuste ühtlustamine\)](#), 11 May 2022.

⁶ Estonia, Parliament (*Riigikogu*), [Kaitseväge korralduse seaduse muutmise seadus 783 UA](#).

⁷ Estonia, President of the Republic (*Vabariigi President*), [Vabariigi Presidendi taotlus tunnistada Kaitseväge korralduse seaduse muutmise seadus põhiseadusega vastuolus olevaks](#), 14 June 2019.

⁸ Estonia, Supreme Court (*Riigikohus*), [Case No. 5-19-38](#), 19 December 2019.

⁹ Estonia, Chancellor of Justice (*Õiguskantsler*), [Julgeolekuasutuste seaduse § 29 põhiseadusega kooskõlla viimine](#), 10 March 2020.

¹⁰ Estonia, Parliament (*Riigikogu*), [Kaitseväge korralduse seaduse, julgeolekuasutuste seaduse ja õiguskantsleri seaduse muutmise seadus 152 SE](#).

least every two years, over justification for non-notification of persons based on the Security Authorities Act and the Defence Forces Organisation Act.¹¹

In 2021, the Supreme Court found that indiscriminate retention of electronic communications metadata based on § 111¹ (2) of the Electronic Communications Act (*Elektroonilise side seadus*) is in conflict with EU law.¹² The Supreme Court's decision was based on a preliminary ruling of the CJEU requested by the Supreme Court in the same case.¹³ The Electronic Communications Act § 111¹ requires general and indiscriminate retention of metadata by providers of electronic communications services for one year from the date of the communication.¹⁴ The same provision lists the authorities who are entitled to request the stored metadata, including security authorities.¹⁵ The Electronic Communications Act was amended in the end of 2021 in order to transpose Directive (EU) 2018/1972 establishing the European Electronic Communications Code, however, the provision in question was left unchanged.¹⁶

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
EE	Estonian Internal Security Service/ <i>Kaitsepolitseiamet (KAPO)</i>	Estonian Foreign Intelligence Service/ <i>Välisluureamet</i> ¹⁷		Military Intelligence Branch of the Estonian Defense Forces/ <i>Kaitseväge peastaabi luureosakond</i>

According to the explanatory memorandum of the amendment to the Security Authorities Act (*Julgeolekuasutuste seadus*), the new name Estonian Foreign Intelligence Service (*Välisluureamet*) conveys the content of the work of the agency better.¹⁸

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:

¹¹ Estonia, Riigi Teataja, [Chancellor of Justice Act \(Õiguskantsleri seadus\)](#), § 1 (9), 25 February 1999.

¹² Estonia, Supreme Court (*Riigikohus*), [Case No 1-16-6179](#), 18 June 2021.

¹³ Court of Justice of the European Union, [Case C-746/18](#), 2 March 2021.

¹⁴ Estonia, Riigi Teataja, [Electronic Communications Act \(Elektroonilise side seadus\)](#), § 111¹, 8 December 2004.

¹⁵ Estonia, Riigi Teataja, [Electronic Communications Act \(Elektroonilise side seadus\)](#), § 111¹ (11), 8 December 2004.

¹⁶ Estonia, Parliament (*Riigikogu*), [Elektroonilise side seaduse, ehitusseadustiku ja riigilõivuseaduse muutmise seadus 437 SE](#).

