# Short Thematic Report

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

## Legal update

Country: Finland

Version of 20 June 2016

FRANET contractor: Finnish League for Human Rights

Author(s) name(s): Liisa A. Mäkinen

# 1 Description of tasks – Phase 3 legal update

## 1.1 Summary

**The legislative reform(s) that took place or are taking place and highlight the key aspect(s) of the reform.**

A major legislative reform in the area of surveillance by intelligence services is currently taking place in Finland as Finland is in the process of establishing the entire intelligence legislation. A working group appointed by the Ministry of Defence to develop intelligence legislation completed its work at the end of 2014, and as a result submitted its report Guidelines for Developing Finnish Intelligence Legislation (*Suomalaisen tiedustelulainsäädännön suuntaviivoja/Riktlinjer för en finsk underrättelselagstiftning)*[1] on the 14th of January 2015. According to the report, the existing legislation in Finland does not adequately address intelligence gathering as 'the powers of the police and Defence Forces to use secret methods of intelligence gathering […] cannot be used just for gathering intelligence about plans threatening national security that have not yet progressed to the stage of preparing an offence or that are not in themselves punishable' (see report, page 42). Thus the working group proposed that the Government should initiate the necessary measures to create a legal basis for telecommunications intelligence activities. The purpose of the new legislation would be to collect information to protect national security against serious domestic and international threats, either military or civilian in nature. Following the report of the working group, on the 20th of August 2015 the Government decided to initiate preparations for new legislation regarding civil and military intelligence. These legislative changes are based on the current Government Programme which proposes a statutory base for foreign and network traffic intelligence. The preparations take place within three ministries: the Ministry of the Interior, Ministry of Justice and Ministry of Defence. A working group in the Ministry of the Interior focuses on preparing legislation for civil intelligence. The objective is to improve the ability of the security authorities to predict and prevent any harmful actions and measures which could endanger national interests considered particularly important. Another working group in the Ministry of Defence investigates methods for military intelligence and aims to improve intelligence gathering on potential threats regarding among other things the tasks of the Finnish Defence Forces. The purpose of military intelligence is to ensure accurate, reliable and up-to-date information for governmental decision-making. Since some of the legislative changes might require amending the constitution, the Ministry of Justice is in charge of considering the necessary constitutional changes. The time period for these three working groups is set until the end of 2016.[2]

In addition to the ongoing legal reform, three legislative changes regarding surveillance and gathering of information have taken place during the report period. Firstly, the new Information Society Code (*Tietoyhteiskuntakaari/Informationssamhällsbalken,* Act no. 917/2014) was passed by the Parliament on the 6th of November 2014. It entered into force on the 1st of January 2015. The Act includes key pieces of legislation on electronic communications, including the provisions on the obligation of communications service



[1] Ministry of Defence (Finland) (2015), *Guidelines for Developing Finnish Intelligence Legislation. Working Group Report*, Helsinki, Ministry of Defence (Finland), available at: www.defmin.fi/files/3144/GUIDELINES_FOR_DEVELOPING_FINNISH_INTELLIGENCE_LEGISLATION.pdf. All hyperlinks were accessed on 31 May 2016.

[2] Finland, Ministry of the Interior (*Sisäministeriö/Inrikseministeriet*) (2015), 'Siviili- ja sotilastiedustelua koskevan lainsäädännön valmistelu käyntiin', Press release, 21 August 2015; See Also Finland, Ministry of the Interior (*Sisäministeriö/Inrikseministeriet*) (2015), 'Tiedustelulainsäädännön hankkeet käynnistettiin', Press release, 1 October 2015.

providers to store private communications data for the purposes of the authorities.[3] Secondly, an amendment to Section 13 of the Act on the Processing of Personal Data by the Police (*Laki henkilötietojen käsittelystä poliisitoimessa/Lag om behandling av personuppgifter i polisens verksamhet*, Act no. 761/2003) entered into force on the 27th of January 2015. As amended, the Act authorises the police to obtain information from the passenger and personnel name records of public transportation companies for the purposes of crime prevention, detection and prosecution.[4] Thirdly, due to an amendment to the Police Administration Act (*Laki Poliisin hallinnosta/Polisförvaltningslag*, Act no. 110/1992)[5], on the 1st of January 2016 The Finnish Security Intelligence Service (*Suojelupoliisi/Skyddspolisen*) was transferred from the supervision of the National Police Board to operate directly under the Ministry of the Interior.

**The important (higher) court decisions in the area of surveillance**

During the report period only one landmark decision in the area of surveillance, information society, privacy and data protection was delivered by the Finnish Supreme Court. The Supreme Court established a precedent in a case concerning the right of an individual to be fully informed of issues relating to them being the target of covert intelligence gathering (KKO:2015:45). In the case the National Bureau of Investigation had petitioned and received a permission from the District Court for the use of covert coercive means on target A, who was a suspect in an ongoing criminal investigation. After the use of the measure had ceased, target A was informed that they had been under surveillance. Two years later target A asked to see the appendix of the original application for the use of covert coercive means. The appendix included the justifications for the petition given by the officer in charge of the investigation as is required by the Criminal Procedure Act (*Laki oikeudenkäynnistä rikosasioissa/Lag om rättegångi brottmål*, Act no. 689/1997). The District Court denied access to the due to the fact that it included tactical and technical information of the methods used by the Police which, if made public, would endanger the prevention and investigation of crimes in the future. Target A complained about the decision to the Court of Appeal, and won the case as the court ruled that once the decision had been made to notify target A on the covert intelligence gathering, the original ruling on allowing surveillance had become public and thus the decision to conceal the appendix could no longer be made. The National Bureau of Investigation then complained to the Supreme Court which confirmed the ruling made by the Court of Appeal.[6]

**The reports and inquiry by oversight bodies (parliamentary committes, specialised expert bodies and data protection authorities) in relation to the Snowden revelations**

The Data Protection Ombudsman (*Tietosuojavaltuutettu/Dataombudsman*) and the Data Protection Board made no reports or inquiries in relation to the Snowden revelations during the time period of this research. The Data Protection Ombudsman's stand is that in Finland such reports should be made by the Finnish Communications Regulatory Authority (*Viestintävirasto/Kommunikationsverket*), an agency under the Ministry of Transport and Communications (*Liikenne- ja viestintäministeriö/ Kommunikationsministeriet*)of Finland.[7]



[3] Finland, The Information Society Code (*Tietoyhteiskuntakaari/Informationssamhällsbalk*), 7 November 2014.
[4] Finland, The Act on the Processing of Personal Data by the Police (*Laki henkilötietojen käsittelystä poliisitoimessa/Lag om behandling av personuppgifter i polisens verksamhet),* 22 August 2003.
[5] Finland, The Police Administration Act (*Laki Poliisin hallinnosta/Polisförvaltningslag*), 14 February 1992.
[6] Finland, Supreme Court (*Korkein oikeus/Högsta domtolen*), R2014/128, 22 June 2015.
[7] Finland, Data Protection Ombudsman Reijo Aarnio (2016), Interview, 7 April 2016.

