FRA EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

SURVEILLANCE BY INTELLIGENCE SERVICES

FUNDAMENTAL RIGHTS SAFEGUARDS AND REMEDIES IN THE EU - 2023 UPDATE

REPORT



Contents

About this publication 4

Executive summary 5

Introduction 6

Reforms of legal frameworks for surveillance 7

Applicability of European Union Law 9

Convention 108+ 11

Fundamental rights safeguards: recent case law 12

1. Accountability 14

1.1 Relevant updated key findings 14

1.2 Selected 2017 FRA opinions 14

1.3 Intelligence services' accountability scheme 16

1.4 An imperative: internal control within intelligence services 16

1.5 Stages of oversight and diversity of players 17

1.5.1 Ex ante authorisation 17

1.5.2 Ongoing and ex post oversight 20

Parliaments 21

Expert bodies and data protection authorities 22

1.5.3 Models of oversight frameworks of intelligence services based on different players involved 30

Model 1 30

Model 2 31

Model 3 32

Model 4 33

Model 5 34

2. Remedies 36

2.1 Relevant updated key findings 36

2.2 Selected 2017 FRA opinions 37

2.3 Remedial powers of data protection authorities 42

2.4 Remedial powers of other non-judicial oversight bodies 43

3. Conclusions 45

Case law (post-2017) 46

Court of Justice of the European Union 46

European Court of Human Rights 46

National courts 46

Annex 1 - Overview of intelligence services in the EU-27 48

Annex 2 - Oversight and review of surveillance 54

Endnotes 55

About this publication

© European Union Agency for Fundamental Rights, 2023

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the European Union Agency for Fundamental Rights copyright, permission must be sought directly from the copyright holders.

Neither the European Union Agency for Fundamental Rights nor any person acting on behalf of the Agency is responsible for the use that might be made of the following information.

HTML

- ISBN: 978-92-9489-117-4
- DOI:10.2811/197238
- TK-09-23-126-EN-Q

PDF

- ISBN: 978-92-9489-116-7
- DOI:10.2811/079962
- TK-09-23-126-EN-N

Photo credits (cover & inside):

- Cover: © ImageFlow/stock.adobe.com

FRA – EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS
Schwarzenbergplatz 11 – 1040 Vienna – Austria
T +43 158030-0 – F +43 158030-699

- Website
- Facebook
- Twitter
- LinkedIn

Executive summary

This report provides a partial update on the findings of the 2017 European Union Agency for Fundamental Rights (FRA) report *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU*. It was prepared at the request of the European Parliament, which asked FRA to update its 2017 findings to support the work of its committee of inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA).

The 2017 report highlighted that fundamental rights related to the respect for private and family life (Article 7), the protection of personal data (Article 8) and an effective remedy and a fair trial (Article 47) of the Charter of Fundamental Rights of the European Union should be protected by setting up strong oversight systems and effective remedies open to individuals in the context of surveillance by intelligence services.

The current report updates relevant parts of the 2017 report. Like the 2017 report, this update focuses on the work of intelligence services. It describes the developments that have taken place since 2017 in intelligence laws in the European Union (EU).

Significant developments that have taken place include the welcomed establishment of new oversight bodies following constitutional courts' decisions and the impact of the 2016 European data protection reform on data protection authorities' powers in the field of intelligence services' activities. In 2023, 18 expert bodies are overseeing the work of intelligence services in the EU-27, compared with 16 in the EU-28 in 2017.

These developments are viewed in the light of minimum requirements shaped by the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR). In this context, the current report refers to a selection of relevant FRA opinions drawn from the 16 opinions published in the 2017 FRA report, alongside key findings from this earlier report. It also highlights relevant developments over time.

In particular, it provides, as per the European Parliament's request, up-to-date information on existing models of oversight mechanisms and remedies, illustrating them with examples from selected Member States. The report describes five distinct models of oversight frameworks. These encapsulate the diverse spectrum of frameworks across the EU Member States.

In 2017, FRA concluded that protecting the public from security threats while respecting fundamental rights can be achieved through strong oversight systems and effective remedies open to individuals. This conclusion remains valid in 2023.

Introduction

This report provides a partial update of the 2015 and 2017 European Union Agency for Fundamental Rights (FRA) reports entitled *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU* (the 2017 report is henceforth referred to as the 2017 FRA report). [1] The 2017 FRA report was FRA's response to the European Parliament's request for in-depth research on the impact of surveillance on fundamental rights. [2]

Following the 2013 Snowden revelations, FRA focused on the large-scale technical collection of intelligence, referred to as the general surveillance of communications and colloquially known as "mass surveillance". In the context of surveillance by intelligence services, the 2017 FRA report highlighted how the right to respect for private and family life (Article 7), the right to protection of personal data (Article 8) and the right to an effective remedy and a fair trial (Article 47) of the Charter of Fundamental Rights of the European Union (the Charter) should be protected by setting up strong oversight systems and effective remedies open to individuals.

The European Parliament's request

In the latter part of 2022, the European Parliament asked FRA to prepare this update to support the work of the committee of inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA Committee). In particular, the Parliament asked FRA to present different existing models of oversight mechanisms and to illustrate them with examples from selected Member States.

The European Parliament asked the PEGA Committee to gather information on how much Member States or non-European Union (EU) countries are using intrusive surveillance to the extent that it violates the rights and freedoms enshrined in the Charter. [3] In undertaking this task, the PEGA Committee held a significant number of hearings, published various studies and briefings, and undertook fact-finding missions. [4]

The present update builds on the 2017 FRA report and the 16 FRA opinions therein. This update refers to relevant FRA opinions and key findings from the 2017 FRA report. FRA's multidisciplinary research network (Franet) provided updated national data that formed the basis of this comparative analysis.

Like the 2017 FRA report, this update focuses on the work of intelligence services. It presents developments since 2017 in intelligence laws in the EU. The report specifically addresses the work of intelligence services, as listed in Table 5 (see Annex 1). Just as the 2017 FRA report did not address in detail the use of intelligence techniques such as spyware in the EU, or secret surveillance in the context of police work and criminal investigations, this update does not deal

with these issues. [5]

The legal frameworks on spyware are discussed in detail in the draft report the PEGA Committee prepared, [6] in a proposed Recommendation of the European Parliament [7] and in reports prepared as part of the committee's work. [8] The United Nations High Commissioner for Human Rights also dealt with the widespread abuse of intrusive hacking tools and the need for enhanced safeguards on their use. [9] The Council of Europe's Parliamentary Assembly is also addressing the issue, [10] and the Commissioner for Human Rights issued a comment. [11]

This update focuses on two key aspects of the accountability of intelligence services, namely oversight and remedies. These two aspects should be enshrined in every secret surveillance framework to protect against abuse, as both the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) emphasise.

> **"In view of the risk that a system of secret surveillance set up to protect national security (and other essential national interests) may undermine or even destroy the proper functioning of democratic processes under the cloak of defending them, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on […] the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law."**
>
> *ECtHR, Big Brother Watch and Others v. the United Kingdom, Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021*

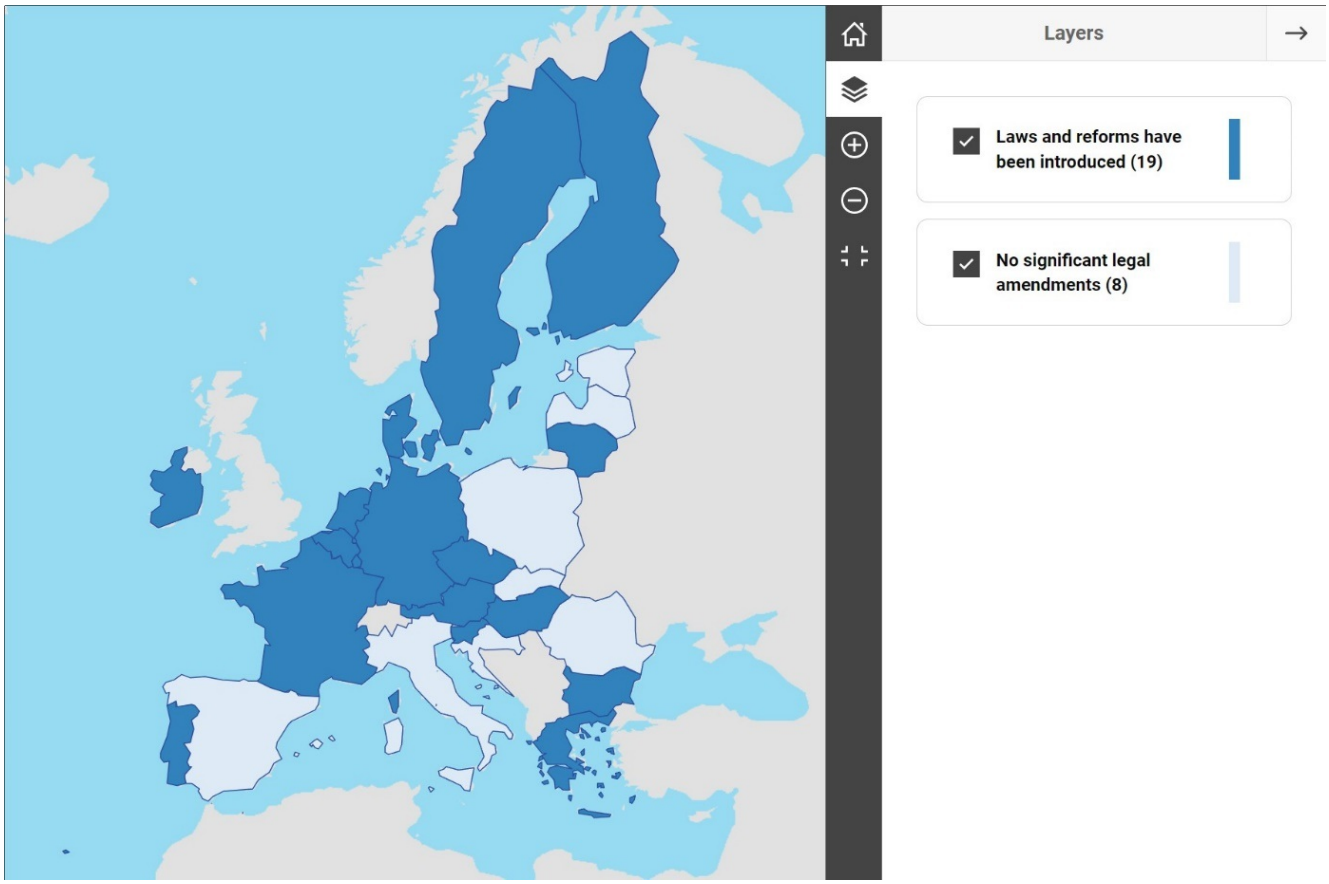
Reforms of legal frameworks for surveillance

Several key legal developments have taken place since the publication of the 2017 FRA report. For example, the CJEU and ECtHR issued seminal judgments on the transatlantic flow of data and surveillance by intelligence services; the General Data Protection Regulation (GDPR) [12] and the Law Enforcement Directive [13] entered into force at EU level, (hereafter referred to as the 2016 European data protection reform); and the Council of Europe adopted the modernised convention for the protection of individuals with regard to the processing of personal data (Convention 108+). [14] Such legal developments have necessitated changes to national intelligence laws, thus

requiring FRA to update its data to reflect such legal reforms.

Figure 1 presents an overview of reforms of legal frameworks on surveillance that have taken place in the EU-27 since the 2017 FRA report was published. The majority of EU Member States (17) have reformed, or are in the process of reforming, their legal frameworks on intelligence services. Legal changes have been quite diverse, ranging from changes in organisational issues to changes in the accountability regimes of intelligence services and remedies against their actions.

Figure 1 – EU Member States' legal frameworks for surveillance – reforms since mid-2017



Source: FRA, 2023

Reforms were triggered for various reasons beyond legal developments at EU level, requiring incorporation at EU Member State level. In Austria, for example, findings of a parliamentary enquiry on serious misconduct and corruption of intelligence officials and the response to the terrorist attack in Vienna on 2 November 2020 led to the creation of a new agency. [15] A new specialised and independent oversight body was also established as a result of the reforms. [16]

Greece has also amended its legal framework several times since 2017. The changes involved various issues, such as the organisation of intelligence services, [17] the authorisation of surveillance, and the abolishment and subsequent reintroduction of notification of surveillance. [18] The latest of these amendments were made in response to complaints against the intelligence services regarding the inappropriate monitoring of communications of politicians

and journalists. Allegations that unknown actors were using illegal spyware to monitor the communications of politicians, journalists and other public figures, as reported in the media, also necessitated these changes. [19] In response to the spyware allegations, investigations were initiated by the Greek data protection authority (DPA) and criminal authorities.

FRA data suggest that spyware revelations since 2021 have had almost no impact on national reforms to date, except in Greece, where reforms in December 2022 addressed the regulation of spyware. [20] In August 2022, the Prime Minister of Spain announced plans to reform the law on intelligence services. [21] At the time of writing, no draft law had been published. In addition, the government's 2023 action plan does not refer to such a reform. [22]

In some cases, court judgments on successful constitutional or administrative law challenges against intelligence laws necessitated amendments to such laws, such as in France, [23] Germany [24] and Portugal. [25] In Germany, for example, among other changes, a new oversight body was set up in 2021. [26]

Data protection reforms following the implementation of the 2016 European data protection reform also led to restrictions on or exclusions in the powers of national DPAs to exercise oversight over intelligence services in some countries, such as Bulgaria, [27] Croatia, [28] Greece [29] and Lithuania. [30] In others, such as Hungary, changes do not appear to have substantially strengthened the DPAs. [31] In some Member States, such as Cyprus and Luxembourg, reforms appear to have reinforced the role of national DPAs (see the section 'Expert bodies and data protection authorities').

Applicability of European Union Law

Member States' activities protecting national security do not fall under EU competence, according to Article 4 (2) of the Treaty on European Union. The "national security exemption" is also reflected in the GDPR and the Directive on Privacy and Electronic Communications. [32]

Nonetheless, the 2017 FRA report discussed this exemption and highlighted examples of intelligence services' activities that are within the scope of EU law and therefore subject to EU law protecting fundamental rights, in addition to guarantees applying to the same rights under national constitutional provisions and international human rights treaties. The report suggested that the protection the GDPR offers could well apply to the transfer of communications data by service providers to intelligence services for national security purposes. [33] The 2017 FRA report concluded that "the 'national security' exemption thus cannot be seen as entirely excluding the applicability of EU law". [34] A report requested by the PEGA Committee concurred with this finding. [35]

The CJEU has since confirmed this conclusion, stating that invoking national security cannot justify the avoidance of EU law, including scrutiny under the Charter. [36] The court clarified this in relation to general data retention and access, and real-time access to communications data when

protecting national security. [37] The court also defined protecting national security as the "protection of the essential functions of the State and the fundamental interests of society" against actions "destabilising the fundamental structures of a country" and threatening the population. [38]

Moreover, the court specified that protecting public security and combating serious crime cannot be treated in the same way. [39] By defining the protection of national security, the court tried to rule out the possibility of invoking it as a pretext for other purposes.

> **"[T]he mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law".**

> **"[N]ational security […] corresponds to the primary interest [of Member States] in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities".**

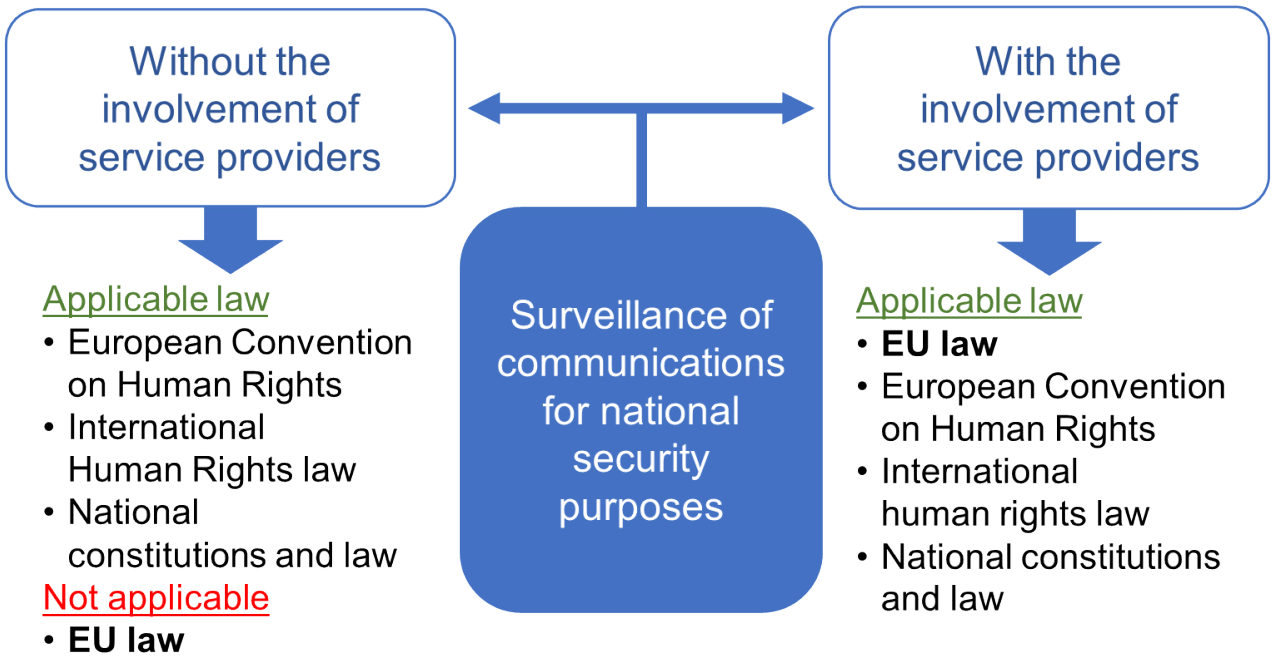
CJEU, Joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v. Premier ministre and Others and Ordre des barreaux francophones et germanophone and Others v. Conseil des ministres [GC], 6 October 2020, paragraphs 99 and 135

In the field of surveillance for national security purposes, the CJEU found that it is always private parties (i.e. service providers) that retain and provide access to communications data – in real time or not – on the request of state authorities, based on law. These activities are not performed directly by state organs. Retaining and providing access to data or transmitting data to state authorities for national security purposes are permitted by provisions that derogate from the principle of the confidentiality of communications established in the Directive on Privacy and Electronic Communications. Hence, data retention and access for national security purposes fall within the scope of EU law. [40]

CJEU case law also had a significant impact at national level. In France, for example, a CJEU ruling led to a decision of the Council of State (*Conseil d'État*) [41] that triggered an amendment of the intelligence law in relation to the binding character of the opinions of the French oversight body. In 2020, noting the pending case before the CJEU at the time, the German Federal Constitutional Court (*Bundesverfassungsgericht*) ruled that surveillance by intelligence services on foreign communications violated fundamental rights set out in the German Basic Law. [42] One of the reasons was that the powers and the organisational and institutional design of the competent bodies did not ensure extensive independent and continuous oversight. [43]

In a nutshell, some aspects of the intelligence services' work, namely surveillance of communications data, cannot be completely excluded from the scope of EU law, including the Charter. The CJEU also highlighted that secret surveillance techniques that are outside the scope of EU law should comply with the corresponding requirements of the European Convention on Human Rights. [44] Figure 2 summarises the applicability of EU law in the context of the national security exemption, as defined in the CJEU case law to date.

