

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

November 2022 Update

Country: Ireland

FRANET contractor: Irish Centre for Human Rights

Author name: Dr TJ McIntyre

**DISCLAIMER:** This document was commissioned under contract as background material for comparative analysis by the European Union Agency for Fundamental Rights (FRA) for the project '*National intelligence authorities and surveillance in the EU*'. The information and views contained in the document do not necessarily reflect the views or the official position of the FRA. The document is made publicly available for transparency and information purposes only and does not constitute legal advice or legal opinion.

## Table of Contents

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

# 1. Summary

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

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

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

### FRA 2017 Report:

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

### FRANET data collection for the FRA 2017 Report:

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

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

### FRA 2015 Report:

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

### FRANET data collection for the FRA 2015 Report:

[Country studies for the project on National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies](#)

### Murray Report

A 2017 study commissioned by the Department of Justice and Equality to review the law on data retention found that it was contrary to EU law, with the report by former Chief Justice John Murray finding that:

“[t]he central finding in *Tele2* is clear: legislation providing for a system of general and indiscriminate communications data retention without exception is precluded by Article 15(1) of Directive 2002/58/EC. By the same token [...] it is also clear that the blanket data retention measures imposed by the Communications (Retention of Data) Act, 2011 are in essence indistinguishable from those impugned in *Tele2*.”<sup>1</sup>

In that report, the former Chief Justice also found numerous other problems apart from the central issue of indiscriminate retention:

“The *principal* frailties of the 2011 Act... include: allowing statutory bodies an effective power of self-certification when making disclosure requests; failure to provide for prior independent authorisation of

---

<sup>1</sup> Murray, John L., [Review of the Law on the Retention of and Access to Communications Data](#), Dublin, Department of Justice, 2017, p. 71.

disclosure requests; failure to adhere to the clear statement principle by permitting undue legislative scatter of the rules governing data retention and disclosure; failure to articulate sufficiently clear objective criteria governing the conditions, circumstances and purposes surrounding data retention and disclosure; failure to provide clear procedures and protocols for the statutory bodies given a right of access to retained data; failure to make provision for the notification of persons affected, either directly or indirectly, by disclosure requests; failure to make appropriate provision for a remedy for wrongful access to retained data; failure to provide for the storage of retained data within the European Union.”<sup>2</sup>

#### *G.D. Judgment*

In Case C-140/20, *G.D. v Commissioner of An Garda Síochána and others*, the CJEU confirmed that provisions of the Communications (Retention of Data) Act 2011 are contrary to EU law insofar as they provide for indiscriminate retention of communications data for criminal justice purposes and for access to that data by police without independent authorisation.

#### Communications (Retention of Data) (Amendment) Act 2022

The Communications (Retention of Data) (Amendment) Act 2022<sup>3</sup> was adopted to amend the law in relation to data retention. While not yet in force, when brought into force it will permit a judge to order indiscriminate retention of communications traffic and location data for state security purposes, and in all cases will require indiscriminate retention of user data (such as usernames and addresses) and internet source data (such as IP addresses) for criminal law purposes. It also provides for temporary preservation (quick freeze) orders in relation to communications traffic and location data for use in criminal law matters. Controls on access to this data depend on the nature of the data sought: judicial authorisation is required only in relation to accessing traffic data, location data and internet source data; no independent authorisation is required for police to access user data. The Act provides for limited notification of users whose data has been accessed but does not reform oversight of state surveillance.

#### Police CCTV and Facial Recognition

The Garda Síochána (Recording Devices) Bill 2022<sup>4</sup> is currently before the Oireachtas (Parliament). The Bill provides for very significantly wider police use of CCTV and body worn cameras, and the Government has stated that it plans to amend the Bill to also permit the use of real time FRT (Facial Recognition Technologies) on police cameras.<sup>5</sup> The Bill also permits any member of the police to demand CCTV footage from any person without any independent authorisation, with failure to comply being a criminal offence.<sup>6</sup>

In September 2022 four UN Special Rapporteurs on human rights wrote to the Irish Government expressing concern that “authorization of the use of FRT by law enforcement could significantly limit the exercise of fundamental freedoms, including the rights of freedom of expression, privacy and freedom of peaceful assembly and of association. Further, such a proposal is out of step with the growing international consensus against the use of FRT [...]”.<sup>7</sup>

---

<sup>2</sup> Murray, John L., [Review of the Law on the Retention of and Access to Communications Data](#), Dublin, Department of Justice, 2017, p. 115.