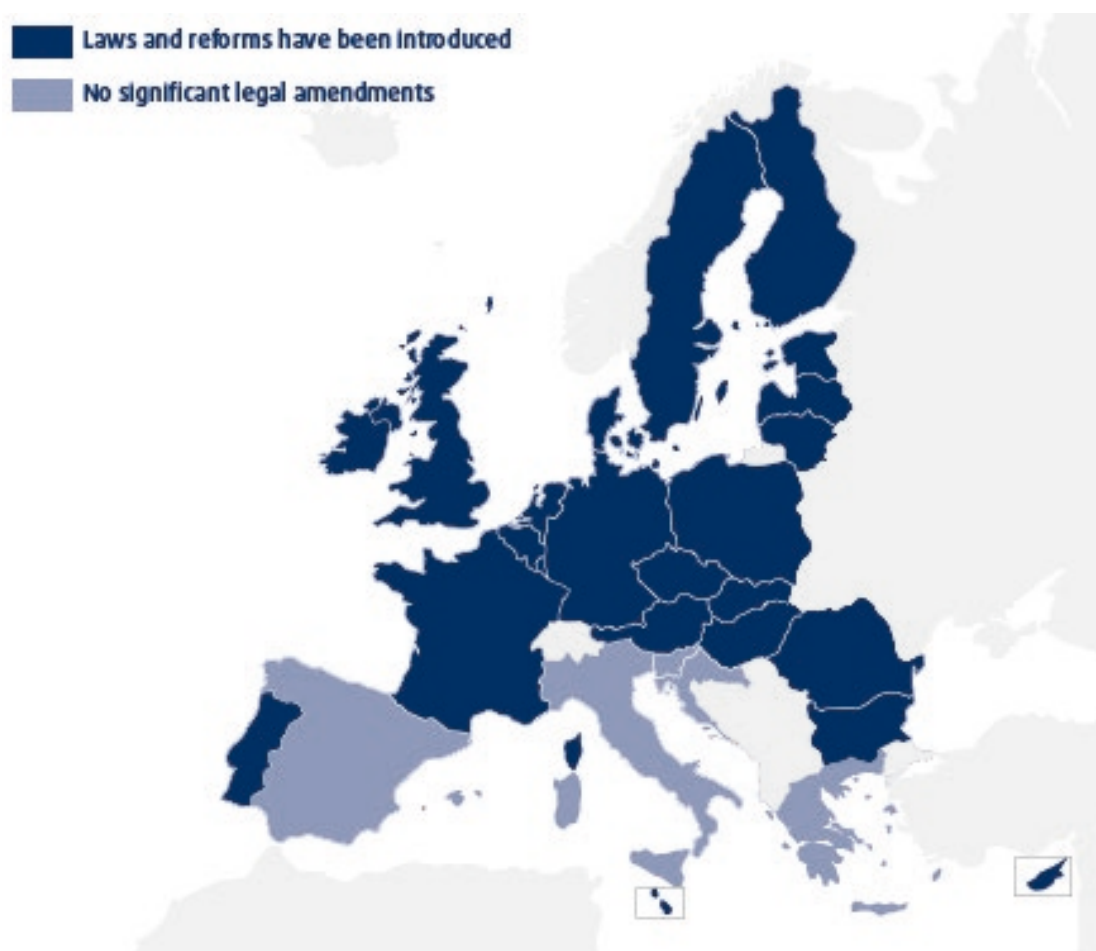
¹⁷ Estonia, Riigi Teataja, [Security Authorities Act \(Julgeolekuasutuste seadus\)](#), § 5, 20 December 2000.

¹⁸ Estonia, Parliament (*Riigikogu*), [Julgeolekuasutuste seaduse ja teiste seaduste muutmise seadus 383 SE, Seletuskiri julgeolekuasutuste seaduse ning teiste seaduste muutmise seaduse eelnõu juurde](#).

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.*

In Estonia, legal framework on surveillance has not been reformed since mid-2017 in a significant manner, only small amendments have been made to the relevant legal acts.