Figure 2 – Applicability of EU law in the context of intelligence services' activities



Source: FRA, 2023

Convention 108+

In 2018, the Committee of Ministers of the Council of Europe decided to open Convention 108+ for signature. Once the convention enters into force, it will play an important role in surveillance by intelligence services. Article 3 of Convention 108+ does not exclude from its scope of application actions that States Parties take to protect national security. [45] Furthermore, States Parties are no longer provided with the opportunity to make declarations granting complete exemption from the application of the convention data processing in the context of national security.

Under Article 11 of Convention 108+, States Parties may introduce exceptions in the areas outlined, provided that such exceptions respect "the essence of the fundamental rights" and comply with the principles of necessity and proportionality. Furthermore, Article 11 (3) of the convention states that data processing for national security and defence purposes should be subject to independent and effective review and supervision by a supervisory authority. This supervisory authority should have the powers and characteristics set out in Article 15 of Convention 108+.

Convention 108+ allows intelligence services to engage in surveillance activities to protect national security, provided that such activities "are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the data subjects". [46] Moreover, intelligence services should be subject to independent and effective review and supervision by one or more authorities. The authorities should also ensure their compliance with the convention's applicable provisions.The explanatory report on the convention makes clear reference to the applicability of requirements developed in the case law of the ECtHR in this regard. [47]

Fundamental rights safeguards: recent case law

The 2017 FRA report was structured based on the ECtHR case law requirements. The report focused on three key aspects:

- the legal framework on surveillance and the requirement for clear, foreseeable and accessible laws regulating secret surveillance;
- the accountability of intelligence services, focusing on existing oversight bodies with appropriate powers;
- the availability of effective remedies for individuals before remedial bodies with appropriate powers.

Since 2017, both the CJEU and the ECtHR have further elaborated their case law requirements regarding surveillance by intelligence services. With regard to oversight and remedies in particular, their requirements are essentially aligned. Some notable developments include the following.

The CJEU held that:

- intelligence services can apply secret surveillance when it genuinely pursues the protection

of national security based on the court's definition; [48]

- only a "genuine and present or foreseeable" serious threat to national security justifies measures that apply indiscriminately to all users of communications systems. [49]

Both European courts stressed the following key aspects of accountability in the surveillance of communications by intelligence services.

- Secret surveillance should be subject to clear and publicly accessible legal rules, which include the necessary safeguards against abuses of surveillance techniques carried out for national security purposes. [50]
- Independent authorities and the courts should review and supervise the implementation of the relevant rules and conditions during the authorisation and implementation of surveillance measures by intelligence services. [51]
- Individuals under surveillance should have recourse to remedies that are effective in practice for reviewing the lawfulness and proportionality of any surveillance against them and redressing any violations of their rights. [52]
- The ECtHR emphasised that remedial bodies should possess guarantees of "objectivity and thoroughness" to ensure that there are no conflicts of interest with the body that authorised and supervised the surveillance. [53]
- The ECtHR also clarified that notification of surveillance, which is required as soon as the purpose of the surveillance would not be jeopardised, cannot depend on a national security exemption. [54] Unless remedies depend on it, notification may be omitted when affected individuals can request and receive relevant information through a competent independent authority. [55]

Both courts confirmed that the above main requirements apply to the targeted surveillance of data, the bulk interception of communications data, and service providers' retention of communications data and authorities' subsequent access, real time or not, to the data. [56] The treatment of different types of data once obtained may differ. [57]

Recent European case law has elaborated on the requirements applicable to the life cycle of surveillance activities that intelligence services conduct. Figure 13 (in Annex 2) summarises the requirements the ECtHR and the CJEU have developed.

This update is structured as follows: the first part focuses on accountability through the oversight of intelligence services, while the second part discusses remedies available at EU Member State level.

1. Accountability

1.1 Relevant updated key findings

Oversight bodies have diverse roles, including overseeing the legality of the intelligence services' functioning, efficiency and policies.

The judiciary and/or an expert body normally oversee surveillance. Currently, in 18 of the 27 Member States that this report covers, compared with the 28 that were covered in the 2017 report, expert bodies are part of the oversight system. In 19 Member States – not necessarily including the same ones – judicial authorities authorise targeted surveillance measures.

In 25 Member States, parliaments are involved in oversight. In 22 of these, one or two specialised parliamentary committees are involved in overseeing intelligence services. In the other three of these, a non-specialised committee is responsible for this task.

In five Member States, DPAs have the same powers over intelligence services as over all other data controllers. In 15 Member States, DPAs have no power over intelligence services. In seven Member States, their powers are limited. Following the entry into force of the 2016 European data protection reform, seven Member States have restricted or excluded DPAs from exercising supervision over data processing by intelligence services.

Five Member States have detailed provisions on the general surveillance of communications. Of these Member States, three provide for the binding involvement of an independent body in the authorisation of surveillance measures. In the other two Member States, the opinions of the oversight body are not binding.

There is a great diversity of oversight frameworks in the EU Member States. Five models of oversight frameworks based on the different actors overseeing the intelligence services illustrate this diversity.

1.2 Selected 2017 FRA opinions

Opinion 2: Ensuring broad consultation and openness during the legislative process

EU Member States should undertake broad public consultations with a full range of stakeholders, ensure transparency of the legislative process, and incorporate relevant international and European standards and safeguards when introducing reforms to their legislation on surveillance.

Opinion 3: Providing independent intelligence oversight with sufficient powers and competences

EU Member States should establish a robust oversight framework adequate to the powers and capacities that intelligence services have. The independence of oversight bodies should be enshrined in law and applied in practice. EU Member States should grant oversight bodies adequate financial and human resources, including diverse and technically-qualified professionals. Member States should also grant oversight bodies the power to initiate their own investigations as well as permanent, complete and direct access to necessary information and documents for fulfilling their mandate. Member States should ensure that the oversight bodies' decisions are binding.

Opinion 4: Bolstering oversight with sufficient technical expertise

EU Member State laws should ensure that oversight bodies have staff with the required technical expertise to assess independently the intelligence services' often highly technical work.

Opinion 5: Ensuring oversight bodies' openness to public scrutiny

EU Member States should ensure that oversight bodies' mandates include public reporting to enhance transparency. The oversight bodies' reports should be in the public domain and contain detailed overviews of the oversight systems and related activities (e.g. authorisations of surveillance measures, on-going control measures, ex-post investigations and complaints handling).

Opinion 6: Fostering continuity of oversight

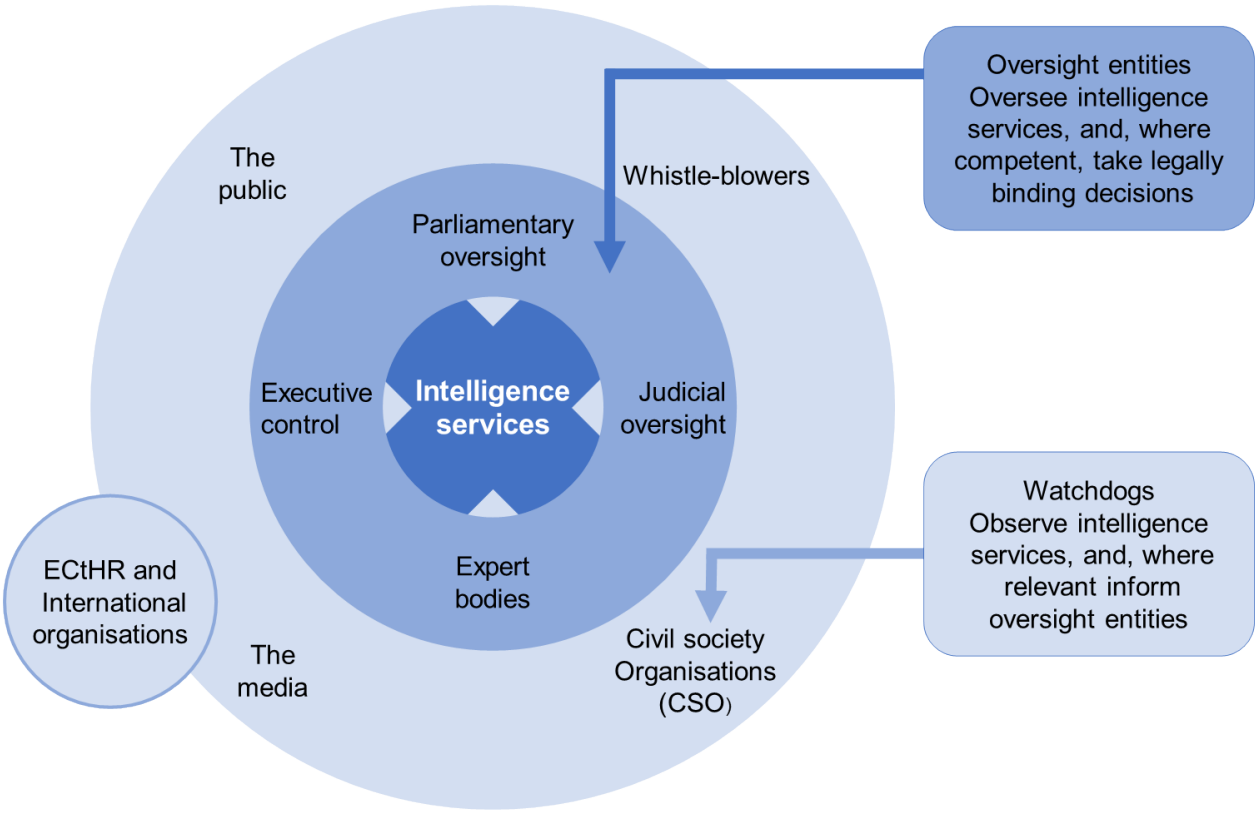
EU Member States should ensure that the oversight bodies' mandates complement each other, so that, overall they provide continuous control and ensure proper safeguards. Such complementarity can be achieved with informal cooperation between oversight bodies or statutory means.

Source: FRA 2017

1.3 Intelligence services' accountability scheme

In preparing this update, FRA confirmed the accuracy of the intelligence services' accountability scheme, as presented in the 2017 FRA report. This update will focus on entities performing oversight during the different stages of surveillance, while recognising the important role that watchdogs, such as the media, whistle-blowers and civil society organisations, play. The Pegasus revelations provided us with yet another example of the essential role that civil society organisations and the media play. Figure 3, first presented in the 2017 FRA report, illustrates the main actors that contribute to the oversight of intelligence services and their accountability.

Figure 3 – Intelligence services' accountability scheme



Source: FRA, 2023

1.4 An imperative: internal control within intelligence services

The 2017 FRA report emphasised that a crucial precondition for the effective oversight of intelligence services' activities is the proper internal control of the services themselves. [58] FRA did not collect up-to-date data on the control exercised by intelligence services or government bodies.

A clear understanding of the legal obligations of intelligence services facilitates effective supervision of them. For example, the French oversight body justifies the low number of negative opinions on requested surveillance techniques based on intelligence services' good understanding of the law. [59] Awareness can also be enhanced through a memorandum of understanding. For example, in Italy the DPA and the coordinator of the intelligence services (the Security Intelligence Department– DIS). [60]

1.5 Stages of oversight and diversity of players

1.5.1 Ex ante authorisation

Notes on terminology

General surveillance of communications

Intelligence can be collected by technical means and on a large scale. This surveillance technique is referred to in different ways, including as "signals intelligence", "strategic surveillance", "bulk investigatory powers", "mass digital surveillance" and "storage of data on a generalised basis". Whenever possible, FRA uses the national laws' terminology. However, it also uses – as a generic, all-encompassing term – "general surveillance of communications".

Targeted and untargeted surveillance

Based on whether or not a target exists, surveillance measures can be divided into targeted and untargeted surveillance. Targeted surveillance presupposes the existence of prior suspicion of a targeted individual or organisation. Untargeted surveillance is conducted without prior suspicion or a specific target.

Source: FRA, 2017

Effective oversight of surveillance operations requires, among other things, that independent oversight be present when the surveillance measures are first ordered, as the 2017 FRA report stressed. [61] Both the CJEU and the ECtHR underline that any measure for secret surveillance should be subject to prior authorisation, preferably by a court or another independent authority. [62] The authorising authority should ensure that any requested measures are proportionate and necessary in practice to protect national security. [63]

Table 1 shows the different bodies that have a binding/final decision in the authorisation or approval processes for different types of targeted surveillance measures. The information

provided for an individual Member State covers all potential actors with binding decision-making powers in authorising targeted surveillance measures. Pegasus and the other spyware related to the PEGA Committee's work fall within the category of targeted surveillance. [64]

In several Member States, two or more bodies authorise surveillance techniques. The modalities and details of this authorisation process vary considerably among Member States and depend on the different types of surveillance measures involved, as the 2017 FRA report states.

Table 1 – Binding authorisation/approval of targeted surveillance measures in the EU-27

Member State	Judicial bodies	Executive	Expert bodies	Intelligence services
AT			✓	
BE		✓	✓	✓
BG	✓			
CY		✓		
CZ	✓			
DE		✓	✓	
DK	✓			
EE	✓			
EL	✓			
ES	✓			
FI	✓			
FR	✓*	✓		
HR	✓			
HU	✓	✓		✓
IE	✓	✓		
IT	✓			
LT	✓			
LU		✓	✓	✓
LV	✓			

Member State	Judicial bodies	Executive	Expert bodies	Intelligence services
MT		✓		
NL	✓	✓	✓	
PL		✓		✓
PT**				
RO	✓			
SE	✓			
SI	✓			✓
SK	✓			

Notes:

* In France, when the expert body issues a negative opinion on the use of a surveillance technique, if the Prime Minister wishes to disregard the opinion the expert body immediately brings the matter before the Council of State. The council then issues a final binding decision.

** In Portugal, the constitution only allows public authorities to interfere with correspondence, telecommunications and other means of communication in criminal proceedings, which the intelligence service is not allowed to conduct. The intelligence service is therefore prohibited from carrying out this type of surveillance.

Source: FRA, 2023

One notable example of a legal reform regarding the authorisation of surveillance measures is the 2021 reform in France. This reform strengthened the decision-making power of the expert body. If the Prime Minister decides not to consider a negative opinion delivered by the National Commission for Control of Intelligence Techniques (*Commission nationale de contrôle des techniques de renseignement*, CNCTR), the CNCTR must immediately refer the case to the Council of State. The council takes the final decision. [65] While a negative opinion used to be non-binding, it has now become “blocking”. [66]

The Netherlands provides another example, with the establishment of a new body – the Investigatory Powers Commission (*Toetsingscommissie inzet bevoegdheden*) – in 2017. The commission became operational in May 2018. [67] Its task is to assess in advance the legality of the government’s authorisation of the surveillance techniques that intelligence agencies employ. [68] If it deems the authorisation unlawful, surveillance cannot proceed. [69]

Five EU Member States have detailed laws on the general surveillance of communications. As anticipated in the 2017 FRA report, since 2017, Finland has completed its wide-reaching

intelligence law reform. The reform included new legislation that details the general surveillance of communications by intelligence services. [70] Table 2 presents the bodies that have the power to provide final authorisation for the general surveillance of communication measures in the Member States that implement such surveillance techniques.

Table 2 – Approval/authorisation of general surveillance of communications in EU Member States

Member State	Judicial bodies	Parliamentary committees	Executive	Expert bodies
DE		✓		✓
FI	✓			
FR	✓*		✓	
NL			✓	✓
SE				✓

Note: * In France, when the expert body issues a negative opinion on the use of a surveillance technique, if the Prime Minister wishes to disregard the opinion, the expert body immediately brings the matter before the Council of State. The council then issues a final binding decision.

Source: FRA, 2023

The 2021 reform in Germany specified the threshold for the general surveillance of foreign communications. In addition, it tasked its new expert body – the Independent Supervisory Council (Unabhängiger Kontrollrat) – with approving the general surveillance of foreign communications ordered by the Federal Intelligence Service (Bundesnachrichtendienst). [71] In the Netherlands, the Investigatory Powers Commission (*Toetsingscommissie inzet bevoegdheden*) assesses the legality of the ministerial authorisation provided to intelligence services to acquire real-time and fully automated access to databases or for the large-scale monitoring of internet traffic. [72] In Finland, 2019 laws granted intelligence services the power to conduct the general surveillance of communications techniques, albeit under strict conditions and court authorisation.

