6-2023

Opaque Notification: A Country-by-Country Review

Lauren Mantel

AMERICAN UNIVERSITY
WASHINGTON
COLLEGE of LAW

TECH, LAW & SECURITY
PROGRAM

Opaque Notification: A Country-by-Country Review

June 2023

Lauren Mantel

Privacy Across Borders

Tech, Law & Security Program (TLS)

TLS is a rapidly expanding initiative at the American University Washington College of Law that tackles the challenges and opportunities posed by emerging technologies — offering innovative solutions, engaging our students, and training the leaders of tomorrow.

Privacy Across Borders (PAB)

Privacy Across Borders is a TLS project that brings together global experts and practitioners from the government, private sector, and civil society to develop practical, actionable recommendations for challenges to cross-border data flows.

Author

Lauren Mantel, PAB Research Assistant

Editors

Alex Joel, PAB Senior Project Director
Shanzay Pervaiz, PAB Senior Staff Researcher

I. Introduction

On October 7, 2022, in support of the EU-US Data Privacy Framework,[1] President Biden issued Executive Order (EO) 14086,[2] supplemented by a Department of Justice (DOJ) regulation,[3] which, in conjunction, established a novel redress mechanism. At the conclusion of the redress process outlined in that mechanism, the new Data Protection Review Court (DPRC) provides notification to the complainant (through intermediaries) "without confirming or denying that the complainant was subject to United States signals intelligence activities."[4] The European Data Protection Board (EDPB) opinion on the adequacy EU-US Data Privacy Framework issued on February 28, 2023, expressed concern over the "general application" and "non-appealability" of the DPRC's response notifying complainants that "either no covered violations were identified or a determination requiring appropriate remediation was issued."[5] Although the EDPB recognizes the legitimate purpose of the response as articulated in EO 14086 in "protecting sensitive information about U.S. intelligence activities" and that complainants "will be notified if the information pertaining to a review by the DPRC has been declassified," the Board is apprehensive that the EO neglects to include "any exemptions to the standard response of the DPRC."[6]

At Privacy Across Borders, we have been researching how other countries contend with providing notification to individuals about whether they have been the target of surveillance by their country's intelligence agencies. In his paper, *"Without Confirming or Denying": Opaque Notification and National Security Redress*, Alex Joel explores the law and logic behind "opaque" notification under U.S. and EU law.[7] In this paper, we delve into the notification provisions of other countries.

Notably, in the Declaration on Government Access to Personal Data Held by Private Sector Entities, the Organization for Economic Co-Operation and Development (OECD) declared "shared principles as reflecting commonalities drawn from OECD Members' existing laws and practices," one of

---

[1] Press Release, The White House, United States and European Commission Joint Statement on Trans-Atlantic Data Privacy Framework (Mar. 25, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/united-states-and-european-commission-joint-statement-on-trans-atlantic-data-privacy-framework/.

[2] Exec. Order No. 14086, 87 Fed. Reg. 62283, 62290 (Oct. 14, 2022), https://privacyacrossborders.org/wp-content/uploads/2022/10/Executive-Order-14086-on-Enhancing-Safeguards-for-United-States-Signals-Intelligence-Activities.pdf.

[3] 28 C.F.R Part 201 (2022), https://www.ecfr.gov/current/title-28/chapter-I/part-201.

[4] Exec. Order No. 14086, 87 Fed. Reg. at 62290.

[5] Opinion of the European Data Protection Board on European Commission Draft Implementing Decision on the Adequate Protection of Personal Data Under the EU-US Data Privacy Framework, at 5 (2023 [hereinafter EDPB Draft Decision]), https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf.

[6] *See id.* at ¶¶ 239, 241

[7] *See* Alex Joel, *"Without Confirming or Denying": Opaque Notification and National Security Redress*, Privacy Across Borders (Feb. 22, 2023), https://privacyacrossborders.org/wp-content/uploads/2023/02/Opaque-Notification-and-National-Security-Redress.pdf.

such commonalities being redress.[8] The report defines this term as a "legal framework [that] provides individuals with effective judicial and non-judicial redress to identify and remedy violations of the national legal framework," and that "mechanisms take into account the need to preserve confidentiality of national security and law enforcement activities."[9] Similar to the commonalities found in the OECD Declaration, our research indicates that countries indeed limit the ability to inform individuals in order to 'preserve [the] confidentiality of national security and law enforcement activities.'[10]

II. Background

EO 14086 establishes a two-tier independent mechanism for investigating and resolving complaints regarding U.S. signals intelligence activities.[11] The framework provides that the Office of the Director of National Intelligence Civil Liberties Protection Officer (ODNI CLPO) will investigate and determine whether a violation occurred and the appropriate remedy, and the DPRC "independently reviews" the determinations.[12] In the first tier, the ODNI CLPO receives and investigates a "qualifying complaint." The EO defines a qualifying complaint as "a complaint, submitted in writing, that alleges: a covered violation has occurred that pertains to personal information of or about the complainant," which is neither non-frivolous nor made in bad faith, is "brought on behalf of the complainant, not a representative of a governmental, nongovernmental, or intergovernmental organization," and "is transmitted by the appropriate public authority in a qualifying state."[13] Furthermore, a qualifying complaint must include "basic information to enable a review," such as the "basis for alleging that a covered violation has occurred . . . ; the nature of the relief sought; the specific means by which personal information of or about the complainant was believed to have been transmitted to the United States; the identities of the United States Government entities believed to be involved in the alleged violation (if known); and any other measures the complainant pursued to obtain the relief requested and the response received through those other measures."[14]

After the CLPO has completed their investigation and remedial measures have been finalized, the CLPO transmits to the complainant a notice that contains the following statement: "The review either did not identify any covered violations or the Civil Liberties Protection Officer of the Office of the

---

[8] Org. for Econ. Co-Operation and Dev. [OECD], *Declaration on Government Access to Personal Data Held by Private Sector Entities*, at 6, 8, OECD/LEGAL/0487 (Feb. 12, 2023), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.

