

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

November 2022 Update

Country: Belgium

FRANET contractor: Vrije Universiteit Brussel (VUB)

Author(s) name(s): Erika Ellyne

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

Table of Contents

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

1. Summary

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

*the most significant legislative reform/s that took place or are taking place and highlight the key aspect/s of the reform, focusing on oversight and remedies.
relevant oversight bodies' (expert bodies (including non-judicial bodies, where relevant), data protection authorities, parliamentary commissions) reports/statements about the national legal framework in the area of surveillance by intelligence services.*

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

FRA 2017 Report:

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

FRANET data collection for the FRA 2017 Report:

Country studies for the project on National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies - Legal update

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

FRA 2015 Report:

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

FRANET data collection for the FRA 2015 Report:

Country studies for the project on National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

Legislatively, Belgium has seen several laws related to surveillance being promulgated in the past 6 years.

The law of 30 March 2017 modifying the law of the 30 November 1998 on Security and Intelligence Services generally increased the scope and powers of the General Intelligence Service's. It extended the material and territorial scope of the General Intelligence Services' powers to cover the fight against extremism and to be able to capture/intercept communications transmitted (from) abroad. This power could potentially cover software, and can be done to carry out/in the missions of the surveillance services.¹ The law introduced rules and very specific conditions to grant access requests made by individuals placed under surveillance to be informed of basic information on the legal justification underlying any surveillance measures they have been a subject of.² Furthermore, it establishes

¹ Belgian law does not distinguish between target or general measures of surveillance. The law identifies, "ordinary" versus "specific and exceptional" measures of surveillance.

² It is worth noting that this article was subject to annulment by the Constitutional court and was reformulated. Arrêt n° 41/2019 du 14 mars 2019, p.10. Disponible sur: <https://www.const-court.be/public/f/2019/2019-041f.pdf>. The article now allows for the director of the surveillance services to inform any person justifying a personal

conditions under which agents can commit infractions and make use of ‘specific surveillance measures’³ conditional upon their prior notification to the Administrative Commission.⁴ The law also revised the procedures applicable in case of urgency allowing for verbal authorizations to be given (such authorization must be confirmed in writing by the head of the department within a maximum of 24 hours following this verbal authorization).

The **law of the 3 December 2017** on the creation of the Belgian Data Protection Authority. This law created a national data protection authority (DPA) to replace the previous data protection commission. The DPA is in charge of controlling the respect for personal data protection legislation unless such competence has been attributed to another authority. The DPA is endowed with all the powers recognized by the GDPR to national enforcement authorities. In this respect, the most novel aspect is the creation of a ‘litigation’ chamber and investigatory branch.

The **law of 30 July 2018**⁵ related to protection of personal data was introduced in the Belgian landscape as a result of GDPR implementation. Articles 72 to 98 of the law focus on data protection rules adapted for intelligence services. On a national level, the exercise of those rules and any data subject rights is overseen by the Standing Committee I (*Le Comité permanent de contrôle des services de renseignement*).⁶ The DPA’s powers are mostly residuary, it being recognized that, however there is some ambiguity relating to the interpretation of article 185§4 of the law of 20 July 2018. This has been partially addressed in the protocol concluded between the Standing Committee I (and others) and the DPA.⁷ On the one hand, the Standing Committee I is clearly identified as the ‘control authority’ when it comes to processing activities falling under Title III of the law (i.e. control of the application of the law of 30 July 2018 with regard to processing activities carried out by the two Belgian Security and Intelligence Services in view of the performance of their mission/purpose under the law of 30 November 1998).⁸ On the other hand, the DPA is competent for controlling all “personal data processing in the context of national security” activities carried out by the Standing Committee I, with only the processing activities carried out by the said committee as a Control Authority or a judicial authority in the field of SIM-methods being excluded.⁹ However, the DPA also indicates that the legal framework for this

and legitimate interest, upon their request, of the use of certain exceptional surveillance methods (such as: reading mail; accessing data on an IT system; accessing and inspecting private property/objects ...), applied to them so long as 4 conditions are met: i) the method was applied more than 10 years ago; ii) the notification cannot undermine an ongoing investigation; iii) the notification does not violate the security of any sources or third parties having assisted in the investigation, iv) the notification will not harm Belgium’s relationship with foreign nations or international/supranational organisations.