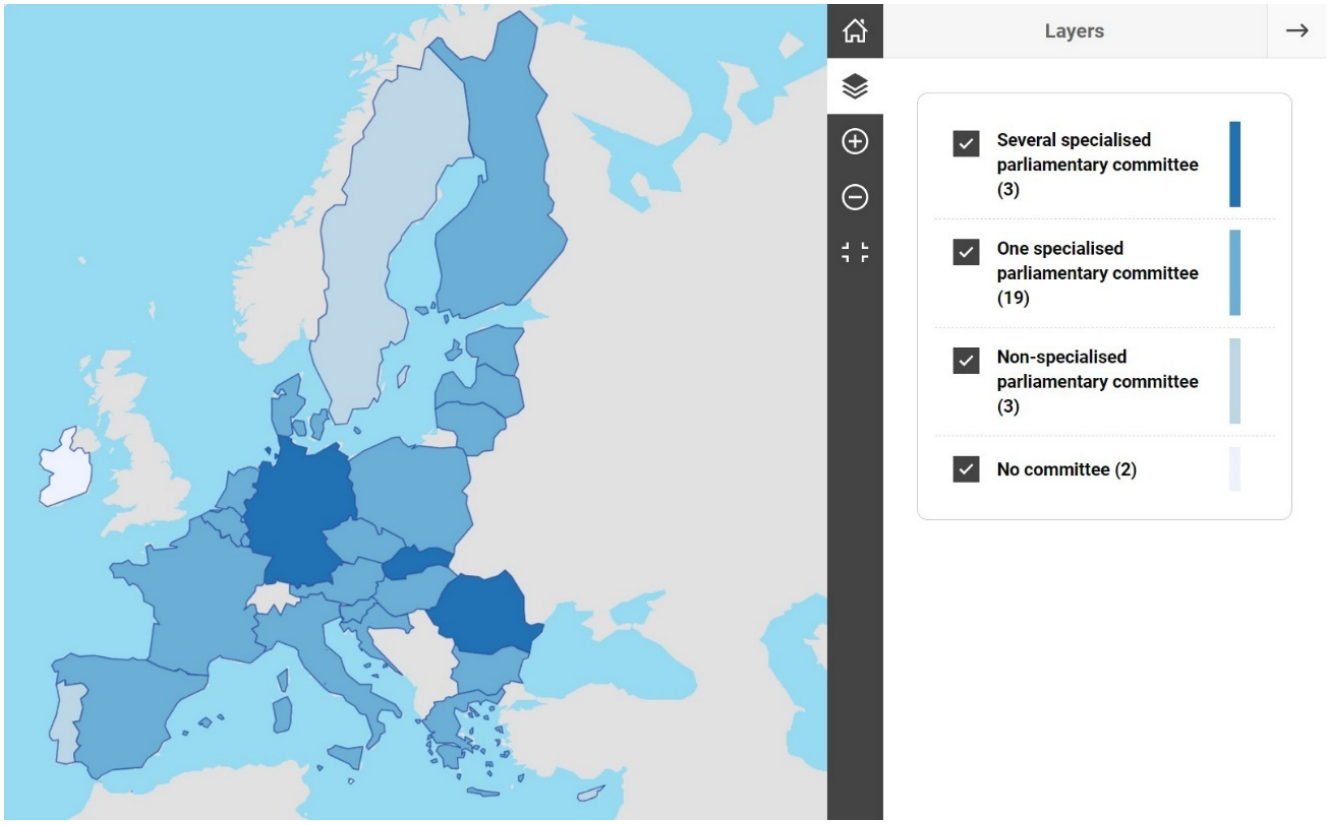
Intelligence services can acquire communications data based on the automated segregation of data traffic and the processing of acquired data concerning transborder data traffic.Network traffic is selected based on objective criteria – search terms or search term categories – subject to court authorisation.For the court to grant authorisation, the intelligence service must justify that it is necessary to screen specific traffic during a specific period. [73] Such data should provide information about activities that pose a serious threat to national security that is otherwise unattainable. [74]

1.5.2 Ongoing and ex post oversight

Parliaments

National parliaments are responsible for holding the executive accountable for its actions. The findings of the 2017 FRA report are still relevant, namely that the vast majority of EU Member States provide for parliamentary oversight through specialised or non-specialised parliamentary committees (see Figure 4). The only two exceptions are Ireland and Malta, which do not provide for some sort of parliamentary oversight of intelligence services. In three Member States – Cyprus, Poland and Sweden – this task is assigned to a non-specialised committee. In the other 22 Member States, parliamentary oversight is exercised by specialised parliamentary committees.

Figure 4 – Parliamentary oversight of intelligence services in the EU-27



Source: FRA, 2023

For example, in Finland, the newly established Intelligence Oversight Committee (*Tiedusteluvalvontavaliokunta*) oversees the proper implementation and appropriateness of intelligence operations; monitors and evaluates the focus areas of intelligence operations; monitors and promotes the effective exercise of fundamental and human rights in intelligence operations; provisionally considers reports of the Intelligence Ombudsman, before a discussion in plenary; and processes the supervisory findings of the Intelligence Ombudsman. [75]

In addition, in France, the powers of the parliamentary committee responsible for intelligence services (*Délégation parlementaire au renseignement*, DPR) have been enhanced. [76] Among other things, it can now request any document or information, implement any assessment consideration needed to carry out its duties and hold hearings of people exercising management duties within intelligence services. The scope of the DPR has been extended to include the monitoring of current issues and the determination of future challenges to public intelligence policy. It is in this context that the DPR addressed Pegasus in its latest report. [77]

The role of parliamentary oversight of intelligence services can be crucial for the overall functioning of intelligence services. In Austria, for example, the abolishment and replacement of the intelligence service in 2021 is mainly attributed to the findings of a parliamentary enquiry committee that established serious shortcomings in the service. [78] The effectiveness of parliamentary oversight must be assessed in practice, as required by case law. In the case of *Zoltan Varga v. Slovakia*, the ECtHR highlighted some shortcomings in relation to parliamentary oversight. [79] Shortcomings were also detailed in the case of *Ekimdzhiev and Others v. Bulgaria*. The court noted, first, that the committee members do not need to have legal qualifications or experience and, second, that the committee "has no power to order remedial measures in concrete cases". [80]

Expert bodies and data protection authorities

The 2017 FRA report presented the various expert oversight bodies established in the Member States and analysed the oversight frameworks, alongside the features and powers of these bodies. The report stated that these bodies should have "two essential qualities: be independent and have sufficient powers to carry out continuous control that is subject to public scrutiny". [81] These powers relate, on the one hand, to the appropriate review of the measures and, on the other hand, to the oversight bodies' ability to ensure that effective action is taken if they find irregularities. [82]

Since 2017, six Member States – Czechia, Finland, Germany, Lithuania, Luxembourg, and the Netherlands – have set up new, or replaced old, expert bodies dedicated to the oversight of intelligence services.

In Czechia, the establishment of a new oversight body is regulated by a 2018 law. This body has not become operational yet because of the high number of requirements imposed on its members. They should, among other things, hold top secret clearance, have no connection to the intelligence services and be over the age of 40. Additional requirements were removed in 2022 to facilitate the procedure for nominating members. [83]

The section below provides an updated list of bodies specialised in intelligence oversight, excluding DPAs. For the purpose of this report, DPAs are considered expert bodies. However, as they are not specialised in intelligence oversight, except in Belgium, they are dealt with separately.

Expert bodies, excluding DPAs, overseeing intelligence services in the EU-27

Austria

- Legal Protection Commissioner at the federal Ministry of the Interior (*Rechtsschutzbeauftragter beim Bundesminister für Inneres*)
- Independent Control Commission on the Protection for the Constitution (*Unabhängige Kontrollkommission Verfassungsschutz*)

Belgium

- Standing Intelligence Agencies Review Committee (Standing Committee I) (Vast Comité van Toezicht op de inlichtingen – en veiligheidsdiensten/Comité permanent de Contrôle des services de renseignement et de sécurité)*
- Administrative Commission (Bestuurlijke Commissie/Commission Administrative)

Bulgaria

- National Bureau for Control over Special Intelligence Means (Национално бюро за контрол на специалните разузнавателни средства)

Croatia

- Office of the National Security Council (*Ured Vijeća za nacionalnu sigurnost*)
- Council for Civilian Oversight of Security and Intelligence Services (*Vijeće za građanski nadzor sigurnosno-obavještajnih agencija*)

Cyprus

- Three-Member Committee (*Τριμελής Επιτροπή*)

Czechia

- Independent Control Body of the Intelligence Services (Orgán nezávislé kontroly zpravodajských služeb České republiky)

Denmark

- Danish Intelligence Oversight Board (*Tilsynet med Efterretningstjenesterne*)

Estonia

- Not applicable

Finland

- Intelligence Ombudsman (Tiedusteluvalvontavaltuutettu/ Underrättelsetillsynsombudsman)

France

- National Commission for Control of Intelligence Techniques (Commission nationale de contrôle des techniques de renseignement)
- Specialised Formation of the Council of State (formation spécialisée du Conseil d'État)

Germany

- G 10 Commission (*G 10-Kommission*)
- Independent Supervisory Council (*Unabhängiger Kontrollrat*)

Greece

- Hellenic Authority for Communication Security and Privacy (*Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών*)

Hungary

- Not applicable

Ireland

- A designated judge of the High Court oversees the interception of communications and data retention, while another judge of the High Court is designated to oversee the use of surveillance devices such as audio bugs and location-tracking devices.

Italy

- Not applicable

Latvia

- Not applicable

Lithiuania

- Intelligence Ombudsman (*Žvalgybos kontrolierius*)

Luxembourg

- Special Commission (*Commission Spéciale*)

Malta

- Commissioner of the Security Service (*Kummissarju tas-Servizz ta' Sigurtà*)
- Security Committee (*Kumitat ta' Sigurtà*)

Netherlands

- Review Committee on the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten*, CTIVD)
- Investigatory Powers Commission (*Toetsingscommissie Inzet Bevoegdheden*, TIB)

Poland

- Not applicable

Portugal

- Council for the Oversight of the Intelligence System of the Portuguese Republic (*Conselho de Fiscalização do Sistema de Informações da República Portuguesa*)

Romania

- Not applicable

Slovakia

- Not applicable

Slovenia

- Not applicable

Spain

- Not applicable

Sweden

- Swedish Foreign Intelligence Inspectorate (Statens inspektion för försvarsunderrättelseverksamheten)
- Commission on Security and Integrity Protection (Säkerhets- och integritetsskyddsnämnden)
- Foreign Intelligence Court (Försvarsunderrättelsedomstolen)

Notes:

* The 2018 data protection reform in Belgium established Standing Committee I as the supervisory authority in the area of data protection.

Source: FRA, 2023

In 2021, Austria reformed its oversight framework and established a new expert body: the Independent Control Commission on the Protection for the Constitution (*Unabhängige Kontrollkommission Verfassungsschutz*). [84] This body identifies systemic deficiencies in and ways to improve the intelligence services. It acts either on its own initiative or at the request of the Minister for the Interior or the parliamentary committee on intelligence oversight. In addition, it serves as a contact point for whistle-blowers. [85]

This new expert body consists of five independent people appointed by the National Council with a two-thirds majority. These people must possess legal qualifications and experience and undergo a trustworthiness test before appointment. [86] To safeguard the body's independence, it has

separate office premises from the intelligence agency. This body does not deal with matters in the area of expertise of the Legal Protection Commissioner at the federal Ministry of the Interior or any other legal protection authority.

Another example of a new oversight body is the Finnish Intelligence Ombudsman (*tiedusteluvalvontavaltuutettu / underrättelsetillsynsombudsmannen*), set up in 2019. It oversees both the civilian intelligence authorities and the military intelligence authorities. It is an independent body with investigative powers and an extensive right to access information. The body can order the suspension or cessation of surveillance if it considers that the intelligence authority has acted unlawfully.

The body can also temporarily stop a surveillance technique authorised by a court and refer the matter to the authorising court. It also receives investigation requests and complaints from individuals and acts on them. [87]

Similarly, in Lithuania, a new expert body – the Intelligence Ombudsman (*Žvalgybos kontrolierius*) – was set up through a 2021 law that came into effect on 1 January 2022. [88] This body was established after the national DPA was excluded from exercising any control over data processing by national institutions for national security and defence purposes. [89] It is composed of two ombudspersons who are appointed by the parliament for a five-year term. The body has its own staff and budget, and one of the two ombudspersons is appointed as its head.

The Intelligence Ombudsman is independent and accountable only to parliament, to which it submits an annual report. It supervises intelligence services and their compliance with human rights standards and data protection regulations. It also carries out assessments of the legality of intelligence services' activities and methods.

The ombudsman can investigate intelligence services' activities and processing of personal data, and may access the data they collect. It can initiate investigations on its own initiative, or based on complaints received from individuals, parliamentarians or other public institutions.

Germany established the Independent Supervisory Council (*Unabhängiger Kontrollrat*) in 2021. This council acts as a quasi-judicial oversight body tasked with the authorisation of surveillance measures, and as an administrative oversight body for ex post oversight. Its members are six judges of the Federal Supreme Court and/or the Federal Administrative Court, who are elected by the Parliamentary Oversight Panel (*Parlamentarisches Kontrollgremium*) for 12 years.Cooperation among the different German intelligence oversight bodies is provided for by an amendment of the Parliamentary Oversight Panel Act. The act authorises the panel to request information from the G 10 Commission, the Federal Commissioner for Data Protection and Freedom of Information, and the Independent Supervisory Council, if deemed necessary for the panel's investigations. [90]

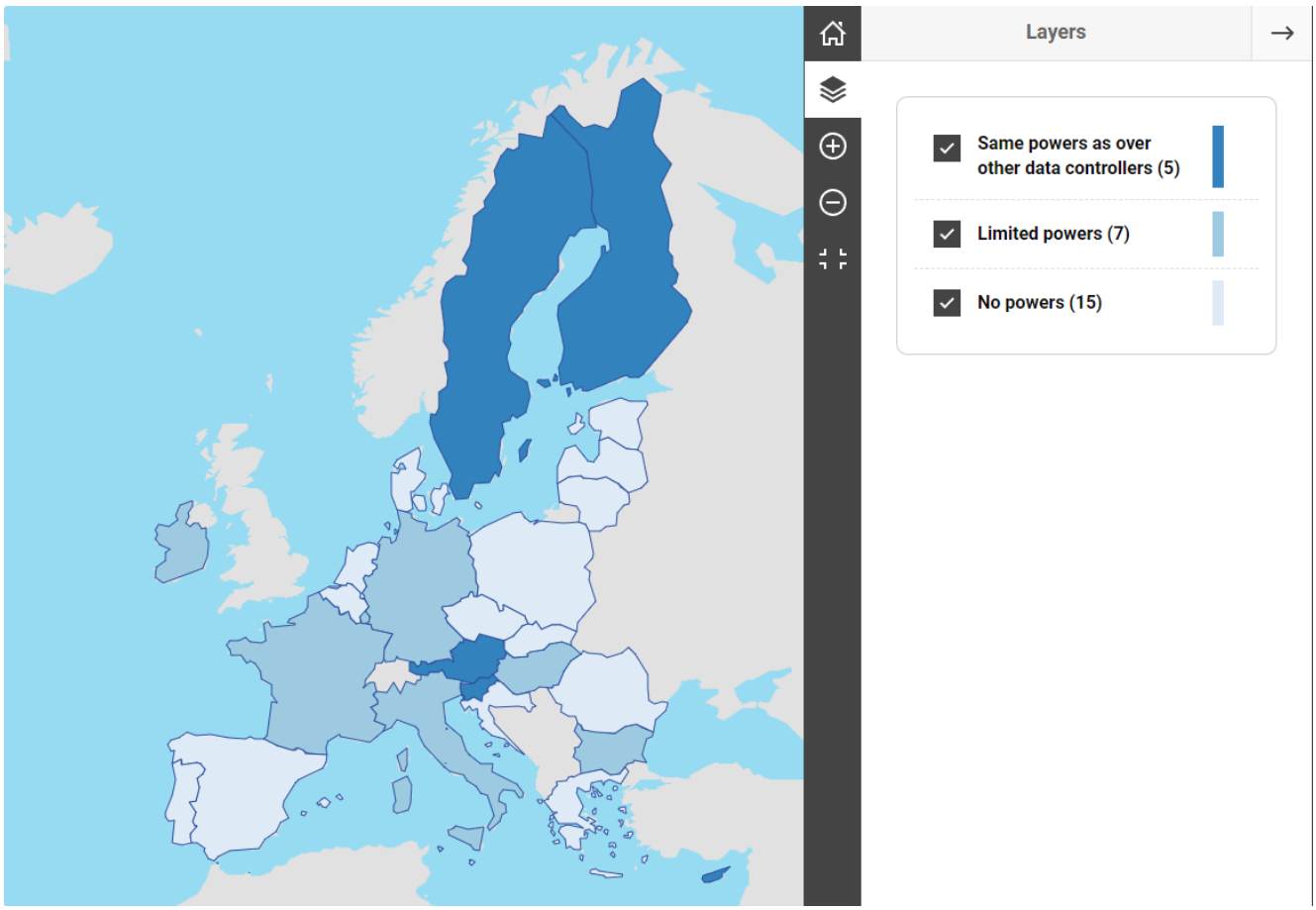
In the Netherlands, the Investigatory Powers Commission assesses the legality of the authorisation the responsible ministers grant to intelligence services to perform surveillance activities.This body supplements the main oversight body, the Review Committee on the Intelligence and Security Services (*Commissie Van Toezicht op de Inlichtingen- en Veiligheidsdiensten*). This committee is tasked with the ongoing supervision of surveillance

activities that intelligence services conduct after authorisation. [91]

The 2016 European data protection reform also led to important changes in intelligence oversight. FRA research indicates that national data protection laws passed after 2016 led mostly to broader restrictions on or even the prevention of DPAs exercising oversight and reviewing the data processing activities of intelligence services (see Figure 5), such as in Bulgaria, Croatia and Greece. These changes concerned not only the oversight functions of DPAs over intelligence activities, but also authorities' remedial powers, as described in the section 'Remedies'.

However, in some states, such as France, Italy and Slovenia, no important changes affected the general oversight framework. In Slovenia, under the 2022 data protection reform, the Director of the intelligence service can delay the DPA's inspections in very limited circumstances. [92] In some countries, such as Belgium and Lithuania, the exclusion of DPAs from overseeing the activities of intelligence services was accompanied by the provision of supervisory powers in the area of data protection to oversight bodies.

