## Interfaz de usuario gráfica Descripción generada automáticamente con confianza media

**Nota informativa**

**Sobre el mecanismo de recurso para los particulares de la UE y el EEE en relación con supuestas violaciones de la legislación de EE. UU. con respecto a sus datos recogidos por las autoridades competentes en materia de seguridad nacional**

*(unofficial courtesy translation)*

## **Contexto sobre las reclamaciones de acceso gubernamental por parte de las autoridades de inteligencia de EE. UU.**

El 10 de julio de 2023, la Comisión Europea adoptó su Decisión de Ejecución (2023) 4745 sobre el nivel adecuado de protección de los datos personales con arreglo al **Marco de Privacidad de Datos UE-EE. UU.** (“Decisión de Adecuación del DPF”)**[[1]](#footnote-2)**.

Un elemento importante del marco jurídico de EE. UU., en el que se basa la Decisión de Adecuación, se refiere a la Orden Ejecutiva 14086 sobre “Mejora de las salvaguardias para las actividades de interceptación de las comunicaciones por parte de Estados Unidos”[[2]](#footnote-3) (“**O.E. 14086**”), que fue firmada por el presidente Biden de EE. UU. el 7 de octubre de 2022 y acompañada de reglamentos adoptados por el Fiscal General, así como de políticas y procedimientos adoptados por la Oficina del Director de Inteligencia Nacional y los organismos de inteligencia de EE. UU.

La O.E. 14086 estableció un **nuevo mecanismo de recurso en el ámbito de seguridad nacional** para tramitar y resolver las reclamaciones de los interesados en la UE y el EEE[[3]](#footnote-4), que aleguen el acceso y uso ilícitos de datos por parte de las actividades de interceptación de las comunicaciones de EE. UU. a sus datos personales transmitidos desde la UE y el EEE a EE. UU[[4]](#footnote-5). Así pues, solo se considerarán en el marco de este mecanismo de recurso las reclamaciones relacionadas con la seguridad nacional. **Se aplica independientemente del instrumento de transferencia utilizado para transferir los datos personales de los reclamantes a los EE. UU.** (es decir, Decisión de Adecuación del DPF, cláusulas contractuales estándar o ad hoc[[5]](#footnote-6), normas corporativas vinculantes[[6]](#footnote-7), códigos de conducta[[7]](#footnote-8), mecanismos de certificación[[8]](#footnote-9), excepciones)[[9]](#footnote-10), aunque únicamente se aplicará a los datos transmitidos **después del 10 de julio de 2023**.

*Tenga en cuenta que la información sobre la posibilidad de reclamar sobre el cumplimiento de los principios en el Marco de Privacidad de Datos por parte de una organización estadounidense puede encontrarse aquí:* [*EU-US Data Privacy Framework Template Complaint Form for Submitting Commercial Related Complaints to EU DPAs | European Data Protection Board (europa.eu)*](https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_en)

## **¿Cómo presentar una reclamación?**

Las reclamaciones deben enviarse **a la autoridad nacional de protección de datos de la UE/EEE** competente para el particular en concreto **(“APD”)**. Aquí encontrará una lista de las APD de los Estados miembros de la UE/EEE: <https://www.edpb.europa.eu/about-edpb/about-edpb/members_en>

*[El CEPD ha adoptado un* ***Reglamento interno*** *para orientar a las APD en relación con sus respectivas tareas y responsabilidades.]* Se ha establecido un **formulario de reclamación individual de la UE** para la presentación de reclamaciones a la CLPO por particulares de la UE o del EEE: [https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-](https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_en) [complaint-form-us-office-director-national en](https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_en)

## **¿Cómo tramitará la denuncia la APD?**

La APD nacional de la UE/EEE **verificará la identidad de los reclamantes individuales[[10]](#footnote-11)** (para más información sobre cómo las APD gestionan dicha verificación, véase también: [Política de privacidad y aviso legal | AEPD](https://www.aepd.es/politica-de-privacidad-y-aviso-legal)) **y comprobará que la reclamación está completa y cumple las condiciones** establecidas en la legislación estadounidense[[11]](#footnote-12).