<sup>3</sup> Ireland, Houses of the Oireachtas, [Communications \(Retention of Data\) \(Amendment\) Act 2022](#). (Act 25 of 2022).

<sup>4</sup> Ireland, Minister for Justice, [Garda Síochána \(Recording Devices\) Bill 2022](#), (Bill 79 of 2022).

<sup>5</sup> Ireland, Minister for Justice (2021), [Answer to Parliamentary Question 1286](#), 14 June 2022.

<sup>6</sup> Ireland, Minister for Justice, [Garda Síochána \(Recording Devices\) Bill 2022](#), (Bill 79 of 2022), Section 40.

<sup>7</sup> Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Special Rapporteur on the rights to freedom of peaceful assembly and of association, Special Rapporteur on the right to privacy, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, [OL IRL 3/2022](#), 30 September 2022.

## 2. Annexes- Table and Figures

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

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

	Civil (internal)	Civil (external)	Civil (internal and external)	Military
<b>IE</b>	(Garda Síochána National Surveillance Unit (NSU) – belonging to the police)  Police/ <i>An Garda Síochána</i> Crime and Security Branch. <sup>8</sup>			Defence Forces/ <i>Óglaigh na hÉireann</i> Directorate of Intelligence (G2)

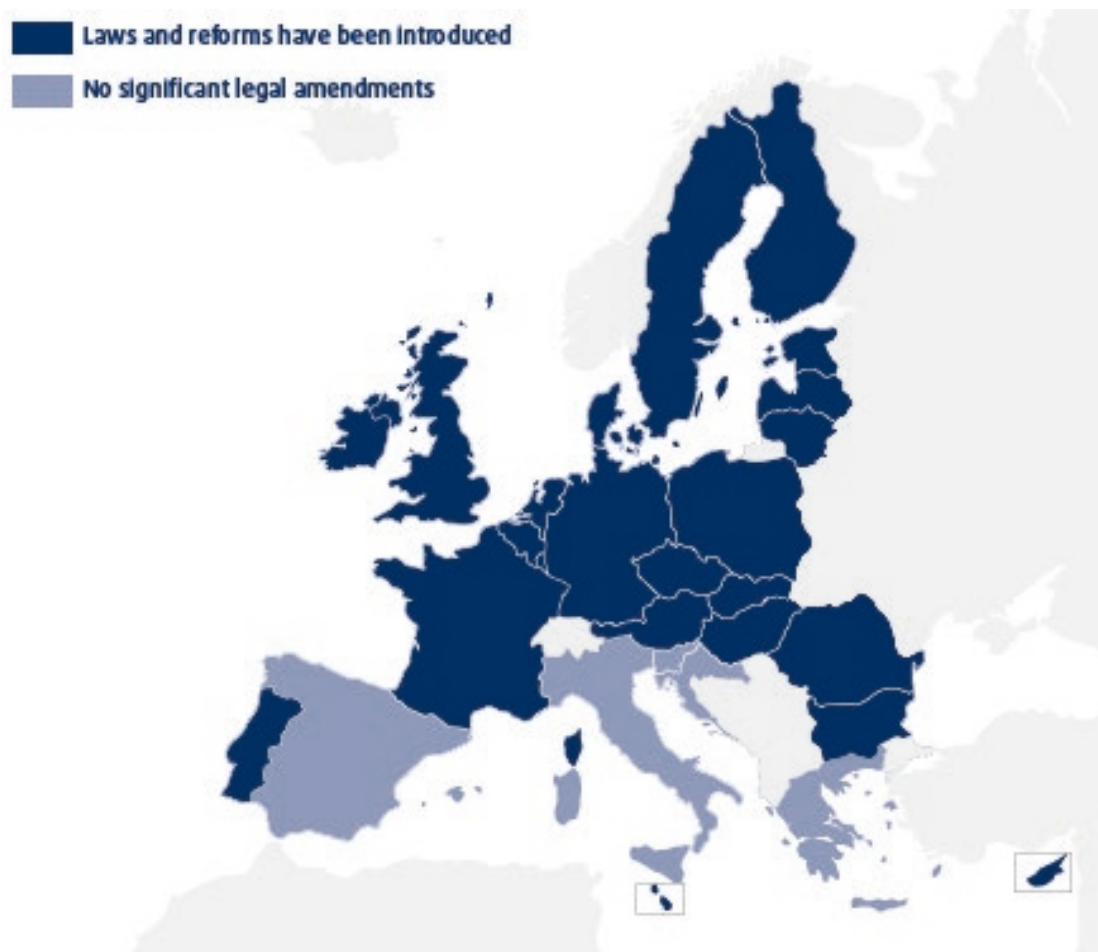
### 2.2. EU Member States' legal framework on surveillance reformed since 2017