³ These specific surveillance measures include, but are not limited to: i) Using a false identity and/or the creation and use of false documents; ii) Requesting transportation and travel data from any private transportation or travel service provider; iii) Inspecting the contents of locked or unlocked items in public places; iv) take such items away for a strictly limited period of time, if their examination cannot be done on site for technical or security reasons; v) may take cognizance of the identification data of the sender or the addressee of a mail entrusted or not to a postal operator and of the identification data of the holder of a mailbox; vi) asking the telecom services for the location of the origin or destination of electronic communications

⁴ Entity in charge of the review of the specific and exceptional surveillance means.

⁵ Law of July 30 2018 on the protection of individuals with regard to the processing of personal data.

⁶ The Permanent Control Committee referred to in the Law of 18 July 1991.

⁷ Cooperation Protocol between Belgian Control Authorities/Protocole de coopération entre les autorités de contrôle fédérales belges en matière de protection des données <https://www.autoriteprotectiondonnees.be/publications/protocole-de-cooperation-entre-les-autorites-de-contrôle-federales-belges-en-matiere-de-protection-des-donnees.pdf> p.5, 24 November 2020.

⁸ Article 95 of the law of 30 July 2018.

⁹ Protocole de coopération entre les autorités de contrôle fédérales belges en matière de protection des données convention entre l'autorité de protection des données, l'organe de contrôle de l'information policière, le comité permanent de contrôle des services de renseignement et le comité permanent de contrôle des services de police, available at : <https://www.autoriteprotectiondonnees.be/publications/protocole-de-cooperation-entre-les-autorites-de-contrôle-federales-belges-en-matiere-de-protection-des-donnees.pdf> p.5; "A contrario, il ressort de

power is absent: "The substantive framework is essentially non-existent; Article 185 consists of only two paragraphs".¹⁰

More recently, the **law of 14 July 2022**¹¹ broadened certain powers, not including the use of software, for intelligence and security service agents. For instance, the text introduces a procedure for the use of a fictitious identity in the collection of information and data and extends the possibilities for intelligence agents and their sources to commit certain criminal offences in the course of their duties.

Moreover, the **law of 20 July 2022**¹² relating to the collection and storage of identification data and metadata in the electronic communications sector and the supply of these data to authorities introduced new powers for the Belgian authorities, allowing them, inter alia, to proceed to a generalized retention of IP addresses and other information. In its opinion on the draft law, the Belgian data protection authority insisted that the draft must truly effect the change of perspective required by the case law of the CJEU and the Constitutional Court and therefore cannot impose new traffic and location data retention measures that would result in the reintroduction, de jure or de facto, of obligations to retain the traffic or location data of all or too large a proportion of the users of electronic communications means in Belgium. The authority stated that unless the draft was thoroughly reviewed to ensure that it made the required change of perspective, both the retention of such traffic and location data by operators and their communication to the authorities would infringe the Privacy Directive, interpreted in light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.¹³

At the end of 2022, the Federal ombudsman was given new powers in cases of public service integrity breaches within public authorities (as the external reporting authority).¹⁴ However, when it comes to signaling breaches within an intelligence and security service, the Standing Committee I is the competent external reporting authority to investigate.¹⁵

Finally, a revision of the **law of 30 November 1998 on Security and Intelligence Services**, the benchmark text for surveillance matters and intelligence institutions, is pending approval from the *Chambre des Représentants*¹⁶. If approved, the amendments would, inter alia, introduce an active notification obligation towards subjects regarding certain specific methods of data collection.

From an institutional perspective, Belgium has also seen many initiatives being taken by intelligence-related establishments in the past years. For instance, a National Surveillance Strategy Plan, distinguishes between the responsibilities attributed to the Sûreté de l'Etat and the General Intelligence

l'article 185, § 4 de la LTD que l'APD est compétente pour les traitements de sécurité nationale" des deux Comités. Seuls les traitements réalisés par le CPP & le CPR ainsi que par le COC en tant qu'AC sont exclus du contrôle de l'APD."

¹⁰ Protocole de coopération entre les autorités de contrôle fédérales belges en matière de protection des données convention entre l'autorité de protection des données, l'organe de contrôle de l'information policière, le comité permanent de contrôle des services de renseignement et le comité permanent de contrôle des services de police, available at : <https://www.autoriteprotectiondonnees.be/publications/protocole-de-cooperation-entre-les-autorites-de-contrôle-federales-belges-en-matiere-de-protection-des-donnees.pdf> p.5 "Le cadre de référence matériel est pour ainsi dire inexistant ; l'article 185 n'est composé que de deux paragraphes."

¹¹ Law of July 14, 2022 amending the law of November 30, 1998 on the organization of intelligence and security services.

¹² Law of July 20, 2022, relating to cybersecurity certification of information and communications technologies and designating a national cybersecurity certification authority.

