Complaint Form to the U.S. Office of the Director of National Intelligence's Civil Liberties Protection Officer (CLPO)[1]

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

Adopted on 17 April 2024

[1] 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').

Purpose of this Form

With this form, individuals in EU or EEA Member States may submit complaints alleging unlawful access and use of data by U.S. intelligence agencies to their personal data transmitted from the EU to companies in the U.S. This redress mechanism applies to any personal data transferred from the EU/EEA[2] to the U.S. (i.e., not just those transferred on the basis of the EU-U.S. Data Privacy Framework[3] ('**DPF'**)[4], but only applies to data transmitted **after 10 July 2023**[5].

This form only applies to complaints in the area of national security signals intelligence activities. It cannot be used to submit a complaint relating to access to data by U.S. authorities for purposes other than national security purposes. Please also note that this form cannot be used to submit a complaint relating to an U.S. Organization's compliance with the EU-U.S. Data Privacy Framework ('**DPF'**). Information about how to complain on the commercial aspects of the DPF, can be found here: *[link]*

To whom to address your complaint?

You have to submit this complaint form **to your competent national data protection authority ('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.

Additional information

Please note that once you submit your complaint to your national DPA, the latter will check its completeness, namely it will verify your identity, subject to the DPAs' discretion on the modalities for such verification, and that your complaint satisfies the conditions set forth in Section 4(k)(i)-(iv) of Executive Order 14086[6]. If found complete, your DPA may provide a

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

[3] Commission implementing decision of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf).

[4] This redress mechanism also applies to individuals whose personal data were transferred to the U.S. under binding corporate rules (Article 46(2)(b) GDPR, standard contractual clauses under Article 46(2)(c) or (d) GDPR, codes of conduct under Article 46(2)(e) GDPR, certifications under Article 46(2)(f) GDPR, or ad hoc contractual clauses under Article 46(3)(a) GDPR.

[5] Further specifications regarding this redress mechanism are also provided in the Executive Order 14086 ('**E.O. 14086**'), available at https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf, as complemented by the U.S. Attorney General Regulation on the Data Protection Review Court (available at https://www.justice.gov/d9/pages/attachments/2022/10/07/dprc_final_rule_signed.pdf); 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.

[6] E.O. 14086, Section 4(k)(v) stipulates that: '*"Qualifying complaint" means a complaint, submitted in writing, that (..) is transmitted by the appropriate public authority in a qualifying state,* ***after it has verified the identity of the complainant*** *and that the complaint satisfies the conditions of section 5(k)(i)-(iv) of this order.*' Also, Intelligence Community Directive (ICD) 126 stipulates, in **Section E(1)(c)(8)**: '*Specifically, for a transmitted complaint to be a "qualifying complaint" consistent with Executive Order 14086's definition of "covered violation" and "qualifying complaint," the complaint must: (..)* ***contain a verification*** *by the appropriate public authority in a qualifying state: (a) of the identity of the complainant, and (b) that the complaint satisfies the conditions of Section E.1.c.(l) - (7) of this Directive*'; and in **Section E(1)(e) of the ICD**: '*The transmission of the complaint from an appropriate public authority in a qualifying state* ***must also contain a description of the manner in which the authority verified the identity of the complainant.*** *The CLPO shall rely on the verification of the identity of the complainant by the appropriate public authority in a qualifying state, but should either the information provided by the appropriate public authority in a qualifying state or subsequent investigation of the complaint call into question the identity of the complainant, the CLPO may request additional information from the public authority in a qualifying state in a manner*

translation of your request into English, if and to the extent necessary.[7] After this first verification, your DPA will transmit your complaint to the EDPB Secretariat, including your personal data, who will in turn transfer it to the U.S. Civil Liberties Protection Officer ('CLPO') of the U.S. Office of the Director of National Intelligence[8]. The EDPB Secretariat will transmit your complaint to the CLPO for verification, in an encrypted format. Once the CLPO verifies that the complaint meets the necessary criteria, the CLPO will investigate, review, and, as necessary, order appropriate remediation (i.e., lawful measures designed to fully redress an identified violation regarding a specific complainant and complaint)[9]. Once the CLPO completes the review, the CLPO will send their response, in an encrypted format, to the EDPB Secretariat, who will transfer it to your DPA, so the latter can inform you of its outcome. That standardised response will specify that: '*the review either did not identify any covered violations or that the CLPO issued a determination requiring appropriate remediation*'.[10] Please be aware that this response will neither confirm nor deny whether you have been the target of surveillance nor will it confirm the specific remedy that was applied. With this notification, the CLPO will also inform you, through the same channel, of the possibility to appeal to the Data Protection Review Court ('**DPRC'**) for a review of the CLPO's determinations.

You have the possibility to **appeal** the decision of the ODNI CLPO before the DPRC **within 60 days** after receiving the notification by your DPA of the ODNI CLPO's reply. You may submit your appeal to your DPA (which, similarly to your initial complaint, will transmit it (including a translation from English, if and to the extent necessary), in an encrypted format, to the EDPB Secretariat, 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[11]. After the DPRC has completed the review of your appeal, you will be notified via your DPA (including a translation from English, if and to the extent necessary) of the conclusion of the DPRC's review. The DPRC's notification will provide a standardised answer, stating that the '*review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation'*[12]. Please be aware that this notification will neither confirm nor deny whether you have been the target of surveillance nor will it confirm the specific remedy that was applied.