[9] *Id.* at 8.

[10] *See id.*

[11] *See generally* Joel, *supra* note 7 (discussing the two-tier redress mechanism in greater detail).

[12] *See* 28 C.F.R Part 201 (2022). The steps the ODNI CLPO takes in this process are outlined in Intelligence Community Directive 126, which the PAB team described in Overview of Implementation Procedures for EO 14086.

[13] Exec. Order No. 14086, 87 Fed. Reg. 62283, 62295 (Oct. 14, 2022).

[14] *Id.* As identified by the EDPB: "Under this new mechanism, the standing requirement is not applicable: according to Section 4(k)(ii) of EO 14086, the claimant does not need to show that their data has in fact been subject to U.S. signals intelligence." EDPB Draft Decision, *supra* note, 5 at ¶ 215.

Director of National Intelligence issued a determination requiring appropriate remediation."[15] After receipt of this notice, the complainant may "apply for review of the CLPO's determinations by the Data Protection Review Court."[16] Under the DOJ regulation, upon receipt of an application for review, the DPRC will convene a panel, appoint a special advocate,[17] and conduct its review to determine "whether a covered violation occurred and, if so, to determine any appropriate remediation."[18] The panel will issue a "final and binding" written decision,[19] and the Department of Justice will transmit a notification that the DPRC completed its review and "the review either did not identify any covered violations or the [DPRC] issued a determination requiring appropriate remediation."[20]

In the last several years, the Court of Justice of the European Union (CJEU) has issued several judgments addressing notification, emphasizing the importance of a country's ability to safeguard national security.[21] The CJEU established that in the national security context, providing notification of surveillance to a claimant is necessary "only to the extent that and as soon as it is no longer liable to jeopardise the tasks for which those authorities are responsible."[22] Equivalently, the European Court of Human Rights (ECtHR) held that notification is required except when doing so would jeopardize national security: "as soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should . . . be provided to the persons concerned."[23] Moreover, the ECtHR ruled that it is permissible for notification to be "delayed, restricted or omitted to the extent necessary, and as long as it proves necessary and proportionate . . . to protect public and national security."[24]

Notably, in *Kennedy v. The United Kingdom*, the ECtHR held that notification is not required when the targeted individual is provided with an effective remedy. In this instance, the complainant could "lodge an application" with the United Kingdom Investigatory Powers Tribunal (IPT) without an

---

[15] *See* Off. of the Dir. of Nat'l Intel., Intelligence Community Directive No. 126: Implementation Procedures for the Signals Intelligence Redress Mechanism Under Executive Order 14086 at 6 (2022), https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf.

[16] *Id.*

[17] *See* 28 C.F.R. § 201.8.

[18] *Id.* § 201.9.

[19] *Id.* § 201.9(g)).

[20] *Id.* § 201.9(h)(2).

[21] *See* Case C-140/20, Commissioner of An Garda Síochána and others, ECLI:EU:C:2022:258, ¶¶ 48, 57, 61 (Apr. 5, 2022); *see also* Joel, *supra* note 7 (discussing this topic further).

[22] *See* Joined Cases C-511, 512 and 520/18, La Quadrature du Net and others, ECLI:EU:C:2020:791, ¶ 191 (Oct. 6, 2020).

[23] *See* Weber and Saravia v. Germany, App. No. 54934/00, ¶ 135 (June 29, 2006), https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-76586%22%5D%7D.

[24] *See* Ringler v. Austria, App. No. 2309/10, ¶ 34 (May 12, 2020), https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-203068%22%5D%7D.

evidentiary burden,[25] and the jurisdiction of the Tribunal did not require the complainant to be notified of an interception of their communications.[26] Like the proposed U.S. redress mechanism, the IPT is an independent body with access to relevant information and materials and maintains the power to remedy non-compliance.[27] Similarly, in *Centrum för rättvisa v. Sweden*, the ECtHR found that notification may not be required when the complainant has an adequate remedy.[28] Furthermore, the Court noted that "in the absence of a notification requirement . . . [a] remedy should be before a body which . . . is independent of the executive and ensures the fairness of the proceedings, offering, insofar as possible, an adversarial process."[29]

In *Klass and Others v. Germany*, the ECtHR reasoned that "notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance."[30] Moreover, the Court found that explicit notification might "reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents." Consequently, the Court determined that it is not incompatible with Article 8 for States to continue withholding notifying an individual about surveillance even after the surveillance has ceased, as "it is this very fact which ensures the efficacy of the 'interference.'"[31]

III. Adequacy Decisions

In exploring how other countries provide for notification in the national security context, we turn first to the European Commission's adequacy decisions for the United Kingdom and the Republic of Korea. The European Commission issued these decisions after *Schrems II*, and thus took care to assess national security redress as part of its review of the applicable legal frameworks.