¹³ Avis n°66/2022 du 1er Avril 2022, available at : <https://www.autoriteprotectiondonnees.be/publications/avis-n-66-2022.pdf>

¹⁴ Article 14 and 71 of the law of the 8 December 2022 on reporting channels and protection of whistleblowers regarding integrity breaches in federal public sector bodies and in the integrated police

¹⁵ Article 14 of the law of 8 December 2022

¹⁶ Proposal for a law amending the law of 30 November 1998 on the organization of the intelligence and security services with a view to introducing an active notification obligation for certain specific data collection methods - <https://www.lachambre.be/kvvcr/showpage.cfm?section=flwb&language=fr&cfm=/site/wwwcfm/flwb/flwbn.cfm?lang=F&legislat=55&dossierID=1763>

and Security Service, the two national intelligence institutions in Belgium (subject to different Ministers). This plan was published to clarify the collaboration between the organizations regarding methods for gathering data, logistical operations, etc¹⁷. In a similar line, Sate security (la Sûreté de l'Etat) publishes a report on its activities annually¹⁸ It addresses different subjects the institution works on and in particular its work in counter espionage.

2. Annexes- Table and Figures

2.1. Overview of security and intelligence services in the EU-27

FRANET contractors are requested to check the accuracy of the table below (see Annex pp. 93 - 95 of the FRA 2015 report) and correct or add in track changes any missing information concerning security and intelligence services in their Member State (incl. translation and abbreviation in the original language). Please provide the full reference in a footnote to the relevant national law substantiating all the corrections and/or additions made in the table.

	Civil (internal)	Civil (external)	Civil (internal and external)	Military
BE	State Security/ <i>Staatsveiligheid</i> <i>/Sûreté de l'Etat</i> (SV/SE)			General Intelligence and Security Services of the armed forces/ <i>Algemene Dienst Inlichting en Veiligheid/ Service général du renseignement et de la sécurité des Forces armées</i> (VSSE/SGRS) SGRS)

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

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

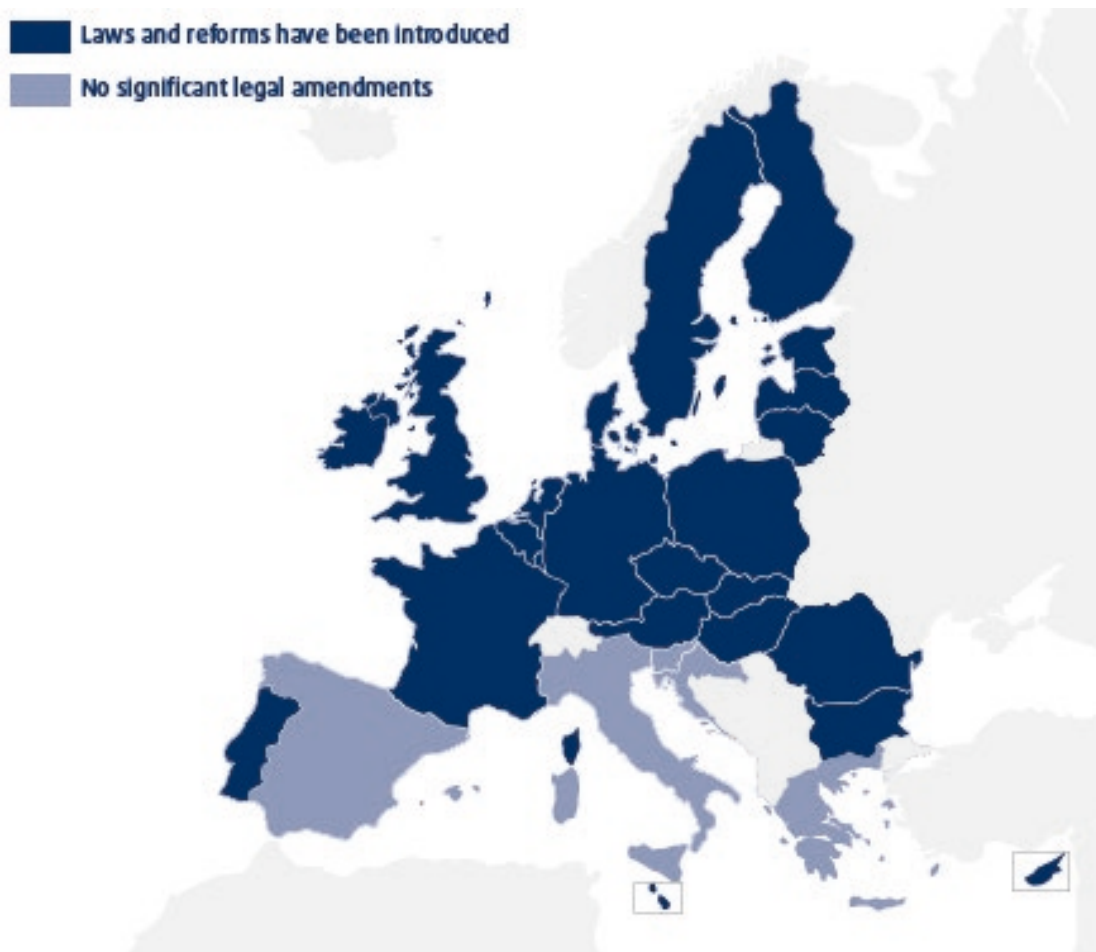
1. Whether their legal framework on surveillance has been reformed or is in the process of being reformed since **mid-2017** – see the Index of the FRA 2017 report, pp. 148 - 151. Please do not to describe this new legislation but only provide a full reference.
2. whether the reform was initiated in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