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

1. *Whether their legal framework on surveillance has been reformed or is in the process of being reformed since **mid-2017** – see the Index of the FRA 2017 report, pp. 148 - 151. Please do not to describe this new legislation but only provide a full reference.*
2. *whether the reform was initiated in the context of the PEGASUS revelations.*
  1. The legal framework for data retention was sanctioned in July 2022, but it has not been brought into force as of 27 October 2022: Houses of the Oireachtas, Communications (Retention of Data) (Amendment) Act 2022 (Act 25 of 2022).
  2. This was not done in response to the PEGASUS revelations.

<sup>8</sup> The Crime and Security branch has a specific [National Crime and Security Intelligence Service](#) which is in turn divided into two subsections focusing on terrorism and organised crime respectively. For an overview of Ireland's National Security policies, see Mulqueen, M. (2008), 'A Weak Link? Irish National Security Policy on International Terrorism', *Contemporary Security Policy*, Vol. 28, No. 2, pp. 331–332.

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



### **2.3. Intelligence services' accountability scheme**

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

**Figure 5: Intelligence services' accountability scheme**

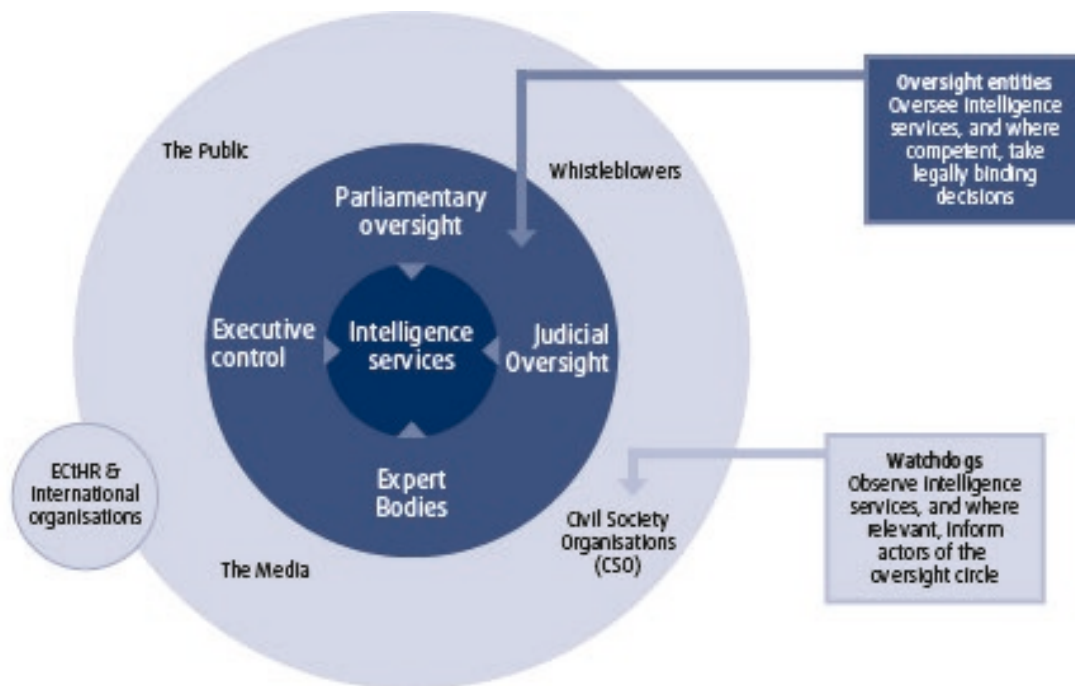


Figure 5 does not illustrate the Irish situation accurately. Specifically, there is no parliamentary oversight of intelligence services in Ireland.