En particular, la APD verificará:

* La identidad del reclamante, y que actúa en nombre propio y no como representante de una organización gubernamental, no gubernamental o intergubernamental;
* Que el reclamante cree que se ha infringido una o varias leyes de EE. UU. si agencias de inteligencia de EE. UU. accedieron ilegalmente a datos personales de o sobre reclamante después de que aquellos fueran transmitidos desde la UE a EE. UU.;
* La reclamación contiene, por escrito (también por correo electrónico), toda la información pertinente (**que no tiene por qué demonstrar que los datos del reclamante han sido efectivamente objeto de actividades de interceptación de las comunicaciones por parte EE. UU.)**:
  + cualquier información que constituya la base de la reclamación, incluidos los detalles de la cuenta online o de la transferencia de datos personales, a los que se cree que se ha podido acceder;
  + la naturaleza de la reparación solicitada;[[12]](#footnote-13)
  + los medios específicos por los que se entiende que se han transmitido a EE. UU. datos personales de o sobre los reclamantes;
  + qué entidad o entidades del Gobierno de EE. UU. se cree que han participado en el acceso a los datos personales del reclamante o sobre él (si se conoce);
  + y cualquier otra medida que el reclamante haya adoptado para obtener la información o la reparación solicitada, y la respuesta recibida a través de esas otras medidas;
  + se refiere a datos personales de o sobre los reclamantes, que se cree que han sido transferidos a EE. UU. después del 10 de julio de 2023;
* La reclamación no es frívola, ofensiva o presentada de mala fe.

Tras esta verificación, y si la denuncia se considera completa, la APD la transmitirá, en formato

cifrado, a la **Secretaría del Comité Europeo de Protección de Datos (Secretaría del CEPD)[[13]](#footnote-14)**.

A continuación, la Secretaría citada **la transmitirá,** en formato cifrado[[14]](#footnote-15) a las autoridades estadounidenses competentes para gestionar la reclamación, a saber, el **Responsable de la Protección de Libertades Civiles** **(‘CLPO’)** de la Oficina del Director de Inteligencia Nacional[[15]](#footnote-16).

## **¿Cuál es el papel del CLPO?**

El CLPO se encarga de llevar a cabo una investigación de la reclamación para determinar si se han vulnerado las salvaguardias previstas en la O.E. 14086 u otra(s) ley(es) estadounidense(s) aplicable(s) y, en caso afirmativo, determinar la reparación vinculante adecuada[[16]](#footnote-17). El CLPO proporcionará una respuesta[[17]](#footnote-18) a la APD, a través de la Secretaría del CEPD, dentro de los plazos previstos. Esta respuesta confirmará que:

1. “La revisión o bien no identificó ninguna violación cubierta o bien el funcionario de Protección de las Libertades Civiles de la Oficina del Director de Inteligencia Nacional emitió una resolución que exigía una reparación adecuada”[[18]](#footnote-19). En su respuesta normalizada[[19]](#footnote-20), el CLPO de la ODNI no confirmará ni negará si el reclamante ha sido objeto de vigilancia ni confirmará la solución especifica que se aplicó;
2. El reclamante o un elemento de la Comunidad de Inteligencia de EE. UU. podrá solicitar la revisión de la decisión de la CLPO presentando un recurso ante el Tribunal de Revisión de Protección de Datos (“TRPD”); y
3. Si el reclamante o un elemento de la Comunidad de Inteligencia solicita la revisión por el TRDP, un abogado especial será seleccionado por el TRPD para defender los intereses del reclamante en el asunto (**“Abogado** **Especial”**).

La decisión del CLPO es vinculante para los elementos de la Comunidad de Inteligencia[[20]](#footnote-21).

El CLPO envía su respuesta a la Secretaría del CEPD en formato cifrado, que a su vez la transmitirá, también en formato cifrado, a la ADP nacional que recibió originalmente la reclamación. Esta APD, a su vez, informará al reclamante de la respuesta del CLPO (incluida una traducción del inglés, si es necesario y en la medida en que lo sea).

## **¿Cómo recurrir la decisión del CLPO?**

Los reclamantes tienen la posibilidad de recurrir la decisión del CLPO ante el **Tribunal de Revisión de la Protección de datos (“TRPD”) en un plazo de 60 días** a partir de la notificación de la respuesta del CLPO[[21]](#footnote-22) por parte de la APD nacional. Para recurrir, el reclamante puede presentar una solicitud a **su APD** en el plazo 60 días[[22]](#footnote-23). El TRPD puede investigar reclamaciones de particulares en la UE/EEE, incluida la obtención de información pertinente de elementos de la Comunidad de Inteligencia de EE. UU., y puede adoptar decisiones correctoras vinculantes.[[23]](#footnote-24)

El procedimiento de recurso seguirá un cauce y un procedimiento similares a los de la reclamación inicial: La APD transmitirá el recurso a la Secretaría del CEPD, en formato cifrado, que a su vez lo transmitirá, en formato cifrado, a la Oficina de Privacidad y Libertades Civiles (“OPCL”, por sus siglas en inglés) del Departamento de Justicia de EE. UU, que presta apoyo al TRPD, para que este pueda revisar el recurso.

