

EDPB Personal data records of processing activities (Article 31 of the Regulation 2018/1725¹)

Record of EDPB activities processing personal data, based on Article 31 of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

Nr.	Item	Description
1.	Title of the processing operation	Redress mechanism for national security purposes – Recital 177 of the EU-U.S. Data Privacy Framework (the “DPF”) ²
2.	Number of record	EDPB-0011
3.	Last updated	March 2026
4.	Data controller	European Data Protection Board Secretariat Edpb [at] edpb.europa.eu Rue Montoyer, 30 Belgium, Brussels
5.	Joint controllers	N/A
6.	Processor(s)	N/A

¹ Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the EU institutions, bodies, offices and agencies.

² Commission Implementing Decision EU 2023/1795 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 (notified under document C(2023)4745).

7.	Data Protection Officer (DPO)	EDPB Data Protection Officer Edpb-dpo [at] edpb.europa.eu Rue Montoyer, 30 Belgium, Brussels
8.	Description of the processing operation	<p>The present record concerns the processing of personal data by the Secretariat of the EDPB (the “EDPB Secretariat”), as provided in Recital 177 of the DPF for the purpose of the redress mechanism for national security purposes. Under this mechanism, the EDPB Secretariat facilitates the communication between the EU/EEA Data Protection Authorities (“DPAs”) and the competent U.S. authorities acting as an intermediary in the exchange of information between one and another.</p> <p>More specifically, Recitals 176–194 DPF provide that, in line with the U.S. Executive Order 14086, individuals from the EU/EEA can submit a complaint on alleged violations of U.S. law with respect to their personal data collected and used by U.S authorities competent for national security. According to this redress mechanism, data subjects submit such complaints to their competent DPA in the EU/EEA. As stipulated in Recital 177 DPF, the DPAs send such complaints to the EDPB Secretariat, which transmits them to the competent U.S. authorities. In the case of complaints, this entails the EDPB Secretariat transmitting them to the U.S. Office of the Director of National Intelligence’s Civil Liberties Privacy Officer (the “ODNI CLPO”). In case a data subject lodges, via its competent DPA, an appeal against the ODNI CLPO’s determinations, the EDPB Secretariat will transmit such appeal received from the competent DPA to the U.S. Department of Justice’s Office of Privacy and Civil Liberties (the “OPCL”), which further transmits it to the U.S. Data Protection Review Court (the “DPRC”), the latter being responsible for treating them.</p> <p>The EDPB Secretariat is also responsible for transmitting to the competent DPA any reply received from the ODNI CLPO or from the DPRC (in the latter case, received via the OPCL). Further, the EDPB Secretariat transmits to the competent DPA any communication it receives from the the U.S. Department of Commerce (the “DoC”) that notify</p>

		the data subject of declassified information pertaining to the review of a complaint by the ODNI CLPO or the DPRC, as appropriate, which may be available to the data subjects under applicable U.S. law ³ .
9.	Purpose of processing operation	<p>According to Recital 177 DPF, as further specified by the EDPB Rules of Procedure on the DPF redress mechanism for national security purposes⁴, the EDPB Secretariat processes personal data for the purposes of:</p> <ul style="list-style-type: none"> a) verifying that complaints have been submitted to and sent by a competent DPA in the EU/EEA; b) checking whether the complaint was based on the EU Common Complaint Form⁵. In view of ensuring consistency, the EDPB Secretariat might have to exchange on procedural matters with the DPA that forwarded to it the complaint or appeal; c) forwarding the complaint to the ODNI CLPO, as well as then forwarding the reply of the latter to the DPA; d) communicating to the ODNI CLPO the date of the notification, by the DPA, of the ODNI CLPO's reply to the complainant; e) where an appeal is lodged with the DPRC, sending such appeal to the OPCL, which will further transmit it to the DPRC, as well as forwarding to the DPA the reply of the DPRC including the DPRC's statement that it has concluded its review (both of which are sent to the EDPB Secretariat by the OPCL); f) sending any communication from the DoC to the competent DPA that information pertaining to the review of a complaint by the ODNI CLPO or DPRC, as appropriate, may be available to the data subject under applicable U.S. law; and g) bringing to the attention of all members of the EDPB any matters of general interest that would occur from this process relating to all the above-mentioned tasks.
10.	Legal basis	The legal basis for the processing of personal data is Article 5(1)(a) and 5(2) ("Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union

³ More detailed information on the redress mechanism under the DPF for national security purposes can be found at: https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_en, and a template complaint form is available at: https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_pt.