a. United Kingdom

In 2021, the European Commission adopted adequacy decisions for the United Kingdom (U.K.) and concluded that the U.K. system had adequate safeguards largely because of its independent judicial body. In the U.K., intelligence services are not obligated "to notify individuals that they have been

---

[25] *See* Kennedy v. United Kingdom, App. No. 26839/05, ¶ 190 (May 18, 2010), https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-98473&filename=001-98473.pdf.
[26] *See id.* at ¶ 167.
[27] *See id.*
[28] *See* Centrum För Rättvisa v. Sweden, App. No. 35252/08, (May 25, 2021), https://hudoc.echr.coe.int/fre#%7B%22documentcollectionid2%22:[%22GRANDCHAMBER%22],%22itemid%22:[%22001-210078%22]%7D.
[29] *Id.* at ¶ 273.
[30] *See* Klass and Others v. Germany, App. No. 5029/71, ¶ 58 (Sept. 6, 1978), https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]}.
[31] *See id.*

subjected to surveillance."[32] The relevant governing bodies are the Data Protection Review Board (DPRB), Information Commissioner's Office (ICO), and Investigatory Powers Tribunal (IPT).[33] The IPT is composed of eight members with investigative powers and the ability to make remedial orders and grant compensation.[34] Both the ICO and IPT were regarded as independent bodies with the power to issue binding decisions and pursue corrective measures.[35] The Tribunal's function is not to notify complainants of whether they have been subject to surveillance,[36] and in the case of a "no determination" notice, the Tribunal is not "to disclose whether or not the complainant is, or have been, of interest to the security, intelligence or law enforcement agencies. Nor is the Tribunal permitted to disclose what evidence it has taken into account in considering the complaint."[37] Furthermore, the Commission found that the redress entitlements in the U.K., including the right to access the ICO and IPT for redress, provided an effective judicial remedy that was essentially equivalent to those granted in the EU.[38]

b. Republic of Korea

Shortly after the UK adequacy decision, the European Commission adopted an adequacy decision on the Republic of Korea. In Korea, the Personal Information Protection Act (PIPA) governs the processing of personal data.[39] The Personal Information Protection Commission (PIPC), an administrative nine-member body with investigative and enforcement functions, enforces and monitors compliance

---

[32] *See* Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update United Kingdom, at 14 (2016) [hereinafter FRA UK Update], https://fra.europa.eu/sites/default/files/fra_uploads/united-kingdom-study-data-surveillance-ii-uk.pdf.

[33] Additionally, the Investigatory Powers Act (IPA) "provides the legal framework for the use of investigatory powers." *See* Commission Implementing Regulation (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, 2021 O.J. L360, ¶ 177 [hereinafter UK Adequacy Decision], https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D1772&from=EN.

[34] *See id.* at ¶ 266.

[35] *See id.* at ¶ 271.

[36] *See Frequently Asked Questions*, The Investigatory Powers Tribunal (July 5, 2016), https://www.ipt-uk.com/content.asp?id=24.

[37] *See Investigatory Power Tribunal Report,* The Investigatory Powers Tribunal (2010), https://ipt-uk.com/docs/IPTAnnualReportFINAL.PDFl*; see also* UK Adequacy Decision, *supra* note 33, at ¶ 266 n. 494 ("According to the information provided by UK authorities, the low threshold for making a complaint determines that it is not unusual for the Tribunal's investigation to determine that the complainant was in fact never subject to investigation by a public authority. The latest Statistical Report of the Investigatory Powers Tribunal specifies that in 2016 the Tribunal received 209 complaints, 52% of those were considered frivolous or vexatious and 25% received a "no determination" outcome. UK authorities explained that this either means that no covert activity/powers were used in relation to the complainant, or that covert techniques were used and the Tribunal determined that the activity was lawful. . . 7% were found in favour of the complainant.").

[38] *See* UK Adequacy Decision, *supra* note 33, at ¶ 271.

[39] *See Questions & Answers on the Adoption of the Adequacy Decision Ensuring Safe Data Flows Between the EU and the Republic of Korea*, European Commission (Dec. 17, 2021), https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_6916.

with PIPA.[40] Regarding notification, including national security cases, if at least one party is a Korean national, "notification must be provided in writing within 30 days from the date on which the collection ended . . . and may only be deferred if and as long as it would put national security at risk or would harm people's life and physical safety."[41] In Korea, there are several means to access administrative and judicial redress, including the right to complain 1) directly to a controller; 2) to the PIPC; 3) by submitting a mediation claim; and 4) by filing a criminal complaint.[42] When evaluating the redress mechanisms in the Korean system, the Commission determined that the protections granted were essentially equivalent to what EU law requires.

IV. Member States

In two volumes—one published in 2015 and the other in 2017—the EU's Fundamental Rights Agency (FRA) produced an extensive report on the laws governing surveillance by intelligence services in EU Member States.[43] In 2023, the FRA published an update noting that the circumstances remain similar to those covered in the earlier report.[44] As stated in the FRA report in 2017 (Volume II), all European Union Member States have a national security exception that limits an individual's right to be notified by the government whether they have been under surveillance for the "protection of national security or of on-going surveillance operation."[45] Also, in Volume II, the FRA's research concluded that in the surveillance context, there were only a few individuals who sought a remedy. In 2023, the FRA found that in the last several years, an average of ten to twenty individuals sought a remedy against illegal surveillance activities.[46]

---

[40] *See* Commission Implementing Decision (EU) 2022/254 of 17 December 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act, 2022 O.J. L 44, ¶¶ 113, 116, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022D0254&qid=1676846306538&from=EN.