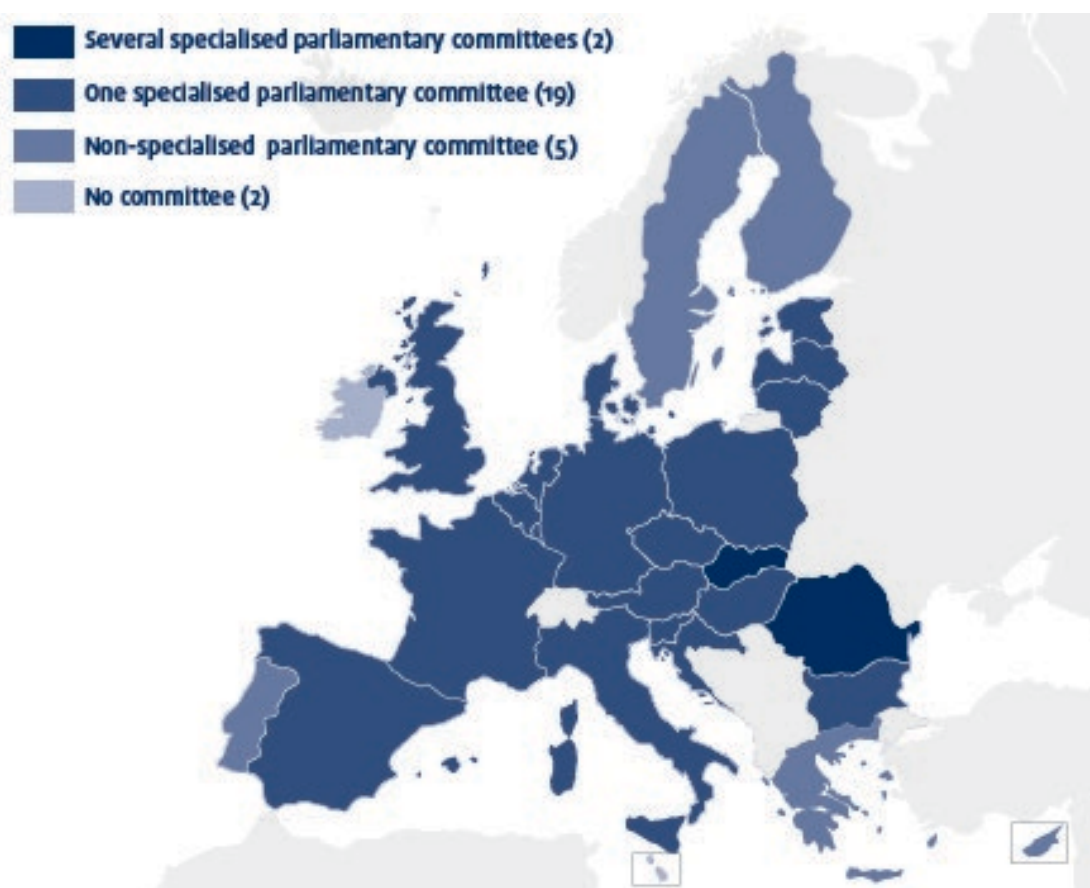
## 2.4. Parliamentary oversight of intelligence services in EU Member States

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

Figure 6 is accurate for Ireland. There is no parliamentary oversight of intelligence services.



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



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

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

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

EU Member State	Expert Bodies
IE	A designated judge of the High Court oversees interception of communications and data retention, while a separate designated judge of the High Court oversees the use of surveillance devices such as audio bugs and location tracking devices. <sup>9</sup>