In the parliamentary context, two important statements were given during the report period. First, the Ministry of Transport and Communications gave their dissenting opinion to the report Guidelines for Developing Finnish Intelligence Legislation. In their view preparing legislation enabling signals intelligence cannot be recommended. They particularly point out that the report does not mention or describe the changes in the public opinion and attitudes towards mass surveillance since the Snowden revelations.[8] Second, the Constitutional Law Committee (*perustuslakivaliokunta/grundlagsutskottet*) ruled in its statement 18/2014[9] that the data retention provisions of Section 157 of Government Bill for the New Information Society Code contradicted the right to private life and protection of personal data and secrecy of communications as provided by Section 10 of the Constitution of Finland. Therefore, the provisions needed to be substantially changed so that data would only be retained when absolutely necessary. The Committee's statement was based on the CJEU's judgment in Digital Rights Ireland and Seitlinger and Others. Moreover, the Committee also revised its earlier doctrine about the constitutional protection of the identification data related to private communications. In the earlier doctrine, the Committee had held that the identification data falls in the borderline of the protection of private life and secrecy of communications. According to the new doctrine, the categorical differentiation between the core and borderline of the right to private life is no longer appropriate.

**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.**

In addition to the three working groups mentioned above in charge of preparing legislation regarding intelligence, a fourth parliamentary follow-up group is set to operate as a link between the three working groups and the Parliament. Besides this group, no specific ad hoc commissions discussing the mentioned issues exist.



[8] Ministry of Transport and Communications (*Liikenne- ja viestintäministeriö/Kommunikationsministeriet*) (Finland) (2015), *The Future of Digital Society. Dissenting opinion of representative of the Ministry of Transport and Communications (Finland) to Guidelines for Developing Finnish Intelligence Legislation. Working Group Report (Digitaalisen yhteiskunnan tulevaisuus. Liikenne- ja viestintäministeriön edustajan eriävä mielipide tiedonhankintalakityöryhmän mietintöön)*, Helsinki, Ministry of Defence (Finland). Available at: www.defmin.fi/files/3016/Suomalaisen_tiedustelulainsaadannon_suuntaviivoja.pdf

[9] Finland, Constitutional Law Committee of Parliament (*perustuslakivaliokunta/grundslagsutskottet*) (2014), Opinion 18/2014, Helsinki, 17 June 2014.

## 1.2 International intelligence services cooperation

**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.**

Finland has no general legislation specifying the purpose of intelligence work or permissible intelligence operations beyond targeted surveillance measures. However, there are five national authorities in Finland with statutory duties concerning surveillance or gathering of information for the prevention or detection of offences or for criminal investigation: the Police of Finland (*Poliisi/Polisen*), the Finnish Border Guard (*Rajavartiolaitos/Gränsbevakningsväsendet*), the Finnish Customs (*Tulli/Tull*), and the Finnish Defence Forces (*Puolustusvoimat/Försvarsmakten*).

The Police of Finland is tasked with upholding social order and the judicial system; maintaining public order and safety; preventing and investigating crime; and referring investigated offences to a prosecutor for consideration of charges.[10] The powers of the Police to acquire information required for preventing and discovering offences are defined in the Police Act (*Poliisilaki/Polislag*, Act no. 872/2011)[11] and the powers to acquire information required for investigating offences are defined in the Coercive Measures Act (*Pakkokeinolaki/Tvångmedelslag*, Act no. 806/2011)[12] and in the Criminal Investigation Act (*Esitutkintalaki/Förundersökningslag*, Act no. 805/2011)[13]. The key difference is in the purpose for which the information acquisition measures are used: preventing and detecting offences are regulated in the Police Act and investigating offences in the Coercive Measures Act and the Criminal Investigation Act. These powers may only be used in Finnish territory.[14] The Finnish Border Guard and the Finnish Customs can conduct domestic surveillance in issues falling under their powers of inquiry as stipulated by the Customs Act (*Tullilaki/Tullag*, Act no. 29.12.1994/1466)[15] and the Border Guard Act (*Rajavartiolaki/Gränsbevakningslag*, Act no. 15.7.2005/578)[16].

The two Government agencies conducting international intelligence cooperation activities are the Finnish Security Intelligence Service and the Finnish Defence Intelligence Agency (*Puolustusvoimien tiedustelulaitos/Försvarsmaktens underrättelsetjänst*).

The Finnish Security Intelligence Service, operating under Section 10 of the Police Administration Act, is a national police unit whose task is to prevent and investigate such undertakings and offences that might compromise the Government, the public order, or internal or external national security. Furthermore, the Finnish Security Intelligence Service is required to maintain and improve general readiness for preventing actions that compromise national security. The Police Administration Act does not specify what are considered security threats; instead, this is decided by the Ministry of the Interior after hearing from the National Police Board. The Finnish Security Intelligence Service has no special statutory powers for intelligence gathering; its powers are defined in the legislation governing the police in general. Thus, the use of the powers for intelligence gathering is contingent on the prevention and detection of offences, as stipulated by the Police Act. These powers may only



[10] Finland, The Finnish Police (*Poliisi/Polisen*), 'About the Police', available at: http://poliisi.fi/about_the_police
[11] Finland, The Police Act (*Poliisilaki/Polislag*), 22 July 2011.
[12] Finland, The Coercive Measures Act (*Pakkokeinolaki/Tvångmedelslag*), 22 July 2011.
[13] Finland, The Criminal Investigation Act (*Esitutkintalaki/Förundersökningslag*), 22 July 2011.
[14] See Also Ministry of Defence (Finland) (2015), *Guidelines for Developing Finnish Intelligence Legislation. Working Group Report*, Helsinki, Ministry of Defence (Finland), pages 13-14.
[15] Finland, The Customs Act (*Tullilaki/Tullag*), 29 December 1994.
[16] Finland, The Border Guard Act (*Rajavartiolaki/Gränsbevakningslag*), 15 July 2005.

be used in Finnish territory and there is no legislation concerning the gathering of intelligence by the Finnish Security Intelligence Service abroad.

In practice, beyond monitoring public sources, the acquiring of information from abroad by the Finnish Security Intelligence Service depends on international intelligence cooperation and collaboration with liaison officers. The international cooperation of the police is based on the Police Act (Chapter 9, Section 9), which stipulates that 'What is separately laid down by law or agreed on by an international agreement binding on Finland applies to assistance given by the police to police officers of a foreign State. In matters not covered by legislation or not otherwise requiring the consent of Parliament, the Ministry of the Interior can make cooperation agreements of a conventional kind that fall within the scope of the police with the neighbouring States, coastal States around the Baltic Sea and the States belonging to the European Economic Area.' The manners and forms of the abovementioned cooperation are regulated in more detail in the [Prüm] council decision [2008/615/YOS].[17]

Furthermore, Chapter 6 of the Act on the Processing of Personal Data by the Police includes some special provisions on processing personal data in connection with international police cooperation. Sections 29 and 30 of the Act stipulate that 'the police may supply data from a police personal data file to the European Police Office and the national units of the European Police Office for the prevention and investigation of crime'. Furthermore, 'the police may supply data from a police personal data file to the International Criminal Police Organization (ICPO–Interpol) or to the police authorities of the Member States of Interpol other than those referred above, or to other authorities in such States whose duties include securing judicial and social order, maintaining public order and security, or preventing or investigating offences and forwarding them to a prosecutor for consideration of charges'. Additionally, Section 31 of the Act regulates information received from another state or international body.