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

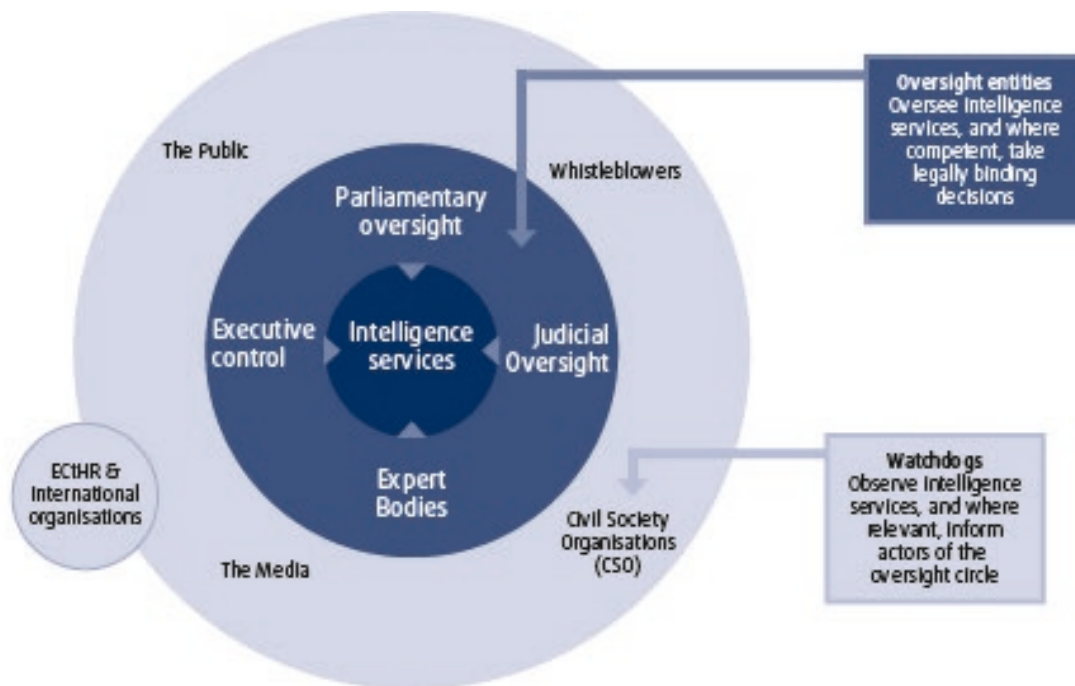


2.3. Intelligence services' accountability scheme

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

The diagram illustrates the situation in Estonia accurately.

