Ref. Ares(2026)10404145 - 06/11/2026

European Data Protection Board

Information Note

on the redress mechanism for EU/EEA individuals in relation to alleged violations of U.S. law with respect to their data collected by U.S authorities competent for national security

Version 1.1

Version history

Version 1.0	17 April 2024	Noting of the information note
Version 1.1	6 November 2026	Updates to selected links in footnote 33

Context about complaints on government access by U.S. intelligence authorities

On 10 July 2023, the European Commission adopted its Implementing Decision C(2023) 4745 on the adequate level of protection of personal data under the **EU-U.S. Data Privacy Framework (**'DPF Adequacy decision'**)**[1].

An important element of the U.S. legal framework, on which the adequacy decision is based, concerns **Executive Order 14086** on 'Enhancing Safeguards for United States Signals Intelligence Activities'[2] ('**E.O. 14086**'), which was signed by U.S. President Biden on 7 October 2022 and is accompanied by regulations adopted by the U.S. Attorney General, as well as relevant policies and procedures adopted by the U.S. Office of the Director of National Intelligence and U.S. Intelligence agencies.

E.O. 14086 established a **new redress mechanism in the area of national security** to handle and resolve complaints from data subjects in the EU and EEA,[3] alleging unlawful access and use of data by U.S. signals intelligence activities to their personal data that was transmitted from the EU and EEA to the U.S.[4] Thus, only complaints relating to national security will be considered under this redress mechanism. **This redress mechanism applies regardless of the transfer tool used to transfer the complainants' personal data to the U.S.** (i.e., DPF Adequacy decision, standard or ad hoc contractual clauses[5], binding corporate rules[6], codes of conduct[7], certification mechanisms[8], derogations[9]). However, this redress mechanism only applies to data transmitted **after 10 July 2023**.

Please note that information about the possibility to complain about a private U.S. organization's compliance with the principles set out in the Data Privacy Framework can be found here: https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_en

How to lodge a complaint?

Complaints have to be sent **to the national EU/EEA data protection authority** competent for the individual **('DPA')**. A list of DPAs in the EU/EEA Member States can be found here: https://edpb.europa.eu/about-edpb/about-edpb/members_en.

[1] Implementing Decision C(2023) 4745 of the European Commission, pursuant to 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 ('**GDPR'**) on the adequate level of protection of personal data under the EU-US Data Privacy Framework ('**the DPF Adequacy Decision**') of 10 July 2023. By doing so, the Commission decided that the United States ('**the U.S.**'), for the purpose of Article 45 of the GDPR ensures an adequate level of protection for personal data transferred from the EU to organisations in the US that are included in the 'Data Privacy Framework List', maintained and made publicly available by the U.S. Department of Commerce (Article 1 of the Adequacy Decision), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32023D1795.

[2] Executive Order of October 7, 2022 on Enhancing Safeguards for United States Signals Intelligence Activities.

[3] References the "**EU**" made throughout this document should be understood as references to the "**EEA**".

[4] Further specifications regarding this redress mechanism are also provided in the E.O. 14086, as complemented by the Attorney General Regulation on the Data Protection Review Court; see also Implementation Procedures for the Signals Intelligence Redress Mechanism Under Executive Order 14086 ('Intelligence Directive 126), available at: https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf

[5] Standard contractual clauses in accordance with Article 46(2)(c) or (d) GDPR, or ad hoc contractual clauses in accordance with Article 46(3)(a) GDPR.

[6] Article 46(2)(b) GDPR.

[7] Article 46(2)(e) GDPR.

[8] Article 46(2)(f) GDPR.

[9] Article 49 GDPR.

*[The EDPB has adopted **Rules of Procedure** to provide guidance to DPAs in relation to their respective tasks and responsibilities.]* An **EU individual complaint form** has been established for the submission of complaints to the CLPO by EU/EEA individuals https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_en

How will the DPA handle the complaint?

The EU/EEA national DPA will **verify the identity of the individual complainants**[10] (for more information on how DPAs handle such verification, please also see: Link to each DPAs' procedure **and** will **check that the complaint is complete and satisfies the conditions** set forth in U.S. law[11].

In particular that, the DPA will verify:

- The identity of the complainant, and that he/she is acting only on his/her own behalf and not as a representative of a governmental, non-governmental, or intergovernmental organisation;
- That the complainant believes that one or more U.S. law(s) have been violated if personal data of or about the complainant was unlawfully accessed by U.S. intelligence agencies after his/her personal data was transmitted from the EU to the U.S.;
- The complaint contains, in writing (also via email) all relevant information (**which need not demonstrate that the complainants' data has in fact been subject to US signals intelligence activities)**:
    - any information that forms the basis of the complaint, including the details of the online account or personal data transfer believed to may have been accessed;
    - the nature of the relief sought[12];
    - the specific means by which personal data of or about the complainants is believed to have been transmitted to the US;
    - which U.S. Government entity or entities believed to be involved in accessing the personal data of or about the complainant (if known);
    - and any other measures the complainant may have pursued to obtain the information or relief requested, and the response received through those other measures;
    - it pertains to personal data of or about the complainants, believed to have been transferred to the US after 10 July 2023;
- The complaint is not frivolous, vexatious or made in bad faith.