Second, Finland's military defence is the duty of the Defence Forces, which belongs to the administrative branch of the Ministry of Defence. The Finnish Defence Intelligence Agency is a unit subordinate to the Defence Command and is in charge of monitoring, analysing and reporting of the military strategic situation and the military situation of the neighbouring area.[18] There is no specific legislation providing for the powers of military intelligence. Military intelligence work undertaken by the Defence Forces is considered to derive from the statutory mandate of the Defence Forces to defend Finland's sovereignty and territorial integrity. Military intelligence is not separately mentioned in the Act on the Defence Forces (*Laki Puolustusvoimista/Lag on förvarsmakten*, Act no. 551/2007)[19], but it is considered to be subsumed in the provisions of Chapter 2, Section 1, Subsection a and b of the Act.[20] The international cooperation of the Defence Administration is based on bilateral or multilateral arrangements. These arrangements can either be judicially binding or non-binding and can relate to a single joint exercise or larger cooperation. Finland has about 20 accredited defence attachés who report to the Defence Command Intelligence Division on the country where they



[17] Council of the European Union (2008), Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ 2008 L 210.; See Also Finland, Finnish Security Intelligence Service (2016), Personal Communicae, March/April 2016.

[18] Finland, The Finnish Defence Forces (*Puolustusvoimat/Försvarsmakten*), available at: www.puolustusvoimat.fi.

[19] Finland, The Act on the Defence Forces (*Laki Puolustusvoimista/Lag on förvarsmakten*), 11 May 2007.

[20] See Ministry of Defence (Finland) (2015), *Guidelines for Developing Finnish Intelligence Legislation. Working Group Report*, Helsinki, Ministry of Defence (Finland), page 25.

are stationed. There are no provisions in the legislation on the Defence Forces on the powers of Defence Forces officials posted to diplomatic missions.[21]

**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.**

No specialised parliamentary oversight body with a specific statutory task to oversee the Finnish Security Intelligence Service or the international cooperation of the Defence Forces exists.

The internal oversight of the Finnish Security Intelligence Service is based on internal instructions[22] of the agency and the Ministry of the Interior concerning legality oversight (SMDnro-2016-329). The essential oversight actions include monitoring the use of personal data registers, processing complaints and conducting inspections. The external legality control of the Finnish Security Intelligence Service is conducted by several agencies. As the supreme guardians of law in Finland, the Chancellor of Justice (*Oikeuskansleri/Justitiekansler*) and the Parliamentary Ombudsman (*Eduskunnan oikeusasiamies/Riksdagens justitieombudsman)* execute oversight based on Section 111 of the Constitution (*Perustuslaki*/*Grundlag*) stipulating their right to receive information. The Data Protection Ombudsman supervises the processing of personal data as stipulated in the Personal Data Act (*Henkilötietolaki/Personuppgiftslag*, Act no 22.4.1999/523)[23], Section 38. Administrative courts rule based on the Act on the Openness of Government Activities (*Laki viranomaisen toiminnan julkisuudesta/Lag om offentlighet i myndigheternas verksamhet*, Act no. 21.5.1999/621). Finally, the National Audit Office of Finland (*Valtiontalouden tarkastusvirasto/Statens revisionsverk*) audits the state's finances and monitors and evaluates fiscal policy.

General parliamentary oversight of the Finnish Security Intelligence Service takes place within general parliamentary committees, i.e. the Constitutional Law Committee, the Administration Committee (*hallintovaliokunta*) and the Foreign Affairs Committee (*ulkoasiainvaliokunta*) as is stipulated in the Constitution of Finland, Section 47 on the parliamentary right to receive information: 'The Parliament has the right to receive from the Government the information it needs in the consideration of matters. (…) A Committee has the right to receive information from the Government or the appropriate Ministry on a matter within its competence. (…) A Representative has the right to information which is in the possession of authorities and which is necessary for the performance of the duties of the Representative, in so far as the information is not secret or it does not pertain to a State budget proposal under preparation.' These committees are competent to oversee some aspects of intelligence agencies' work. However, as noted before[24], 'the committees provide only perfunctory oversight of intelligence agencies because they typically handle numerous other issues and often lack the time, resources, access to classified information and/or knowledge to focus on these agencies.'



[21] Finland, Ministry of Defence (Finland) (2016), Personal Communicae, 1 April 2016; See Also Ministry of Defence (Finland) (2015), *Guidelines for Developing Finnish Intelligence Legislation. Working Group Report*, Helsinki, Ministry of Defence (Finland), page 25.
[22] Finland, Ministry of the Interior (2011), *The Internal Legality Control in the Ministry of the Interior and its Administrative Branch* (*Sisäinen laillisuusvalvonta sisäasiainministeriössä ja sen hallinnonalalla*), Internal Guidelines for the Ministry of the Interior and its administrative branch, 26 August 2011.
[23] Finland, The Personal Data Act (*Henkilötietolaki/Personuppgiftslag)*, 22 April 1999.
[24] European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' rights and constitutional affairs (2011), *Parliamentary oversight of security and intelligence agencies in the European union*, page 27.

Similarly, the oversight of the international cooperation of the Defence Forces takes places as part of the normal internal legality control of the administration.[25] There are no external oversight agencies monitoring these activities.



[25] Finland, Ministry of Defence (2016), Personal communicae, 1 April 2016.

8

## 1.3 Access to information and surveillance

*Please refer to the Global Principles on National Security and the Right to Information (the Tshwane Principles)[26] (in particular Principle 10 E. – Surveillance) and describe the relevant national legal framework in this context.*

In Finland surveillance is currently only allowed when preventing, detecting and investigating an offence, and it must target individual suspects or their communications. Furthermore, the crimes allowing for surveillance must be of a serious nature, such as treason, offences committed with terrorist intent or offences for which the most severe punishment is imprisonment for at least four years. The specific titles of offences are listed in each act regulating surveillance.

Section 2 of Chapter 5 of the Police Act and Section 2 of Chapter 10 of the Coercive Measures Act stipulate that the use of secret methods of gathering intelligence and covert coercive means, including telecommunications interception, telecommunications monitoring and technical surveillance is only allowed when it can be assumed to result in gaining information necessary for preventing, detecting or averting the threat of an offence or the use of such methods may be assumed to produce information needed to clarify an offence. Section 86 of Chapter 9 of the Act on Soldier Discipline and Crime Prevention in the Finnish Defence Forces (*Laki sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa/ Lag om militär disciplin och brottsbekämpning inom försvarsmakten*, Act no. 28.3.2014/255) gives the Defence Forces jurisdiction over the prevention and revelation of crimes related to endangering military defence and intelligence activity targeting Finland. Furthermore, the Finnish Border Guard and the Finnish Customs can also conduct surveillance in issues falling under their powers of inquiry such as cross-border crime prevention and customs offences.