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

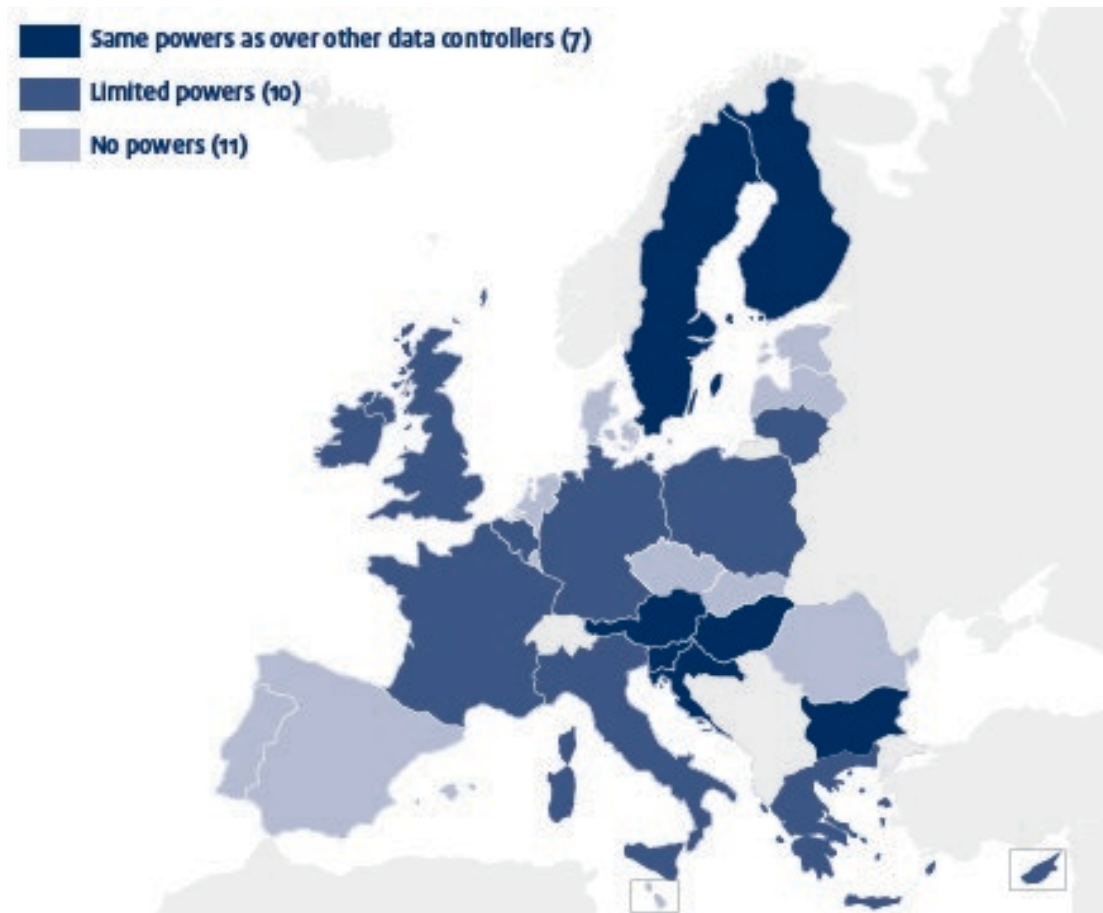
*FRANET contractors are requested to confirm that the map below (Figure 7 (p. 81) of the FRA 2017 report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the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

<sup>9</sup> The oversight roles of the two designated judges in Ireland are established by the [Interception of Postal Packets and Telecommunications Messages \(Regulation\) Act 1993 \(Act 10 of 1993\)](#), the [Criminal Justice \(Surveillance\) Act 2009 \(Act 19 of 2009\)](#), and the [Communications \(Retention of Data\) Act 2011 \(Act 3 of 2011\)](#). This oversight is summarised in McIntyre, T.J. (2016), 'Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective,' in: Scheinin, M., Krunke, H., and Aksenova, M. (eds.), *Judges as Guardians of Constitutionalism and Human Rights*, Cheltenham, Edward Elgar, pp. 136-162.



Figure 7 is accurate for Ireland.