After this verification and if the complaint is found complete, the DPA will transmit it, in an encrypted format, to the **Secretariat of the European Data Protection Board ('EDPB**

[10] E.O. 14086, Section 4(k)(v) and Section E(1)(c)(8) of ICD 126.
[11] E.O 14086, Section 4(k)(i)-(iv).
[12] Such relief may include lawful measures designed to fully redress an identified violation. In a non-exhaustive manner, this may include administrative measures to remedy procedural or technical violations; deleting your personal data acquired without lawful authorization; deleting results of inappropriate queries on lawfully collected personal data; restricting access to your personal data.

Secretariat')[13]. The latter **will then transmit it,** in an encrypted format[14] to the U.S. authorities that are competent to handle the complaint, namely the Office of the Director of National Intelligence's **Civil Liberties Protection Officer ('CLPO')**.[15]

What is the role of the CLPO?

The CLPO is in charge of conducting an investigation of the complaint to determine whether the safeguards provided in E.O. 14086 or other applicable U.S. law(s) were violated and, if so, to determine the appropriate binding remediation[16]. The CLPO will provide a response[17] to the DPA, via the EDPB Secretariat, within a timely manner. This response will confirm that:

> (1) "The review either did not identify any covered violations or the Civil Liberties Protection officer of the Office of the Director of National Intelligence issued a determination requiring appropriate remediation" [18]. In its standardised response[19], the ODNI CLPO will neither confirm nor deny whether the complainant has been the target of surveillance nor will it confirm the specific remedy that was applied;
> (2) The complainant or an element of the U.S. Intelligence Community may apply for review of the CLPO's decision by submitting an appeal with the Data Protection Review Court ('DPRC'); and
> (3) If either the complainant or an element of the Intelligence Community applies for review by the DPRC, a special advocate will be selected by the DPRC to advocate regarding the complainant's interest in the matter ('**Special Advocate'**).

The decision of the CLPO is binding on the elements of the Intelligence Community[20].

The CLPO sends its response to the EDPB Secretariat in an encrypted format, which will then transmit it, also in an encrypted format, to the national DPA that originally received the complaint. This DPA will, in turn, inform the complainant of the CLPO's response (including a translation from English, if and to the extent necessary).

How to appeal against the CLPO's decision?

Complainants have the possibility to appeal the decision of the CLPO before the **Data Protection Review Court ('DPRC') within 60 days** after receiving the notification by the national DPA of the CLPO's response[21]. In order to appeal, the complainant may submit an application to **their DPA** within 60 days[22]. The DPRC can investigate complaints from

[13] Recital 177 of the Adequacy Decision.
[14] Section E(1)(f) of Intelligence Community Directive 126 states that: 'If the CLPO determines that the complaint is not a qualifying complaint because it does not meet the conditions of Section E.1.c., or does not meet the conditions of Section E.1.d., of this Directive, the CLPO will provide written notification via **encrypted electronic communication and in the English language** to the appropriate public authority in a qualifying state of the deficiencies in the complaint.'
[15] For the purposes of this document, any references to the Civil Liberties Protection Officer ('CLPO') mean the Office of the Director of National Intelligence's Civil Liberties Protection Officer ('ODNI CLPO').
[16] Section 3(c)(i)(E) and Section 3(d)(i)(H) of E.O. 14086.
[17] E.O. 14086, Section 3 (c)(i)E.
[18] E.O. 14086, Section 3 (c)(i)E(1).
[19] The standardised response will state that the CLPO's "*review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation*" (E.O. 14086, Section 3 (c)(i)E).
[20] Section 3(c)(H)(ii) of E.O. 14086.
[21] The dates that will be taken into account to assess if the appeal was submitted within 60 days will be the date of notification to the complainant, by the DPA, of the CLPO's determination, and the date of submission, by the complainant, of their appeal to the DPA.
[22] Recital 177 Adequacy Decision.

individuals in the EU/EEA, including obtaining relevant information from elements of the U.S. Intelligence Community, and can take binding remedial decisions[23].

The appeal procedure will follow a similar channel and procedure as the initial complaint: The DPA will transmit the appeal to the EDPB Secretariat, in an encrypted format, which will in turn, transmit it, in an encrypted format, to the U.S. Department of Justice's Office of Privacy and Civil Liberties ('OPCL'), which provides support to the DPRC, so that the DPRC can review the appeal.