Figure 5 – DPAs' oversight powers over national intelligence services in the EU-27



Source: FRA, 2023

In Bulgaria, processing for "national defence and national security" was excluded from the scope of personal data legislation and the GDPR, restricting the oversight of intelligence services by its

national DPA: the Commission for Personal Data Protection (*Комисия за защита на личните данни*). [93] This change was accompanied by corresponding amendments to the laws governing the different intelligence services. These amendments excluded the State Intelligence Agency from the Commission for Personal Data Protection's oversight but retained the agency's limited oversight of the activities of the Military Intelligence Service and the State Agency for National Security. [94]

A similar change was passed in Greece in 2019. The new data protection law excluded the Greek DPA from supervising operations involving the processing of classified personal data carried out for activities concerning national security. [95] A similar change occurred in Croatia. The new data protection laws prevented bodies of the security intelligence system from conducting data processing for the purpose of protecting national security and, hence, exempted them from any oversight by the national DPA. [96]

While Lithuania established a new oversight body in 2021, by enacting the European data protection reform in 2018 the country had specifically removed the DPA's powers over intelligence services' data processing for the purposes of national security and defence. [97] In Belgium, the 2018 data protection reform designatedthe Standing Intelligence Agencies Review Committee (Standing Committee I) (*Le Comité permanent de contrôle des services de renseignement, Comité permanent R*) as the supervisory authority for all data processing activities of intelligence services linked to national security. [98] The Belgian DPA (*L'Autorité de protection des données*) is excluded from performing any oversight on data processing by intelligence services.

However, data protection law calls for cooperation between the various sectoral supervisory authorities. Accordingly, in 2020, a protocol for cooperation was adopted. [99] It clarifies the division of tasks and the scope of powers of the data protection supervisory authorities in Belgium. Since 2018, the Standing Committee I has reported annually on its activities as a supervisory authority in the area of data protection. [100]

Other data protection reforms were enacted in other Member States. In Germany, for example, the data protection reform revised the framework for data processing in the field of national security. [101] The laws of the three federal intelligence services included new provisions on the specific role and oversight of the Federal Commissioner for Data Protection and Freedom of Information (*Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, BfDI), thus transferring the supervisory powers from the old Federal Data Protection Act to intelligence legislation. [102] In particular, with regard to the Federal Intelligence Service (*Bundesnachrichtendienst*), the BfDI's power to issue ad hoc opinions on critical issues to the parliament and the general public is limited in that the BfDI may inform other oversight bodies only confidentially. [103]

The oversight powers of DPAs appear to have been reinforced since 2017 in only a few countries. For example, in Luxembourg, based on the 2018 data protection reform, the National Commission for Data Protection (*Commission Nationale pour la Protection des Données*) is responsible for monitoring and verifying the legal compliance of the processing of personal data by the State Intelligence Service. In this regard, the National Commission for Data Protection enjoys significant

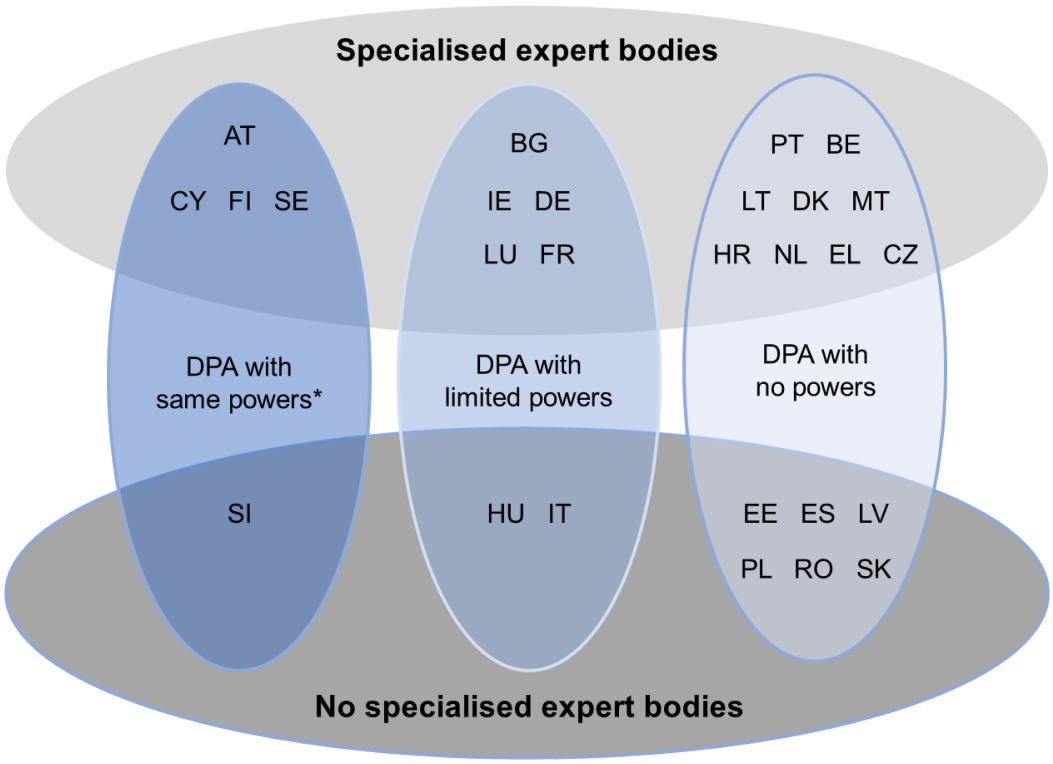
investigative, corrective, authorisation and advisory powers. It also hears complaints and provides for remedies, subject to judicial appeal. [104]

In Cyprus, following the 2018 reforms, the DPA has access to all personal data and information necessary to perform its mandate. The confidentiality of the data is not maintained, unless they are covered by legal professional privilege. Past restrictions on accessing records, which were kept for national security purposes, were abolished. [105] In Sweden, the Swedish Authority for Privacy Protection (*Integritetsskyddsmyndigheten*) can, on its own initiative, now issue warning orders but also injunctions requiring the intelligence services to take measures to secure the lawfulness of data processing. [106]

In Hungary, the implementation of the GDPR allowed the National Authority for Data Protection and Freedom of Information (*Nemzeti Adatvédelmi és Információszabadság Hatóság*), which oversees the activities of intelligence services, to start investigations on its own initiative. This power was relied on in its review of Pegasus-related allegations. [107] However, the ECtHR recently found a violation of the ECHR in respect of the limited powers of the authority. The authority can perform its tasks by sending its fact-finding requests to the overseeing minister and rely on their findings. [108]

Figure 6 summarises the current situation with regard to expert bodies' and DPAs' oversight of intelligence services across EU Member States.

Figure 6 – Oversight of surveillance by intelligence services by expert bodies and DPAs



Note: * As over other data controllers.

Source: FRA, 2023

1.5.3 Models of oversight frameworks of intelligence services based on different players involved

The oversight of intelligence services is organised differently across EU Member States, as highlighted in the 2017 FRA report and considering the recent developments in the frameworks of oversight bodies described in previous sections. The jurisprudence of the CJEU and the ECtHR has set minimum standards but leaves states with significant leeway to organise the oversight of the activities of their own intelligence services. This section specifically responds to the European Parliament's request for FRA to determine which oversight models were prevalent in the EU. FRA's research identified 18 different oversight frameworks in the EU.

The following section describes five models covering most EU Member States, identified from the 18 oversight frameworks. When assessing the efficiency of an oversight framework, two key elements should be considered. First, the oversight framework should have oversight powers that correlate with the surveillance powers of the intelligence services, along with adequate resources and expertise to ensure effective oversight (see FRA opinion 3 above). Second, the oversight structure, including through the collaboration of different entities, should cover the full surveillance cycle, which the ECtHR refers to as "continuous control" (see FRA opinion 6 above). The models in this section focus on expert bodies exercising oversight over intelligence services during and after secret surveillance measures. In FRA's understanding, ex post oversight starts once the surveillance measure has been authorised by the bodies mentioned in the section '*Ex ante* authorisation'.

The models neither describe nor extend to the judicial control of surveillance measures at the stage of remedies. This choice does not disregard the important role that courts play in the overall framework for the oversight of intelligence services, especially at the remedial stage.

None of the five models cover Ireland or Malta [109] because these Member States do not rely on any arrangement of parliamentary oversight.

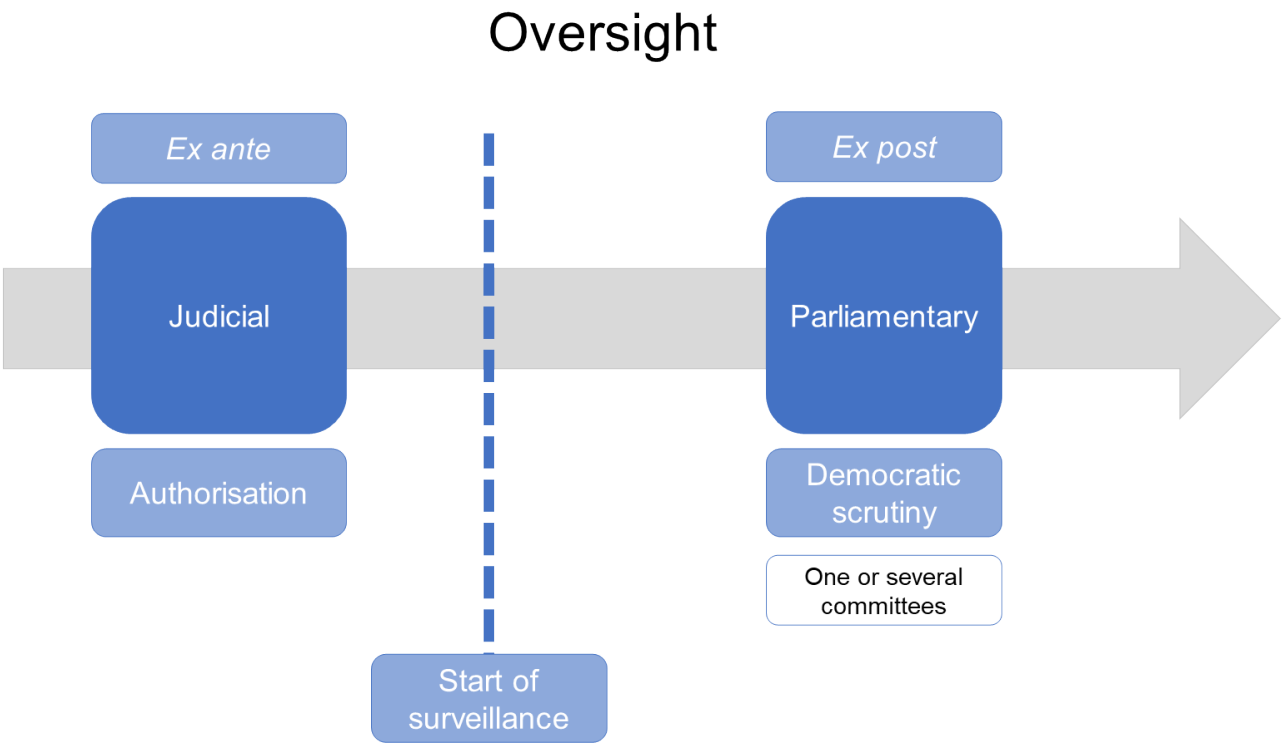
Model 1

The multitude of models across the EU is due to the diversity of actors contributing to the oversight frameworks. Several Member States emphasise the role of parliament in the oversight structure. This forms the basis for the first model that FRA identified. The model mainly relies on two actors: an authority authorising the surveillance measure and a parliamentary committee exercising subsequent oversight.

Figure 7 illustrates the model. It is present in Estonia, Latvia, Romania, Slovakia and Spain. Poland has features of this model, but instead of a judge authorising the surveillance measure it is the

executive or the intelligence services, depending on the surveillance measure, that approves the surveillance technique.

Figure 7 – Model 1 – reliance on parliamentary oversight



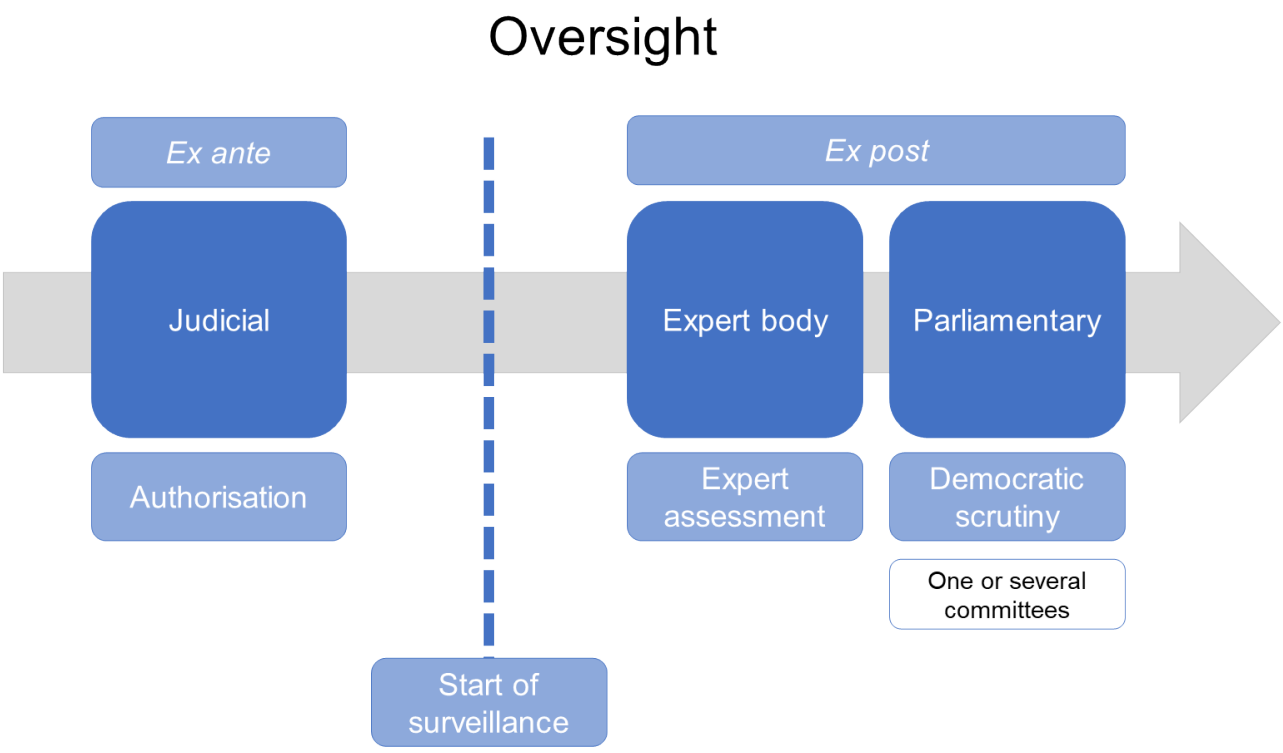
Source: FRA, 2023

Model 2

As noted above, the majority of EU Member States have set up specialised expert bodies to oversee the work of intelligence services. In this second model, the specialised expert body focuses its work on ex post oversight alongside a parliamentary committee. A judicial authority authorises the surveillance measure.

Figure 8 illustrates the role played by the expert body, which has no power at the authorisation stage. This model has been adopted in Croatia, Czechia, Denmark, Greece and Lithuania. The Dutch system also resembles this model. However, in the Netherlands, a judicial authority, the executive or an expert body can authorise the surveillance measure, depending on the measure at stake.

Figure 8 – Model 2 – ex post oversight by an expert body and parliament



Source: FRA, 2023

Model 3

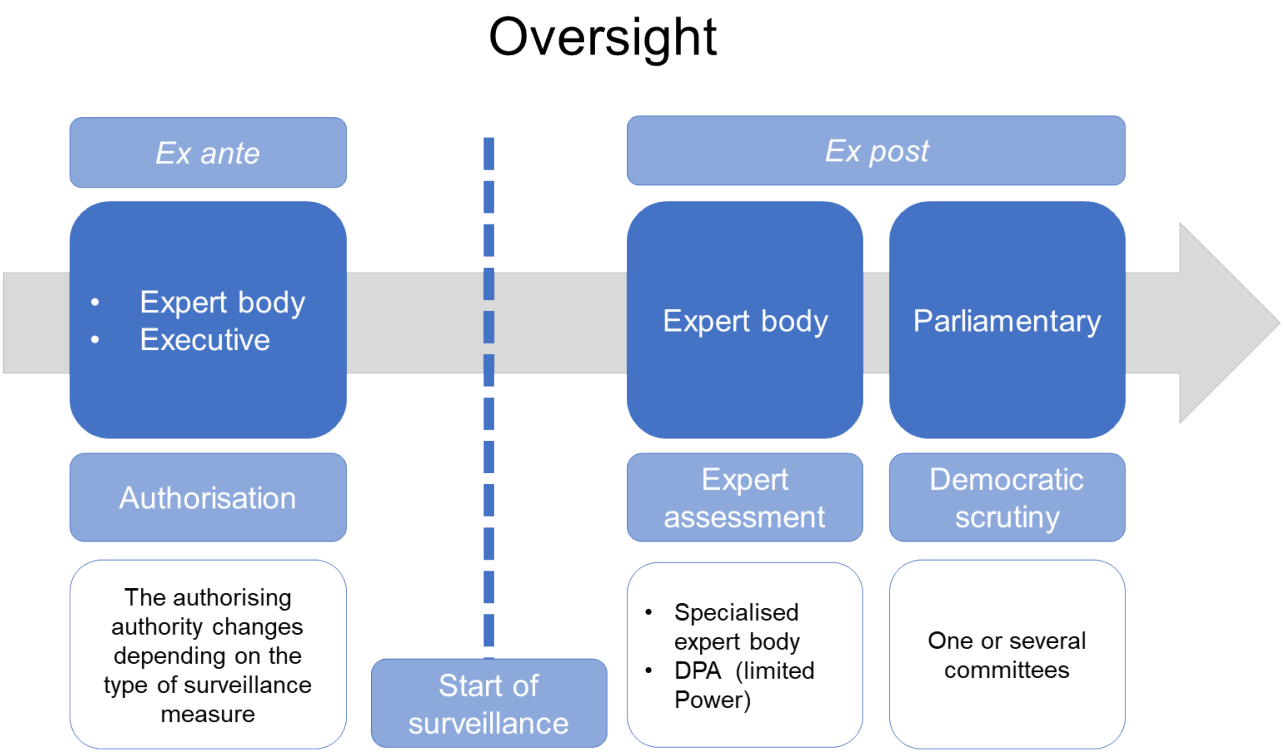
A significant number of Member States not only rely on specialised expert bodies to oversee the activities of intelligence services but also include DPAs in their oversight frameworks. In most cases, the DPA has limited power compared with that of the specialised expert body, which leads the ex post oversight of activities of intelligence services. In this third model, a parliamentary committee also contributes to the oversight function.