Figure 1 is accurate: legal reforms have been introduced as explained in the foregoing section. It was not in reaction to Pegasus revelations.

¹⁷ <https://www.sgrs.be/fr/cooperation/>

¹⁸ <https://www.vsse.be/fr/publications>

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

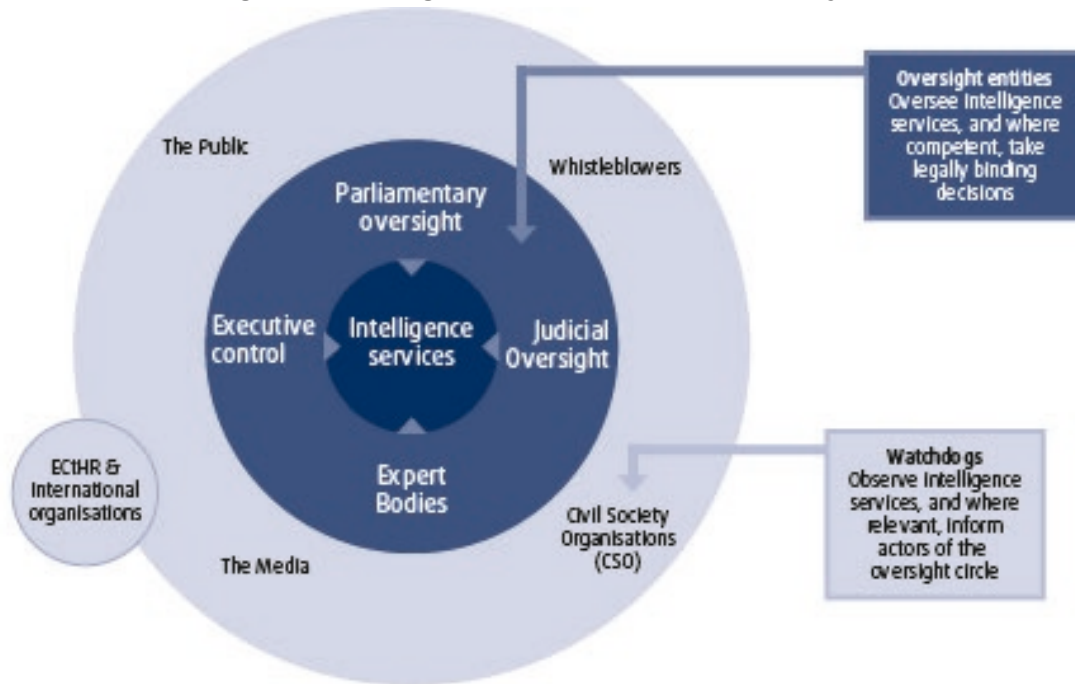


2.3. Intelligence services' accountability scheme

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

Figure 5 correctly depicts the Intelligence services' accountability scheme in an accurate manner.