En particular, el TRPD revisará las resoluciones llevadas a cabo por el CLPO (tanto si se ha producido una violación de la legislación estadounidense aplicable como en lo que respecta a la reparación adecuada) basándose, como mínimo, en el expediente de la investigación del CLPO, así como en cualquier información y alegaciones presentados por el reclamante, el Abogado Especial o un elemento la Comunidad de Inteligencia.[[24]](#footnote-25) Un panel del TRPD tiene acceso a toda la información necesaria para llevar a cabo una revisión, que puede obtener a través del CLPO (por ejemplo, el panel puede solicitar al CLPO que complemente su expediente con información adicional o conclusiones fácticas si es necesario para llevar a cabo la revisión).[[25]](#footnote-26) El Abogado Especial también tiene acceso a toda la información necesaria para desempeñar su función de asistir al panel

del TRPD en su examen de la solicitud, incluso defendiendo los intereses del reclamante en el asunto y asegurándose de que el panel del TRPD esté bien informado de los problemas y de la(s) ley(es) con respecto al asunto.

Al concluir su revisión, el TRPD podrá:

1. decidir que no hay pruebas que indiquen que se produjeron actividades de interceptación de las comunicaciones relacionadas con datos personales del reclamante;
2. decidir que las resoluciones CLPO eran jurídicamente correctas y basadas en pruebas sustanciales; o
3. si el TRPD no está de acuerdo con las resoluciones del CLPO (si se produjo una violación de la(s) ley(es) estadounidense(s) aplicable(s) o la reparación apropiada), emitir sus propias resoluciones.[[26]](#footnote-27)

La decisión del TRPD es vinculante y definitiva con respecto a la reclamación presentada[[27]](#footnote-28). En los casos en los que la revisión del TRPD haya sido desencadenada por una solicitud del reclamante[[28]](#footnote-29), se notificará al reclamante la decisión del TRPD. Una vez que el TRPD finaliza su revisión, este proporcionará al reclamante una declaración estandarizada indicando que ha finalizado su revisión, y declarando que “*la revisión o bien no identificó ninguna violación o el Tribunal de Revisión de la Protección de Datos emitió una resolución que requería una reparación adecuada*.”[[29]](#footnote-30)

El TRPD transmitirá dicha declaración, en formato cifrado, a la Secretaría del CEPD, que a su vez la transmitirá a la APD en formato cifrado. La APD notificará al reclamante la declaración del TRPD (incluida una traducción del inglés, si es necesario y en la medida en que lo sea). Esta declaración no confirmará ni negará si el reclamante ha sido objeto de vigilancia ni confirmará la solución específica que se aplicó. Cada decisión del TRPD se transmite también al CLPO.[[30]](#footnote-31)

## **¿Cuál es el papel del Departamento de Comercio de EE.UU. en relación con la información desclasificada?**

El Departamento de Comercio de EE. UU. (“**DoC”**) se pondrá periódicamente en contacto con los elementos pertinentes de la Comunidad de Inteligencia en relación con si se ha desclasificado la información relativa a la revisión de una reclamación por parte del CLPO o el TRPD. Si los elementos de la Comunidad de Inteligencia informan al DoC de que la información relativa al examen de la reclamación por parte del CLPO o el TRPD ha sido desclasificada, el DoC notificará al reclamante, a través de la Secretaría del CEPD, que a la vez lo transmitirá a la APD, que la información relativa a la revisión de su reclamación por parte de la CLPO o el TRPD, según proceda, pueda estar a disposición del reclamante en virtud de la legislación estadounidense aplicable.[[31]](#footnote-32) Una de estas leyes es la Ley estadounidense sobre la Libertad de Información (“**FOIA”**)[[32]](#footnote-33), en virtud de la cual el reclamante puede presentar una solicitud FOIA directamente a la ODNI, al elemento pertinente de la Comunidad de Inteligencia, o al Departamento de Justicia (es decir, sin pasar por la APD y la Secretaría del CEPD) para obtener información desclasificada sobre su reclamación. Las instrucciones sobre cómo presentar solicitudes FOIA están disponibles en las respectivas páginas web públicas[[33]](#footnote-34), los elementos pertinentes de la Comunidad de Inteligencia y el TRPD.[[34]](#footnote-35)

Cabe señalar que las reclamaciones de los interesados en la UE o el EEE por medio de las que aleguen determinadas infracciones de la legislación de los EE. UU. que afecten negativamente a su intimidad individual y a sus libertades civiles y que se refieran a sus datos personales transmitidos desde la UE o el EEE a los EE. UU., sólo deben presentarse al CLPO y no a las oficinas de la FOIA antes mencionadas.