[41] *Id.* at ¶ 192.

[42] *Id.* at ¶¶ 131-37.

[43] *See* Report of the European Union Agency for Fundamental Rights on Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU—Volume II: Field Perspectives and Legal Update (2017) [hereinafter FRA Report Volume II], https://fra.europa.eu/en/publication/2017/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies-eu, Report of the European Union Agency for Fundamental Rights on Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU— Volume I: Member States' Legal Frameworks, at 63 (2015) [hereinafter FRA Report Volume I], https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services-voi-1_en.pdf.

[44] *See* Report of the European Union Agency for Fundamental Rights on Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU—Update 2023 (2023) [hereinafter FRA Report Update], https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/PEGA/DV/2023/02-28/FRASubmissiontothePEGACommittee_EN.pdf (providing a partial update to the 2015 and 2017 reports "on the work of intelligence services . . . present[ing] developments," such as that "six DPAs … lost their remedial powers in this area").

[45] *See* FRA Report Volume II, *supra* note 43, at 14.

[46] *See* FRA Report Update, *supra* note 44, at 43. In a majority of 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

We present below the text relevant to the notification issue extracted from each FRA country report and the updated FRA Report. In some cases, we conducted additional research, reflected in footnotes. As indicated, all EU member states surveyed allow the government to restrict notification and other access to data to protect national security.

Austria: "The general obligation of authorities to provide information is provided in Art. 20 (4) of the Federal Constitutional Act. This provision foresees an obligation of authorities to provide information. Restrictions to provide information are only possible in case an "official secret" (Amtsgeheimnis) speaks against providing such information. Moreover, the Duty of Disclosure Act 1987 (Auskunftspflichtgesetz 1987) forsees the obligation of authorities to provide information, as long as the duty to secrecy (Verschwiegenheitspflicht) according to Art. 20 (3) of the Federal Constitutional Act is not opposed to it."[47]

Belgium: "In accordance with Principle 10E(1) of the Global Principles on National Security and the Right to Information, an individual can, under a different legal basis, obtain information on the surveillance measure(s) to which he/she has been subjected. Nevertheless, the practice shows that there are very few cases where an individual requests access to documents concerning him/her held by the intelligence services. Furthermore, these requests are most, if not all, rejected on the basis of article 6 of the Act of 11 April 1994 or on the basis of the Law of 11 December 1998 on classification and security clearances . . ."[48]

"In 2021, the Belgian Standing Committee I received 72 complaints (compared to 62 in 2020). In 2020, most of them were dismissed (55 out of 62). By contrast, in 2021, 23 were rejected as manifestly ill-founded and 28 because the Standing Committee I was not competent. 14 of the remaining 24 were handled within 2021."[49]

Bulgaria: "The National Special Intelligence Devices Control Bureau . . . is obliged to notify persons about any unlawful use of surveillance on them. Persons are not notified when such notification would: (a) endanger the achievement of the objectives of surveillance; (b) reveal the used means and techniques;

---

related to activities of intelligence services. In this regard, the situation remains unchanged since 2017." *Id.* The three Member States that only offer judicial remedies are Czachia, Latvia, and Poland. *Id.* at 47.

[47] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Austria, at 8 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/austria-study-data-surveillance-ii-legal-update-at.pdf.

[48] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Belgium, at 14 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/belgium-study-data-surveillance-ii-be.pdf. Additionally, note that due to national data protection reforms, in Belgium, Bulgaria, Croatia, Greece, and Lithuania, "DPAs no longer have competency to control matters linked to national security. They have consequently lost their power to investigate complaints lodged by individuals in the context of intelligence services' activities." FRA Report Update, *supra* note 44, at 48.

[49] FRA Report Update, *supra* note 44, at 52.

or (c) create a risk for the life and health of the undercover officer or their close ones (Principle 10E(4) of the Tshwane Principles)."[50]

Croatia: "Article 40 of ZSOS states that the security-intelligence agencies are obliged, upon a citizen's request, to inform the citizen by written notice, and within 15 days, if he/she was the subject of secret data collection measures (including surveillance). However, paragraph 3 of the same article stipulates exemptions to this rule. The agencies are not obliged to inform the citizens about the measures of secret data collection if: 1. this information could endanger the execution of the tasks of the agencies, 2. the information could lead to endangering the safety of another person or 3. the information could have adverse consequences for the national security or national interests of the Republic of Croatia."[51]

"In Croatia, the Civilian Oversight Council of Security Intelligence Agencies, re-established in 2018 after several years of inactivity, may now access data collected by intelligence services, and may inform complainants once it performs an investigation based on their complaints."[52]

Cyprus: "Under the national data protection legislation, all persons have the right to be informed if their personal data are or have been the subject of processing. However, the duty of the controller to so inform the data subjects may be lifted with a decision of the Commissioner for the Protection of Personal Data, following a request by the controller, where the processing was carried out for reasons of national needs or national security or for the prevention, investigation and prosecution of criminal offences or for other reasons of important economic of financial interests of a member state of the EU."[53]

---

[50] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Bulgaria, at 9 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/bulgaria-study-data-surveillance-ii-legal-update-bg.pdf.

[51] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Croatia (2016), https://fra.europa.eu/sites/default/files/fra_uploads/croatia-study-data-surveillance-ii-legal-update-hr.pdf.