Figure 5: Intelligence services' accountability scheme

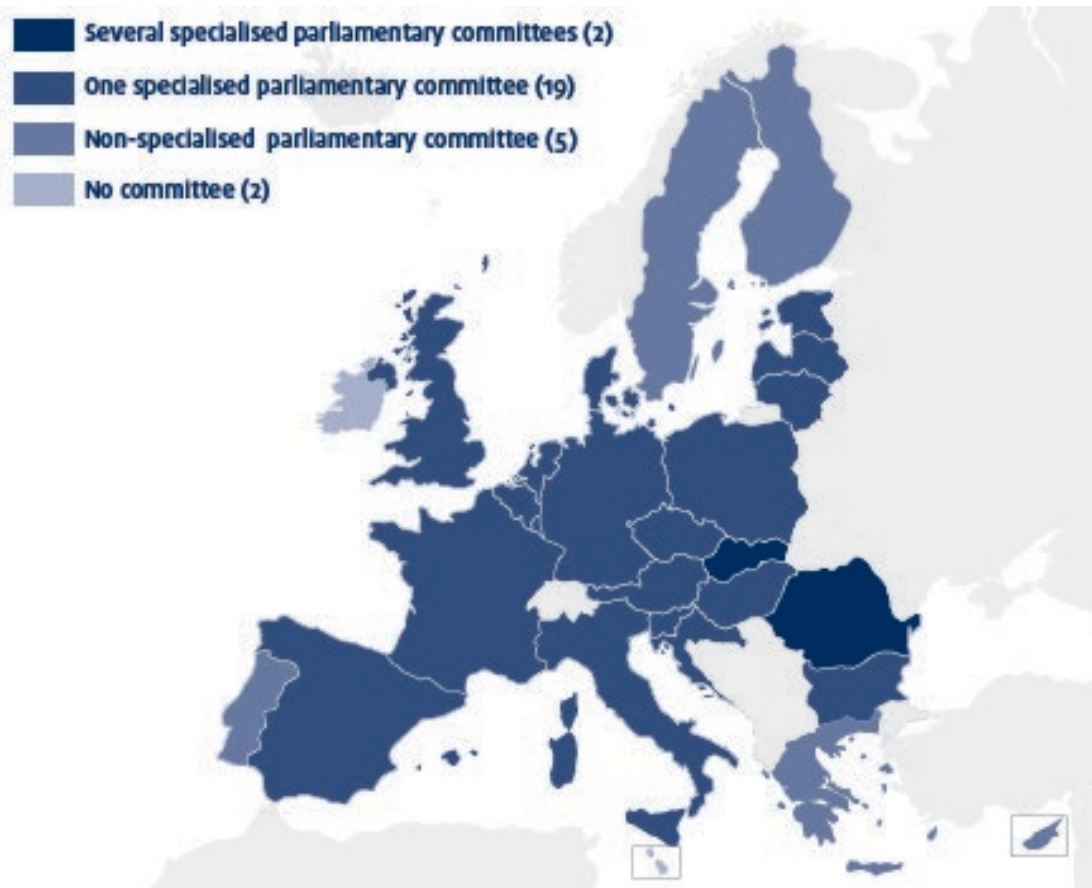


2.4. Parliamentary oversight of intelligence services in EU Member States

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

The map illustrates the situation in Estonia accurately – there is one specialised parliamentary committee which exercises supervision over intelligence services.

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



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

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

The table reflects the situation in Estonia accurately.

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

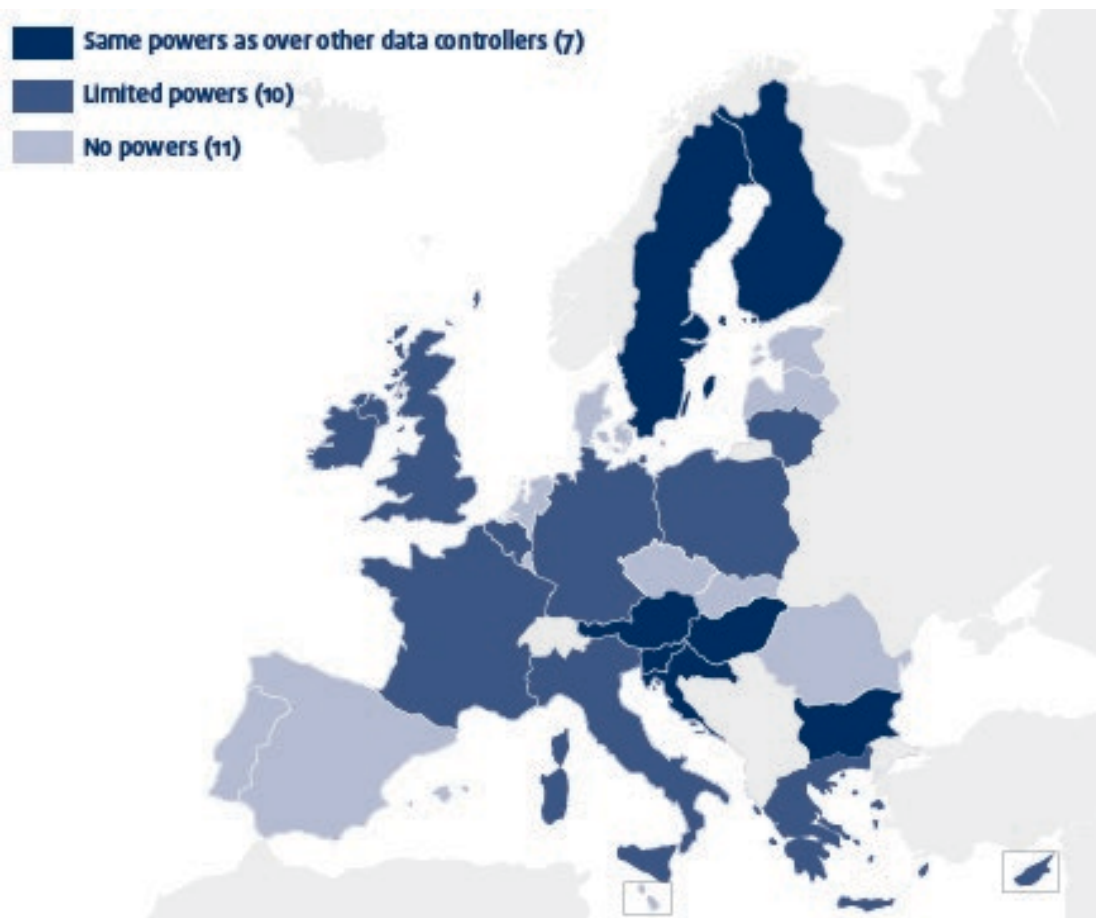
EU Member State	Expert Bodies
EE	N.A.