Figure 5: Intelligence services' accountability scheme



2.4. Parliamentary oversight of intelligence services in EU Member States

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

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

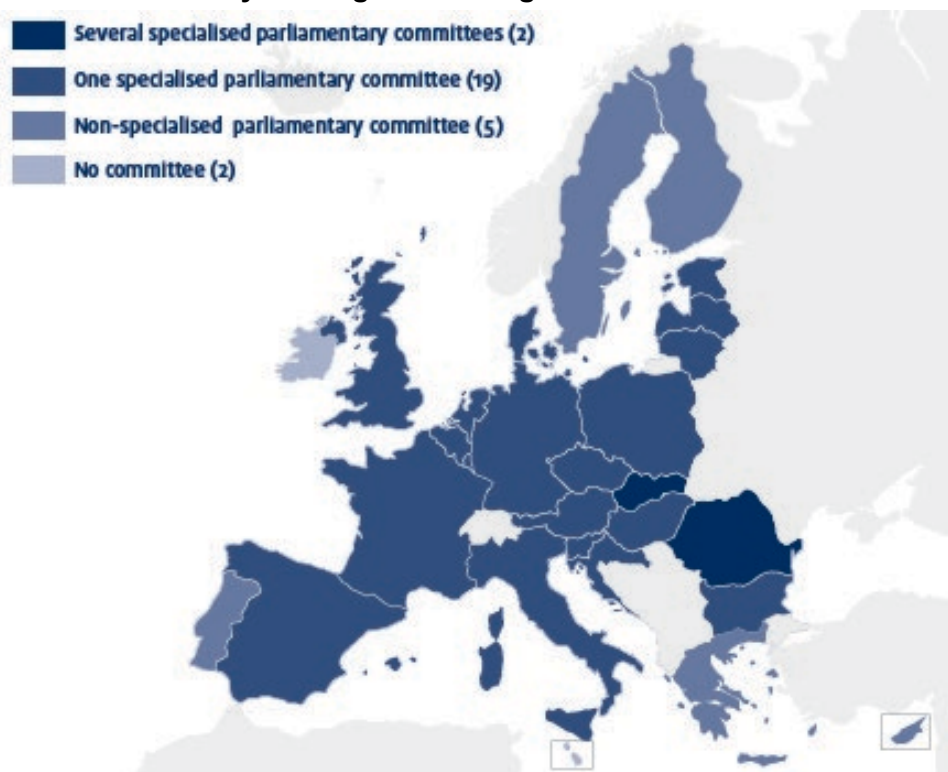


Figure 6 correctly depicts the Parliamentary oversight of intelligence services in Belgium. Indeed, one “monitoring committee”, part of the Chamber of Representatives, is in charge of monitoring the Standing Committee.

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

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

We confirm that Table 2 correctly depicts the situation in Belgium.

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

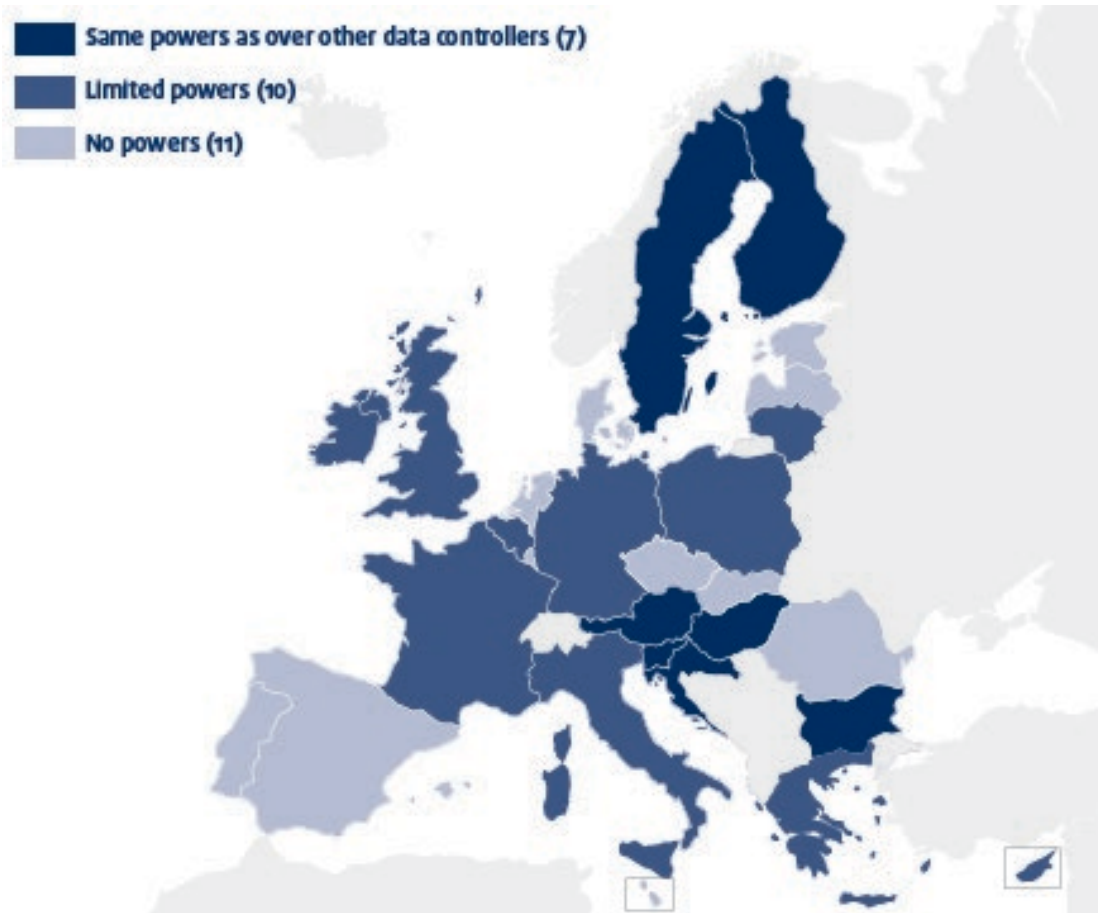
EU Member State	Expert Bodies
BE	Standing Intelligence Agencies Review Committee (<i>Vast Comité van Toezicht op de inlichtingen - en veiligheidsdiensten/Comité permanent de Contrôle des services de renseignement et de sécurité</i>) Administrative Commission (<i>Bestuurlijke Commissie/Commission Administrative</i>)