Luxembourg provides an example of this model, as illustrated in Figure 9. Germany also largely adheres to this model, the only difference being that the parliamentary committee approves certain surveillance measures. France also follows the same model, but the executive has the binding approval power when authorising a surveillance technique.

This model also largely fits the Belgian and Bulgarian oversight frameworks. In Belgium, the executive, an expert body (e.g. the Administrative Commission) or the intelligence services authorise the surveillance measure, depending on the measure at stake. In Bulgaria, only a judge can authorise surveillance measures. In exceptional cases, the DPA holds the same powers over intelligence services as over any other data controller. This is the case in Austria and Finland.

In Belgium, the specialised expert body (Standing Committee I) is the supervisory authority in the area of data protection (DPA).

Figure 9 – Model 3 – ex post oversight by an expert body, a DPA and parliament

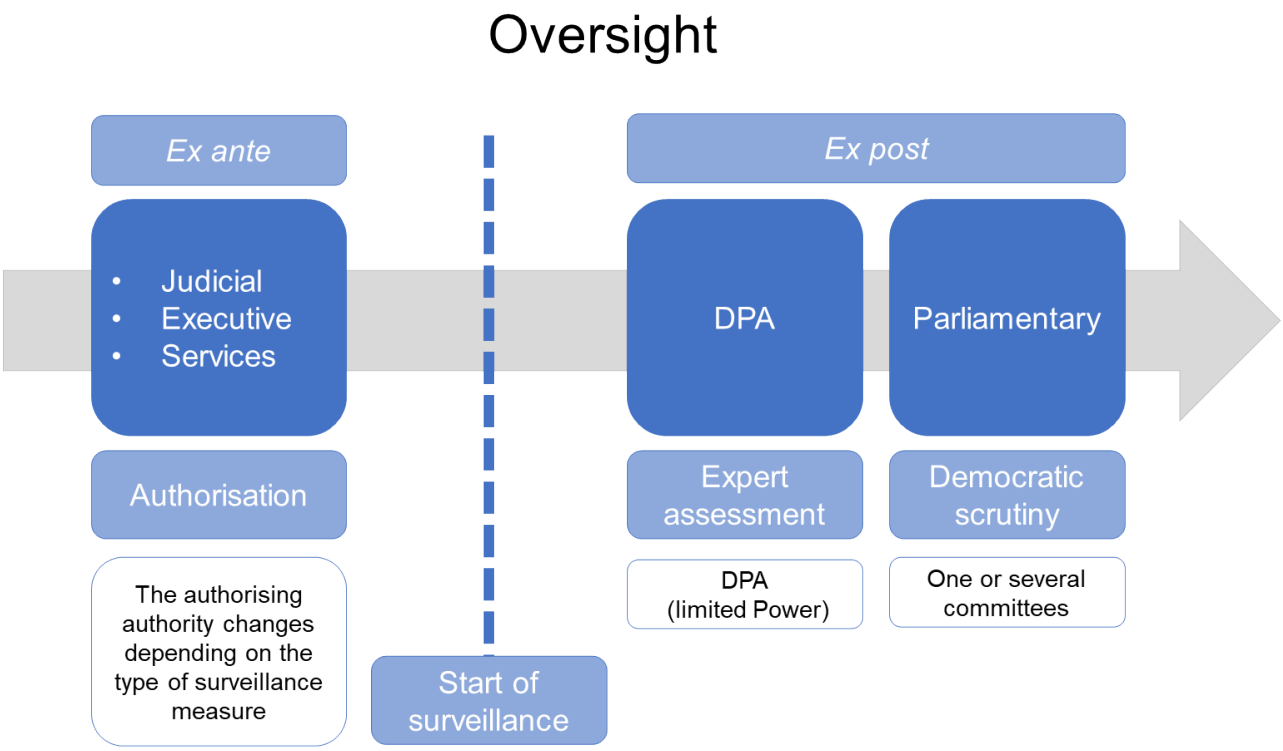


Source: FRA, 2023

Model 4

The fourth model relies on the DPA and the parliamentary committee to conduct the oversight of intelligence services, with no separate oversight body with a mandate wider than data protection. In Hungary, Italy and Slovenia, where this model is applied, there is no specialised expert body. The DPA has either limited power (Hungary and Italy) or the same power as over any other data controller (Slovenia). Figure 10 illustrates the Hungarian model. In Italy, a judge always authorises the use of surveillance measures.

Figure 10 – Model 4 – ex post oversight by a DPA and parliament



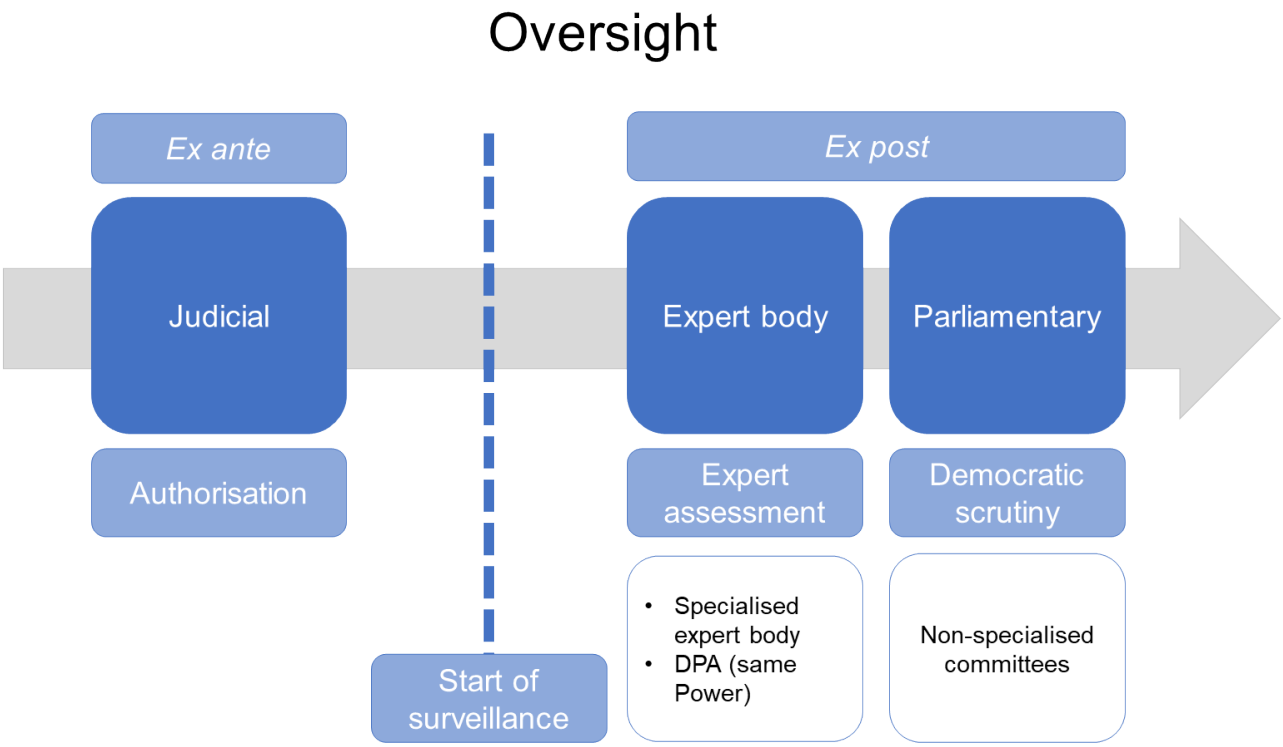
Source: FRA, 2023

Model 5

The fifth and final model is characterised by a non-specialised parliamentary committee at the *ex post* oversight stage. This model is present in Sweden, where the expert body works with a DPA with the same powers over intelligence services as over any other data controller, while a judge authorises the use of surveillance measures. Figure 11 illustrates this model.

Non-specialised parliamentary committees are also present in Cyprus and Portugal. In Cyprus, the executive authorises the use of surveillance measures, with an expert body and a DPA performing the expert oversight. In Portugal, a judge authorises the use of these measures, while an expert body oversees them.

Figure 11 – Model 5 – ex post oversight by an expert body and a non-specialised parliamentary committee



Source: FRA, 2023

2. Remedies

2.1 Relevant updated key findings

The 2017 FRA report highlighted the challenge of accessing effective remedies when it comes to surveillance. On the one hand, the need for secrecy that is inherent to the field of intelligence impedes effective access to classified information, and, on the other hand, a lack of expertise among the staff of remedial bodies may create specific issues. In addition to these specific issues, classic challenges hampering access to effective remedies also apply. For example, judicial avenues are often costly and slow, and entail complex procedural rules. In the context of surveillance, non-judicial avenues may provide individuals with important complementary remedial avenues.

In 2017, FRA's research showed that, overall, in the context of surveillance, only few individuals seek remedy. The average of 10 to 20 individuals per year in 2017 stayed stable in more recent years.

FRA highlighted the need to ensure minimum requirements for remedies to be effective. Non-judicial bodies must be independent. They must tackle the following challenges: raising awareness of surveillance measures among individuals, either through notification or through any other opportunity to obtain information about interceptions; ensuring access to classified information for remedial bodies; ensuring appropriate redress, for example the destruction of the data collected or monetary relief; and ensuring proper expertise within remedial bodies.

In 2023, the situation appears much like that in 2017. However, the 2016 European data protection reform affected six DPAs, which lost their remedial powers in the area of surveillance.

In most EU Member States, non-judicial bodies can offer individuals remedies. Only three Member States do not offer non-judicial remedial avenues to lodge a complaint related to activities of intelligence services. In this regard, the situation has remained unchanged since 2017.

In 12 Member States, individuals may lodge a complaint with only a single non-judicial body with remedial powers. In 2017, this was the case in 10 out of the 28 EU Member States. In the remaining 12 Member States – out of a total of 24 that offer non-judicial remedies – two or more such bodies have remedial powers.

Since 2017, the situation with regard to the scope of remedial powers of expert bodies has remained largely unchanged. Basically, expert bodies still enjoy broader powers than other non-judicial bodies with remedial powers: in nine of the 14 Member States that have expert bodies, these bodies have the strongest powers to offer an effective remedy. However, the following changes should be noted. In the three Member States where new expert bodies were established, two were granted significant remedial powers, to take binding decisions, to fully access collected data and to communicate that controls have been implemented to the complainant. The other only granted the new expert body full access to the data, including classified information.

Remedial bodies' effectiveness depends foremost on their binding decision-making powers. In 15 Member States, remedial bodies can issue binding decisions. Most of them are expert bodies and DPAs. While in 2017 six Member States had not granted any of their non-judicial bodies the power to take binding decisions, this is now the case in seven Member States.

2.2 Selected 2017 FRA opinions



Opinion 12: Providing for effective remedies before independent bodies with remedial powers

EU Member States should ensure that judicial and non-judicial bodies with remedial powers have the powers and competences to effectively assess and decide on individuals' complaints related to surveillance.

Opinion 13: Ensuring availability of non-judicial bodies with remedial powers

EU Member States should ensure that both judicial and non-judicial remedial bodies are accessible to individuals. Notably, Member States should identify what potential gaps prevent individuals from having their complaints effectively reviewed, and ensure that non-judicial expert bodies can complement the remedial landscape where needed.

Opinion 14: Allowing for awareness of completed surveillance measures

EU Member States should ensure that the legitimate aim and proportionality tests are conducted by intelligence services before limiting access to information based on national security. A competent authority should assess the confidentiality level. Alternatively, controls should be carried out by oversight bodies in the name of complainants when notification or disclosure are not possible.

Opinion 15: Ensuring a high level of expertise among remedial bodies

EU Member States should ensure that where judicial or non-judicial remedial bodies lack relevant expertise to effectively assess individuals' complaints, specific systems are established to address these gaps. Cooperation with expert oversight bodies, technical experts or members of the intelligence services can support effective remedial systems.

Source: FRA, 2017

In line with the well-established European case law, any individual may claim to be a victim of an interference with their privacy rights based on the existence of intelligence laws prescribing secret surveillance. [110] Individuals should have recourse to remedies that are effective in law and practice for reviewing the lawfulness and proportionality of any surveillance of them and redressing any violations of their rights. While such remedies do not need to be of a judicial nature, they need to be effective.

The courts have an important role to play in reviewing surveillance ex post at the remedial stage, either when directly handling complaints against intelligence services or when examining appeals against the decisions of non-judicial oversight bodies. [111] While in principle all Member States provide the opportunity for individuals to complain about privacy and other rights violations before a judge, judicial avenues are not necessarily effective, as the 2017 FRA report highlighted.

Strict procedural rules on evidence and legal standing may hinder recourse to courts. The ECtHR has acknowledged the common ineffectiveness of judicial recourse in surveillance cases. It affords a much broader meaning to the term 'victim' based on the European Convention on Human Rights. It therefore has not required the prior exhaustion of domestic judicial remedies in a number of cases regarding surveillance by intelligence services. [112] At the same time, recourse to non-judicial bodies raises issues relating to power, independence and expertise. [113]

In this regard, the ECtHR has repeatedly found the notification of surveillance measures, or, at least, an adequate opportunity to request and obtain information about interceptions from the authorities, to be a relevant factor in assessing the effectiveness of remedies and hence the existence of effective safeguards against the abuse of surveillance powers. [114]

> **"As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is a relevant factor in assessing the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of surveillance powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspects that he or she has been subject to surveillance can apply to courts, whose jurisdiction does not depend on notification to the surveillance subject of the measures taken."**

ECtHR, Centrum för rättvisa v. Sweden[GC], No. 35252/08, 25 May 2021, paragraph 251

Providing individuals with the necessary information, although crucial, is not sufficient and is only a precondition for effective access to remedies. Excessive formal requirements, for example short time frames within which a complaint can be brought, would severely undermine the effectiveness of any available remedies. [115]

In the case of Centrum för rättvisa v. Sweden, the ECtHR stressed the need for guarantees that exclude any conflicts of interest of remedial bodies with the body authorising the surveillance or exercising regular oversight of intelligence services. [116] In addition, in the case of Ekimdzhiev and Others v. Bulgaria, the court highlighted other challenges to the effectiveness of remedies and notably the ability of any remedial body to take binding decisions, including on the destruction of collected information.

> **"[S]everal shortcomings undermine its [the special parliamentary committee's] effectiveness. First, its members need not be persons with legal qualifications or experience. Secondly, it has no power to order remedial measures in concrete cases, such as the destruction of retained or accessed communications data; it can only give instructions designed to improve the relevant procedures. If it detects irregularities, it can only bring the matter to the attention of the prosecuting authorities, or inform the heads of the relevant access-requesting authorities and communications service providers. In view of the shortcomings outlined above, the system of overseeing the retention of communications data and [their] subsequent accessing by the authorities in Bulgaria, as currently organised, does not appear capable of providing effective guarantees against abusive practices in this respect."**

ECtHR, Ekimdzhiev and Others v. Bulgaria, No. 70078/12, 11 January 2022, pp. 414–415.

As Table 3 shows, in most EU Member States, different models exist in terms of non-judicial bodies such as DPAs, expert bodies, executive bodies, parliamentary committees and ombuds institutions that can offer remedies. Only three Member States (Czechia, Latvia and Poland) do not offer non-judicial remedial avenues but only provide individuals with judicial avenues to lodge a complaint. In these Member States, neither DPAs nor any other oversight bodies have remedial powers over intelligence services. In this regard, the situation remains unchanged compared with 2017.

Table 3 – Non-judicial bodies with remedial powers in the context of surveillance: different models in the EU-27

Member State	Executive (ministry)	Expert body (or bodies)	DPA	Parliamentary committee(s)	Ombuds institution
AT		✓	✓		✓
BE		✓			✓
BG		✓		✓	
CY			✓		

Member State	Executive (ministry)	Expert body (or bodies)	DPA	Parliamentary committee(s)	Ombuds institution
CZ					
DE		✓	✓	✓	
DK		✓			
EE					✓
EL		✓			
ES					✓
FI		✓	✓		✓
FR		✓	✓		✓
HR		✓		✓	✓
HU	✓		✓	✓	✓
IE		✓	✓		
IT			✓		
LT		✓		✓	
LU			✓		
LV					
MT		✓			
NL		✓			
PL					
PT		✓			✓
RO				✓	
SE		✓	✓		
SI			✓	✓	✓
SK				✓	

Source: FRA, 2023

2.3 Remedial powers of data protection authorities

In relation to DPAs' remedial powers over intelligence services, the situation has evolved in seven Member States since 2017. In Belgium, Bulgaria, Croatia, Greece and Lithuania, as a result of the national data protection reforms, DPAs no longer have control over matters linked to national security. They have consequently lost their power to investigate complaints lodged by individuals in the context of intelligence services' activities. These modifications were introduced by the Member States while implementing the 2016 EU data protection reform.