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

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

The map illustrates the situation in Estonia accurately.

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

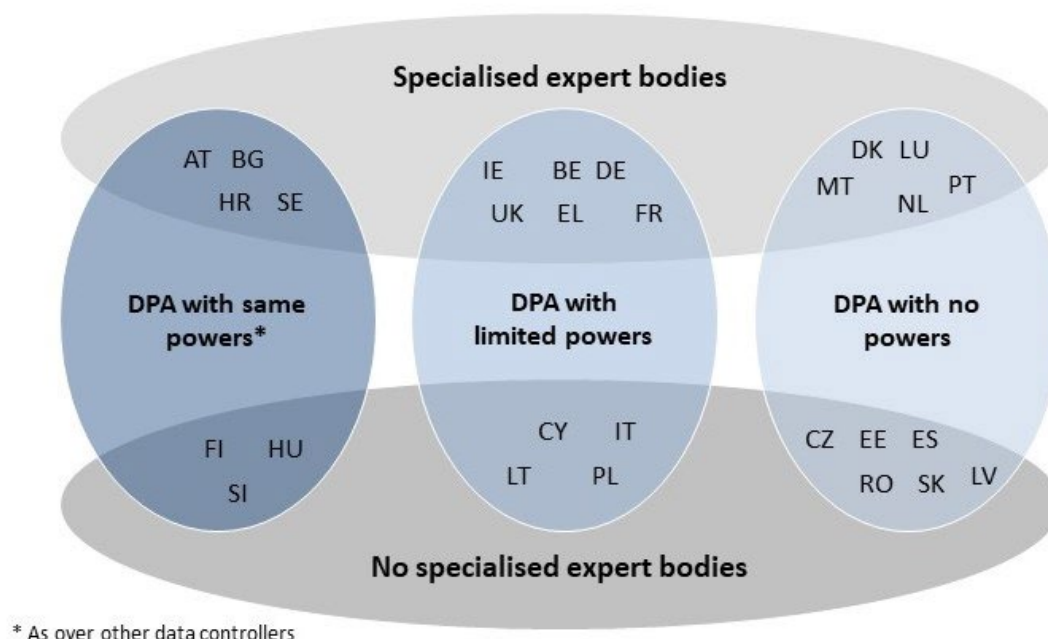


2.7. DPAs' and expert bodies' powers over intelligence techniques, by EU Member State

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

The figure illustrates the situation in Estonia accurately.

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



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

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

The table reflects the situation in Estonia accurately.

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

	Judicial	Executive	Expert bodies	Services
EE	✓			

2.9. Approval/authorisation of general surveillance of communication

All FRANET contractors are requested to check the accuracy of the table below (Table 5 (p. 97) of the FRA 2017 report), and to update/include information as it applies to their Member State (if not previously referred to). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework, in particular where - since 2017 - your Member State regulates these type of surveillance methods (for a definition of general surveillance, see FRA 2017 Report, p. 19).

