# Short Thematic Report

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

## Legal update

Country: ESTONIA

Version of 15 July 2016

FRANET contractor: Institute of Baltic Studies

Author(s) name(s): Katre Luhamaa, Kristjan Kaldur
Reviewed by: Berit Aaviksoo

# 1 Description of tasks – Phase 3 legal update

## 1.1 Summary

*FRANET contractors are requested to highlight in 1 to 2 pages **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 snap shot of the evolution during the report period (last trimester of 2014 until mid-2016). It should in particular mention:*

1. *the legislative reform(s) that took place or are taking place and highlight the key aspect(s) of the reform.*
2. *the important (higher) court decisions in the area of surveillance*
3. *the reports and inquiry by oversight bodies (parliamentary committees, specialised expert bodies and data protection authorities) in relation to the Snowden revelations*
4. *the work of specific ad hoc parliamentary or non-parliamentary commission (for example the NSA inquiry of the German Parliament) discussing the Snowden revelations and/or the reform of the surveillance focusing on surveillance by intelligence services should be referred to.*

As noted in the 2014 report, the specific term mass surveillance does not exist in Estonian legislation, and there is no specific regulation for mass surveillance measures undertaken by state security or surveillance authorities. The only measure, according to which information about the whole population or large groups of the population is collected and retained, is so-called metadata retention by telecom and internet companies according to Article 111[1] (*primus*) of the Electronic Communications Act (*Elektroonilise side seadus*, hereinafter ECA).[1] The act incorporated into Estonian law the Directive 2006/24/EC (Data Retention Directive) and obliges electronic communications companies to preserve certain data. Articles 112-113 of the ECA relate to the obligation to provide information, notify the European Commission and grant access to the retained data. Article 111[1] (primus) paragraph 11 of the ECA obliges the collected data to be forwarded for a variety of purposes and to a variety of institutions, including the security authorities. This law itself does not specify the basic rights to be protected, therefore the general constitutional and data protection rights apply.

ECA was amended several times in 2015 and 2016. However, most of these amendments were minor in their substance and did not relate directly to the preservation of the data.

Amendments to the Act adopted in December 2015 relate to the obligation to grant access to the communications network and the deletion of the collected data.[2] Paragraphs 5 and 6 of Article 113 of the ECA relating to the obligation to grant access to the communications network were amended. The obligation to keep and preserve independent log files was complemented with an obligation to "*delete or destroy the log files which are older than five years and to forward to the Technical Surveillance Authority, the special security authorities surveillance committee of the Riigikogu (Parliament) and the Office of the Prosecutor*



[1] Estonia, Electronic Communications Act (*Elektroonilise side seadus*), 16 January 2016, available at: www.riigiteataja.ee/en/eli/519022016002/consolide.

[2] Estonia, Law amending the Electronic Communications Act and the Law on the Amendments of the Electronic Communications Act and the State Fees Act (*Elektroonilise side seaduse ning elektroonilise side seaduse ja riigilõivuseaduse muutmise seaduse muutmise seadus*), 24 December 2015, available at: www.riigiteataja.ee/akt/123122015001.

*General a statement which indicates the time period covered by the deleted or destroyed log files, the time and place of their deletion or destruction and the name, personal identification code, and position of the individual who has performed this act*". Similar deletion and informing obligation was included also to the obligation to log applications for transmission of messages.

The functions of the Chancellor of Justice were specified and general right to supervise the observance of fundamental rights by the state agencies were specified to include "the supervision over observance of fundamental rights and freedoms in the organisation of covert collection of personal data and information related thereto, processing, use and supervision by authorities of executive power" (Chancellor of Justice Act (*Õiguskantsleri seadus*, hereinafter CJA)[3] Article 1 para 9). Therefore, there is now an *expressis verbis* authority of the Chancellor of Justice to exercises control over the covert collection of data by the national intelligence services in accordance with the Article $111^{1\ (primus)}$ of the ECA. This control is limited, as, specified in Articles $11^{1\ (primus)}$ and $37^{2\ (secundus)}$ of the CJA, the chancellor does not have unlimited access to state secrets including information on the international cooperation of intelligence services.[4]

During the reference period, there were no substantive amendments to the Security Authorities Act (*Julgeolekuasutuste seadus*)[5] nor to the regulation or structure of the national intelligence services.

In terms of judicial reviews, the analysis department of the Supreme Court of Estonia (*Riigikohus*) has analysed[6] the legal framework and rights connected to the surveillance and data retention entailed in Article $111^{1\ (primus)}$ of the Electronic Communications Act (*Elektroonilise side seadus*).[7] The Criminal Law Chamber of the Supreme Court (*Riigikohtu kriminaalkolleegium*) also dealt with the effect of the decision of CJEU case C-293/12 on Estonian legislation in its decision No. 3-1-1-51-14.[8] It concluded that the invalidity of an EU Directive did not necessarily mean that the respective national legislation was also invalid. This is especially true in cases in which the EU legal act leaves the states some discretion or flexibility. The court found that there were sufficient procedural guarantees in place, and that the surveillance measures followed the principle of *ultima ratio* and were proportional. Although the case related to the use of data in criminal proceedings, this decision has relevance also for the general application of Article $111^{1\ (primus)}$ of the ECA.



[3] Estonia, Chancellor of Justice Act (*Õiguskantsleri seadus*), 1 May 2016, available at: https://www.riigiteataja.ee/en/eli/507042016001/consolide.
[4] Estonia, Chancellor of Justice Act (*Õiguskantsleri seadus*), 1 May 2016, available at: https://www.riigiteataja.ee/en/eli/507042016001/consolide
[5] Estonia, Security Authorities Act (*Julgeolekuasutuste seadus*), State Gazette I, 17.12.2015, 38, available at: www.riigiteataja.ee/en/eli/504022016001/consolide.
[6] Estonia, Aleksander Lott (2015), 'Surveillance for the protection of the Constitutional order' (*Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis*), pp. 31-32, Estonian Supreme Court (*Riigikohus*), available at: http://www.riigikohus.ee/vfs/1906/PKK%20j%E4litustegevuse%20anal%FC%FCs.pdf
[7] Estonia, Electronic Communications Act (*Elektroonilise side seadus*), 16 January 2016, available at: https://www.riigiteataja.ee/en/eli/519022016002/consolide.
[8] Estonia, The Supreme Court (*Riigikohus*), Decision of the Criminal Law Chamber No. 3-1-1-51-14, 23 February 2015, available at: www.nc.ee/?id=11&tekst=222577237.