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

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

We confirm that Figure 7 correctly depicts the situation in Belgium. The Belgian DPA does not have full powers, but it has some. However, the exact scope of their powers is ambiguous in the law and in the Protocol negotiated between the Belgian DPA and the other control authorities.

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



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

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

The Standing Committee I is the authority of control when it comes to processing of personal data by security and intelligence services for carrying out the objectives of the law of 1998 on state security and surveillance, and when it comes to the processing of data by the Standing Committee I when it performs its tasks as an expert body only (so not as a DPA or a judicial body), the DPA is competent, under article 185 §4 of the law of 2018. However the legal framework for this 'control' is absent because article 185 is only 2 paragraphs.

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

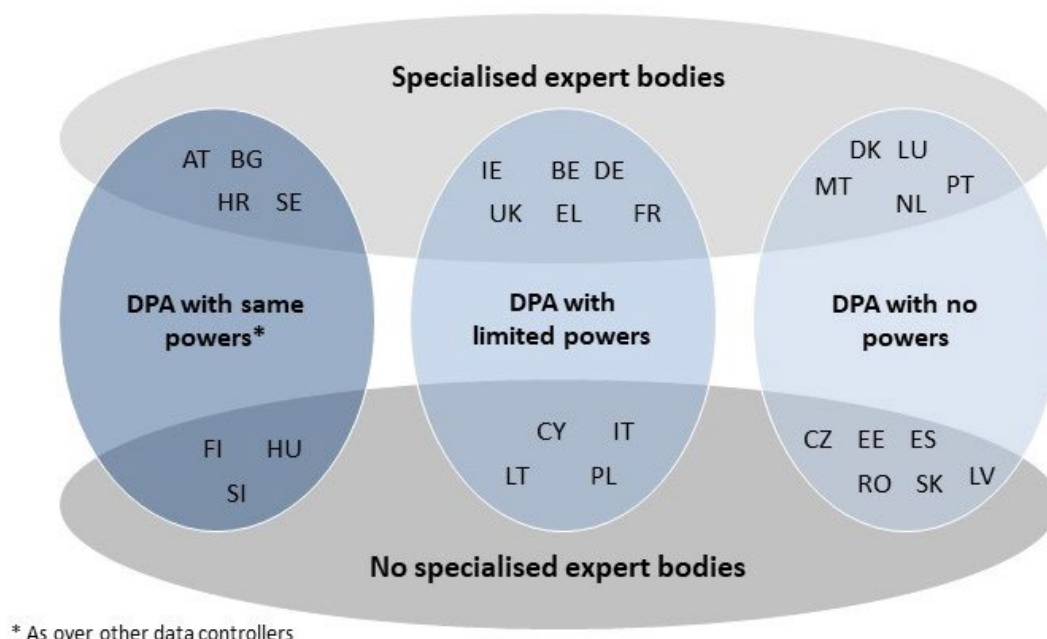


Figure 8 correctly depicts the situation in Belgium.

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

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

	Judicial	Executive	Expert bodies	Services
BE		✓	✓	✓*

Table 4 correctly depicts the situation in Belgium. It should be noted that Belgian law does not use the distinction targeted/general surveillance but rather ordinary or specific and exceptional. *Specific measures can be implemented upon the intelligence services director's decision with notification to the Administrative Committee, whereas exceptional measures require the Administrative Commission's prior approval (positive opinion).