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

	Judicial	Parliamentary	Executive	Expert
DE		✓		✓

FR			✓	
NL	✓		✓	✓
SE				✓

In Estonia, Electronic Communications Act (*Elektroonilise side seadus*) § 111¹ requires general and indiscriminate retention of metadata by providers of electronic communications services for one year from the date of the communication.¹⁹ The same provision lists the authorities who are entitled to request the stored metadata, including security authorities.²⁰

This refers to metadata retention by providers of electronic communications services rather than general surveillance of communication, Estonia should not be included in the table above.

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.

The table reflects the situation in Estonia accurately.

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
EE					✓

2.11. Implementing effective remedies

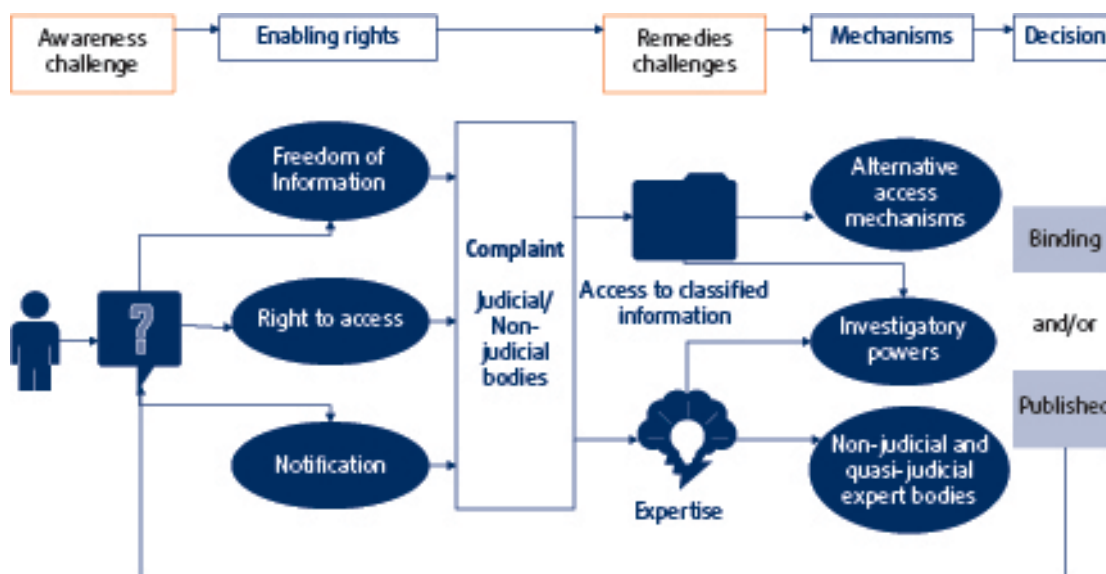
FRANET contractors are requested to confirm that the diagram below (Figure 9 (p. 114) of the FRA 2017 report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to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

The diagram illustrates the situation in Estonia accurately.

¹⁹ Estonia, Riigi Teataja, [Electronic Communications Act](#) (*Elektroonilise side seadus*), § 111¹, 8 December 2004.

²⁰ Estonia, Riigi Teataja, [Electronic Communications Act](#) (*Elektroonilise side seadus*), § 111¹ (11), 8 December 2004.

Figure 9: Implementing effective remedies: challenges and solutions



2.12. Non-judicial bodies' remedial powers

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

The table reflects the situation in Estonia accurately.

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
EE	Chancellor of Justice				

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 figure reflects the situation in Estonia accurately, the Estonian Data Protection Inspectorate (*Andmekaitseinspeksioon*) does not have any remedial competence in this field.

Figure 10: DPAs' remedial competences over intelligence services