[52] FRA Report Update, *supra* note 44, at 51. Note that the FRA Report Update makes this statement without a citation to legal authority in Croatia. The FRA commissioned a country report about Croatia in 2022 which notes that Croatia now prohibits the data protection authority from having oversight over intelligence activities. The report refers to the role of the Civilian Oversight Council but makes no mention of notification to complainants. Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—November 2022 Update Croatia (2022), http://fra.europa.eu/sites/default/files/fra_uploads/hr-surveillance-report-update-2022_en.pdf. Moreover, Article 84 of the law establishing the Oversight Council states: "The President and members of the Council are obliged to keep as a secret all information they learn in the performance of the Council's work." Law: About the Security Services of the Republic of Croatia, no. 01-081-02-1319/2, Narodne Novine (2002), https://narodne--novine-nn-hr.translate.goog/
clanci/sluzbeni/2002_03_32_693.html?_x_tr_sl=hr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=wapp.

[53] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Cyprus, at 10 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/cyprus-study-data-surveillance-ii-cy.pdf.

"The law on the confidentiality of private communications, which regulates interference with private communications by law enforcement agencies, requires the Attorney General to inform persons involved in private communications subjected to interception or surveillance, of the issue of the court order and of whether surveillance actually took place or not, within a reasonable time and no later than 90 days from the issue of the court order sanctioning surveillance . . . Such notification to the applicant may however be delayed following an ex parte application by the Attorney General if this is in the interests of: public security, constitutional order, public order, the security of the Republic, public health, public morals, protection of rights and freedoms, the dignity of others, preventing the discovery of information collected confidentially or in the pubic interests or for the need to protect investigations."[54]

Czech Republic: "[I]ndividuals do not have [the] right" to access information on whether they are subject to surveillance. "The Act on the Security Information Service and the Act on the Intelligence Services both stipulate that the information that a person is subject to surveillance by these services and the content of the surveillance are not provided to the person."[55]

Denmark: "In Denmark, there is a general rule to inform the individual at the end of the surveillance measures. If notification would jeopardise the investigation or there are other arguments against it, the judiciary may permit withholding – or delaying the provision of – the information. In addition to this basic rule, specific rules foresee that in extraordinary cases, an individual may receive the information in part or in full—even while the surveillance is being carried out—directly from the surveillance authority or by filing a claim to the Oversight Board (TET)."[56]

Estonia: The Public Information Act (Avaliku teabe seadus, PIA) is not applicable to "information which is classified as a state secret or as classified foreign information, until the expiry of classification of such information" (Article 2 para 2 point 1 of the PIA). The same is stressed in the State Secrets and Classified Information of Foreign States Act (Riigisaladuse ja salastatud välisteabe seadus) which generally treats

---

[54] *Id.*

[55] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Czech Republic, at 6 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/czech-republic-study-data-surveillance-ii-legal-update-cz.pdf.

[56] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Denmark, at 15 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/denmark-study-data-surveillance-ii-legal-update-dk.pdf. That said, according to the TET's annual report, the individual may not be provided with information that would allow them to infer whether they have been the subject of surveillance: "According to the explanatory notes to the DDIS Bill concerning this provision, however, it must only be possible to infer from TET's reply that no information is being processed about the data subject in violation of DDIS legislation. Accordingly, it must not be stated in or possible to infer from the reply whether any information is being or has been processed at all, whether any information has been processed in violation of DDIS legislation or whether information is being processed in compliance with DDIS legislation." Danish Defence Intelligence Service (DDIS), Annual Report 2021, s. 38 (2022), https://www.tet.dk/wp-content/uploads/2022/06/FE_UK_2021_web.pdf. Only a few individuals, however, have filed complaints requesting the "TET to investigate whether an intelligence service has illegally processed information about them." *See* FRA Report Update, *supra* note 44, at 51.

as a state secret both national (Article 7 and 8 of the SSCIFSA) and international (Article 6 and 7 of the SSCIFSA) surveillance that is not directly connected to the specific criminal cases. Exempted is only the information 'the disclosure of which would not damage the security of the Republic of Estonia.'"[57]

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

A new oversight body in Finland, "the Finnish Intelligence Ombudsman (tiedusteluvalvontavaltuutettu/ underrättelsetillsynsombudsmannen), set up in 2019, [] oversees both the civilian intelligence and military intelligence authorities. This is an independent body with investigative powers and an extensive right to access information. It can order the suspension or cessation of surveillance if it considers that the intelligence authority has acted unlawfully. It 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 by individuals and acts upon them."[59] The Intelligence Ombudsman has yet to receive any complaints.[60] However, "[w]hen an investigation has been carried out, the Intelligence Ombudsman may inform individuals, but only stating that an investigation has been carried out."[61]

France: "Under the Internal security code, any person wishing to check that no intelligence technique is unlawfully implemented on them may refer to the CNCTR. The CNCTR verifies the technique or techniques involved in order to check that they have been or are being implemented in compliance with the Code of internal security. It notifies the applicant that it has carried out the necessary checks, without confirming nor denying their implementation. Any person wishing to check that no intelligence technique is unlawfully implemented on them and able to prove they have referred to the CNCTR under article L 833-4, may refer to the Council of State. When the Council of State notes the absence of any illegality in the implementation of an intelligence collection technique, the decision indicates to the

[57] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Estonia, at 8–9 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/estonia-study-data-surveillance-ii-ee.pdf.

[58] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Finland, at 10 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/finland-study-data-surveillance-ii-legal-update-fi.pdf.