More information on this complaint form and the underlying redress mechanism can be found here: [LINK to infonote]

---

that does not reveal intelligence sources or methods or otherwise indicate whether an individual has, in fact, been the subject of signals intelligence activities.'

[7] 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.'

[8] 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').

[9] For example, this may include: administrative measures to remedy procedural or technical violations relating to otherwise lawful access; terminating acquisition of data where collection is not lawfully authorized; deleting data acquired without lawful authorization; deleting results of inappropriate queries on lawfully collected data; restricting access to data.

[10] E.O. 14086, Section 3(c)(E)(1).

[11] The dates that will be taken into account to assess if your appeal was submitted within 60 days will be the date of notification, by your DPA, of the CLPO's determination, and the date of submission of your appeal to your DPA.

[12] E.O. 14086, Section 3(d)(i)(H).

The Form to complete

The following information is sought for the verification of your complaint by your DPA and for the further handling of your complaint by the CLPO.

1. **Your Identification**

Please provide the following information for your identification:
a. Surname / Family name:
b. First Name(s):
c. Maiden / Other names:
d. Place of Birth:
e. Date of Birth:
f. Title (where relevant):
g. Telephone number[13]:
h. Residential address:

Your DPA will verify your identity.[14] For this purpose, you may be asked to provide evidence of your identity (for more information on how your DPA handles such verification, please also see: Link to each DPAs' procedure/the info note as supplemented by DPAs). This may include providing in annex a copy of one of the following identity documents:
a. Passport:
b. Driving license:
c. ID card:
In such case, you are free to black out any information on the copy of your identity document that is not necessary for the verification of the data provided above under a.-h. **Alternatively**, if provided for by your DPA, you may use an electronic identification system or any other means as provided by the national law of the Member State where you made your complaint. The modalities for verifying your identity are subject to the discretion of your DPA (**see: Link to each DPAs' procedure/the info note as supplemented by DPAs).**

2. **Your Complaint**

Please find below a list of information to provide within your complaint to show that the complaint is qualifying for review by the CLPO.

[13] This information will only be used to contact you if some additional information are required regarding your request or, where applicable, to communicate to you the reply to your request.

[14] E.O. 14086, Section 4(k)(v) and Section E(1)(c)(8) of Intelligence Community Directive 126.

Please note that the questions below correspond to the specific conditions set forth in Section 4(k)(i)-(iv) of E.O. 14086.[15] Please tick the corresponding boxes.

a. Please provide a general description of your complaint alleging unlawful access by U.S. intelligence agencies to personal data transmitted from the EU to the U.S.
Please note that **you do not need to demonstrate that your data was in fact collected by the U.S. intelligence agencies.**

b. Please provide additional information relating to your complaint.

i. Please provide the information or details of any online account or personal data transfer you believe may have been accessed, including the relevant email addresses or usernames relating to online accounts and any other relevant information such as flight, hotel or contact information.

Your DPA will verify that the details provided (i.e. email address or usernames) are actually yours. Please provide evidence that those details are yours. This can be done for instance by providing a confirmation from the provider of the service you are using, or a screenshot, which clearly shows that you are the one using the account.

ii. Do you know which company has sent or otherwise made available personal data of or about you to the U.S.? If so, please provide the details. In case you are not sure which company has sent or otherwise made available your data, please provide any relevant information you may have.

iii. Do you know which company has processed personal data of or about you in the U.S.? If so, please provide any details you have.

iv. Do you know the specific means[16] by which personal data of or about you is believed to have been transferred or otherwise made available to the U.S.?

v. Do you confirm that you used the service, which you believe transferred personal data of or about you **after the 10th of July 2023**?
Yes ☐

vi. Do you believe that one or more U.S. law(s) have been violated if personal data of or about you was accessed?
Yes ☐

c. When submitting this complaint, are you acting in a personal capacity?
Yes ☐

[15] See E.O. 14086, Section 4(k)(v); Intelligence Community Directive (ICD) 126 (https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf), **Sections E(1)(c)(8)**and **E(1)(e)** .'

[16] This may be a phone number or an email address (a mere reference to a name will not be sufficient).

d. If you are aware of this information, which, US Government entity or entities are believed to be involved in accessing personal data of or about you?

e. What is the nature of the information or relief sought?[17]

f. Please provide information relating to other measures which you may have taken to obtain the information or relief requested and the response received through those other measures (for example: a Freedom of Information Act('FOIA') request under U.S. law[18])?

Please provide your signature below to confirm that all information provided is correct and made in good faith.

Signature:

Date of the complaint:

[17] Such relief may include lawful measures designed to fully redress an identified covered 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.

[18] Section 3(d)(v)(C) of E.O. 14086; See also Recital 199 of Adequacy Decision, stating that: '*Finally, in addition to the redress avenues mentioned in recitals 176-198, any individual has the right to seek access to existing federal agency records under FOIA (Freedom of Information Act), including where these contain the individual's personal data*'. Please note that complaints alleging certain violations of U.S. law concerning U.S. signals intelligence activities adversely affecting your individual privacy and civil liberties and relating to your personal data that was transmitted from the EU and EEA to the U.S. **should only be submitted to the U.S. CLPO** and not to U.S. FOIA offices. You can find more information regarding the FOIA at https://www.dni.gov/index.php/foia. Instructions on how to submit FOIA requests are on the ODNI's website (https://www.dni.gov/index.php/make-a-records-request), the relevant Intelligence Community element's website, and the Department of Justice's webpage (https://www.justice.gov/oip/make-foia-request-doj).