In 2015 and 2016, the Chancellor of Justice carried out a two-part analysis on the constitutionality of the Article 111[1] (*primus*) of the Electronic Communications Act[9] (*Elektroonilise side seadus*) with the aim of analysing whether the collection of data by communications enterprises has been in accordance with the Estonian Constitution. In 2015, the Chancellor concluded that although Article 111[1] (*primus*) of the ECA limits the right to privacy, it was not possible to conclude that this regulation violated rights protected by the Constitution.[10] This limitation is in her opinion proportional and necessary in a democratic society and, thus, is in accordance with the right to privacy. The Chancellor, nevertheless, expressed a concern relating to the possible misuse of the data; there are no adequate legal guarantees in place to prevent the mismanagement and misuse of the preserved data. In 2016, in the second part of the analysis, the Chancellor of Justice concluded that the regulation in place is unbalanced and incomplete and should be revised as a whole, as it does not include special procedural guarantees, supervision or other limiting requirements.[11]

On April 2016, the Security Authorities Surveillance Committee of the Estonian Parliament (*Riigikogu Julgeolekuasutuste järelevalve erikomisjon*) conducted a random sample check of the surveillance and information files of the Estonian Internal Security Service (*Kaitsepolitseiamet*) to verify the lawfulness of surveillance activities.[12] The Committee examined data in around 10% of the surveillance and information files, collected between 2013 and 2014. The Committee found that the surveillance activities were conducted in compliance with the rulings issued by the judge and within the timeframe set out in the ruling. The Committee also found that in the cases where the persons were *not* notified of the restriction of their fundamental rights, the files had corresponding legal references as well as authorisations given by the prosecutor. There is no information on the precise nature of the sample i.e. whether such files were solely related to the surveillance done in the framework of criminal proceedings or if it included other cases as well.

The Code of Criminal Procedure Article 126[17] (septimus decimus) stipulates the creation of the surveillance activities information system; the system enables electronic access to surveillance documents.[13] This information system on surveillance activities



[9] Estonia, Electronic Communications Act (*Elektroonilise side seadus*), 16 January 2016, available at: www.riigiteataja.ee/en/eli/519022016002/consolide.

[10] Estonia, Chancellor of Justice (*Õiguskantsler*), 20 July 2015, 'Opinion of the Legal Chancellor on the Constitutionality of the ECA Article 111[1]' (*Õiguskantsleri seisukoht elektroonilise side seaduse Artikkel 111[1] põhiseaduspärasuse kohta*), available at (in Estonian): oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_seisukoht_vastuolu_mittetuvastamise_kohta_elektroonilise_side_andmete_kogumine_sideettevotete_poolt.pdf

[11] Estonia, Chancellor of Justice (*Õiguskantsler*), 22 April 2016, 'Constitutionality of the obligation to preserve data on the basis of the ECA Article 111[1]' (*Elektroonilise side seaduse Article 111[1] alusel sideandmete töötlemise põhiseaduspärasus*), in particular para 29, available at: oiguskantsler.ee/et/seisukohad/seisukoht/elektroonilise-side-seaduse-ss-111-prim-alusel-sideandmete-tootlemise.

[12] Estonia, Riigikogu pressiteenistus (2016), 'Julgeolekuasutuste erikomisjon kontrollis KAPO jälitustegevust', press release, 18.04.2016, available at: http://www.riigikogu.ee/pressiteated/julgeolekuasutuste-jarelvalve-erikomisjon-et-et/julgeolekuasutuste-erikomisjon-kontrollis-kapo-jalitustegevust/

[13] Estonia, Code of Criminal Procedure (*Kriminaalmenetluse seadustik*), 16 January 2016, available at: https://www.riigiteataja.ee/en/eli/ee/527012016001/consolide/current.

(*jälitustoimingute infosüsteem*, JÄTIS) was launched in 2015. The system facilitates easier access to the collected information. It should be noted that this change relates also to the use of information collected on the basis of Article 111[1] (*primus*) of the Electronic Communications Act[14] (*Elektroonilise side seadus*) in criminal proceedings.

Furthermore, the Snowden case has been mentioned in three speeches by the Members of the Parliament during Parliamentary sessions.[15] However, none of these were substantive in their content. Thus, the Snowden case was not discussed in official parliamentary debates, and is not visible in the official records of the various surveillance committees. This was confirmed by the relevant ministries and national security services.[16] Replies to information requests on this issue were received from the following institutions:

- Internal Security Service (*Kaitsepolitseiamet*),
- Security Authorities Surveillance Committee of the Riigikogu (*Riigikogu Julgeolekuasutuste järelevalve erikomisjon)*,
- Ministry of Internal Affairs (*Siseministeerium)*,
- Chancellor of Justice (*Õiguskantsler*),
- Data Protection Inspectorate (*Andmekaitse Inspektsioon*),
- Estonian Human Rights Centre (*Eesti Inimõiguste Keskus*).

There are no (public) reports by the experts or human rights institutions on the Snowden case,[17] nor has it given cause to any internal investigation or research.[18]



[14] Estonia, Electronic Communications Act (*Elektroonilise side seadus*), 16 January 2016, available at: https://www.riigiteataja.ee/en/eli/519022016002/consolide.
[15] Estonia, Verbatim Records of the Parliament (*Riigikogu Stenogrammid*) from 7 May 2014, 14 October 2013, 9 September 2013, available at (in Estonian): http://stenogrammid.riigikogu.ee/.
[16] Estonia, Estonian Internal Security Service (*Kaitsepolitseiamet*), e-mail correspondence, 1 June 2016. Estonia, Security Authorities Surveillance Committee of the Riigikogu (*Riigikogu Julgeolekuasutuste järelevalve erikomisjon)*, e-mail correspondence, 2 June 2016. Estonia, Ministry of Internal Affairs (*Siseministeerium)*, e-mail correspondence, 30 May 2016.
[17] Estonia, Estonian Human Rights Centre (*Eesti Inimõiguste Keskus*), e-mail correspondence, 11 May 2016.
[18] Estonia, Estonian Internal Security Service (*Kaitsepolitseiamet*), e-mail correspondence, 1 June 2016. Estonia, Security Authorities Surveillance Committee of the Riigikogu (*Riigikogu Julgeolekuasutuste järelevalve erikomisjon)*, e-mail correspondence, 2 June 2016. Estonia, Ministry of Internal Affairs (*Siseministeerium)*, e-mail correspondence, 30 May 2016.