⁴ EDPB Rules of Procedure on the DPF redress mechanism for national security purposes⁴ of 17 April 2024, available at: https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_pt

⁵ The form is available here: https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_pt

		<p>institution or body”) of Regulation (EU) 2018/1725. In particular, this task is provided for in Recital 177 DPF⁶ and it has been further specified in the EDPB Rules of Procedure on the DPF redress mechanism for national security purposes. The task in question is the responsibility of the EDPB Secretariat. For the processing of any special categories of personal data which the data subject might refer to in their complaint, the EDPB Secretariat relies on Article 10(2)(g) Regulation (EU) 2018/1725.</p> <p>Further, the EDPB may be required to store and further process personal data in the context of any audits or enquiries by specific EU bodies, when it handles requests for access to documents under Regulation (EC) 1049/2001⁷, or if data subjects request to exercise their rights under Regulation (EU) 2018/1725. In such cases, lawfulness of processing is based on the necessity of such processing for compliance with a legal obligation to which the EDPB is subject under Article 5(1)(b) and 5(2) of Regulation (EU) 2018/1725. The legal obligations are foreseen in different legislation applicable to the different institutions responsible for auditing and inspections. Where any special categories of data that the complainant has shared are processed, depending on the purpose, Article 10(2)(f) and (g) Regulation (EU) 2018/1725 may apply.</p>
11.	Description of categories of data subjects	<ul style="list-style-type: none"> • Individuals submitting their complaint or appeal; • DPAs’ staff members responsible for handling complaints and appeals; • U.S. authorities’ staff members responsible for handling said complaints, appeals and transmitting information on declassification of files; • EDPB Secretariat staff members in charge of channelling said complaints, appeals and information on declassification of files; and • Any other person mentioned in the documents that the EDPB Secretariat has to channel in the context of the redress mechanism for national security purposes.
12.	Description of processed	<p>Any personal data relating to a complainant or appellant such as:</p> <ul style="list-style-type: none"> • Names;

⁶ Recital 177 DPF provides that: “After the requirements for filing a complaint referred to in recital 178 have been verified, the competent DPA will channel, via the secretariat of the European Data Protection Board, the complaint to the redress mechanism.”

⁷ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

	<p>personal data / categories</p>	<ul style="list-style-type: none"> • Place and date of birth; • Title (where relevant); • Contact details such as email address, telephone number and residential address; • Signature; • Any information relating to the complaint or appeal, including any special categories of personal data that the data subject might include in their complaint; and • The replies of the competent U.S. authorities in relation to the complaint, the appeal (where relevant) or the declassification of a case (where relevant). <p>Personal data of competent DPA's and U.S. authorities' staff members such as:</p> <ul style="list-style-type: none"> • Names and contact details; and • Opinions expressed in relation to the submitted complaints or appeals. <p>Personal data of EDPB Secretariat staff members such as:</p> <ul style="list-style-type: none"> • Names and contact details; and • Opinions expressed in relation to the verification checks that the EDPB Secretariat has to carry out. <p>Any personal data of other individuals than the above which might be included in the documents that the EDPB Secretariat has to transmit in the context of the redress mechanism for national security purposes.</p>
13.	<p>Description of procedure to ensure data subjects' rights</p>	<p>A specific privacy statement is available on the EDPB website, with details on how data subjects can exercise their rights. Some DPAs also share this specific privacy statement with data subjects.</p>
14.	<p>Description of recipients of personal data</p>	<ul style="list-style-type: none"> • The ODNI CLPO; • Where an appeal is lodged with the DPRC, the OPCL providing administrative support to the DPRC. The OPCL will transmit the appeal to the DPRC; • The DPA which received the complaint;