[59] FRA Report Update, *supra* note 44, at 30.

[60] *Id.* at 51.

[61] *Id.*

applicant or to the referring jurisdiction that no illegality was present, without confirming or denying the implementation of a technique."[62]

Germany: "Citizens have no right at all to request information from the three federal intelligence services and "authorities and other bodies of the federal state" that are listed, according to the Security Check Act (Sicherheitsüberprüfungsgesetz), by ordinance of the federal government to be handling information which is classified as 'secret' or 'top secret' . . .[T]his general exemption from the right to freedom of access to documents does also cover documents originating from the intelligence services which are held by authorities of executive supervision."[63]

"The BfV has to dismiss a subject access request that is justified under [Section 15 of the BVerfSchG] if the disclosure of information a) would threaten the implementation of its tasks, b) could put sources at risk or if there are reasons to fear that the request aims to investigate the state of knowledge or operational methods of the BfV, c) could threaten public security or would have detrimental effects on the well-being of the federation or a German state, or d) would conflict with the secret legal status or the secret nature of the information or the fact that it is being held, in particular if legitimate interests of third parties prevail. Exempt from the disclosure of information are details about originators or parties who received the information."[64]

---

[62] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update France (2016), https://fra.europa.eu/sites/default/files/fra_uploads/france-study-data-surveillance-ii-fr.pdf. The CNCTR received 33 complaints in 2020 and 48 complaints in 2021, and each complaint was "handled within two months." *See* FRA Report Update, *supra* note 44, at 52. Furthermore, similar to the redress mechanism outlined in EO 14086, without confirmation from the CNCTR that "intelligence collection was targeting them," individuals can refer their complaint to the Specialised Formation of the Conseil d'Etat to verify that no illegal intelligence technique has been employed against them. *See id;* Florent Le Divelec, Intelligence Law in France, *in* Intelligence Law and Policies in Europe: A Handbook 545 (Jan-Hendrik Dietrich & Satish Sule eds., 2020). In both 2020 and 2021, the Conseil d'Etat received 8 applications. FRA Report Update, *supra* note 44, at 52.

[63] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Germany, at 13 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/germany-study-data-surveillance-ii-legal-update-de.pdf. Moreover, German notification requirements only extend to telecommunications involving German persons or persons within Germany and do not include affected foreigners in other States. *See* BVerfG, 1 BvR 2835/17, ¶ 269, May 19, 2020, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/05/rs20200519_1bvr283517en.html (judgment of the German Federal Constitutional court on the constitutionality of the German Federal Intelligence Service's powers to conduct surveillance of foreign telecommunications).

[64] *Id.* at 14. In 2020, the "German G 10 commission received four complaints . . . three of which were ill-founded." FRA Report Update, *supra* note 44, at 52.

Greece: "Under Article 5A: '1. All persons have the right to information, as specified by law. Restrictions to this right may be imposed by law only insofar as they are absolutely necessary and justified for reasons of national security, of combating crime or of protecting rights and interests of third parties.'"[65]

The Updated report notes that Greece has "amended its legal framework several times since 2017. The changes involved various issues, such as the organization of intelligence services, the authorisation of surveillance or the abolishment and the following re-introduction of notification of surveillance."[66] However, the new law maintains the exemption for national security if notification would compromise the purpose of the measure: "After the expiration of three (3) years from the termination of the validity of the provision for the removal of confidentiality for reasons of national security, the imposition of the restrictive measure on the affected person is notified, provided that the purpose for which it was ordered is not compromised."[67]

Hungary: "[T]he National Security Services Act stipulates that in the interest of national security or to protect the rights of others, the general director of the national security services may deny the request to disclose information about the surveillance operation. Therefore, the right to information self-determination granted by the Informational Self-determination and the Freedom of Information Act are restricted in cases of secret surveillance on the basis of external and internal security of the state. It results that the person subject to surveillance gets no information about the surveillance operation at all, and the general director of the national security services may deny the disclosure of the information by referring to the excuse of national security interest or the protection of others' rights without further conditions."[68]

Ireland: "No," individuals do not have the right to access information on whether they are subject to surveillance. "The exemptions discussed above in relation to freedom of information requests apply equally to requests by individuals for information about themselves, including requests asking whether they have been subject to surveillance."[69]

---

[65] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Greece, at 5 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/greece-study-data-surveillance-ii-legal-update-el.pdf.

[66] FRA Report Update, *supra* note 44, at 9.

[67] Greece, Law No. 5002/2022, Government Gazette Issue A' 228/09.1.2022, "Waiving privacy procedure, cyber security and protection of citizens' personal data." ("Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών"), Art. 4(7), http://www.opengov.gr/ministryofjustice/?p=16473.

[68] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Hungry, at 9 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/hungary-study-data-surveillance-ii-hu.pdf.

[69] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Ireland, at 11 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/ireland-study-data-surveillance-ii-legal-update-ie.pdf.