## 1.2 International intelligence services cooperation

*FRANET contractors are requested to provide information, in 1 to 2 pages **maximum**, on the following two issues, drawing on a recent publication by Born, H., Leigh, I. and Wills, A. (2015), Making international intelligence cooperation accountable, Geneva, DCAF.*[19]

1. *It is assumed that in your Member State international cooperation between intelligence services takes place. Please describe the legal basis enabling such cooperation and any conditions that apply to it as prescribed by law. If the conditions are not regulated by a legislative act, please specify in what type of documents such cooperation is regulated (e.g. internal guidance, ministerial directives etc.) and whether or not such documents are classified or publicly available.*
2. *Please describe whether and how the international cooperation agreements, the data exchanged between the services and any joint surveillance activities, are subject to oversight (executive control, parliament oversight and/or expert bodies) in your Member States.*

There is no national legislation that regulates the international cooperation of surveillance bodies of Estonia. Although, the Security Authorities Act (*Julgeolekuasutuste seadus*, SAA) does oblige domestic cooperation between national bodies; it also regulates the legal status of the employees working temporarily in international organisations[20], there is no similar legislation in place for international cooperation. Communications from the Security Authorities as well as the relevant Ministries confirmed that it is not possible to identify such specific legislation or international treaties. International cooperation of security authorities is classified, in accordance with Article 9 paragraph 1 of the State Secrets and Classified Information of Foreign States Act (*Riigisaladuse ja salastatud välisteabe seadus*)[21], as a state secret, and this information is thus, not available.[22]

The general oversight over the intelligence services including international cooperation between intelligence services is exercised by the Chancellor of Justice (*Õiguskantsler*) and the Security Authorities Surveillance Committee of the Riigikogu (*Riigikogu Julgeolekuasutuste järelevalve erikomisjon*, SCOSA)[23]. The SCOSA was created on the basis of Article 36 of the Security Authorities Act (*Julgeolekuasutuste seadus*)[24] and its main function is the "*supervision over authorities of executive power in matters relating to the*



[19] www.dcaf.ch/Publications/Making-International-Intelligence-Cooperation-Accountable
[20] Estonia, Security Authorities Act (*Julgeolekuasutuste seadus*), 1 January 2016, available at: https://www.riigiteataja.ee/en/eli/504022016001/consolide.
[21] Estonia, State Secrets and Classified Information of Foreign States Act (*Riigisaladuse ja salastatud välisteabe seadus*), State Gazette I, 12.03.2015, 46, available online: https://www.riigiteataja.ee/en/eli/515012016001/consolide.
[22] Estonia, Estonian Internal Security Service (*Kaitsepolitseiamet*), e-mail correspondence, 1 June 2016. Estonia, Security Authorities Surveillance Committee of the Riigikogu (*Riigikogu Julgeolekuasutuste järelevalve erikomisjon)*, e-mail correspondence, 2 June 2016. Estonia, Ministry of Internal Affairs (*Siseministeerium)*, e-mail correspondence, 30 May 2016.
[23] For a general overview and the mandate and functions of the SCOSA see Estonia, Security Authorities Surveillance Committee of the Riigikogu (*Riigikogu Julgeolekuasutuste järelevalve erikomisjon*), available at: www.riigikogu.ee/en/parliament-of-estonia/committees/security-authorities-surveillance-select-committee/
[24] Estonia, Security Authorities Act (*Julgeolekuasutuste seadus*), 1 January 2016, available at: www.riigiteataja.ee/en/eli/504022016001/consolide.

*activities of the security authorities and surveillance agencies, including guarantee of fundamental rights and efficiency of the work of the security authorities and surveillance agencies, and also in matters relating to supervision exercised over the security authorities and surveillance agencies.*" However, in the opinion of the Estonian Human Rights Centre (*Eesti Inimõiguste Keskus*), SCOSA oversight is generally ineffective.[25] This opinion relates partly to the members of SCOSA lack of security clearances, which limits their ability to gain access to relevant information. They also found that SCOSA members are generally uninterested in conducting effective oversight and the committee's limited capacity, having only two persons on staff compared to many more in the security authorities making it much more asymmetric than in other countries.[26]The oversight exercised by the Chancellor of Justice is also limited, due to Articles$11^{1\ (primus)}$ and $37^{2\ (secundo)}$ of the Chancellor of Justice Act, which does not give her automatic access to state secrets relating to the work of the security authorities or international co-operation of these authorities.[27] Article $11^{1\ (primus)}$ (6) 4 of the same Act stipulates that: "*The Chancellor of Justice shall have no access to classified information of foreign states or state secrets about joint international operations of security agencies or information forwarded by foreign states or international organisations, if the person who forwarded the information has not granted consent for access*". According to the Estonian Internal Security Service (*Kaitsepolitseiamet*), all such information and the exact content of the international cooperation is classified as a state secret.[28]

Communication with the SCOSA seems to support these findings. Although it confirmed that it oversees the work of the security agencies including their international cooperation, it was not able to specify the frequency of such overview or the types of analysis performed as it was all classified as a state secret.[29]

The Constitutional Review Chamber of the Supreme Court (*Põhiseaduslikkuse järelevalve kolleegium*) published an analysis "Surveillance aimed at the protection of the Constitutional order" where it analysed the effect of different surveillance measures on basic rights. The report covers all areas of surveillance including the work of the Estonian Internal Security Service (*Kaitsepolitseiamet*), its international cooperation and gives an overview of the relevant legislation as well as its findings regarding the efficiency of the oversight of such measures.[30] The report's main criticism relates to the formality of the supervision of the SCOSA as it mainly deals with the control of the documented surveillance but does not have



[25] Estonia, Estonian Human Rights Centre (*Eesti Inimõiguste Keskus*), e-mail correspondence, 11 May 2016.
[26] Estonia, Estonian Human Rights Centre (*Eesti Inimõiguste Keskus*) (2014), 'National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies', short-thematic report of Estonia conducted for FRANET.
[27] Estonia, Chancellor of Justice Act (*Õiguskantsleri seadus*), 1 May 2016, available at: https://www.riigiteataja.ee/en/eli/507042016001/consolide
[28] Estonia, Estonian Internal Security Service (*Kaitsepolitseiamet*), e-mail correspondence, 1 June 2016.
[29] Estonia, Security Authorities Surveillance Committee of the Riigikogu (*Riigikogu Julgeolekuasutuste järelevalve erikomisjon)*, e-mail correspondence, 2 June 2016.
[30] Estonia, Aleksander Lott (2015), 'Surveillance for the protection of the Constitutional order' (*Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis*), pp. 31-32, Estonian Supreme Court (*Riigikohus*), available at: http://www.riigikohus.ee/vfs/1906/PKK%20j%E4litustegevuse%20anal%FC%FCs.pdf.