In Bulgaria, for example, the 2019 legislative reform excluded surveillance activities from the overall scope of application of the Personal Data Protection Act. [117] The explanatory report accompanying the amendments referred to the EU data protection reform to justify the amendments. [118] Similarly, in Croatia, the act adopted in 2018 to implement the GDPR prescribes that the law does not apply to the processing of personal data carried out by competent authorities to, among other things, protect against threats to public security, including in the areas of national security and defence. [119]

In Lithuania, both the DPA and the ombudsperson lost their remedial powers through the adoption of two legislative reforms. The law of 2018 incorporating the EU Law Enforcement Directive in national legislation precludes the Lithuanian DPA from exercising any control over data processing by national institutions for national security and defence purposes. [120] In addition, amendments made in 2022 to the Law on Seimas Ombudsmen preclude the ombudsperson from investigating activities of intelligence institutions. [121] During the 2022 reform, a new expert body, the Intelligence Ombudsman, was set up and was given remedial powers concerning intelligence services' processing of personal data and other activities. [122]

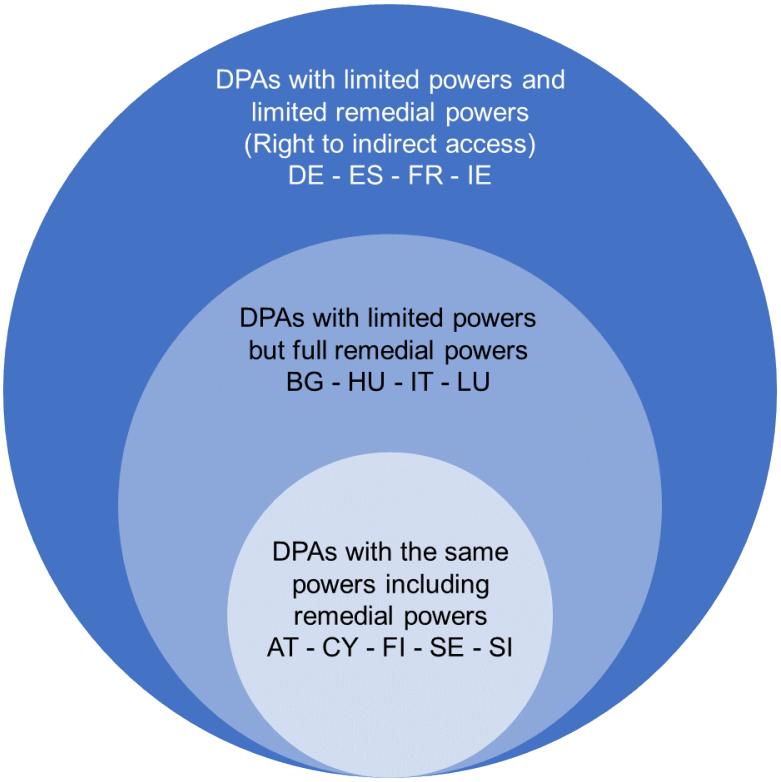
In Belgium, the 2018 law implementing the 2016 European data protection reform specifically shifted the remedial powers from the DPA to the expert oversight body.

However, in Cyprus and Sweden, the implementation of the GDPR at national level provided the DPA with new powers that strengthen its ability to provide effective remedies.

In Cyprus, the adoption of the 2018 law implementing the GDPR provided the DPA with the legal basis to access data held by the intelligence services and take binding decisions. [123] Similarly, in Sweden, the DPA was granted access to all personal data processed by intelligence services, including to implement safety and protective measures. The DPA may order the Swedish Security Service to stop processing or destroy personal data but cannot order the Swedish Armed Forces or the National Defence Radio Establishment to do so. Finally, decisions the DPA takes may be reviewed by a court.

Figure 12 illustrates the diversity of DPAs' remedial powers over intelligence services across the EU.

Figure 12 – DPAs' remedial powers over intelligence services compared with powers over other data controllers



Source: FRA, 2023

2.4 Remedial powers of other non-judicial oversight bodies

In 2023, the situation regarding the remedial powers of non-judicial oversight bodies other than DPAs remains largely unchanged. A few developments are, however, worth noting.

In a few Member States, including Croatia, Denmark and Finland, oversight bodies have gained certain aspects of remedial powers over intelligence authorities. In Finland, the Intelligence Ombudsman may fully access data collected by intelligence services and may take binding decisions. Since the Intelligence Ombudsman was established in 2019, it has not received any individual complaints but has received more than 50 requests for investigations. [124] When an investigation has been carried out, the ombudsman may inform individuals, but only stating that an investigation has been carried out. [125]

A natural or legal person living in Denmark may file a complaint and request the oversight body (the Danish Intelligence Oversight Board (TET)) to investigate whether the intelligence service has illegally processed information about them, in accordance with the act on the Danish Security and Intelligence Service and the act on the Danish Defence Intelligence Service. These acts were consolidated in 2017. [126] The TET can only inform the individual that the service does not illegally process information regarding them, without providing any further information. Where it is

established during an examination that intelligence services processed information illegally, TET has the power to issue binding decisions requesting the services to delete the data.

If special circumstances so warrant, TET has the power to instruct intelligence services to wholly or partially specify what information was processed concerning the complainant. However, the TET highlighted in 2021 that in practice these provisions have limited application, as few individuals have so far requested TET to investigate whether an intelligence service has illegally processed information about them. [127]

In Croatia, the Council for Civilian Oversight of Security and Intelligence Agencies, re-established in 2018 after several years of inactivity, may now access data that intelligence services have collected, and may inform complainants once it performs an investigation based on their complaints.

As was shown in the 2017 FRA report, only very few individuals accused intelligence services of performing unlawful activities before oversight bodies. [128] The following examples confirm the 2017 findings.

In 2021, the Belgian Standing Committee I received 72 complaints, compared with 62 in 2020. In 2020, most of them were dismissed (55 out of 62). [129] By contrast, in 2021, 23 were rejected as manifestly ill-founded and 28 because Standing Committee I was not competent. A total of 14 of the remaining were handled in 2021. [130]

In France, the CNCTR received 48 complaints in 2021, compared with 33 in 2020. Complaints are handled within two months. Once the individual has received the response from the CNCTR, they can bring the case before the Specialised Formation of the Council of State (*la formation spécialisée du Conseil d'État*). In 2021, like in 2020, it received 8 applications. [131]

The German G 10 Commission received four complaints in 2020, three of which were ill-founded. [132] The Dutch Review Committee on the Intelligence and Security Services handled 23 complaints in 2021. [133]

3. Conclusions

This update presented developments in a field of law that is continuously evolving: intelligence laws need to continuously improve the capacity of intelligence services to deal with threats and technical developments.

At the same time, the CJEU case law has made clear that secret surveillance has an impact on, among other things, the right to respect for private and family life (Article 7), the right to the protection of personal data (Article 8), and the right to an effective remedy and a fair trial (Article 47) of the Charter. It also makes clear that bodies exercising oversight over intelligence services should evolve in a similar fashion to intelligence laws and capacities of intelligence services. Their power and technical abilities should match those of the services they oversee to fulfil the requirements the case law of the CJEU and the ECtHR set. The crucial concept of continuous control developed by the ECtHR should be a reality in practice.

In all EU Member States, several entities contribute to the oversight framework. Enhanced collaboration between relevant oversight authorities should ensure the oversight of the full surveillance cycle. The efficiency of the five oversight models presented in this report should be assessed based on two principles: matching powers and continuous control over the intelligence cycle.

The report also addresses the issue of remedies. A number of challenges in the field of surveillance by intelligence services need to be overcome to ensure access to effective remedies, as FRA highlighted in 2017. In this area, individuals wishing to complain about alleged fundamental rights violations face several issues. These include a challenge that undermines the right to a fair hearing, namely secrecy.

The 2017 FRA report discussed how Member States addressed this key aspect of surveillance. In this update, FRA found that in 2023 the situation had not evolved much since 2017. Pursuing a claim against an alleged illegal surveillance measure places the individual in a situation where they need to trust the remedial body. The effectiveness of a remedial body is the crucial element from which such trust stems. Furthermore, the 2016 EU data protection reform led to some Member States significantly reducing DPAs' remedial competencies in the field of national security. In other Member States, the reform reinforced the DPAs' powers.

In 2023, as was the case in 2017, a strong independent oversight structure offering effective remedies to individuals would "pave the way […] to renewed trust among European citizens towards their intelligence services and, as a result, a more effective defence of national security". [134] Enhanced security measures should be enshrined in a strong fundamental rights framework, where the necessity and proportionality of surveillance measures are regularly assessed.

Case law (post-2017)

Court of Justice of the European Union

Joined cases C-793/19 and C-794/19, Bundesrepublik Deutschland v. SpaceNet AG and Telekom Deutschland GmbH [GC], 20 September 2022.

C-140/20, G.D. v. Commissioner of An Garda Síochána and Others [GC], 5 April 2022.

Joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v. Premier ministre and Others and Ordre des barreaux francophones et germanophone and Others v. Conseil des ministres [GC], 6 October 2020.

C-623/17, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others [GC], 6 October 2020.

European Court of Human Rights

Big Brother Watch and Others v. the United Kingdom, Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021.

Centrum för rättvisa v. Sweden, No. 35252/08, 25 May 2021.

Hüttl v. Hungary, No. 58032/16, 29 September 2022.

Haščák v. Slovakia, Nos. 58359/12, 27787/16 and 67667/16, 23 June 2022.

Ekimdzhiev and Others v. Bulgaria, No. 70078/12, 11 January 2022.

Zoltán Varga v. Slovakia, Nos. 58361/12, 25592/16 and 27176/16, 20 July 2021.

Tretter and Others v. Austria, No. 3599/10 (dec.), 29 September 2020.

Marie Ringler v. Austria (dec.), No. 2309/10, 12 May 2020.

Breyer v. Germany, No. 50001/12, 30 January 2020.

National courts

France, Council of State (*Conseil d'État*), French Data Network and Others v. France, Decision

No. 393099, 21 April 2021.

Germany, Federal Constitutional Court (*Bundesverfassungsgericht*), 1 BvR 2835/17, 19 May 2020.

Germany, Federal Constitutional Court (*Bundesverfassungsgericht*), 1 BvR 2354/13, 28 September 2022.

Portugal, Constitutional Court (*Tribunal Constitucional*), Judgment No. 464/2019, 21 October 2019.

Annex 1 - Overview of intelligence services in the EU-27

Austria

- Directorate State Protection and Intelligence Service (*Direktion Staatsschutz und Nachrichtendienst*, DSN)
- Military Intelligence Service (*Heeresnachrichtenamt*, HNaA)
- Military Defence Agency (*Abwehramt*, AbwA)

Belgium

- State Security Service (Veiligheid van de Staat/Sûreté de l'Etat, VSSE)
- General Intelligence and Security Service of the Armed Forces (Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht (ADIV)/Service Général du Renseignement et de la Sécurité (SGRS))

Bulgaria

- State Intelligence Agency (SIA) (*Nationalna Razuznavatelna Služba*, NRS)
- State Agency for National Security (Държавна Агенция "Национална сигурност", SANS)
- State Agency for Technical Operations (SATO) (Държавна агенция „Технически операции)
- Military Information Service (MIS) (Sluzhba Voenna Informatsia, СВР)

Croatia

- Security and Intelligence Agency (*Sigurnosna-Obavjestanja Agencija*, SOA)
- Military Security and Intelligence Agency (*Vojna Sigurnosna-Obavjestanja Agencija*, VSOA)
- Information Office (*Informacios Hivatal*, IH)

Cyprus

- Cypriot Intelligence Service (*Κυπριακή Υπηρεσία Πληροφοριών*, ΚΥΠ)

Czechia

- Security Information Service (Bezpečnostní informační služba, BIS)
- Office for Foreign Relations and Information (*Úřad pro Zahraniční Styky a Informace*, UZSI)
- Military Intelligence Service (*Vojenské Zpravodajství*, VZ)

Denmark

- Danish Defence Intelligence Service (DDIS) (*Forsvarets Efterretningstjenst*, FE)

- Danish Security and Intelligence Service (DSIS) (*Politiets Efterretningstjeneste*, PET) (part of the police)

Estonia

- Estonian Foreign Intelligence Service (*Välisluureame*)
- Estonian Internal Security Service (*Kaitsepolitseiamet*, KAPO)
- Military Intelligence Branch of the Estonian Defence Forces (*Kaitseväe peastaabi luureosakond*)

Finland

- Finnish Defence Intelligence Agency (*Tiedustelulaitos*, FDIA),
- Intelligence Division of the Defence Command (*Pääesikunnan tiedusteluosasto/Huvudstabens underrättelseavdelning*)
- Finnish Security and Intelligence Service (*Suojelupoliisi/Skyddspolisen*, SUPO) (part of the police)

France

- Directorate General of External Security (*Direction Générale de la Sécurité Exterieure*, DGSE)
- Directorate of Military Intelligence (*Direction du renseignement militaire*, DRM)
- Directorate General of Interior Security (*Direction générale de la sécurité intérieure*, DGSI)
- National Directorate of Customs Intelligence and Investigations (*Direction nationale du renseignement et des enquêtes douanières*, DNRED)
- Intelligence processing and action against clandestine financial circuits – The Financial Investigation Unit (*Service du traitement du renseignement et action contre les circuits financiers clandestins*, Tracfin)

Germany

- Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*, BfV)
- Federal Intelligence Service (*Bundesnachrichtendienst*, BND)
- Federal Office for Military Counter-Intelligence Service (*Bundesamt für den Militärischen Abschirmdienst*, BAMAD)
- State Office for the Protection of the Constitution of Baden-Württemberg (*Landesamt für Verfassungsschutz Baden-Württemberg*)
- Bavarian Office for Protection of the Constitution (*Bayerische Landesamt für Verfassungsschutz*)
- Berlin Senate Administration for Home Affairs, Department of Protection of the Constitution (*Senatsverwaltung für Inneres, Abteilung Verfassungsschutz Berlin*)

- Brandenburg Ministry of the Interior and Municipalities, Department of Protection of the Constitution (*Ministerium des Innern und für Kommunales, Abteilung Verfassungsschutz Brandenburg*)
- Bremen State Office for the Protection of the Constitution (*Landesamt für Verfassungsschutz Bremen*)
- State Office for the Protection of the Constitution of the Free and Hanseatic City of Hamburg (*Landesamt für Verfassungsschutz der Freien und Hansestadt Hamburg*)
- Hessen State Office for the Protection of the Constitution (*Landesamt für Verfassungsschutz Hessen*)
- Lower Saxony Ministry of the Interior, Sport and Integration, Department 5 (*Ministerium für Inneres, Sport und Integration, Abteilung 5 Niedersachsen*)
- Mecklenburg-Western Pomerania Ministry of the Interior, Department II 5 (*Mecklenburg-Vorpommern Innenministerium, Abteilung II 5*)
- North Rhine-Westphalia Ministry of the Interior and Municipalities, Department for the Protection of the Constitution (*Nordrhein-Westfalen Ministerium für Inneres und Kommunales, Abteilung Verfassungsschutz*)
- Rhineland-Palatinate Ministry of the Interior and Sport, Department for the Protection of the Constitution (*Rheinland-Pfalz Ministerium des Innern und für Sport, Abteilung Verfassungsschutz*)
- Saarland State Office for the Protection of the Constitution (*Landesamt für Verfassungsschutz Saarland*)
- Saxony State Office for the Protection of the Constitution (*Landesamt für Verfassungsschutz Sachsen*)
- Saxony-Anhalt Ministry of the Interior and Sport, Department for the Protection of the Constitution (*Sachsen-Anhalt Ministerium für Inneres und Sport, Abteilung Verfassungsschutz*)
- Schleswig-Holstein Ministry of the Interior, Department for the Protection of the Constitution (*Schleswig-Holstein Innenministerium, Abteilung Verfassungsschutz*)
- Thuringia Ministry of the Interior and Municipalities, Office for the Protection of the Constitution (*Thüringen Ministerium für Inneres und Kommunales, Amt für Verfassungsschutz*)

Greece

- National Intelligence Service (*Εθνική Υπηρεσία Πληροφοριών*, EYP)
- Directorate of Military Intelligence of the National Defence General Staff (*Διεύθυνση Στρατιωτικών Πληροφοριών του Γενικού Επιτελείου Εθνικής Άμυνας*)

Hungary

- Constitution Protection Office (*Alkotmányvédelmi Hivatal*, AH)

- Special Service for National Security (*Nemzetbiztonsági Szakszolgálat*, NBSZ)
- Counter Terrorism Centre (*Terrorelhárítási Központ*, TEK) (service belonging to the police)
- Information Office (*Információs Hivatal*, IH)

Ireland

- Defence Forces (*Óglaigh na hÉireann*), Directorate of Intelligence (G2)
- An Garda Síochána National Surveillance Unit (NSU) (belonging to the police)
- An Garda Síochána Crime and Security Branch

Italy

- Information and Internal Security Agency (*Agenzia informazioni e sicurezza interna*, AISI)
- Information and External Security Agency (*Agenzia Informazioni e Sicurezza Esterna*, AISE)
- Department of Information and Security (*Reparto informazioni e sicurezza*, RIS)

Latvia

- Constitutional Protection Bureau (*Satversmes Aizsardzibas Birojs*, SAB)
- Defence Intelligence and Security Service (*Militārās izlūkošanas un drošības dienests*, MIDD)

Lithuania

- State Security Department (Valstybes Saugumo Departamentas, VSD)
- Second Investigation Department under the Ministry of National Defence (*Antraisi Departamentas Prie Krasto Apsaugos Ministerijos*, AOTD prie KAM)

Luxembourg

- State Intelligence Service (Service de Renseignements de l'État, SREL)

Malta

- Security Service (*Servizz tas-Sigurtà*)

Netherlands

- General Intelligence and Security Service (*Algemene Inlichtingen- en Veiligheidsdienst*, AIVD)
- Military Intelligence and Security Service (*Militaire Inlichtingen- en Veiligheidsdienst*, MIVD)

Poland

- Foreign Intelligence Authority (*Agencja Wywiadu*, AW)
- Military Counterintelligence Service (*Służba Kontrwywiadu Wojskowego*, SKW)
- Internal Security Agency (*Agencja Bezpieczeństwa Wewnętrznego*, ABW)

- Central Anti-Corruption Bureau (*Centralne Biuro Antykorupcyjne*, CBA)
- Military Intelligence Service (*Służba Wywiadu Wojskowego*, SWW)

Portugal

- Strategic Intelligence and Defence Service *(Serviço de Informações Estratégicas de Defesa*, SIED)
- Service of Security Intelligence (*Serviço de Informações de Segurança*, SIS)

Romania

- External Intelligence Service (*Serviciul de Informatii Externe*, SIE)
- General Directorate for Defence Intelligence (*Direcția Generală de Informații a Apărării*, DGIA)
- Romanian Intelligence Service (*Serviciul Roman de Informatii*, SRI)
- Department for Information and Internal Protection (*Direcția Generală de Informații și Protecție Internă*, DGIPI)

Slovakia

- National Security Authority (*Národný bezpečnostný úrad*, NBÚ)
- Slovak Information Service (*Slovenská informačná služba*, SIS)
- Military Intelligence (*Vojenské spravodajstvo*, VS)