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

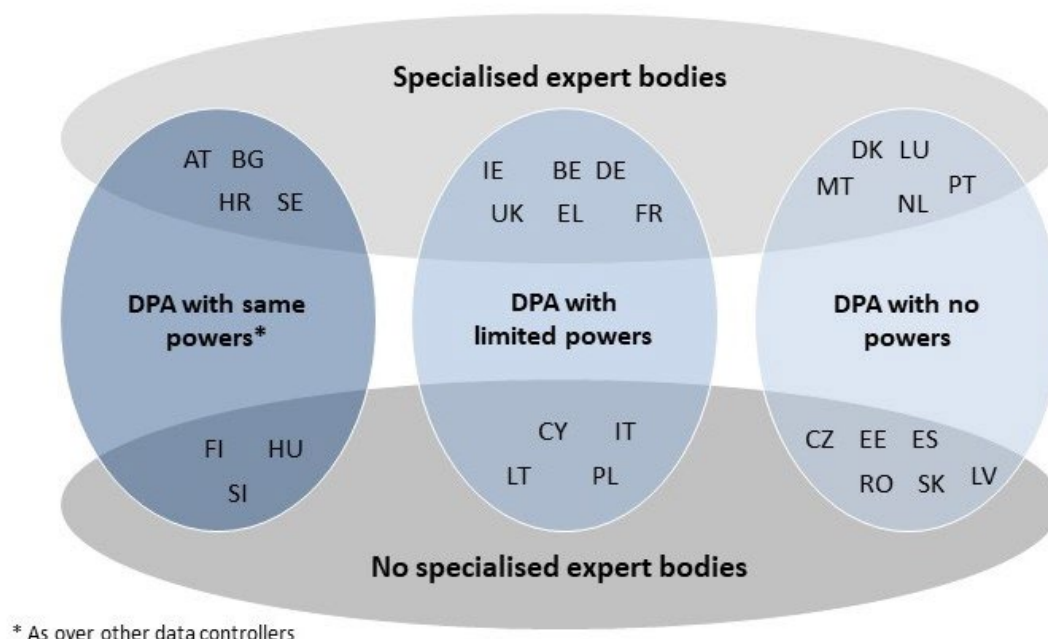


## **2.7. DPAs' and expert bodies' powers over intelligence techniques, by EU Member State**

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

Figure 8 is accurate for Ireland.

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



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

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

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

	Judicial	Executive	Expert bodies	Services
IE	✓	✓		

Table 4 is accurate for Ireland in relation to the specific case of targeted surveillance relating to communications content data.

In relation to surveillance more widely, there are various forms of judicial, executive, and internal approval of targeted surveillance measures, depending on the exact measure being used. For example:

- Judicial authorisation is required in relation to certain types of surveillance devices (such as the planting of audio bugs or covert video cameras) under the Criminal Justice (Surveillance) Act 2009.<sup>10</sup>
- Executive authorisation (a warrant signed by the Minister for Justice) is required in relation to interception of telephone communications under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993.<sup>11</sup>

<sup>10</sup> Ireland, Houses of the Oireachtas, [Criminal Justice \(Surveillance\) Act 2009 \(Act 19 of 2009\)](#).

<sup>11</sup> Ireland, Houses of the Oireachtas, [Interception of Postal Packets and Telecommunications Messages \(Regulation\) Act 1993 \(Act 10 of 1993\)](#).

- Internal police authorisation is sufficient in relation to the use of location tracking devices under the Criminal Justice (Surveillance) Act 2009.<sup>12</sup>

## 2.9. Approval/authorisation of general surveillance of communication

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

Irish law does not provide for general surveillance of the content of communications.

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

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

## 2.10. Non-judicial bodies with remedial powers

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

Table 6 is accurate in relation to Ireland.

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

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

## 2.11. Implementing effective remedies

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

Figure 9 is not entirely accurate in relation to Ireland. In relation to “enabling rights”, Irish law:

- Does not generally provide for notification of individuals that they have been subject to surveillance;<sup>13</sup>
- Does not generally permit Freedom of Information access to data regarding surveillance;<sup>14</sup> and

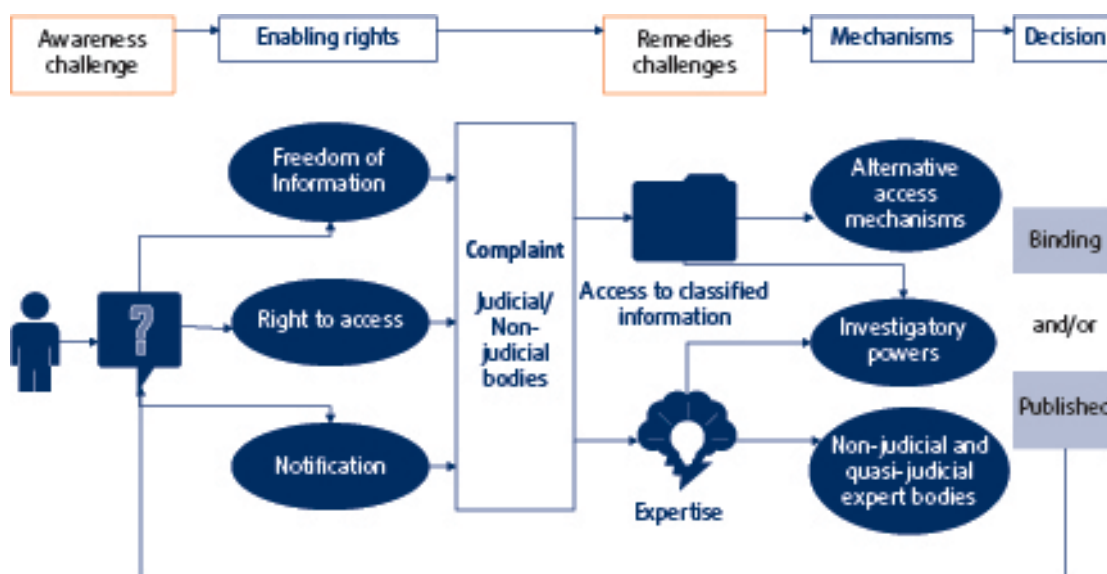
<sup>12</sup> Ireland, Houses of the Oireachtas, [Criminal Justice \(Surveillance\) Act 2009 \(Act 19 of 2009\)](#).