the capability to undertake its own activism.[31] Furthermore, the report concludes that it is "*questionable whether the SCOSA has the competence and resources needed to exercise effective control*".[32]

## 1.3 Access to information and surveillance

*FRANET contractors are requested to summarise, in 1 to 2 pages **maximum**, the legal framework in their Member State in relation to surveillance and access to information.*
*Please refer to the Global Principles on National Security and the Right to Information (the Tshwane Principles)[33] (in particular Principle 10 E. – Surveillance) and describe the relevant national legal framework in this context. FRANET contractors could in particular answer the following questions:*

1. *Does a complete exemption apply to surveillance measures in relation to access to information?*
2. *Do individuals have the right to access information on whether they are subject to surveillance?*

In general, Article 44 of the Constitution (*Põhiseadus*)[34] grants everyone access to public information. However, Article 44 para 2 allows exempting information whose disclosure is prohibited by law. Access to public information is generally regulated under the Public Information Act (*Avaliku teabe seadus*, hereinafter PIA).[35] Public information is everything which is obtained or created during the performance of public duties provided by law or legislation issued on the basis thereof (Article 3 para 1 of PIA). It is possible to limit access to this information in specialised legal acts (Article 3 para 2 of PIA). According to Article $3^{1\,(primus)}$ para 3 of the PIA, when giving information for public use, protection of the national security has to be ensured, and, when necessary, appropriate restrictions have to be established.

PIA is not applicable to "*information which is classified as a state secret or as classified foreign information, until the expiry of classification of such information*" (Article 2 para 2 point 1 of the PIA). The same is stressed in the State Secrets and Classified Information of Foreign States Act (*Riigisaladuse ja salastatud välisteabe seadus*)[36] which generally treats as a state secret both national (Article 7 and 8 of the SSCIFSA) and international (Article 6 and 7 of the SSCIFSA) surveillance that is not directly connected to the specific criminal cases.



[31] Similar criticism was presented in Estonia, M. Kruusamäe, T. Reinthal. 'Ex-ante Judicial Control of the Surveillance in Estonia: Analysis of the Court Practice' (*Jälitustegevuse kohtulik eelkontroll Eestis: kohtupraktika analüüs*) Tartu 2013, p 29, available at (in Estonian): www.nc.ee/?id=1252.
[32] Estonia, Aleksander Lott (2015), 'Surveillance for the protection of the Constitutional order' (*Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis*), p 31, Estonian Supreme Court (*Riigikohus*), available at: http://www.riigikohus.ee/vfs/1906/PKK%20j%E4litustegevuse%20anal%FC%FCs.pdf
[33] www.right2info.org/exceptions-to-access/national-security/global-principles#section-10
[34] Estonia, Constitution (*Põhiseadus*), 21 May 2015, available at: www.riigiteataja.ee/en/eli/521052015001/consolide.
[35] Estonia, Public Information Act (*Avaliku teabe seadus*), 18 January 2016, available at: www.riigiteataja.ee/en/eli/518012016001/consolide
[36] Estonia, State Secrets and Classified Information of Foreign States Act (*Riigisaladuse ja salastatud välisteabe seadus*), 15 January 2016, available at: www.riigiteataja.ee/en/eli/ee/515012016001/consolide

Exempted is only the information "*the disclosure of which would not damage the security of the Republic of Estonia*". Thirdly, the Personal Data Protection Act (*Isikuandmete kaitse seadus*, PDPA)[37] applies only to the processing of state secrets containing personal data, if such processing is provided for in 1) Convention from 19 July 1990 Applying the Schengen Agreement[38]; or 2) Convention from 26 July 1995 based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office[39]. Other types of data is exempted from the application of the PDPA. In practice, the information collected through surveillance by the security authorities is classified and the general public does not have any access to it.

Surveillance information collected in accordance with other legal acts potentially falls under the PIA unless access to such information is restricted in these specific legal acts (Article 35 para 1 point 19 of the PIA). Therefore, the limitations provided in the specialised laws are of central importance for establishing, whether or not the public or the individual on whom the surveillance has been conducted has access to specific information collected by the national intelligence agencies.

Access for the use of the data collected under Article $111^{1\ (primus)}$ of the Electronic Communications Act[40] (*Elektroonilise side seadus*) is given to a limited list of agencies together with the specific authorisation required for it (Article $111^{1\ (primus)}$ para 11 of the ECA); this list includes a security authority and does not include in any form the general public nor the individuals on whom such data was collected. The ECA provides access to individuals only in the case of a data breach[41]. According to Article $102^{1\ (primus)}$ paragraph 4 of the Electronic Communications Act[42] (*Elektroonilise side seadus*), there is an obligation to inform individuals "*If the personal data breach may adversely affect the personal data or privacy of a subscriber or a user whose data has been submitted to the communications undertaking by the subscriber, the communications undertaking is required to notify the subscriber thereof at the earliest opportunity.*" This includes also an obligation to inform individuals on the data breach relating to the information retained on the basis of Article $111^{1\ (primus)}$ of the ECA as the data retained under this provision is not excluded from the application of this article. There is no other obligation to give access to or inform individuals



[37] Estonia, Personal Data Protection Act (*Isikuandmete kaitse seadus*), 6 January 2016, available at: www.riigiteataja.ee/en/eli/507032016001/consolide
[38] European Communities, Protocol (No 19) on the Schengen Acquis Integrated into the Framework of the European Union, Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, OJ C 202, 7.6.2016, p. 1–388.
[39] European Communities, Council Act of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office, OJ C 316, 27/11/1995.
[40] Estonia, Electronic Communications Act (*Elektroonilise side seadus*), 16 January 2016, available at: www.riigiteataja.ee/en/eli/519022016002/consolide.
[41] Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of communications services. (Article $102^{1\ (primus)}$ para 1 of the ECA)
[42] Estonia, Electronic Communications Act (*Elektroonilise side seadus*), 16 January 2016, available at: www.riigiteataja.ee/en/eli/519022016002/consolide.

on the use of data retained on the basis of Article 111[1 (*primus*)] of the ECA, unless the retained data is used in criminal proceedings.

The application of the Personal Data Protection Act (*Isikuandmete kaitse seadus*, PDPA)[43] is excluded in relation to the data stored on the basis of the ECA as it is *lex specialis*, to the PDPA.