2.8. Approval/authorisation of general surveillance of communication

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

Belgian legislation does not provide for such 'general' surveillance measures. The typology in the types of measures that can be ordered is: ordinary, specific, and exceptional.

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

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

2.9. Non-judicial bodies with remedial powers

FRANET contractors are requested to check the accuracy of table below (Table 6 (p. 112) of the FRA 2017 report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

Table 6: Non-judicial bodies with remedial powers in the context of surveillance, by EU Member State

	Executive (ministry)	Expert body(ies)	DPA	Parliamentary committee(s)	Ombuds institution
BE		✓	✗		✓

The Belgian DPA does have a general residuary power (it is competent when no other authority has been recognized by law) and for residuary applications of GDPR (i.e. personal data processing activities Standing Committee for employment purposes).¹⁹ However, article 95 of the law of 2018 on personal data states that the Standing Committee is the control authority when it comes to processing activities carried out by security and surveillance personnel under the law of 30 November 1998 (to fulfil its objectives). Moreover, the Belgian DPA website specifically indicates that any complaints regarding processing carried out by surveillance and security services is to be addressed to the Standing Committee. Thus, the DPA does not appear to have any remedial powers in the context of surveillance activities as such. The DPA does have the power to initiate an investigation/place a complaint with the Standing Committee to review surveillance measures under article 43/4 of the law of 1998.

It is worth noting that the DPA reads article 185§4 in the law of 2018 on personal data as granting it powers to control processing activities for state security/surveillance by the Standing Committee (except for the tasks that the Standing Committee carries out as Control Authority under the law of 30 July 2018 -as mentioned above). However, there is no current legal framework for such competence. So this 'potential power' appears to be moot (ineffective).

2.10. Implementing effective remedies

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

Figure 9 does not reflect the situation in Belgium.

In Belgium the rights provided for under the law of 30 July 2018 on data protection regarding processing of personal data by the surveillance and security authorities/personnel, are the following:

Right to rectification or erasure of incorrect information;

¹⁹ See article 4 of the law of 2017 on the creation of a data protection authority and p. 5 and 10 of the cooperation protocol between Control Authorities available at: <https://www.autoriteprotectiondonnees.be/publications/protocole-de-cooperation-entre-les-autorites-de-controle-federales-belges-en-matiere-de-protection-des-donnees.pdf>

- Right to request that the Standing Committee verify that the law of 2018 is correctly applied
- Right not to be subject to certain types of automated decision making

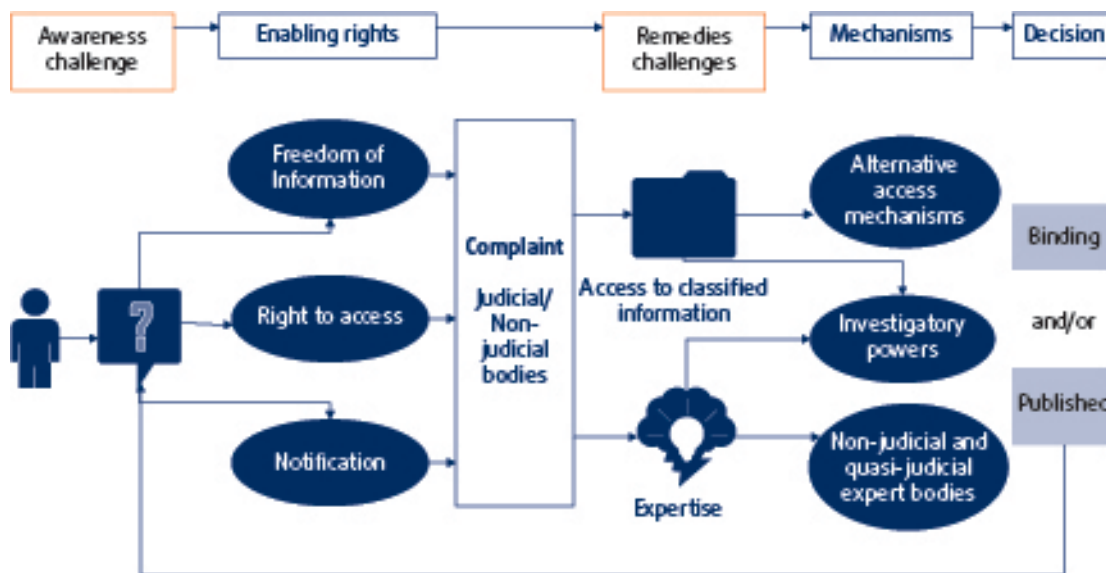
This does not mean access to any collected data.