Italy: "Italian legislation does not provide any legislative tool enabling direct access to the information gathered by intelligence services. In fact, Italian legislation does not envisage specific legislation concerning the right to have access to information possessed by intelligence service."[70]

Latvia: "Subsequently, all the information on operational measures and information obtained during an official operation which is classified as a state secret falls outside of the scope of the application of the Freedom of Information Law of 1998, as the latter sets out the legal framework on the access to information which is 'publicly available' or 'restricted' only (Article 3 of the Freedom of Information Law). If information or measures undertaken during investigatory operations are classified as a state secret, the person has no right to be informed about or to verify the information. However, if the person under surveillance believes that his or her lawful interests and freedoms have been violated, he/she has the right to either submit a complaint to the prosecutor, who after a review issues a compliance statement, or submit a claim in court."[71]

Lithuania: "General statistics about the use of surveillance measures against individuals are made public in the annual report of the State Security Department (Valstybės saugumo departamentas) . . . However, in practice these individuals are neither informed, nor have access to the data collected on them. The Law on Intelligence of the Republic of Lithuania (Lietuvos Respublikos žvalgybos įstatymas) does not contain any specific provisions governing the right of persons concerned to access gathered intelligence data, even if the rights of persons have been violated in the course of the surveillance and the information gathered does not indicate that a crime has been committed."[72]

"[I]n Lithuania, a new expert body – the Intelligence Ombudsman (Žvalgybos kontrolierius, LRT)—was set up with a 2021 law that came into effect on 1 January 2022. This body was established after the national DPA was excluded from exercising any control over data processing by national institutions for the purposes of national security and defence. It is composed of two Ombudspersons who are appointed by the Parliament for a five-year term. This body has its own staff and budget and is headed by one of the two Ombudspersons. It is independent and accountable to Parliament only, to which it submits an annual report. It carries out supervision of intelligence services and their compliance with human rights standards and data protection. It also carries out legality assessments of the intelligence services activities and methods. It can investigate intelligence services' activities and personal data

[70] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Italy, at 7 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/italy-study-data-surveillance-ii-legal-update-it.pdf.
[71] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Latvia, at 6 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/latvia-study-data-surveillance-ii-legal-update-lv.pdf.
[72] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Lithuania, at 5–6 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/lithuania-study-data-surveillance-ii-legal-update-lt.pdf.

processing and may access their collected data. It can initiate investigations on its own initiative, or based on complaints received from individuals, parliamentarians, and other public institutions."[73]

Luxembourg: "Individuals that have been, or believe to have been, subject to surveillance, have access to information in accordance with Article 28 of the Act of 2 August 2002 on the protection of persons with regard to the processing of personal data . . ., which applies also to cases of surveillance. According to this article, any person may request (a) access to data related to him/her; (b) confirmation as to whether or not data relating to him/her are processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed. However, as allowed by Article 29 of the same Act, the right of access to data may be restricted or deferred if necessary in order to safeguard the interests of (a) national security; (b) defense; (c) public safety."[74]

Malta: "[A] document is an exempt document under the Freedom of Information Act if its disclosure would, or could reasonably be expected to, cause damage to the security, the defence, or the international relations of Malta."[75] Additionally, "[t]he Security Services Act does not grant the right of access to information to individuals on whether or not they are subject to surveillance activities."[76]

Netherlands: "Individuals have a right to access information on whether they are subject to surveillance. . . There are some grounds for refusal and limitations: a request will be refused if data concerning the applicant have been processed in the context of an investigation, unless: the data were processed more than five years ago; since that time no new data concerning him or her have been processed in this context; the data in question are not relevant for any current investigation. The request will also be refused if no data concerning the applicant have been processed. If a request is thus rejected, the justification will only be provided in general terms."[77] In addition, for surveillance activities, the government "shall investigate, five years after the exercise of these powers, and every year after that, whether a report may be issued to the person involved…. Issuing a report is not necessary if this is not reasonably possible. The report will be postponed if personal data are involved in an investigation in connection with which a person would not get any information either at their request. The duty to investigate the possibility to issue a report will not be applied if issuing a report about the exercise of powers is reasonably expected to reveal sources of a service, among which intelligence and security

---

[73] FRA Report Update, *supra* note 44, at 30–31.

[74] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Luxembourg, at 7 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/luxembourg-study-data-surveillance-ii-lu.pdf.

[75] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Malta, at 6 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/malta-study-data-surveillance-ii-legal-update-mt.pdf.

[76] *Id.*

[77] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Netherlands, at 12–13 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/the-netherlands-study-data-surveillance-ii-nl.pdf.

services of other countries, seriously damage relations with other countries and with international organisations or reveal a specific application of a method of a service or the identity of the one who has been helpful to the service."[78] "The Dutch CTIVD handled 23 complaints in 2021."[79]

Poland: "The Act on Police states that a person subject to surveillance shall not have access to information gather during the operational control. Such provision was not included in the Act on the Internal Security Agency and Intelligence Agency, but it is interpreted in a similar way. It does not create an obligation of notification of such surveillance."[80]

Portugal: "Article 34 (4) in the Portuguese Constitution states that the public authorities are prohibited from interfering in any way with correspondence, telecommunications or other means of communication, save in such cases as the law may provide for, in relation to criminal proceedings. Now, owing to the fact that the SIED and the SIS are forbidden to exercise powers, practice deeds or develop activities within the specific spheres or powers of the courts, the Public Prosecutor or the police authorities, nor are they (the SIED and the SIS) allowed to launch criminal investigations and proceedings—likewise within the framework of their allotted powers—they may not place people under surveillance without threatening or infringing upon their rights, freedoms and guarantees as laid down in the Constitution and the law (Law 50/2014, Article 6 (1) and (2)). Therefore, pursuant to the Portuguese Republic's lawful intelligence system, the question of individuals having the right to access information about whether they are subject to surveillance does not come up."[81]

Romania: "In accordance with Article 13(1) of Law no. 677/2001 on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of such Data, as amended and supplemented . . ., any concerned individual is entitled to obtain from an operator, upon request and free of charge for one request per year, confirmation that data concerning him or her has or has not been processed by that operator. . . Article 2(7) provides for a broad exception, stating that this law does not apply to the processing and transfer of personal data performed in the areas of national defence and security and within the limits and restrictions established by law."[82]

Slovak Republic: "As stated already in the former section, the Act no. 46/199350 and the Act no. 198/199451 specify in both cases under article 17, section 9, that the information held by the Slovak

---

[78] *Id.* at 13.