When the data retained in accordance with the Article 111[1 (*primus*)] paragraph 11 of the Electronic Communications Act[44] (*Elektroonilise side seadus*) is used for the criminal surveillance, there are different measures in place to protect the rights of the individuals including judicial control of the surveillance. According to the Article 126[1 (primus)] paragraph 2 of the Code of Criminal Procedure (*Kriminaalmenetluse seadustik*, CCP), the use of the surveillance is an *ultima ratio* measure.[45] Furthermore, the Code of Criminal Procedure regulates the notification of the surveillance activities (Article 126[13 (tertius decimus)] para 1of the CCP) after the expiration of the term of the surveillance permission: "*the surveillance agency shall immediately notify the person with respect to whom the surveillance activities were conducted and the person whose private, or family life was significantly violated by the surveillance activities and who was identified in the course of the proceedings. The person shall be notified of the time and type of surveillance activities conducted with respect to him or her*".[46] They are also granted access to the collected information (Article 126[14 (quartus decimus)] of the CCP). There is, however, no independent analysis on the practical implementation of this requirement.

Furthermore, there is no substantive analysis nor other information available on the surveillance in counterintelligence or mass-surveillance. Both the Estonian Information Board as well as the Estonian Internal Security Service publish only general annual reviews on its activities that include selected general information.[47]



[43] Estonia, Personal Data Protection Act (*Isikuandmete kaitse seadus*), 6 January 2016, available at: www.riigiteataja.ee/en/eli/507032016001/consolide

[44] Estonia, Electronic Communications Act (*Elektroonilise side seadus*), 16 January 2016, available at: www.riigiteataja.ee/en/eli/519022016002/consolide.

[45] Estonia, Code of Criminal Procedure (*Kriminaalmenetluse seadustik*), 16 January 2016, available at: www.riigiteataja.ee/en/eli/ee/527012016001/consolide/current.

[46] Estonia, Code of Criminal Procedure (*Kriminaalmenetluse seadustik*), 16 January 2016, available at: www.riigiteataja.ee/en/eli/ee/527012016001/consolide/current.

[47] See e.g. Estonian Internal Security Service (*Kaitsepolitseiamet*), Annual Review 2015 (*Aastaraamat 2015*), available at: kapo.ee/sites/default/files/public/content_page/aastaraamat-2015.pdf; and Estonia, Information Board (*Teabeamet*), 2016, 'International Security and Estonia (*Eesti rahvusvahelises julgeolekukeskkonnas*), pp. 10, 44, available at: www.teabeamet.ee/pdf/2016-en.pdf.

## 1.4 Update the FRA report

*FRANET contractors are requested to provide up-to-date information based on the FRA report on Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – mapping Member States' legal framework.*

*Please take into account the **Bibliography/References** (p. 79 f. of the FRA report), as well as the **Legal instruments index – national legislation** (p. 88 f. the FRA report) when answering the questions.*

**Introduction**

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

No relevant data to be added or updated.

**1 Intelligence services and surveillance laws**

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

No relevant data to be added or updated.

**1.1 Intelligence services**

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

No relevant data to be added or updated.

**1.2 Surveillance measures**

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

No relevant data to be added or updated.

## 1.3 Member States' laws on surveillance

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

[p 19] We would like to point out that Estonian Internal Security Service (as well as Information Board) has an additional and separate act stating the objectives, functions, structure and management of the service.[48] We are slightly unsure on which grounds Estonia was included in the first group in FRA report, and if this additional regulation is a necessary condition to be included in the second group of countries (i.e. with a complex system of laws etc.).

**FRA key findings**

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

No relevant information to be added.

## 2 Oversight of intelligence services

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

No relevant information to be added.

## 2.1 Executive control

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*



[48] Estonia, The Statute of the Internal Security Service (*Kaitsepolitseiameti põhimäärus*), 10 November 2014, available at: https://www.riigiteataja.ee/akt/107112014001.

No relevant information to be added.

## 2.2 Parliamentary oversight

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

No relevant information to be added.

### 2.2.1 Mandate

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

No relevant information to be added.

### 2.2.2 Composition

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Information up to date.

### 2.2.3 Access to information and documents

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

No relevant information to be added.

### 2.2.3 Reporting to parliament

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*

3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

   No relevant information to be added.

## 2.3 Expert oversight

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

   No relevant information to be added.

### 2.3.1 Specialised expert bodies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

   The Chancellor of Justice (*Õiguskantsler*) can be added as a specialised expert body for EE. Since 1 January 2015, the law specially points out that the Chancellor of Justice has a right and an obligation to oversee surveillance from the perspective of fundamental rights in accordance with Article 1 paragraph 9 of the Chancellor of Justice Act (*Õiguskantsleri seadus*).[49]

   According to Article 1, paragraph 9, the Chancellor of Justice exercises supervision over the observance of fundamental rights and freedoms, during the covert collection of personal data, processing, use and supervision by the authorities of executive power.

   Therefore, the Chancellor of Justice also exercises control over covert collection of data by the national intelligence services in accordance with the Article $111^{1\,(primus)}$ of the ECA. This control is limited due to Articles$11^{1\,(primus)}$ and $37^{2\,(secundus)}$ of the CJA, which specifies that the chancellor does not have access to state secrets including information on the international cooperation of the intelligence services.

### 2.3.2 Data protection authorities

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*



[49] Estonia, Chancellor of Justice Act (*Õiguskantsleri seadus*), 1 May 2016, available at: https://www.riigiteataja.ee/en/eli/507042016001/consolide.

14

2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

As the Chancellor of Justice has limited competences to oversee surveillance activities, the position of Estonia could be changed to the group of DPA with no powers and Specialised expert bodies.

According to the Estonian Data Protection Inspectorate (*Andmekaitse Inspektsioon*) they do not have authority to control the surveillance done by the national intelligence services.[50]

**2.4 Approval and review of surveillance measures**

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

No relevant information to be added.

**FRA key findings**

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

No relevant information to be added.

**3 <u>Remedies</u>**

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

No relevant information to be added.



[50] Estonia, Estonian Data Protection Inspectorate (*Andmekaitse Inspektsioon*), e-mail correspondence, 8 June 2016.

15

## 3.1 A precondition: obligation to inform and the right to access

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Information up to date.

## 3.2 Judicial remedies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

No relevant information to be added.

### 3.2.1 Lack of specialisation and procedural obstacles

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

No relevant information to be added.

### 3.2.2 Specialised judges and quasi-judicial tribunals

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

No relevant information to be added.

## 3.3 Non-judicial remedies: independence, mandate and powers

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*

3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

No relevant information to be added.