The overall legal framework, i.e. the laws stipulating the use of secret intelligence methods or covert coercive means in Finland (including procedures to be followed for authorising such use, selecting targets, and using, sharing, storing, and destroying intercepted material), is accessible to the public through a free and open Internet portal[27], as is required by the Tschwane principle 10 E, part 1. However, while the legislation includes information on the permissible objectives of surveillance, limitations on the duration of surveillance measures, procedures for authorising and reviewing the use of such measures, the types of personal data that may be collected and/or processed for national security purposes and the criteria that apply to the use, retention, deletion and transfer of these data (as stipulated in the Tschwane principle 10 E, part 1, notes b, d, e, f and g), it does not include laws governing indirect surveillance such as profiling and data mining (as stipulated in the Tschwane principle 10 E, part 1, notes a and c). There is no legislation that specifically authorises profiling and data mining in Finland. However, the Act on the Processing of Personal Data by the Police (Chapter 2, Section 2) states that 'in the case of suspected offences' the Data system for police matters may contain certain information 'in order to classify and analyse criminal modus operandi'. This would seem to allow some type of databased profiling by the Police. Whether the statutory threshold of suspicion required to initiate or continue surveillance be surpassed or not is decided on a case-by-case basis by the court processing the request for covert surveillance methods.

The second part of the Tschwane principle 10 E states that the public should have access to information about entities authorised to conduct surveillance and statistics about the use of such surveillance. In Finland, legislation dictates which Government entities are granted specific authorisation to conduct surveillance. These include the abovementioned Finnish



[26] http://www.right2info.org/exceptions-to-access/national-security/global-principles#section-10
[27] Finland, Ministry of Justice (*Oikeusministeriö/Justitieministeriet*), Finlex Data Bank available at: www.finlex.fi.

9

Police, the Finnish Border Guard, the Finnish Customs, and the Finnish Defence Forces. The number of surveillance authorisations granted each year and the number of individuals and communications subject to surveillance each year is made public in the Annual report of the Parliamentary Ombudsman in Finland (the most recent report is from 2014).[28] The report reveals both the number of rejected applications for coercive measures regarding intelligence gathering and the number of cases where it was decided that the target of intelligence gathering was not to be informed of the surveillance at all or informing the target was postponed.

Continuing on the second part of the Tschwane principle 10 E, the information on whether any surveillance is conducted without specific authorisation and if so, by which Government entity, is not covered in the Parliamentary Ombudsman's report. However, in the latest report the Parliamentary Ombudsman emphasises the importance of internal monitoring in ensuring the legality of the intelligence practices. The Parliamentary Ombudsman finds it troubling that according to observations made by the National Police Board (*Poliisihallitus/Polisstyrelsen*), the legal unit in some police departments has been assigned so many tasks that actual and due monitoring of coercive measures is not possible. Furthermore, the level of internal monitoring is not consistent between different departments, and neither is the expertise of those conducting the monitoring.[29] These challenges also connect to the third part of the Tschwane principle 10 E which states that the public should be fully informed of the fact of any illegal surveillance. Information about such surveillance should be disclosed to the maximum extent without violating the privacy rights of those who were subject to surveillance.

The fourth part of the Tschwane Principle 10 E underlines that all the Principles address the right of the public to access information and are without prejudice to the additional substantive and procedural rights of individuals who have been, or believe that they may have been, subject to surveillance. In this vein, it is good practice for public authorities to be required to notify persons who have been subjected to covert surveillance insofar as this can be done without jeopardising ongoing operations or sources and methods.

The right of the individual to be informed of whether or not they are subject to surveillance is stipulated in the Police Act and the Coercive Measures Act. The Police Act, Chapter 5, Section 58 states that the target of intelligence gathering shall be notified in writing without delay once the purpose of the intelligence gathering has been achieved, no later than one year after use of the method has ceased. However, if it is justifiable in order to secure ongoing intelligence gathering, to ensure State security or to protect lives or health, a court may postpone sending the notification for up to two years at a time or decide that a notification need not be sent at all. Finally, for extended surveillance, covert intelligence gathering, undercover activities, pseudo purchases and controlled use of covert human intelligence sources, there is no obligation to notify the target of the intelligence gathering unless a criminal investigation has been started into the matter. The content of The Coercive Measures Act, Chapter 10, Section 60, is essentially the same.

The main legal act regulating data protection is the Personal Data Act. Chapter 6 in the Act stipulates the data subject's rights: 'when collecting personal data, the controller shall see to that the data subject can have information on the controller and, where necessary, the representative of the controller, on the purpose of the processing of the personal data, on the regular destinations of disclosed data, as well as on how to proceed in order to make use of the rights of the data subject in respect to the processing operation in question.'



[28] Finland, Parliamentary Ombudsman of Finland (2015), *Annual Report 2014*, Helsinki, March 2015.
[29] See Finland, Parliamentary Ombudsman of Finland (2015), *Annual Report 2014*, Helsinki, March 2015, page 164.

10

In situations where an individual does not have the right to access data collected on them, the Data Protection Ombudsman can access the data in order to inspect the legality of the person register. Chapter 9, Section 39 of the Personal Data Act stipulates that regardless of confidentiality provisions, the Data Protection Ombudsman has the right of access to personal data which are being processed, as well as all information necessary for the supervision of the legality of the processing of personal data.

The right of the public to be informed and have access to information regarding surveillance measures is stipulated in the the Act on the Publicity of Court Proceedings in General Courts (*Laki oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa/Lag om offentlighet vid rättegång i allmänna domstolar*, Act no. 30.3.2007/370)[30] and the Act on the Openness of Government Activities[31]. In general, official documents, court proceedings and trial documents are public unless provided otherwise in these (or other) Acts.

Section 5 of Chapter 2 in the Act on the Publicity of Court Proceedings in General Courts stipulates that in a case concerning secret gathering of intelligence, the basic information does not become public until the latest time at which the suspect in the offence or the subject of the secret intelligence gathering measure or other measure is to be notified of the use of the intelligence gathering measure or other measure. If she or he is to be informed later of the intelligence gathering measure or other measure, when her or his identity is revealed, the basic information becomes public when the court is informed of said notice to the person has been given. The court may decide that the basic information becomes public at an earlier time.

Section 24 of Chapter 6 in the Act on the Openness of Government Activities stipulates that unless specifically provided otherwise, the following official documents shall be secret: the documents of the security police and other authorities concerning the maintenance of State security, unless it is obvious that access will not compromise State security (stipulated in Subsection 9); and documents concerning military intelligence, the supply, formations, locations or operations of the armed forces, the inventions, facilities, installations and systems used in the armed defence of the country or other defence, the other matters significant to the defence of the country, as well as defensive preparations, unless it is obvious that access will not violate or compromise the interests of defence (stipulated in Subsection 10).

The fifth part of the Tschwane principle 10 E stipulates that the high presumptions in favor of disclosure do not apply in respect of information that relates solely to surveillance of the activities of foreign Governments. This type of information is not publicly available in Finland.



[30] Finland, The Act on the Publicity of court proceedings in General Courts (*Laki oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa/Lag om offentlighet vid rättegång I allmänna domstolar*), 30 March 2007.

[31] Finland, The Act of the Openness of Government Activities (*Laki viranomaisen toiminnan julkisuudesta/Lag om offentlighet i myndigheternas verksamhet*), 21 May 1999.

11

## 1.4 Update the FRA report

**Introduction**

Finland is not mentioned in this chapter.

On p. 7 of the FRA Report (Introduction) inquiries regarding the Snowden revelations made by the specialised bodies in charge of overseeing the work on intelligence services are mentioned. In Finland, no such reports were made during the report period.

On p. 9 and 10 of the FRA Report (Introduction) the rulings of the European Court of Human Rights are discussed.