[79] FRA Report Update, *supra* note 44, at 52.

[80] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Poland, at 8 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/poland-study-data-surveillance-ii-legal-update-pl.pdf.

[81] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Portugal, at 11 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/portugal-study-data-surveillance-ii-pt.pdf.

[82] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Romania, at 9–10 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/romania-study-data-surveillance-ii-ro.pdf.

Information Service are exempt from the entitlements governed by the Act no. 211/2000 on free access to information and the Act no. 428/2002 on personal data protection. Thus the individuals cannot approach these bodies with request to access the classified information."[83] More specifically, in the Slovak Republic, "[i]ntelligence services are not required to inform individuals that they are being subjected to surveillance before, during or after the surveillance operation. Similarly, individuals do not have the right to access data and information that are being gathered on them by intelligence services."[84]

Slovenia: "Slovene Intelligence and Security Agency Act . . . stipulates that SOVA, when collecting personal data, is not bound to inform the individual to whom the data refers and the individual does not have the right to access the personal data collected by the Agency (Article 17, § 1)—on condition, that informing or allowing the individual access to personal data would make the tasks of the Agency impossible or difficult to fulfill (Article 17, § 2). Same conditions apply to a request by the Director of SOVA that personal data controllers, which supplied the Agency with personal data, only inform the individual to whom the personal data refer after a period of five years (Article 17, § 3). The exemption is thus not complete and a balancing act is required in order to limit the right to access to information."[85]

Spain: "In Spain, the access to information related to the activity of the national intelligence authorities and surveillance by individuals is not regulated as a constitutional right in the Spanish Constitution, where only mention is made of citizens' access to administrative files and records in Article 105 b) in order to clarify that this kind of access shall be regulated by law.
In this sense, the Law 19/2013 on Transparency, Access to Public Information and Good Governance was recently approved with the aim of guaranteeing the citizens' access to public information. However, under this Law information related to the activity of the national intelligence authorities and surveillance should not be considered public information."[86]

"Spain announced plans for reforming the law on intelligence services. At the time of writing, no draft law was published, while the government's 2023 plan does not include any reference to such a planned reform."[87]

---

[83] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Slovak Republic, at 10 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/slovakia-study-data-surveillance-ii-sk.pdf.
[84] *Id.* at 19.
[85] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Slovenia, at 11 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/slovenia-study-data-surveillance-ii-legal-update-sv.pdf.
[86] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Spain, at 8 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/spain-study-data-surveillance-ii-es.pdf.
[87] FRA Report Update, *supra* note 44, at 10.

Sweden: "The right for individuals to access information on if they have been subject to surveillance is regulated in more detail in the Act on personal data processing Defence intelligence and development activities of the National Defence Radio Establishment . . . The National Defence Radio Establishment (Försvarets radioanstalt) has to answer any person that requests information on if his/her personal data has been processed by the Establishment. If a person's personal data have been processed, and if said person requests information, the National Defence Radio Establishment must provide him/her with written information on 1) the kind of information processed; 2) where the information was collected; 3) the reason behind the data processing; and 4) the institution that has received the collected data from the Establishment. However, this does not apply if the data collection activities that are classified as secret. This is inline with the exceptions stipulated in chapter 2, Section 2 of the Freedom of the Press Act (Tryckfrihetsförordning [1949:105]) and the Freedom of the Press Act (Tryckfrihetsförordning [1949:105]) secrecy provisions of chapter 15 of the Publicity and Secrecy Act (Offentlighets- och sekretesslag [2009:400]), mentioned above."[88]

United Kingdom: "There is no obligation on the intelligence services to notify individuals that they have been subjected to surveillance. The absence of notification is counter-balanced by a system for remedying complaints regarding unlawful activity whereby individuals do not need to establish that they have been subject to surveillance in order to have an admissible claim regarding unlawful activity."[89]

[88] Report of the European Union Agency for Fundamental Rights on National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies—Legal Update Sweden, at 19 (2016), https://fra.europa.eu/sites/default/files/fra_uploads/sweden-study-data-surveillance-ii-legal-update-se.pdf. Furthermore, under the Signals Intelligence Act, the National Defence Radio Establishment (FRA) must provide notification containing information like the date and purpose of the surveillance "as soon as this can be done without detriment to the foreign intelligence activities, but no later than one month after the signals intelligence mission has been concluded." *See* Centrum För Rättvisa v. Sweden, App. No. 35252/08, ¶ 58 (May 25, 2021), https://hudoc.echr.coe.int/fre#%7B%22documentcollectionid2%22:[%22GRANDCHAMBER%22],%22itemid%22:[%22001-210078%22]%7D. However, the FRA may permissibly delay notifying targets "if secrecy so demands." *See id.* at ¶ 59. As the Data Protection Authority reported, "due to secrecy considerations," the FRA, in practice, has never used this authority and notified individuals. *See id.* at ¶ 60.

[89] FRA UK Update, *supra* note 32, at 14.