Slovenia

- Slovene Intelligence and Security Agency (*Slovenska obveščevalno-varnostna agencija*, SOVA)
- Intelligence and Security Service of the Ministry of Defence (*Obveščevalno-varnostna služba Ministrstva za obrambo*, OVS)

Spain

- National Centre for the Protection of Critical Infrastructures (*Centro Nacional de Protección de Infraestructuras Críticas*, CNPIC)
- National Intelligence Centre (*Centro Nacional de Inteligencia*, CNI)
- Intelligence Centre on Terrorism and Organised Crime (*Centro de Inteligencia Contra el Terrorismo y el Crimen Organizado*, CITCO)
- Intelligence Centre of the Armed Forces (*Centro de Inteligencia de las Fuerzas Armadas*, CIFAS)

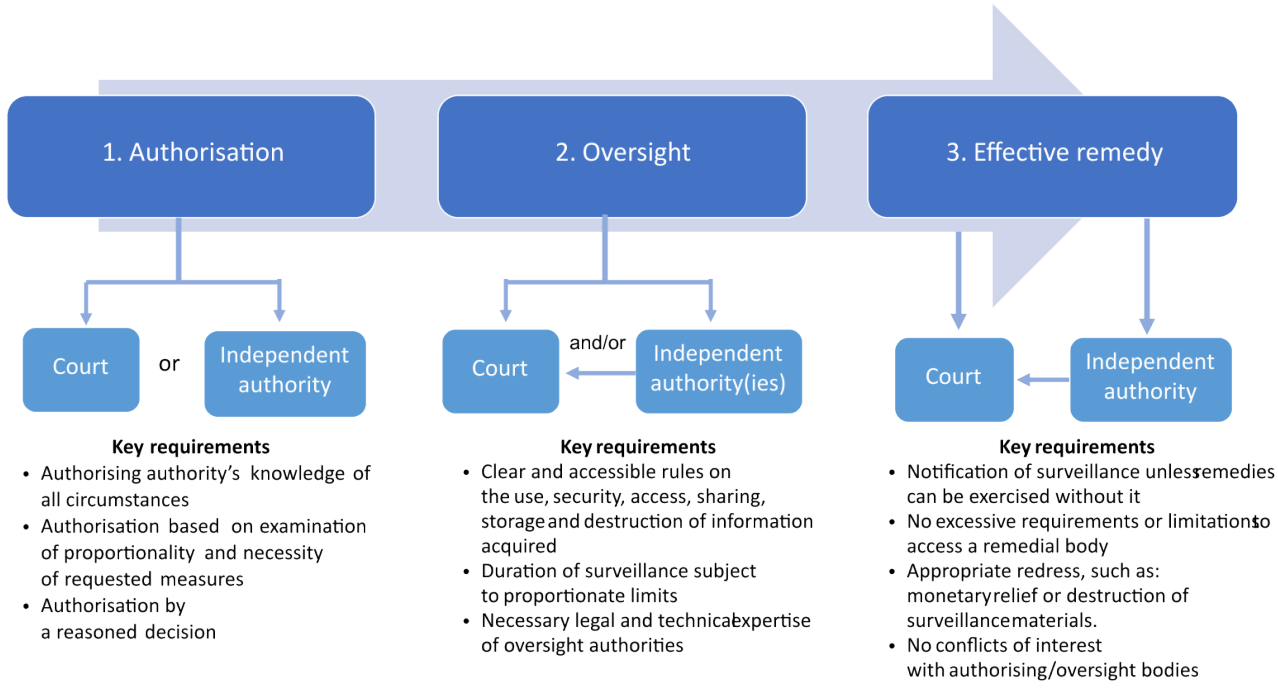
Sweden

- National Defence Radio Establishment (*Försvarets radioanstalt*, FRA)

- Military Intelligence and Security Service (*Militära underrättelse- och säkerhetstjänsten*, MUST)

Annex 2 - Oversight and review of surveillance

Figure 13 – Oversight and review of surveillance – main requirements as per ECtHR and CJEU case law



Source: FRA, 2023

Endnotes

[1] FRA (2015), Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU – Volume I: Member States' legal frameworks, Luxembourg, Publications Office of the European Union (Publications Office); FRA (2015), Surveillance by intelligence services: Fundamental rights safeguards and remedies in the European Union – Summary, Luxembourg, Publications Office; FRA (2017), Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU – Volume II: Field perspectives and legal update, Luxembourg, Publications Office; and FRA (2018), Surveillance by intelligence services: Fundamental rights safeguards and remedies in the European Union – Volume II: Summary, Luxembourg, Publications Office.

[2] European Parliament (2014), Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, P7_TA(2014) 0230, Strasbourg, 12 March 2014.

[3] European Parliament (2022), Decision of 10 March 2022 on setting up a committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, and defining the subject of the inquiry, as well as the responsibilities, numerical strength and term of office of the committee, P9_TA(2022) 0071, Strasbourg, 10 March 2022.

[4] For more details, see European Parliament (n.d.), Committee of inquiry to investigate the use of Pegasus and equivalent surveillance spyware.

[5] The following report covers these areas: European Parliament (2022), The use of Pegasus and equivalent surveillance spyware: The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware, draft study, December 2022.

[6] European Parliament (2022), Draft report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, 8 November 2022.

[7] European Parliament (2023), European Parliament draft recommendation to the Council and the Commission pursuant to Rule 208(12) of the rules of procedure following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, 4 January 2023.

[8] European Parliament (2022), The use of Pegasus and equivalent surveillance spyware: The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware, draft study, December 2022; and European Parliament (2022), The impact of Pegasus on fundamental rights and democratic processes, study, December 2022.

[9] United Nations, Office of the United Nations High Commissioner for Human Rights (2022), The right to privacy in the digital age, A/HRC/51/17, 4 August 2022.

[10]Council of Europe, Committee on Legal Affairs and Human Rights (2022), Pegasus and similar spyware and secret state surveillance, 8 April 2022.

[11] Council of Europe, Commissioner for Human Rights (2023), Highly intrusive spyware threatens the essence of

human rights, human rights comment, Strasbourg, Council of Europe, 27 January 2023; see also Council of Europe, Information Society Department (2022), Pegasus spyware and its impacts on human rights, Strasbourg, Council of Europe, 20 June 2022.

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ 2016 L 119.

[13] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119.

[14] Council of Europe, Committee of Ministers, Protocol amending the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108), ETS No. 223, 18 May 2018.

[15] Austria, Federal Act amending the Act concerning Police State Protection Act, the Security Police Act, the Criminal Code, the Code of Criminal Procedure 1975 and the Expungement Redemption Act 1972 (Bundesgesetz, mit dem das Polizeiliche Staatsschutzgesetz, das Sicherheitspolizeigesetz, das Strafgesetzbuch, die Strafprozeßordnung 1975 und das Tilgungsgesetz 1972 geändert werden, Federal Law Gazette I No. 148/2021, 26 July 2021; Parliament of Austria (n.d.), BAT Committee of Inquiry (3/A-USA) (BVT-Untersuchungsausschuss (3/A-USA); Parliament of Austria (2019), BAT Committee of Inquiry: Valuable findings, but still some questions unanswered (BVT-Untersuchungsausschuss: Wertvolle Erkenntnisse, aber noch einige Fragen offen, Parliamentary Correspondence No. 937, 25 September 2019; and Commission of Inquiry into the Terrorist Attack of November 2nd, 2020 (Untersuchungskommission (2021), Final report (Abschlussbericht, 10 February 2021.

[16] Austria, State Protection and Intelligence Service Act (Bundesgesetz über die Organisation, Aufgaben und Befugnisse des Verfassungsschutzes - Staatsschutz- und Nachrichtendienst-Gesetz, Federal Law Gazette I No. 5/2016, Art. 17a f..

[17] Greece, Emergency regulations for the protection of public health from the ongoing consequences of the COVID-19 pandemic, development, social protection, re-opening of the courts and other matters (Κατεπείγουσες ρυθμίσεις για την προστασία της δημόσιας υγείας από τις συνεχιζόμενες συνέπειες της πανδημίας του κορωνοϊού COVID-19, την ανάπτυξη, την κοινωνική προστασία και την επαναλειτουργία των δικαστηρίων και άλλα ζητήματα, Law No. 4790, Government Gazette Issue A' 48/31.03.2021, Art. 87.

[18] Greece, Waiving privacy procedure, cyber security and protection of citizens' personal data (Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών, Law No. 5002/2022, Government Gazette Issue A' 228/09.1.2022, Art. 4 (7).

[19] Greece, Kathimerini, 'Observations: Against the backdrop of the bill, the conflict', 17 November 2022.

[20] Greece, Waiving privacy procedure, cyber security and protection of citizens' personal data (Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών, Law No. 5002/2022, Government Gazette Issue A' 228/09.1.2022, Arts. 10–14.

[21] Spain, La Moncloa (2022), 'Pedro Sánchez announces a reform of the legal control regulation of the National Intelligence Centre (CNI) to strengthen its guarantees', press release, 26 May 2022.

[22] Spain, Government of Spain(Gobierno de España, General Administration of the State (Administración General

del Estado, Annual Action Plan 2023 (Plan Anual Normativo 2023, 2023.

[23]France, Council of State (Conseil d'État, French Data Network and Others v. France, Decision No. 393099, 21 April 2021.

[24]Germany, Federal Constitutional Court (Bundesverfassungsgericht, BVerfG), 1 BvR 2835/17, 19 May 2020; and BVerfG (2022), 1 BvR 2354/13, 28 September 2022.

[25]Portugal, Constitutional Court (Tribunal Constitucional, Judgment No. 464/2019, 21 October 2019.

[26] Germany, Act to Change the Federal Intelligence Service Act to Implement the Guidelines of the Federal Constitutional Court and the Federal Administrative Court (Gesetz zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts, 19 April 2021, setting up the Independent Supervisory Council (Unabhängiger Kontrollrat.

[27] Bulgaria, Amendments and supplements to the Personal Data Protection Act (Закон за изменение и допълнение на Закона за защита на личните данни, 26 February 2019; State Intelligence Agency Act (Закон за Държавна агенция „Разузнаване", 13 October 2015, last amended 4 August 2020, Arts. 27 and 28; Military Intelligence Act (Закон за военното разузнаване, 13 November 2015, last amended 26 March 2021, Art. 78; and State Agency for National Security Act (Закон за Държавна агенция „Национална сигурност", 13 October 2015, last amended 5 June 2020, Art. 37.

[28]Croatia, General Regulation on Data Protection Act (Zakon o provedbi Opće uredbe o zaštiti podataka, 25 May 2018.

[29] Greece, Hellenic Data Protection Authority (HDPA), measures for implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions, Law No. 4624, Government Gazette Issue A' 137/29.08.2019, Art. 10 (5).

[30] Lithuania, Law on Legal Protection of Personal Data Processed for the Purposes of Prevention, Investigation, Detection, or Prosecution of Criminal Acts, Execution of Sentences, or National Security and Defence (Asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas), No. XIII-1435, 30 June 2018, Art. 39 (3).

[31]Hungary, Act 112 of 2011 on the right to informational self-determination and information freedom (törvény az információs önrendelkezési jogról és az információszabadságról, Art. 51/A; amendment entered into force on 26 July 2018, introduced by Amending Act 38 of 2018, 26 July 2018, Art. 20.

[32]GDPR, Arts. 2 (2) and 23 (1) (a); Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002 L 201, Arts. 1 (3) and 15 (1).

[33] FRA (2017), Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU – Volume II: Field perspectives and legal update, Luxembourg, Publications Office, p. 22.

[34]FRA (2017), Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU – Volume II: Field perspectives and legal update, Luxembourg, Publications Office, p. 22. See also European Parliament

(2022), The impact of Pegasus on fundamental rights and democratic processes , study, December 2022.

[35]European Parliament (2022), The impact of Pegasus on fundamental rights and democratic processes , study, December 2022.

[36]CJEU, Joined cases C-793/19 and C-794/19, Bundesrepublik Deutschland v. SpaceNet AG and Telekom Deutschland GmbH[GC], 20 September 2022, para. 66;Joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v. Premier ministre and Others and Ordre des barreaux francophones et germanophone and Others v. Conseil des ministres [GC], 6 October 2020, para. 99; and C-623/17, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others [GC], 6 October 2020, para. 44.

[37]CJEU, Joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v. Premier ministre and Others and Ordre des barreaux francophones et germanophone and Others v. Conseil des ministres [GC], 6 October 2020, paras. 56–79; and C-623/17, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others [GC], 6 October 2020, paras. 19–29, 30 and 50.

[38]CJEU, Joined cases C-793/19 and C-794/19, Bundesrepublik Deutschland v. SpaceNet AG and Telekom Deutschland GmbH[GC], 20 September 2022, para. 92; Joined cases C-511/18, C-512/18 and C-520/18,La Quadrature du Net and Others v. Premier ministre and Others and Ordre des barreaux francophones et germanophone and Others v. Conseil des ministres[GC], 6 October 2020, para. 135; and C-623/17, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others[GC], 6 October 2020, para. 74.

[39]CJEU, Joined cases C-793/19 and C-794/19, Bundesrepublik Deutschland v. SpaceNet AG and Telekom Deutschland GmbH[GC], 20 September 2022, paras. 72 and 93–94; C-140/20,G.D. v. Commissioner of An Garda Síochána and Others[GC], 5 April 2022, para. 58; Joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v. Premier ministre and Others and Ordre des barreaux francophones et germanophone and Others v. Conseil des ministres[GC], 6 October 2020, para. 136; and C-623/17, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others [GC], 6 October 2020, para. 75.

[40] Directive on privacy and electronic communications, Art. 15 (1); CJEU, Joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v. Premier ministre and Others and Ordre des barreaux francophones et germanophone and Others v. Conseil des ministres[GC], 6 October 2020, para. 58, referring to Joined cases C-203/15 and C-698/15, Tele2 Sverige v. Post- och telestyrelsen and Secretary of State for the Home Department v. Watson and Others [GC], 21 December 2016 and operative part; and C-623/17, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others [GC], 6 October 2020, paras. 38 and 49 and operative part.

[41]French Council of State (Conseil d'État, French Data Network and Others v. France, Decision No. 393099, 21 April 2021.

[42] BVerfG, 1 BvR 2835/17, 19 May 2020.

[43]BVerfG, 1 BvR 2835/17, 19 May 2020, paras. 265–300 and 324.

[44] CJEU,Joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v. Premier ministre and Others and Ordre des barreaux francophones et germanophone and Others v. Conseil des ministres[GC], 6 October 2020, para. 103.

[45] Council of Europe, Convention 108+: Convention for the protection of individuals with regard to the processing of personal data, ETS No. 223, June 2018. See also Council of Europe, The modernised Convention 108: Novelties in a nutshell; and FRA, Council of Europe and European Data Protection Supervisor (2018), Handbook on European

data protection law, Luxembourg, Publications Office, Chapter 8, p. 273.

[46] Council of Europe, Convention 108+: Convention for the protection of individuals with regard to the processing of personal data, ETS No. 223, June 2018, para. 92, p. 26.

[47] Council of Europe, Convention 108+: Convention for the protection of individuals with regard to the processing of personal data, ETS No. 223, June 2018, paras. 98 and 118, pp. 26 and 29.

[48]CJEU, Joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v. Premier ministre and Others and Ordre des barreaux francophones et germanophone and Others v. Conseil des ministres[GC], 6 October 2020, paras. 135–137; C-623/17, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others [GC], 6 October 2020, paras. 74–75 and 77; Joined cases C-793/19 and C-794/19, Bundesrepublik Deutschland v. SpaceNet AG and Telekom Deutschland GmbH[GC], 20 September 2022, paras. 72 and 131 and operative part; and C-140/20,G.D. v. Commissioner of An Garda Síochána and Others[GC], 5 April 2022, para. 58.

[49] CJEU, Joined cases C-793/19 and C-794/19, Bundesrepublik Deutschland v. SpaceNet AG and Telekom Deutschland GmbH[GC], 20 September 2022, paras. 72 and 131 and operative part; C-140/20,G.D. v. Commissioner of An Garda Síochána and Others[GC], 5 April 2022, para. 58; and Joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v. Premier ministre and Others and Ordre des barreaux francophones et germanophone and Others v. Conseil des ministres[GC], 6 October 2020, paras. 137 and 177.

[50] CJEU, Joined cases C-793/19 and C-794/19, Bundesrepublik Deutschland v. SpaceNet AG and Telekom Deutschland GmbH[GC], 20 September 2022, para. 91; Joined cases C-511/18, C-512/18 and C-520/18,La Quadrature du Net and Others v. Premier ministre and Others and Ordre des barreaux francophones et germanophone and Others v. Conseil des ministres[GC], 6 October 2020, para. 132; and C-623/17, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others [GC], 6 October 2020, para. 68; and ECtHR, Big Brother Watch and Others v. the United Kingdom[GC], Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, paras. 332–334, 339 and 425; Haščák v. Slovakia, Nos. 58359/12, 27787/16 and 67667/16, 23 June 2022, paras. 89 and 94–95.

[51] ECtHR, Big Brother Watch and Others v. the United Kingdom[GC], Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, paras. 336, 350–352, 356, 377 and 425.

[52] ECtHR, Big Brother Watch and Others v. the United Kingdom[GC], Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, paras. 337 and 357.

[53] ECtHR, Centrum för rättvisa v. Sweden [GC], No. 35252/08, 25 May 2021, paras. 359 and 372.

[54] ECtHR, Centrum för rättvisa v. Sweden [GC], No. 35252/08, 25 May 2021, para. 272.

[55] ECtHR, Marie Ringler v. Austria (dec.), No. 2309/10, 12 May 2020, paras. 73 and 79.

[56]CJEU, Joined cases C-793/19 and C-794/19, Bundesrepublik Deutschland v. SpaceNet AG and Telekom Deutschland GmbH[GC], 20 September 2022, paras. 61 and 87–89; C-140/20, G.D. v. Commissioner of An Garda Síochána and Others[GC], 5 April 2022, para. 45; and ECtHR, Big Brother Watch and Others v. the United Kingdom[GC], Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, paras. 363–364, 416 and 425.