### 3.3.1 Types of non-judicial bodies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

Since 1 January 2015, the Chancellor of Justice explicitly has authority to oversee surveillance from the perspective of the protection of fundamental rights (Article 1 (9) of the Chancellor of Justice Act), including dealing with individual complaints. However, the decisions of the Chancellor are not binding.[51]

### 3.3.2 The issue of independence

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

No relevant information to be added.

### 3.3.3 Powers and specialisation of non-judicial remedial bodies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

EE is missing from the figure 6. Individuals have the right to make petitions to the Chancellor of Justice; it is specified that from 1 January 2015 they might also include complaints on surveillance measures (Article 1 paragraph 9 of the Chancellor of Justice Act).



[51] Estonia, Chancellor of Justice Act (*Õiguskantsleri seadus*), 1 May 2016, available at: https://www.riigiteataja.ee/en/eli/507042016001/consolide.

17

FRA key findings

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

   No relevant information to be added.

**Conclusions**

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

   No relevant information to be added.

## 1.5 Check the accuracy of the figures and tables published in the FRA report (see the annex on Figures and Tables)

### 1.5.1 Overview of security and intelligence services in the EU-28

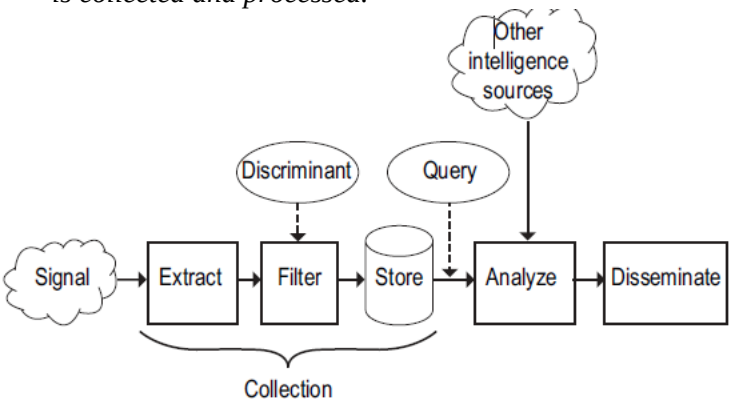
- *Please, delete all lines not referring to your country in the table below (see Annex p. 93 of the FRA Report)*
- *Check accuracy of the data*
- *Add in track changes any missing information (incl. translation and abbreviation in the original language).*
- *Provide the reference to the national legal framework when updating the table.*

| | Civil (internal) | Civil (external) | Civil (internal and external) | Military |
|---|---|---|---|---|
| **EE** | Estonian Internal Security Service/ *Kaitsepolitseiamet (KAPO)* | Information Board/*Teabeamet (TA)* | | Military Intelligence Branch of the Estonian Defense Forces/*Kaitseväe peastaabi luureosakond* |

Table correct.

### 1.5.2 Figure 1: A conceptual model of signals intelligence

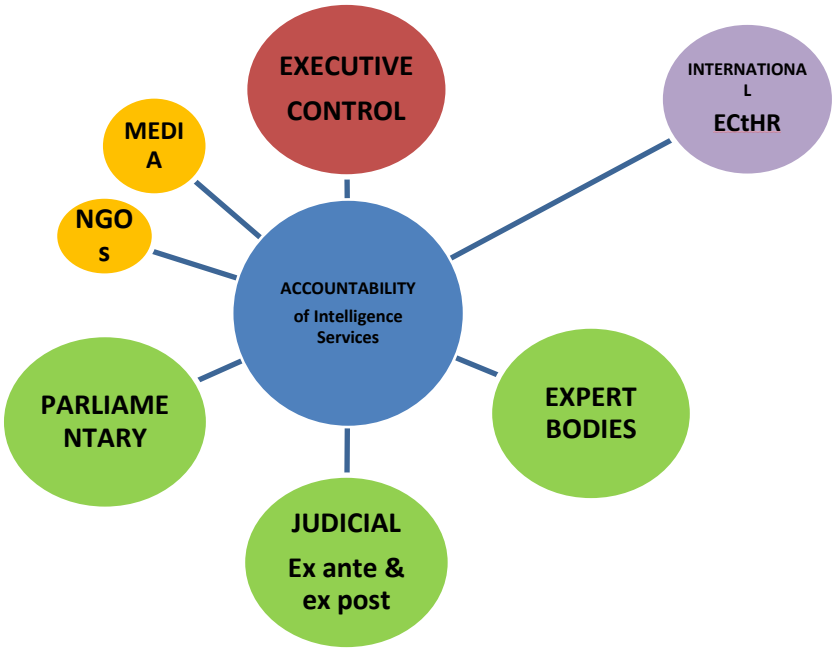
- *Please, provide a reference to any alternative figure to Figure 1 below (p. 16 of the FRA Report) available in your Member State describing the way signals intelligence is collected and processed.*




Conceptual model correct; there are no alternative models proposed in Estonian literature nor by the Estonian agencies.

### 1.5.3 Figure 2: Intelligence services' accountability mechanisms

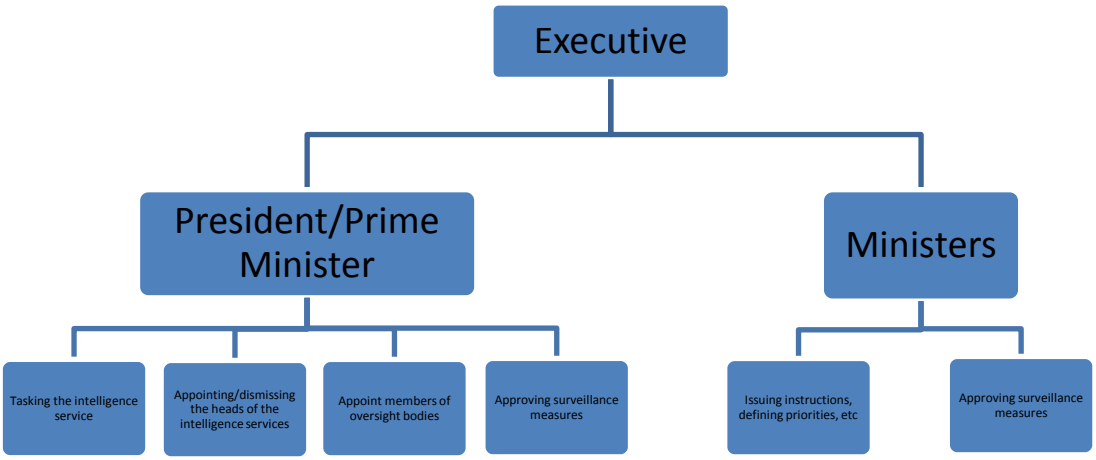
*Please confirm that Figure 2 below (p. 31 of the FRA Report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.*




The table reflects correctly Estonian situation.