Under the law of 30 November 1998 on Surveillance and Intelligence Services there is a right for persons with a legitimate and personal interest:

- to request to know of the existence of the application of measures (without access to the data) and at certain conditions (see footnote 2)
- complain to the standing committee/request a review of the legality of a measure, in which case access to the file will be granted if does not jeopardize state security/surveillance missions. The Standing Committee's decision is binding.

There is no active notification to subjects, implementing such a right/obligation is the purpose of the proposed 2022 amendment bill still under discussion in the parliament.

Figure 9: Implementing effective remedies: challenges and solutions








2.11. Non-judicial bodies' remedial powers

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

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

	Bodies with remedial competence	Decisions are binding	May fully access collected data	Control is communicated to complainant	Decision may be reviewed
BE	Standing Committee II				
	The federal Ombudsman				
	Privacy Commission				

Note:

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

Source: FRA, 2017

This table is no longer accurate. The Privacy Commission does not have remedial powers in the context of controlling processing activities carried out by surveillance and security services. It only has a power to initiate an investigation/place a complaint with the Standing Committee I to review surveillance measures under article 43/4 of the law of 1998 (this possibility has never been used), as well as to request to the Standing Committee I the verification of processing activities/ application of the 2018 data protection law upon complaint from an individual (thereby providing an indirect access right) under article 11 of the law of 2018 on personal data.²⁰ The Belgian Data protection authority will only respond to the complainant that the verification has been carried out.

The Belgian DPA does have a general residuary power (it is competent when no other authority has been recognized by law) and for residuary applications of GDPR (i.e. personal data processing activities carried out by the Standing Committee I for employment purposes).²¹ However, article 95 of the law of 2018 on personal data states that the Standing Committee I is the control authority when it comes to processing activities carried out by intelligence and security personnel under the law of 30 November 1998 (to fulfil its objectives). Moreover, the Belgian DPA website specifically indicates that any complaints regarding processing carried out by intelligence and security services is to be addressed to the Standing Committee. Thus, the DPA does not appear to have any remedial powers in the context of intelligence activities as such.

It is worth noting that the DPA and the Standing Committee I read article 185§4 in the law of 2018 on personal data as granting it powers to control processing activities related to national security by the Standing Committee I (except for the tasks that the Standing Committee carries out as Control Authority under the law of 30 July 2018 -as mentioned above and also excluded is the judicial role of the Committee with regard to the Special Intelligence Methods).²² However, there is no current legal framework for such competence. So, this 'potential power' appears to be moot (ineffective).

Regarding the Standing Committee's powers and informing complainants of the outcome of a control, the Standing Committee's website states that a complainant will be informed of the closing and general results of their complaint. Under 43/6 §2 of the law of 1998, there is only an obligation for the Standing Committee to inform a complainant of the outcome of the review (i.e., decision on legality) of a measure if they have placed a complaint and if that communication does not violate a series of state interest (i.e., national security, ongoing investigations, etc.).

²⁰ See the procedure at page 12 of the cooperation protocol between the Control Authorities, available at: <https://www.autoriteprotectiondonnees.be/publications/protocole-de-cooperation-entre-les-autorites-de-contrôle-federales-belges-en-matiere-de-protection-des-donnees.pdf>.

²¹ See article 4 of the law of 2017 on the creation of a data protection authority and p. 5 and 10 of the cooperation protocol between Control Authorities available at: <https://www.autoriteprotectiondonnees.be/publications/protocole-de-cooperation-entre-les-autorites-de-contrôle-federales-belges-en-matiere-de-protection-des-donnees.pdf>

²² See p. 5 and 10 of the cooperation protocol between Control Authorities available at: <https://www.autoriteprotectiondonnees.be/publications/protocole-de-cooperation-entre-les-autorites-de-contrôle-federales-belges-en-matiere-de-protection-des-donnees.pdf>

2.12. DPAs' remedial competences

FRANET contractors are required to check the accuracy of the figure below (Figure 10 (p. 117) of the FRA 2017 report) with respect to the situation in your Member State. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

Figure 10 does correctly depict the situation in Belgium (see explanation above) The Belgian DPA does not have remedial powers, but has the power to request to the Standing Committee the verification of processing activities/application of the 2018 data protection law upon complaint from an individual (thereby providing an indirect access right – the DPA will respond to an individual that the ‘verifications have been effectuated’) and the power to initiate an investigation/review (by the Standing Committee I) of a surveillance measure.

Figure 10: DPAs' remedial competences over intelligence services