**1 Intelligence services and surveillance laws**

**1.1 Intelligence services**

Finland is mentioned on p. 14 of the FRA Report (Section 1.1. Intelligence Services) as being one of the five Member States where the body responsible for conducting intelligence activities belongs directly to the police and/or law enforcement authorities.

**1.2 Surveillance measures**

Finland is not mentioned in this section.

On p. 16 of the FRA Report (Subsection 1.2.1. Technical collection) a number of terms used to describe signals intelligence are listed. In the Working Group Report 'Guidelines for Developing Finnish Intelligence Legislation', the term network traffic intelligence (*tietoliikennetiedustelu/datatrafikunderrättelse*) is consistently used. However, in their dissenting opinion the Ministry of Transport and Communications suggest that Internet surveillance or mass surveillance would be more appropriate term[32].

On p. 17-18 of the FRA Report (Subsection 1.2.2. Targeted and untargeted collection) reference to legal reforms following technological developments and the Snowden revelations is made. Finland is currently in the process of reforming its legislation regarding signals intelligence.

**1.3 Member States' laws on surveillance**

On p. 19 of the FRA Report (Subsection 1.3.1. surveillance 'in accordance with the law') legal basis framing the intelligence services' mandates and powers are mentioned as being either constituted by one unique legal act or by complex legal frameworks. In Finland, there is not (yet) any one specific law on intelligence, but the use of secret intelligence measures is regulated in several Acts and there are several authorities with permission to conduct surveillance in issues falling under their power of inquiry.



[32] Ministry of Transport and Communications (*Liikenne- ja viestintäministeriö/Kommunikationsministeriet*) (Finland) (2015), *The future of Digital Society. Dissenting opinion of representative of the Ministry of Transport and Communications (Finland) to Guidelines for Developing Finnish Intelligence Legislation. Working Group Report* (*Digitaalisen yhteiskunnan tulevaisuus. Liikenne- ja viestintäministeriön edustajan eriävä mielipide tiedonhankintalakityöryhmän mietintöön*), Helsinki, Ministry of Defence (Finland), pages 109, 114.

12

Finland is mentioned on p. 20 of the FRA Report (Subsection 1.3.1.1. Targeted surveillance) as being one of eight Member States where targets of surveillance measures can be either a group of people or an individual. This information is accurate.

P. 20 of the FRA report (Subsection 1.3.1.2. Signals intelligence) refers to five Member States with specific legislation regarding both targeted surveillance and signals. Finland is currently in the process of reforming the entire intelligence legislation, possibly in this direction.

On p. 25-26 of the FRA Report (Subsection 1.3.2. Surveillance following a legitimate aim) national security as a concept is considered as a basis for national legislation on intelligence. In Finland, the working group appointed by the Ministry of Defence for developing intelligence legislation suggested in its final report that the Government should initiate the necessary measures to create a legal basis for network traffic intelligence activities and that the purpose of these activities would be to collect vital information *to protect national security* against serious domestic and international threats, military or civilian in nature. [33]

**FRA key findings**

Finland is not separately mentioned in this section. The information summarised in this section is accurate in the Finnish context.

## 2 Oversight of intelligence services

Finland is not mentioned in this section. Information in this section is accurate also in Finnish context. Oversight of intelligence services in Finland comprises of executive control, international control, expert bodies (i.e. Data Protection Authorities) and judicial ex ante control. Also media and NGOs have a role in the oversight of intelligence services in Finland. However, there is no specialized parliamentary oversight committees devoted to surveillance or intelligence services in Finland, but the intelligence agencies are overseen as a part of the work of general parliamentary committees.

On p. 31-32 of the FRA report (chapter 2. Oversight of intelligence services) it is mentioned that intelligence services have begun to publish reports on their activities. The Finnish Security Intelligence Agency has published its annual report yearly since 1994.[34]

### 2.1 Executive control

Finland is not mentioned in this section.

On p. 32 of the FRA Report (Section 2.1. Executive control) various ways in which the executive branch can control intelligence services are listed. These include establishing their policies, priorities and guidelines, nominating and/or appointing the service's senior management, formulating the budget that parliament will ultimately vote on and approving cooperation with other services.

The Finnish Security Intelligence Service operates directly under the Ministry of the Interior in Finland. The activities of the Finnish Security Intelligence Service is led by the director of the service with assistant directors. Together with additional members from the administration of the service they form the management group, which is in charge of establishing the



[33] See Ministry of Defence (Finland) (2015), *Guidelines for Developing Finnish Intelligence Legislation. Working Group Report*, Helsinki, Ministry of Defence (Finland), description page.
[34] Finland, the Finnish Security Intelligence Agency (2015), *Annual Report 2014*, Helsinki, The Finnish Security Intelligence Agency.

13

policies, priorities and guidelines of the service and formulating its budget. The director of the service is nominated by the Council of State. The international cooperation of the Finnish Security Intelligence Service is coordinated by the International Relations Office under the service's Information Gathering and Reporting Unit.

Furthermore, Figure 3 on p. 33 of the FRA Report (Section 2.1. Executive control) on the form of control exercised over the intelligence services is not completely accurate in Finnish context. The Finnish Security Intelligence Service operates under the guidance of the Ministry of the Interior, which is responsible for tasking the service, issuing instructions, defining priorities and such. The Council of State appoints/dismisses the heads of the intelligence service. However, there are no oversight bodies, whose members could be appointed. Also, all covert surveillance measures are approved for by the court.

## 2.2 Parliamentary oversight

Finland is mentioned on p. 34 of the FRA Report (Section 2.2. Parliamentary oversight) as being one of the four Member States where no parliamentary oversight over intelligence services takes place. This information is accurate as there are no specialised parliamentary committees overseeing intelligence activities in Finland. Parliamentary oversight of the Finnish Security Intelligence Agency takes place within general parliamentary committees as is stipulated in the Constitution of Finland, Section 47 on the parliamentary right to receive information: 'The Parliament has the right to receive from the Government the information it needs in the consideration of matters. (…) A Committee has the right to receive information from the Government or the appropriate Ministry on a matter within its competence. (…) A Representative has the right to information which is in the possession of authorities and which is necessary for the performance of the duties of the Representative, in so far as the information is not secret or it does not pertain to a State budget proposal under preparation.'

### 2.2.1 Mandate

Finland is not mentioned in this subsection. This subsection is not applicable to Finland as Finland does not have specialised parliamentary committees that deal with intelligence.

### 1.2.2 Composition

This subsection is not applicable to Finland as Finland does not have specialised parliamentary committees that deal with intelligence.

However, on p. 39 of the FRA Report (Subsection 2.2.2. Composition) Finland is mentioned as being one of the five Member States where mandatory proportional representation rules on membership are in effect. This information is accurate.

### 2.2.3 Access to information and documents

Finland is not mentioned in this subsection. This subsection is not applicable to Finland as Finland does not have specialized parliamentary committees that deal with intelligence.

### 2.2.4 Reporting to parliament

Finland is not mentioned in this subsection. This subsection is not applicable to Finland, as Finland does not have specialised parliamentary committees that deal with intelligence.

## 2.3 Expert oversight

### 2.3.1 Specialised expert bodies

Finland is not mentioned in the text in this section. This section is not applicable to Finland as in Finland no expert bodies (except for the DPA) exclusively dedicated to intelligence service oversight operate.