### 1.5.4 Figure 3: Forms of control over the intelligence services by the executive across the EU-28

*Please confirm that Figure 3 below (p. 33 of the FRA Report) properly captures the executive control over the intelligence services in your Member State. 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 table applies with the following amendments and specifications.

The tasks of the Prime Minister should be included to show a more active role with the oversight bodies:

- oversees and co-ordinates the work of the Security Committee of Government of Republic that co-ordinates the work of the security authorities (Article 10 of the SAA)

Furthermore, Prime Minister and the Ministers have to work together to "*organise and harmonise the work of security authorities*" (Article 9 para 1 of the SAA)

There should be a third executive branch mentioned – the Government as a collective body. In Estonia, it has the following tasks:

- appoints and dismisses the head of the intelligence services;
- establishes for each year a plan regarding the obtaining and analysis of state security information (Article 9 para 2 of the SAA) i.e. generally tasking the intelligence service;
- determines the number of posts in a security authority (Article 8 para 1 of the SAA).

"Approving surveillance measures" under the president / prime minister does not correspond completely to the Estonian situation, nor would it fit under the branch of ministers. The approval of measures is usually the case of agencies themselves.

### 1.5.5 Table 1: Categories of powers exercised by the parliamentary committees as established by law

*Please, delete all lines not referring to your country in the table below (see p. 36 of the FRA Report)*

*Please check the accuracy of the data. Please confirm that the parliamentary committee in your Member State was properly categorised by enumerating the powers it has as listed on p. 35 of the FRA Report. Please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.*

| Member States | Essential powers | Enhanced powers |
|---|---|---|
| **EE** | X | |

Table correct.

### 1.5.6 Table 2: Expert bodies in charge of overseeing surveillance, EU-28

*Please, delete all lines not referring to your country in the table below (p. 42 of the FRA Report). Please check the accuracy of the data. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.*

| EU Member State | Expert Bodies |
|---|---|
| EE | The Chancellor of Justice (Õiguskantsler)[52] |

Table correct.

### 1.5.7 Table 3: DPAs' powers over national intelligence services, EU-28

*Please, delete all lines not referring to your country in the table below (p. 49 of the FRA Report). Please check the accuracy of the data. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.*

| EU Member State | No powers | Same powers (as over other data controllers) | Limited powers |
|---|---|---|---|
| EE | X | | |

Table correct.

*Notes: No powers: refers to DPAs that have no competence to supervise NIS.*

*Same powers: refers to DPAs that have the exact same powers over NIS as over any other data controller.*



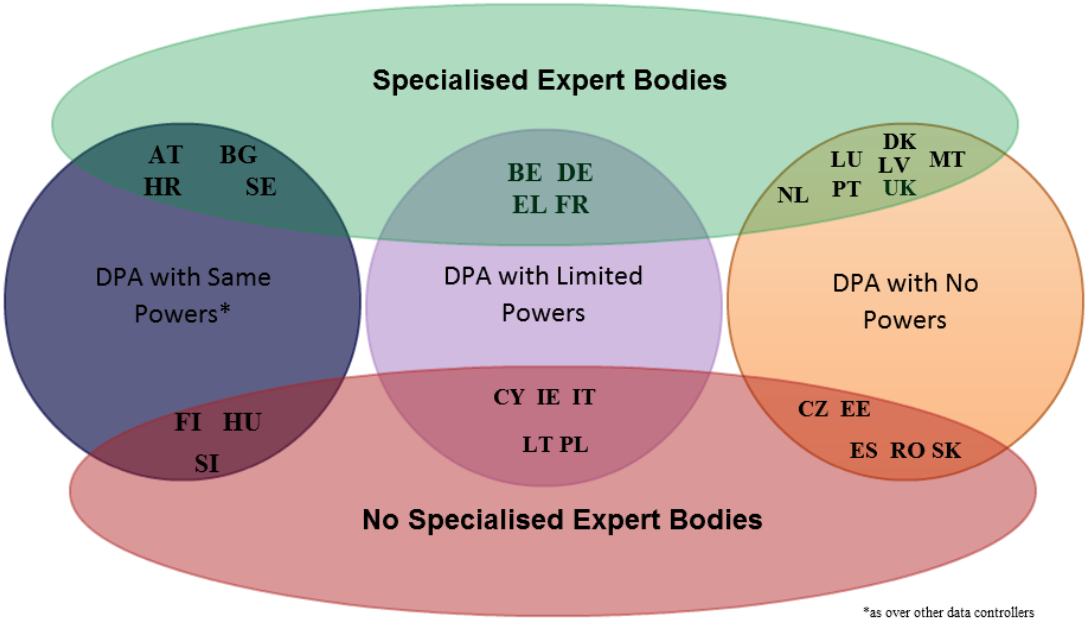
[52] Since 1 January 2015, the Chancellor of Justice has a right and an obligation to oversee surveillance from the perspective of fundamental rights in accordance with Article 1 paragraph 9 of the Chancellor of Justice Act.

*Limited powers: refers to a reduced set of powers (usually comprising investigatory, advisory, intervention and sanctioning powers) or to additional formal requirements for exercising them.*

### 1.5.8 Figure 4: Specialised expert bodies and DPAs across the EU-28

*Please check the accuracy of Figure 4 below (p. 50 of the FRA Report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.*

As the Chancellor of Justice has limited authority to oversee the surveillance activities, the position of Estonia could be changed to the group of DPA with no powers and Specialised expert bodies.




### 1.5.9 Table 4: Prior approval of targeted surveillance measures, EU-28

*Please, delete all lines not referring to your country in the table below (p. 52 of the FRA Report). Please check the accuracy of the data. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.*

| EU Member State | Judicial | Parliamentary | Executive | Expert bodies | None |
|---|---|---|---|---|---|
| EE | X | | | | |

Table correct. However, judicial control applies only in relation to criminal investigations and surveillance done by the national security institutions.