<sup>13</sup> The [Communications \(Retention of Data\) \(Amendment\) Act 2022 \(Act 25 of 2022\)](#) will introduce notification of state access to communications data but has not yet been brought into force.

<sup>14</sup> For example, section 42 of the [Freedom of Information Act 2014](#) excludes any “record held or created by the Garda Síochána that relates to any of the following... the Security and Intelligence Section... the Interception of

- Does not generally permit data subject access requests in relation to personal data regarding surveillance.<sup>15</sup>

**Figure 9: Implementing effective remedies: challenges and solutions**



## 2.12. Non-judicial bodies' remedial powers

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

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

	Bodies with remedial competence	Decisions are binding	May fully access collected data	Control is communicated to complainant	Decision may be reviewed
IE	Complaints Referee				
	Data Protection Commissioner				

Postal Packets and Telecommunications Messages (Regulation) Act 1993... the Criminal Justice (Surveillance) Act 2009 [and] the Communications (Retention of Data) Act 2011" from the scope of that legislation.

<sup>15</sup> Data processing for "the security of the State" is entirely excluded from the scope of the [Data Protection Act 2018](#) and continues to be regulated by the restrictive provisions of the [Data Protection Act 1988](#) and [Data Protection \(Amendment\) Act 2003](#). See section 8(1)(a) of the Data Protection Act 2018. In relation to law enforcement processing, section 94 of the Data Protection Act 2018 provides extensive restrictions on the exercise of the access right.

*Note:*

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

*Source: FRA, 2017*

Table 7 is generally accurate in relation to Ireland, though note that decisions of the Data Protection Commission may be reviewed by appeal to the Circuit Court.

### 2.13. DPAs' remedial competences

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

**Figure 10: DPAs' remedial competences over intelligence services**

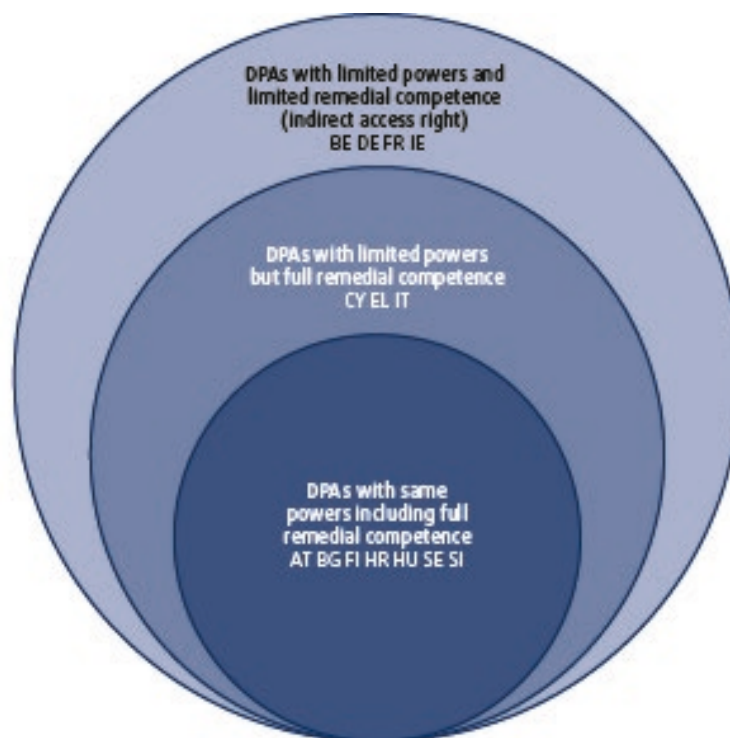


Figure 10 is accurate in relation to Ireland.