### 2.3.2 Data protection authorities

On p. 47 of the FRA report (subsection 2.3.2. Data protection authorities) Finland is mentioned as one of the seven Member States where DPAs have the same powers over national intelligence services as they do over any other data controller. This information is accurate.

## 2.4 Approval and review of surveillance measures

Finland is not mentioned in this section.

However, on p. 54 of the FRA report (Section 2.4. Approval and review of surveillance measures) provisions on Member States laws permitting the primary authority to postpone approvals in exceptional cases are discussed. Such provisions also exist in Finland. In Finland, *ex ante* approval for targeted surveillance measures is required from the court (The Police Act, Chapter 5, Section 7). In certain cases[35], if the matter cannot be delayed, the decision on monitoring may be made by a police officer with the power of arrest until such time as the court has made a decision on the request for an authorisation. The matter shall be brought for decision by a court as soon as possible, but no later than 24 hours after the action was started. (The Police Act, Chapter 5, Section 10.)

In addition, the decision on surveillance in cases of abuse of a victim of prostitution, solicitation of a child for sexual purposes, or procuring is made by the director of the National Bureau of Investigation or the Finnish Security Intelligence Service or the chief of the local police department. If the matter cannot be delayed, the decision on monitoring may be made by a police officer with the power of arrest until such time as the director of the National Bureau of Investigation or the Finnish Security Intelligence Service or the chief of the local police department has made a decision on the matter concerning surveillance measures. The matter shall be brought for decision by the said police officer as soon as possible, but no later than 24 hours after the action was started. (The Police Act, Chapter 5, Section 10.)

**FRA key findings**

Finland is not specifically mentioned in this section. The information summarised in this section is accurate in the Finnish context.

## 3 Remedies

Finland is not specifically mentioned in this section.

On p. 60 of the FRA report (Chapter 3. Remedies), the ECtHR case Segerstedt-Wibers and Others v. Sweden is discussed. The case was about the applicants' access to review



[35] concerning an offence committed using a network address or terminal end device and for which the most severe punishment by law is at least two years' imprisonment; a narcotics offence; an offence for which the most severe punishment by law is at least two years' imprisonment; an offence other than one referred to in paragraph 3, committed using a network address or terminal end device; abuse of a victim of prostitution.

15

surveillance documents on them. A similar case was decided upon by the Finnish Supreme Court. The Supreme Court in Finland established a precedent on a case concerning the right of an individual to be fully informed of issues relating to them being the target of covert intelligence gathering (KKO:2015:45). In the case the National Bureau of Investigation had petitioned and received a permission from the court for covert intelligence gathering on target A, who was a suspect in an ongoing criminal investigation. After the use of the measure had ceased, target A was informed that they had been under surveillance. Two years later target A asked to see the appendix of the original application for covert intelligence gathering. The appendix included the justifications for the petition given by the officer in charge of the investigation. The District Court denied access to the appendix due to the fact that it included tactical and technical information of the methods used by the Police which, if made public, would endanger the prevention and investigation of crimes in the future. Target A complained about the decision to the Court of Appeal, and won the case as the court ruled that once the decision had been made to notify target A on the covert intelligence gathering, the original ruling on allowing surveillance had become public and thus the decision to conceal the appendix could no longer be made. The National Bureau of Investigation then complained to the Supreme Court which confirmed the ruling made by the Court of Appeal.[36]

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

Finland is mentioned on p. 62 of the FRA Report (Section 3.1. A precondition: obligation to inform and the right of access) as one of the Member States where the obligation to inform and right of access are provided for in the law, albeit with restrictions. However, unlike the other Member States, Finnish legislation concerning the right of access and the obligation to inform is not explained in detail in the Report. In Finland, the target of intelligence gathering shall be notified in writing without delay (no later than one year after the use of the method has ceased) once the purpose of the intelligence gathering has been achieved. If it is justifiable in order to secure ongoing intelligence gathering, to ensure State security or to protect lives or health, a court may postpone sending the notification for up to two years at a time or decide that a notification need not be sent at all.[37]

In situations where an individual does not have the right to access data collected on them, the Data Protection Ombudsman can access the data in order to inspect the legality of the person register. Regardless of confidentiality provisions, the Data Protection Ombudsman has the right of access to personal data which are being processed, as well as all information necessary for the supervision of the legality of the processing of personal data.[38]

### 3.2 Judicial remedies

Finland is not mentioned in this section.

#### 3.2.1 Lack of specialisation and procedural obstacles

Finland is not mentioned in this subsection.

On p. 66 of the FRA report (Subsection 3.2.1. Lack of specialisation and procedural obstacles) it is mentioned that national laws may determine which of the ordinary courts are competent to review surveillance complaints, and that in some Member States the DPAs may need to be approached before the courts. In Finland, the Data Protection Board makes decisions concerning the compliance with legislation and the implementation of the rights of



[36] Finland, Supreme Court (*Korkein oikeus/Högsta domtolen*), R2014/128, 22 June 2015.
[37] See Finland, The Police Act (*Poliisilaki/Polislag*), 22 July 2011.
[38] See Finland, The Personal Data Act (*Henkilötietolaki/Personuppgiftslag),* 22 April 1999.

16

data subjects. In matters concerning the implementation of the right of verification and the correction of personal data, the decisions are binding and subject to appeal. The appeals are directed to the Supreme Administrative Court. In addition to the Data Protection Board, the Parliamentary Ombudsman exercises oversight to ensure that public authorities and officials comply with the law. The Ombudsman oversees legality principally by examining the complaints received.

#### 3.2.2 Specialised judges and quasi-judicial tribunals

Finland is not mentioned in this subsection. There are no specialised judges or quasi-judicial tribunals in Finland.

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

Finland is not mentioned in this section. The information summarized in this section is accurate in the context of Finland, thus it is not necessary to mention Finland separately.

#### 3.3.1 Types of non-judicial bodies

Finland is not mentioned in this subsection.

Finland has two data protection authorities: the Data Protection Ombudsman and the Data Protection Board. The Data Protection Ombudsman provides direction and guidance on the processing of personal data, supervises the processing as well as makes decisions concerning right of access and rectification. The Data Protection Board deals with questions of principle relating to the processing of personal data, where these are relevant to the application of the Personal Data Act. The Board has also the power to grant permissions and issue orders.

#### 3.3.2 The issue of independence

Finland is not mentioned in this subsection.

The Office of the Data Protection Ombudsman is an expert organisation in the administrative sector of the Ministry of Justice.

The Data Protection Board is an independent authority affiliated to the Ministry of Justice. It is appointed by the Council of State for three years at a time.

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

Finland is mentioned on p. 74 of the FRA report (Subsection 3.3.3. Powers and specialization of non-judicial remedial bodies) as being one of the Member States where individuals can seek remedies both via DPAs and via ombudsperson institutions in cases where data protection violations are caused by a public entity. This information is accurate.

**FRA key findings**

Finland is not mentioned specifically in the text in this chapter. The information summarised in this section is accurate in the context of Finland.

**Conclusions**

Finland in not mentioned in this chapter.

In the last paragraph on p. 78 of the FRA report (Conclusions chapter) attention is drawn to strengthening legal frameworks concerning intelligence after the Snowden revelations in Member States. Finland is currently in the process of reforming its intelligence legislation.