### 1.5.10 Table 5: Approval of signals intelligence in France, Germany, the Netherlands, Sweden and the United Kingdom

*Please check the accuracy of Table 5 below (p. 55 of the FRA Report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.*

| EU Member State | Judicial | Parliamentary | Executive | Expert |
|---|---|---|---|---|
| FR | | | X | |
| DE | | X (telco relations) | | X (selectors) |
| NL | | | X (selectors) | |
| SE | | | | X |
| UK | | | X | |

### 1.5.11 Figure 5: Remedial avenues at the national level

*Please confirm that Figure 5 below (p. 60 of the FRA 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.*

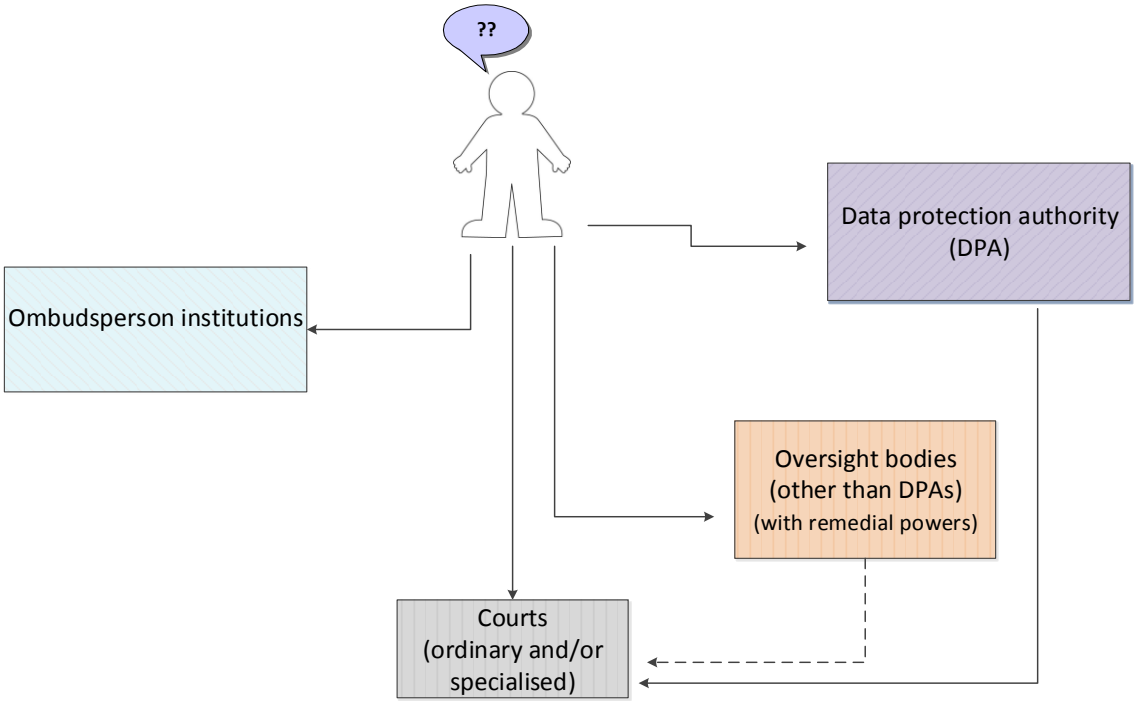
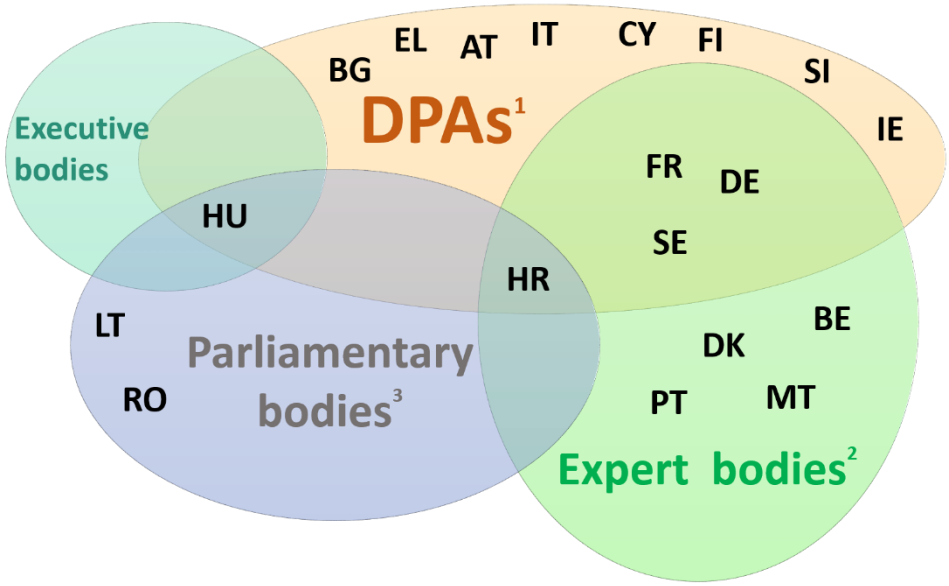



Figure depicts correctly the situation in Estonia.

### 1.5.12 Figure 6: Types of national oversight bodies with powers to hear individual complaints in the context of surveillance, by EU Member States

*Please check the accuracy of Figure 6 (p. 73 of the FRA Report) below. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.*

Individuals have the right to make petitions to the Chancellor of Justice; from 1 January 2015 it is specified that such petitions might also include complaints on surveillance measures (Article 1 paragraph 9 of the Chancellor of Justice Act). Estonia is not included in the figure, however, it has a Chancellor of Justice as an expert body that has the authority to hear complaints. I.e. Estonia should be in the same branch as DK, PT, BE and MT.




*Notes: 1. The following should be noted regarding national data protection authorities: In Germany, the DPA may issue binding decisions only in cases that do not fall within the competence of the G 10 Commission. As for 'open-sky data', its competence in general, including its remedial power, is the subject of on-going discussions, including those of the NSA Committee of Inquiry of the German Federal Parliament*

2. *The following should be noted regarding national expert oversight bodies: In Croatia and Portugal, the expert bodies have the power to review individual complaints, but do not issue binding decisions. In France, the National Commission of Control of the Intelligence Techniques (CNCTR) also only adopts non-binding opinions. However, the CNCTR can bring the case to the Council of State upon a refusal to follow its opinion. In Belgium, there are two expert bodies, but only Standing Committee I can review individual complaints and issue non-binding decisions. In Malta, the Commissioner for the Security Services is appointed by, and accountable only to, the prime minister. Its decisions cannot be appealed. In Sweden, seven members of the Swedish Defence Intelligence Commission are appointed by the government, and its chair and vice chair must be or have been judges. The remaining members are nominated by parliament.*
3. *The following should be noted regarding national parliamentary oversight bodies: only the decisions of the parliamentary body in Romania are of a binding nature.*