[57] See, for example, ECtHR, Big Brother Watch and Others v. the United Kingdom[GC], Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, paras. 364, 416, 421 and 423.

[58] FRA (2017), Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU – Volume II: Field perspectives and legal update, Luxembourg, Publications Office, p. 59.

[59] France, National Commission for Control of Intelligence Techniques (CNCTR) (2022), 6st annual report 2021 (6e rapport d'activité 2021, Paris, CNCTR, p. 67.

[60] Italy, Italian Data Protection Authority (Garante pre la protezione dei dati personali (2019), 'Privacy e sicurezza: l'iniziativa di Garante privacy e Intelligence a tutela dei cittadini', press release, 6 March 2019.

[61]FRA (2017), Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU – Volume II: Field perspectives and legal update, Luxembourg, Publications Office, pp. 93–97.

[62] CJEU, Joined cases C-793/19 and C-794/19, Bundesrepublik Deutschland v. SpaceNet AG and Telekom Deutschland GmbH [GC], 20 September 2022, paras. 72 and 131 and operative part; and ECtHR, Big Brother Watch and Others v. the United Kingdom, Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, paras. 350–352, 377, 416 and 425.

[63]CJEU, Joined cases C-793/19 and C-794/19, Bundesrepublik Deutschland v. SpaceNet AG and Telekom Deutschland GmbH [GC], 20 September 2022, paras. 72 and 131 and operative part and ECtHR, Centrum för rättvisa v. Sweden [GC], No. 35252/08, 25 May 2021, paras. 266, 268, 270, 275, 298–302.

[64] European Parliament (2022), Pegasus and surveillance spyware, in-depth analysis, May 2022, p. 4.

[65]France, Internal Security Code (Code de la sécurité intérieure, Art. L 821-1.

[66] France, CNCTR (2022), 6e annual report 2021 (6e rapport d'activité 2021, Paris, CNCTR, pp. 8–9.

[67] The Netherlands, Intelligence and Security Services Act 2017 (Wet op de inlichtingen- en veiligheidsdiensten 2017, 1 May 2022.

[68] The Netherlands, Intelligence and Security Services Act 2017 (Wet op de inlichtingen- en veiligheidsdiensten 2017,1 May 2022, Arts. 32–37.

[69]The Netherlands, Investigatory Powers Commission (Toetsingscommissie inzet bevoegdheden, TIB) (2020), Annual report TIB 2018/2019, The Hague, TIB.

[70] FRA (2017), Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU – Volume II: Field perspectives and legal update, Luxembourg, Publications Office, p. 40.

[71] Germany, Act amending the BND Act to implement the requirements of the Federal Constitutional Court and the Federal Administrative Court (Gesetz zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts, 19 April 2021, Art. 1 (21), amending Arts. 23 and 42 of the BND Act.

[72] The Netherlands, Intelligence and Security Services Act 2017 (Wet op de inlichtingen- en veiligheidsdiensten 2017, 1 May 2022, Arts. 32–37.

[73] Finland, Ministry of the Interior (sisäministeriö/inrikeministeriet (n.d.), Civilian intelligence protects Finland's national security.

[74] Finland, Act on the Use of Network Traffic Intelligence in Civilian Intelligence (laki tietoliikennetiedustelusta siviilitiedustelussa/lag om civil underrättelseinhämtning avseende datatrafik,Act No. 582/2019, 18 January 2019, Section 7; and Act on Military Intelligence (laki sotilastiedustelusta/lag om militär underrättelseverksamhet), Act No. 590/2019, 26 April 2019.

[75]Finland,Parliament's Rules of Procedure(eduskunnan työjärjestys/riksdagens arbetsordning, Act No. 40/2000, Chapter 3, Section 31 (b). For the English translation of the tasks provided in this section of the act, see Parliament of Finland (n.d.), Intelligence Oversight Committee.

[76] France, Order No. 58-1100 on the functioning of parliamentary assemblies (Ordonnance n° 58-1100 relative au fonctionnement des assemblées parlementaires, 17 November 1958, Art. 6 (9).

[77]France, Buffet, F.-N., Parliamentary Delegation on Intelligence (Délegation parlementaire au renseignement (2022), Activity of the Parliamentary Delegation on Intelligence 2021-2022 (Activité de la délégation parlementaire au renseignement pour l'année 2021–2022, 24 February 2022.

[78] Parliament of Austria (n.d.), BAT Committee of Enquiry (BVT-Untersuchungsausschuss (3/A-USA); Commission of Inquiry into the Terrorist Attack of November 2nd, 2020 (Untersuchungskommission, Final report (Abschlussbericht, 10 February 2021

[79] ECtHR, Zoltán Varga v. Slovakia, Nos. 58361/12, 25592/16 and 27176/16, 20 July 2021, paras. 135 and 159.

[80] ECtHR, Ekimdzhiev and Others v. Bulgaria, No. 70078/12, 11 January 2022, para. 414.

[81] FRA (2017), Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU – Volume II: Field perspectives and legal update, Luxembourg, Publications Office, p. 73.

[82] FRA (2017), Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU – Volume II: Field perspectives and legal update, Luxembourg, Publications Office, p. 75.

[83] Czechia, Act No. 325/2017 Coll., effective from 1 January 2018, which amended Act No. 153/1994 Coll., on the intelligence services of the Czech Republic; and Act No. 150/2021 Coll., amending Act No. 289/2005 Coll. on military intelligence, as amended, and some other acts.

[84] Austria, Federal Act amending the Act concerning Police State Protection Act, the Security Police Act, the Criminal Code, the Code of Criminal Procedure 1975 and the Expungement Redemption Act 1972 (Bundesgesetz, mit dem das Polizeiliche Staatsschutzgesetz, das Sicherheitspolizeigesetz, das Strafgesetzbuch, die Strafprozeßordnung 1975 und das Tilgungsgesetz 1972 geändert werden), Federal Law Gazette I No. 148/2021, 26 July 2021, Art. 4a.

[85]Austria, Explanatory notes to the Federal Act amending the Act concerning Police State Protection Act, the Security Police Act, the Criminal Code, the Code of Criminal Procedure 1975 and the Expungement Redemption Act 1972 (Eräuterungen zum Bundesgesetz, mit dem das Polizeiliche Staatsschutzgesetz, das Sicherheitspolizeigesetz, das Strafgesetzbuch, die Strafprozeßordnung 1975 und das Tilgungsgesetz 1972 geändert werden).

[86]Austria, State Protection and Intelligence Service Act (Bundesgesetz über die Organisation, Aufgaben und Befugnisse des Verfassungsschutzes - Staatsschutz- und Nachrichtendienst-Gesetz, Federal Law Gazette I No. 5/2016, Art. 17b, Section 2a.

[87] Finland, Act on the Oversight of Intelligence Gathering (laki tiedustelutoiminnan valvonnasta/lag om övervakning

av underrättelseverksamheten, Act No. 121/2019, 18 January 2019, Sections 11–14.

[88] Lithuania, Law on Intelligence Ombudsmen (Žvalgybos kontrolierių įstatymas), No. XIV-868, 23 December 2021

[89]Lithuania, Law on Legal Protection of Personal Data Processed for the Purposes of Prevention, Investigation, Detection, or Prosecution of Criminal Acts, Execution of Sentences, or National Security and Defence (Asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas), No. XIII-1435, 30 June 2018, Art. 39 (3).

[90] Germany, Act to Change the Federal Intelligence Service Act to Implement the Guidelines of the Federal Constitutional Court and the Federal Administrative Court (Gesetz zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts,19 April 2021.

[91] The Netherlands, Intelligence and Security Services Act 2017 (Wet op de inlichtingen- en veiligheidsdiensten 2017, 1 May 2022, Arts. 32–37.

[92] Slovenia, Personal Data Protection Act (Zakon o varstvu osebnih podatkov, ZVOP-2), Official Journal of the Republic of Slovenia, No. 136/22, 15 December 2022, Art. 29 (6).

[93] Bulgaria, Amendments and supplements to the Personal Data Protection Act (Закон за изменение и допълнение на Закона за защита на личните данни, 26 February 2019.

[94]Bulgaria, State Intelligence Agency Act (Закон за Държавна агенция „Разузнаване”, 13 October 2015, last amended 4 August 2020, Arts. 27 and 28; Military Intelligence Act (Закон за военното разузнаване, 13 November 2015, last amended 26 March 2021, Art. 78; State Agency for National Security Act (Закон за Държавна агенция „Национална сигурност”, 13 October 2015, last amended 5 June 2020, Art. 37.

[95]Greece, Hellenic Data Protection Authority (HDPA), measures for implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions, Law No. 4624, Government Gazette Issue A’ 137/29.08.2019, Art. 10, para. 5.

[96]Croatia, Implementation of the General Regulation on Data Protection Act (Zakon o provedbi Opće uredbe o zaštiti podataka, Official Gazette No. 42/18, Art. 1 (2); Act on the Protection of Natural Persons in Connection with the Processing and Exchange of Personal Data for the Purposes of Prevention, Research, Detection or Prosecution of Criminal Offenses or Execution of Criminal Sanctions (Zakon o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija,Official Gazette (Narodne novine No. 68/18, Art. 3 (2); Croatian Personal Data Protection Agency (n.d.), Croation Personal Data Protection Agency;Croatian Personal Data Protection Agency (Agencija za zaštitu osobnih podataka (n.d.), Insight into the files of school employees by employees of the Security and Intelligence Agency (Uvid u dosje zaposlenika škole od strane zaposlenika Sigurnosno-obavještajne agencije.

[97] Lithuania, Law on Legal Protection of Personal Data Processed for the Purposes of Prevention, Investigation, Detection, or Prosecution of Criminal Acts, Execution of Sentences, or National Security and Defence (Asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas, No. XIII-1435, 30 June 2018, Art. 39 (3).

[98] Belgium, Act on the protection of natural persons with regard to the processing of personal data (Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 5 September 2018. See Belgium, Standing Intelligence Agencies Review Committee (Standing Committee I) (2019), Activity Report 2018 (Rapport d'activités 2018, p. 71.

[99]Belgium, Autorité de protection des données, Organe de contrôle de l'information policière, Comité permanent de contrôle des services de renseignement and Comité permanent de contrôle des services de police, Protocol for cooperation between the Belgian federal supervisory authorities in the field of data protection agreement between the data protection authority, the police information supervisory body, the permanent committee for the control of the intelligence services and the permanent committee control of police services (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, 20 November 2020.

[100] See the latest report: Belgium, Standing Committee I (2022), Rapport d'activités 2021, p. 123.

[101]Germany, Act for the Adjustment of Data Protection Law to Regulation (EU) 2016/679 and for the Implementation of Directive (EU) 2016/680 (Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, 30 June 2017,

[102]Germany, Federal Act on the Protection of the Constitution (Bundesverfassungsschutzgesetz, after further legal changes, 20 December 1990, Sections 27 and 28; Federal Intelligence Agency Act (Bundesnachrichtendienstgesetz, 20 December 1990, Sections 63 and 64; Military Counter Intelligence Act (Gesetz über den Militärischen Abschirmdienst, Sections 13 and 13a.

[103] Germany, Act to Change the Federal Intelligence Service Act to Implement the Guidelines of the Federal Constitutional Court and the Federal Administrative Court (Gesetz zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts, 19 April 2021.

[104] Luxembourg, Act of 1 August 2018 on the organisation of the National Data Protection Commission, implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), amending the Labour Code and the amended Act of 25 March 2015 stipulating the rules of remuneration and the terms and conditions for the promotion of State civil servants (Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en oeuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État, Arts. 8, 44 and 45.

[105] Cyprus, Law on the protection of individuals with regard to the processing of personal data and the free circulation of personal data of 2018 (Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018, No. 125(I)/2018, Art. 25 (a).

[106] Sweden, Act (2021:1171) on the processing of personal data by the Swedish Armed Forces (Lag [2021:1171] om behandling av personuppgifter vid Försvarsmakten, 2 December 2021, Chapter 6, Sections 3 and 4; Act (2021:1172) on the processing of personal data by the National Defence Radio Establishment (Lag [2021:1172] om behandling av personuppgifter vid Försvarets radioanstalt, 2 December 2021, Chapter 6, Sections 4 and 5. See also

Ministry of Defence (Försvarsdepartementet (2021), Processing of personal data by the Swedish Armed Forces and the National Defence Radio Establishment (Behandling av personuppgifter vid Försvarsmakten och Försvarets radioanstalt, government bill, 13 September 2021, p. 148.

[107] Hungary, Act 112 of 2011 on the right to informational self-determination and information freedom (törvény az információs önrendelkezési jogról és az információszabadságról, Art. 51/A; amendment entered into force on 26 July 2018, introduced by Amending Act 38 of 2018, 26 July 2018, Art. 20.

[108] ECtHR, Hüttl v. Hungary, No. 58032/16, 29 September 2022, para. 18.

[109] See United Nations, Special Rapporteur on Privacy (2019), Comments on legislation and policy – Malta, 2/2019, 12 December 2019.

[110] ECtHR, Ekimdzhiev and Others v. Bulgaria, No. 70078/12, 11 January 2022, para. 262; and Centrum för rättvisa v. Sweden, No. 35252/08, 25 May 2021, para. 167.

[111] CJEU, Joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v. Premier ministre and Others and Ordre des barreaux francophones et germanophone and Others v. Conseil des ministres, 6 October 2020, para. 190; and ECtHR, Centrum för rättvisa v. Sweden, No. 35252/08, 25 May 2021, paras. 166–167, 249, 251, 271, 273, 275 and 362; and Big Brother Watch and Others v. the United Kingdom, Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, paras. 413, 415 and 425.

[112] ECtHR, Ekimdzhiev and Others v. Bulgaria, No. 70078/12, 11 January 2022, paras. 264–277.

[113] FRA (2017), Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU – Volume II: Field perspectives and legal update, Luxembourg, Publications Office, p. 60.

[114]ECtHR,Centrum för rättvisa v. Sweden, No. 35252/08, 25 May 2021, para. 271.

[115] ECtHR, Ekimdzhiev and Others v. Bulgaria, No. 70078/12, 11 January 2022, paras. 264–275, 354–355, 356 (h) and 380–382; and Marie Ringler v. Austria, No. 2309/10, 12 May 2020, para. 73.

[116] ECtHR, Centrum för rättvisa v. Sweden, No. 35252/08, 25 May 2021, paras. 359 and 372.

[117]Bulgaria, Amendments and supplements to the Personal Data Protection Act (Закон за изменение и допълнение на Закона за защита на личните данни, 26 February 2019.

[118]Bulgaria, National Assembly (Народно събрание (2019), Explanatory report to the draft amendments and supplements to the Personal Data Protection Act (Мотиви към Законопроект за изменение и допълнение на Закона за защита на личните данни, 18 July 2015.

[119]Croatia, Act on the Protection of Natural Persons in Connection with the Processing and Exchange of Personal Data for the Purposes of Prevention, Research, Detection or Prosecution of Criminal Offenses or Execution of Criminal Sanctions (Zakon o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, 4 August 2018.

[120] Lithuania, Law on Legal Protection of Personal Data Processed for the Purposes of Prevention, Investigation, Detection, or Prosecution of Criminal Acts, Execution of Sentences, or National Security and Defence (Asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas,No. XIII-1435,

30 June 2018, Art. 39 (3).

[121] Lithuania, Law on Seimas Ombudsmen (Seimo kontrolierių įstatymas, No. VIII-950, 3 December 1998, as amended by Law No. XIV-872 of 23 December 2021, and other amendments, Art. 12 (2).

[122]Lithuania, Law on Intelligence Ombudsmen (Žvalgybos kontrolierių įstatymas, No. XIV-868, 23 December 2021, Art. 3.

[123]Cyprus, Law on the protection of individuals with regard to the processing of personal data and the free circulation of personal data of 2018 (Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018, No. 125(I)/2018,

[124] Finland, Intelligence Ombudsman (Tiedusteluvalvontavaltuutettu (2020), Report of the Intelligence Ombudsman for 2019 (Tiedusteluvalvontavaltuutetun kertomus vuodelta 2019, K 14/2020 vp, 20 May 2020, p. 20; Finland, Intelligence Ombudsman (2021), Report of the Intelligence Ombudsman for 2020 (Tiedusteluvalvontavaltuutetun kertomus vuodelta 2020), K 10/2021 vp, 27 April 2021, p. 8; and Finland, Intelligence Ombudsman (2022), Report of the Intelligence Ombudsman for 2021 (Tiedusteluvalvontavaltuutetun kertomus vuodelta 2021), K 13/2022 vp, 4 May 2022, p. 8.

[125] Finland, Act on the Oversight of Intelligence Gathering (laki tiedustelutoiminnan valvonnasta/lagom övervakning av underrättelseverksamheten, Act No. 121/2019, 18 January 2019, Chapter 2, Section 3.

[126] Denmark, Consolidated Act No. 231 of 7 March 2017 on the Danish Security and Intelligence Service (Bekendtgørelse af lov om Politiets Efterretningstjeneste (PET).

[127] Denmark, Danish Intelligence Oversight Board (TET), Annual report 2021: Politiets Efterretningstjeneste, Copenhagen, TET, p. 28; and TET, Annual report 2021: Danish Defence Intelligence Service, Copenhagen, TET, p. 22.

[128] FRA (2017), Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU – Volume II: Field perspectives and legal update, Luxembourg, Publications Office, p. 118.

[129] Belgium, Standing Committee I (2021), Activity report 2020, Brussels, Standing Committee I, p. 1.

[130] Belgium, Standing Committee I (2022), Activity report 2021 (Rapport d'activités 2021, p. 1.

[131] France, CNCTR (2022), 6e annual report 2021 (6e rapport d'activité 2021, Paris, CNCTR, p. 108.

[132] Germany, Federal Parliament (2022), Bericht gemäß § 14 Absatz 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5, 7a und 8 G 10 (Berichtszeitraum 1. Januar bis 31. Dezember 2020), Document 20/4976, 14 December 2022, p. 7.

[133] Netherlands, Review Committee on the Intelligence and Security Services (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, CTIVD) (2022), Annual report 2021, The Hague, CTIVD, p. 19.

[134] FRA (2017), Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU – Volume II: Field perspectives and legal update, Luxembourg, Publications Office, p. 135.