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

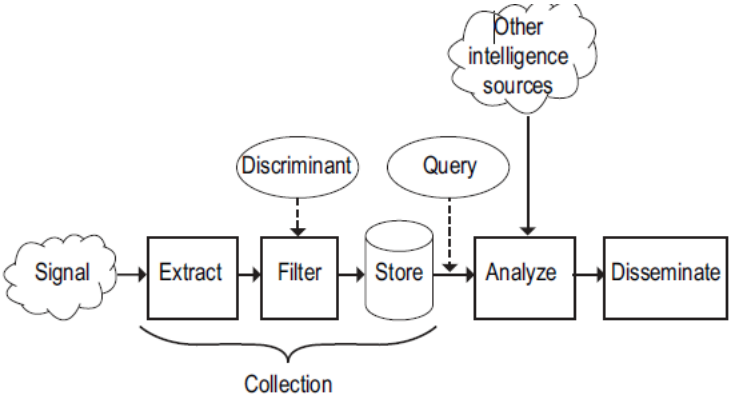
### 1.5.1 Overview of security and intelligence services in the EU-28

- *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** |
|---|---|---|---|---|
| **FI** | Finnish Security Intelligence Service/*Suojelupoliisi/Skyddspolisen* (SUPO) (service under the Ministry of the Interior)<br><br>The Finnish Security Intelligence Service works under section 10 of the Police Administration Act. | | | Finnish Defence Intelligence Agency/ *Tiedustelulaitos/underrättelsetjänst* (FDIA)<br><br>The Military intelligence work undertaken by the Defence Forces and The Finnish Defence Intelligence Agency derives from the Act on the Defence Forces. |

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

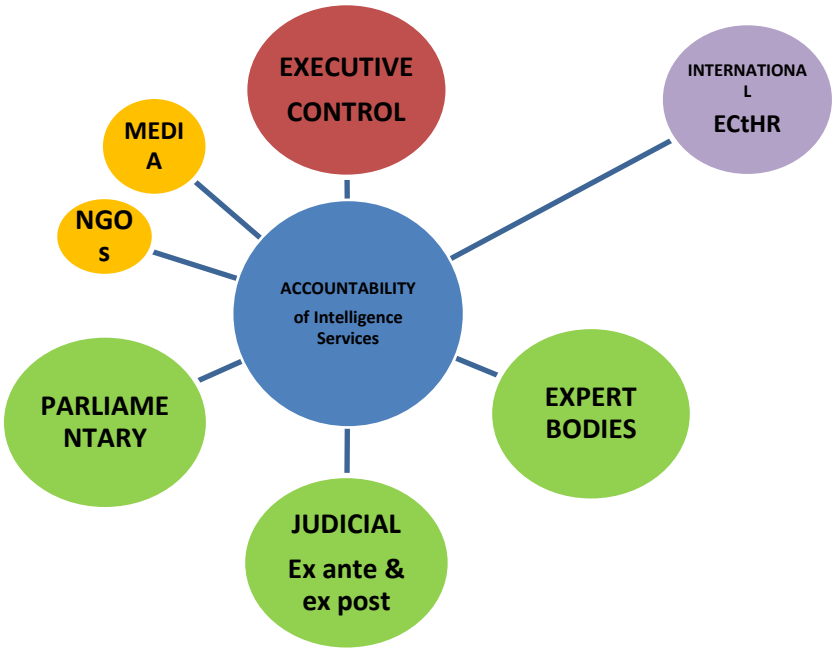
- *Please, provide a reference to any alternative figure to Figure 1 below (p. 16 of the FRA Report) available in your Member State describing the way signals intelligence is collected and processed.*




There are no figures available in Finland describing the collection and processing of signals intelligence as the national legislation only allows for targeted surveillance measures.

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

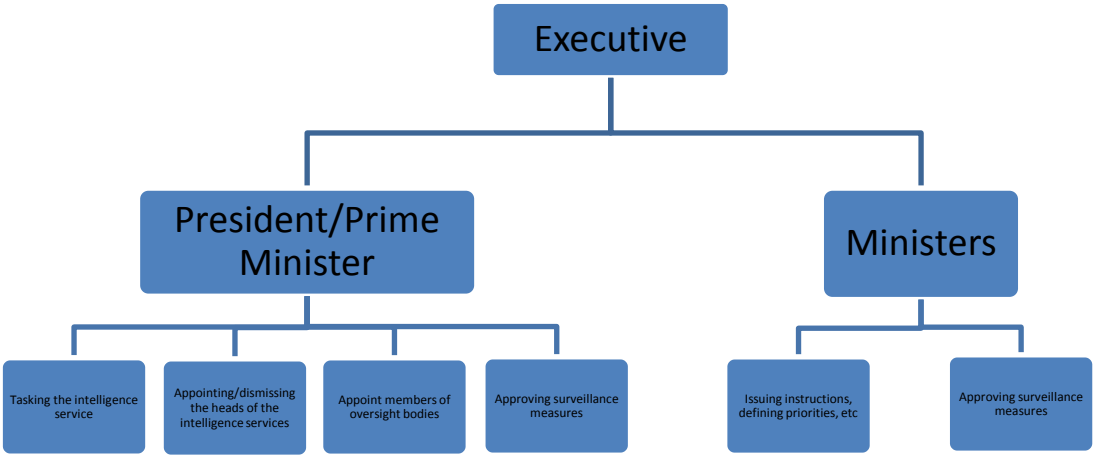
*Please confirm that Figure 2 below (p. 31 of the FRA Report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.*




This figure illustrates the situation in Finland in terms of oversight from NGOs, media, executive control, international control accountability, expert bodies (i.e. Data Protection Authorities) and judicial ex ante control. However, there are no specialised parliamentary oversight committees devoted to surveillance or intelligence services in Finland; instead, the intelligence agencies are overseen as a part of the work of general parliamentary committees.

### 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.*




This figure is not completely accurate in the Finnish context. The Finnish Security Intelligence Service operates under the guidance of the Ministry of the Interior, which is responsible for tasking the service, issuing instructions, defining priorities and so on. The Council of State appoints/dismisses the heads of the intelligence service. However, there are no oversight bodies whose members could be appointed. Furthermore, all covert surveillance measures need to be approved for by a court.

### 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 |
|---|---|---|
| **FI** | | |

*Note:* Finland, Ireland, Malta and Portugal do not have parliamentary committees that deal with intelligence services.

There is no specialised parliamentary committee in Finland that deals with intelligence services.

### 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 |
|---|---|

| FI | N.A. |
|---|---|

There are no expert bodies in charge of overseeing surveillance in Finland.

For covert surveillance measures, judicial *ex ante* permission is required. The Parliamentary Ombudsman in Finland reports annually the number of surveillance authorisations granted, the number of individuals and communications subject to surveillance, the number of rejected applications for coercive measures regarding intelligence gathering and the number of cases where it was decided that the target of intelligence gathering was not to be informed of the surveillance at all or informing the target was postponed.