		<ul style="list-style-type: none"> Members of the public in the context of requests for access to documents, in accordance with the provisions of Regulation (EC) 1049/2001 or Council Regulation (EEC, Euratom) 354/83⁸.
15.	Description of transfers	<p>In line with Recital 177 DPF providing for a redress mechanism for national security purposes, the EDPB Secretariat will forward to the competent U.S. authorities the complaints or appeals submitted to the EU/EEA DPAs. More specifically:</p> <ul style="list-style-type: none"> The EDPB Secretariat will transfer any complaints to the ODNI CLPO; and The EDPB Secretariat will transfer to the OPCL any appeals against the CLPO’s determinations. The OPCL will further forward such appeals to the DPRC, to which it provides administrative support. <p>As the above recipients of the personal data have not adhered to the adequacy decision for the EU-U.S. Data Privacy Framework, the EDPB Secretariat relies for the above transfers on Article 50(1)(d) and (3) Regulation (EU) 2018/1725 (“The transfer is necessary for important reasons of public interest”). In particular, this task is provided in Recital 177 DPF in line with the provisions of Article 47 EU Charter (“Right to an effective remedy and fair trial”) and Article 79 GDPR (“Right to an effective judicial remedy against a controller or processor”).</p> <p>The application of Article 50(1)(d) and (3) Regulation (EU) 2018/1725 is justified by the current very low number of submitted complaints (to this date, only one complaint has it been submitted), as well as by the fact that this processing represents only a highly marginal portion of the tasks of the EDPB Secretariat. Nevertheless, the EDPB Secretariat will establish a more stable system for transfers in the future given the possibility for a future increase of submitted complaints.</p>
16.	Description of envisaged time limits for retention for each processing operation	<p>According to EO 14086 (Section 3(d)(v)(B)), the U.S. Secretary of Commerce must perform a check at least once every five years to see if any information pertaining to complaints or appeals has been declassified. If the U.S. Secretary of Commerce identifies any such information, they will send it to the EDPB Secretariat, which will then transmit that information to the competent DPA, who will in turn transmit it to the relevant complainant/appellant.</p>

⁸ Council Regulation (EEC, Euratom) No 354/83 of 1 February 1983 concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community.

		<p>According to Section 1.5 of the EO 13526 “Classified National Security Information”,⁹ information can remain as classified for a maximum period of 50 years.</p> <p>Therefore, to ensure that the EDPB Secretariat is able to transmit any declassified information received by the U.S. authorities to the competent DPA, it must also keep the personal data until:</p> <ul style="list-style-type: none"> a) such information is declassified – being, at the longest, 50 years following the transmission of the response from ODNI CLPO or the DPRC to the competent DPA; b) the U.S. Secretary of Commerce has performed their check for declassified information, discovered that the information is declassified, and transmitted the relevant information to the EDPB – being, at the longest, five years following the declassification of the information; and c) the EDPB has had sufficient time to process this information and transmit it to the competent DPA – being, at the longest, one year. <p>In practice, this means that the EDPB Secretariat will keep the personal data for a maximum of 56 years following the relevant transmission.</p> <p>At the end of this retention period, if the personal data are contained in documents with historical or administrative value which are selected for preservation in the EDPB records, the selected personal data will be kept indefinitely and – unless an exemption applies – will be made public in accordance with Regulation (EEC, EURATOM) 354/83 on the opening to the public of historical archives after 30 years.</p>
17.	<p>General description of technical and organisational security measures referred to in Article 33</p>	<p><u>IT Measures</u></p> <p>Any personal data collected by the EDPB Secretariat is encrypted and is stored on servers with restricted access that are available only to authorised staff through adequate IT security measures. In general, technical measures include appropriate actions to address online security, protect server hardware, software and the network from accidental or malicious manipulations and risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed.</p>

⁹ <https://obamawhitehouse.archives.gov/the-press-office/executive-order-classified-national-security-information>

		<p>The EDPB Secretariat will transmit all above-mentioned communication from the competent DPAs to the U.S. competent authorities and vice-versa, via appropriate electronic means and in encrypted form.</p> <p><u>Organisational measures</u> Physical access to the EDPB premises is restricted to authorised staff and EDPB members. Only a limited number of EDPB Secretariat staff members are authorised to channel said complaints and appeals and they have access to the dedicated and encrypted tools.</p>
--	--	---