In particular, the DPRC will review the determinations made by the CLPO (both whether a violation of applicable U.S. law(s) occurred and as regards the appropriate remediation) based, at a minimum, on the record of the CLPO's investigation, as well as any information and submissions provided by the complainant, the Special Advocate or an element of the Intelligence Community[24]. A DPRC panel has access to all information necessary to conduct a review, which it may obtain through the CLPO (e.g. the panel may request the CLPO to supplement its record with additional information or factual findings if necessary to carry out the review)[25]. The Special Advocate also has access to all information necessary to fulfil their role of assisting the DPRC panel in its consideration of the application, including by advocating regarding the complainant's interest in the matter and by ensuring that the DPRC panel is well-informed of the issues and the law(s) with respect to the matter.

When concluding its review, the DPRC may:

(1) decide that there is no evidence indicating that signals intelligence activities occurred involving personal data of the complainant;

(2) decide that the CLPO's determinations were legally correct and supported by substantial evidence; or

(3) if the DPRC disagrees with the determinations of the CLPO (whether a violation of applicable US law(s) occurred or the appropriate remediation), issue its own determinations[26].

The decision of the DPRC is binding and final with respect to the complaint before it[27]. In cases where the DPRC's review was triggered by an application from the complainant[28], the complainant is notified of the DPRC's decision. Once the DPRC completes its review, the DPRC will provide the complainant with a standardised statement indicating it has completed its review, and stating that "*the review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation*."[29] The

[23] Section 3(c)(i)(E) and Section 3(d)(i)(H) of E.O. 14086.

[24] Recital 189 of the Adequacy Decision and Section 3(d)(i)(D) EO 14086.

[25] Recital 189 of Adequacy Decision; Section 3(d)(iii) EO 14086 and Section 201.9(b) AG Regulation.

[26] Recital 190 of Adequacy Decision and Section 3(d)(i)(E) EO 14086 and Section 201.9(c)-(e) AG Regulation. According to the definition of 'appropriate remediation', in Section 4(a) EO 14086, the DPRC must take into account "the ways that a violation of the kind identified have customarily been addressed" when deciding on a remedial measure to fully address a violation, i.e. the DPRC will consider, among other factors, how similar compliance issues were remedied in the past to ensure that the remedy is effective and appropriate.

[27] Recital 191 of Adequacy Decision and Section 3(d)(ii) EO 14086 and Section 201.9(g) AG Regulation.

[28] In accordance with Section 3(d)(i)(B) of EO 14086, elements of the Intelligence Community may also lodge applications for review of the determination made by the CLPO.

[29] Recital 192 Adequacy Decision and Section 3(d)(i)(H) EO 14086 and Section 201.9(h) AG Regulation. As regards the nature of the notification see Section 201.9 (h)(3) AG Regulation.

DPRC will transmit such statement, in an encrypted format, to the EDPB Secretariat, which will in turn transmit it to the DPA in an encrypted format. The DPA will notify the complainant of the DPRC's statement (including a translation from English, if and to the extent necessary). This statement will neither confirm nor deny whether the complainant has been the target of surveillance nor will it confirm the specific remedy that was applied. Each decision of the DPRC is also transmitted to the CLPO[30].

What is the role of the U.S. Department of Commerce in relation to declassified information?

The U.S. Department of Commerce ('**DoC'**) will periodically contact the relevant elements of the Intelligence Community regarding whether information pertaining to the CLPO's or DPRC's review of a complaint has been declassified. If elements of the Intelligence Community inform the DoC that information pertaining to the CLPO's or DPRC's review of the complaint has been declassified, the DoC will notify the complainant, through the EDPB Secretariat, which will in turn transmit it to the DPA, that information pertaining to the review of their complaint by the CLPO or DPRC, as appropriate, may be available to the complainant under applicable US law[31]. One such law is the U.S. Freedom of Information Act ('**FOIA'**)[32], under which the complainant may submit a FOIA request directly to the ODNI, to the relevant Intelligence Community element, or to the Department of Justice (i.e., without going through the DPA and the EDPB Secretariat) for declassified information about their complaint. Instructions on how to submit FOIA requests are available on the respective public webpages[33], the relevant Intelligence Community elements, and the DPRC[34].

It should be noted that complaints from data subjects in the EU/EEA alleging certain violations of U.S. law(s) concerning U.S. signals intelligence activities adversely affecting their individual privacy and civil liberties and relating to their personal data that was transmitted from the EU/ EEA to the U.S. should only be submitted to the CLPO and not to the FOIA offices mentioned above.

[30] Recital 192 of Adequacy Decision and Section 201.9(h) AG Regulation.
[31] Section 3(d)(v)(C) of E.O. 14086.
[32] More information regarding the FOIA may be accessed at https://www.dni.gov/index.php/foia.
[33] https://www.dni.gov/accountability/; https://www.dni.gov/accountability/#foia
[34] https://www.justice.gov/opcl/opcl-freedom-information-act.