### 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 |
|---|---|---|---|
| FI | | X | |

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

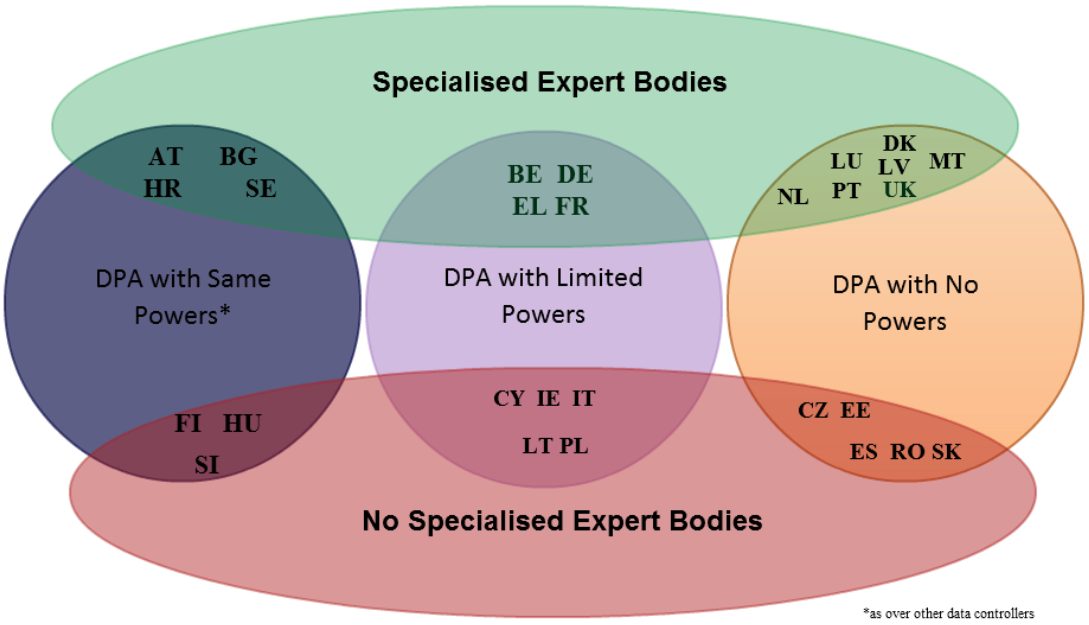
*Same powers: refers to DPAs that have the exact same powers over NIS as over any other data controller.*

*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.*

This information is accurate.

### 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.*




The information is accurate.

### 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 |
|---|---|---|---|---|---|
| FI | X | | | | |

This information is accurate.

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

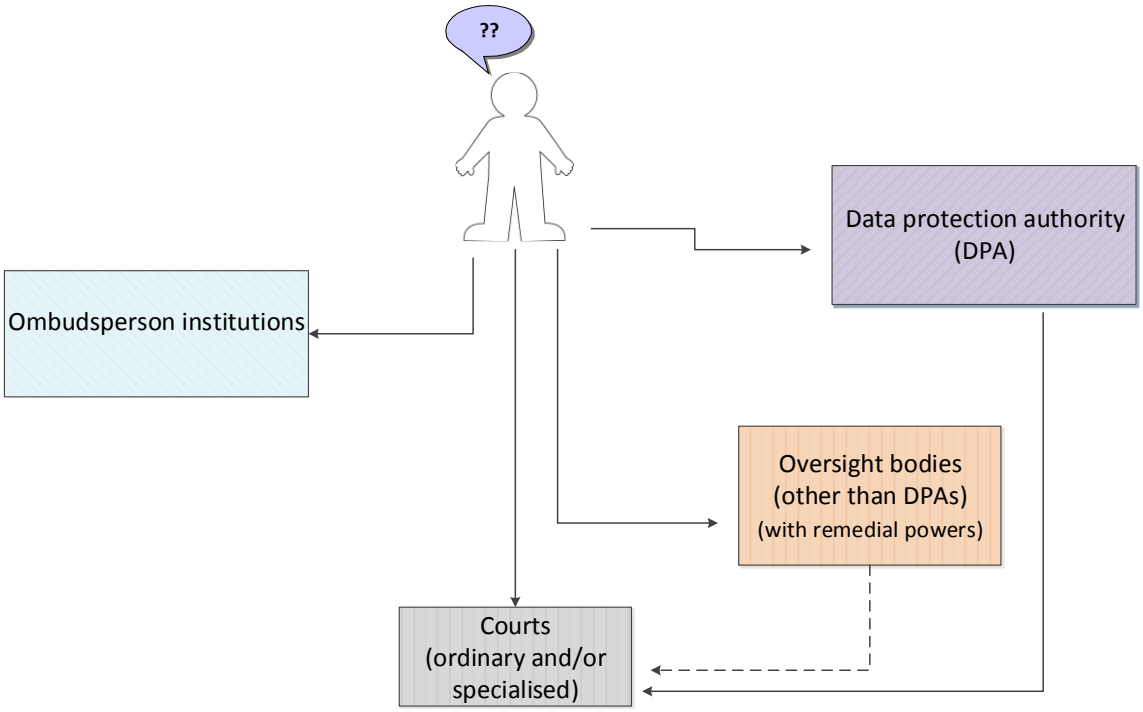
*Please check the accuracy of Table 5 below (p. 55 of the FRA Report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.*

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

Not applicable to Finland.

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

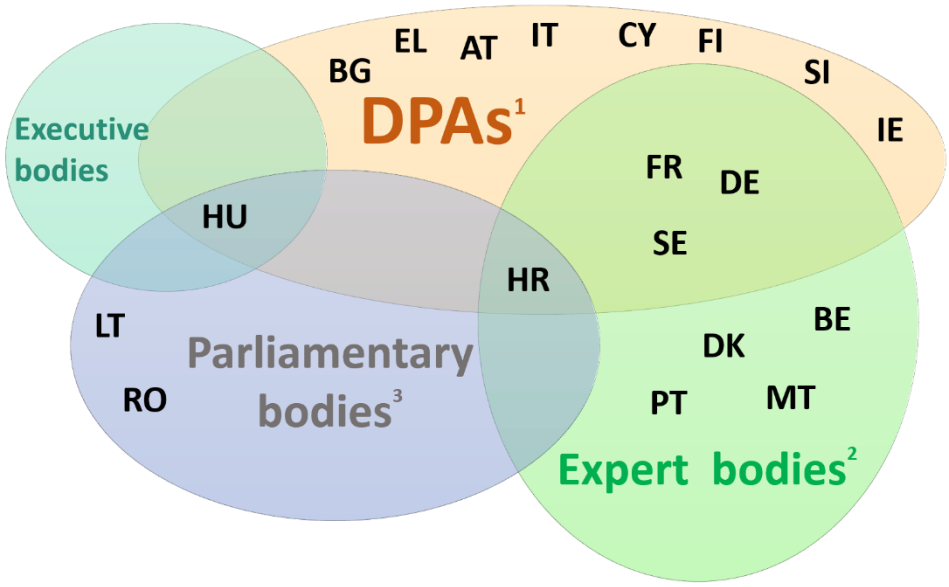
*Please confirm that Figure 5 below (p. 60 of the FRA Report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.*




In Finland, the remedial avenues include the Ombudsperson institutions (the Parliamentary Ombudsman in Finland), the Data protection authority (the Data Protection Board and the Data Protection Ombudsman) and the court (the District Court). However, there are no oversight bodies with remedial powers beyond these.

### 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.*




*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.*

The information in the figure concerning Finland is accurate.