1. Decisión de Ejecución C(2023) 4745 de la Comisión Europea, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos y por el que se deroga la [Directiva 95/46/EC](http://data.europa.eu/eli/dir/1995/46/oj/eng) (“**RGPD”**), sobre el nivel adecuado de protección los datos personales en el Marco de la Privacidad de los Datos entre la UE y los Estados Unidos (“**Decisión de Adecuación del** **DPF”**) de 10 de julio de 2023. Con ello, la Comisión decidió que los Estados Unidos (”**EE. UU.**”), a efectos del artículo 45 del RGPD, garantizan un nivel adecuado de protección de los datos personales transferidos desde la UE a organizaciones de los EE. UU. Que están incluidas en la “Lista del Marco de Privacidad de Datos”, mantenida y puesta a disposición del público por el Departamento de Comercio (artículo 1 de la Decisión de Adecuación), disponible en: [https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32023D1795.](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32023D1795) [↑](#footnote-ref-2)
2. Orden Ejecutiva de 7 de octubre de 2022 sobre la mejora de las salvaguardias para las actividades de interceptación de las comunicaciones de los Estados Unidos. [↑](#footnote-ref-3)
3. Las referencias a la “**UE**” que se hacen en este documento deben entenderse como referencias al “**EEE**”. [↑](#footnote-ref-4)
4. En la [O.E. 14086,](https://www.presidency.ucsb.edu/documents/executive-order-14086-enhancing-safeguards-for-united-states-signals-intelligence) complementada por el Reglamento del Fiscal General sobre el Tribunal de Revisión de la Protección de Datos; también se incluyen más especificaciones sobre este mecanismo de recurso; véase también Procedimientos de aplicación del Mecanismo de Recurso de interceptación de las comunicaciones en virtud de la Orden Ejecutiva 14086 (“Directiva de Inteligencia 126), disponible en: [https://www.dni.gov/files/documents/ICD/ICD 126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf](https://www.dni.gov/files/documents/ICD/ICD%20126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf) [↑](#footnote-ref-5)
5. Cláusulas contractuales tipo de conformidad con el artículo 46(2)(c) o (d) del RGPD, o cláusulas contractuales ad hoc de conformidad con el artículo 46(3)(a) del RGPD. [↑](#footnote-ref-6)
6. Artículo 46(2)(b) del RGPD. [↑](#footnote-ref-7)
7. Artículo 46(2)(e) del RGPD. [↑](#footnote-ref-8)
8. Artículo 46(2)(f) del RGPD. [↑](#footnote-ref-9)
9. Artículo 49 del RGPD. [↑](#footnote-ref-10)
10. O.E. 14086, Sección 4(k)(v) y Sección E(1)(c)(8) de ICD 126. [↑](#footnote-ref-11)
11. O.E. 14086, Sección 4(k)(i)-(iv). [↑](#footnote-ref-12)
12. Dicha reparación puede incluir medidas legales diseñadas para reparar completamente una violación identificada. De manera no exhaustiva, esto puede incluir medidas administrativas para subsanar infracciones de procedimiento o técnicas; la supresión de sus datos personales adquiridos sin autorización legal; la supresión de los resultados de consultas inadecuadas sobre datos personales recopilados legalmente; la restricción del acceso a sus datos personales. [↑](#footnote-ref-13)
13. Considerando 177 de la Decisión de Adecuación. [↑](#footnote-ref-14)
14. La sección E(1)(f) de la Directiva 126 de la Comunidad de Inteligencia establece que: “Si el CLPO determina que la reclamación no es una reclamación admisible porque no cumple las condiciones de la Sección E.1.c., o no cumple las condiciones de la Sección E.1.d., de la presente Directiva, el CLPO notificará por escrito a través de **comunicación electrónica cifrada y en lengua inglesa** a la autoridad pública competente de un Estado admisible las deficiencias de la reclamación”. [↑](#footnote-ref-15)
15. A efectos del presente documento, toda referencia al Responsable de la Protección de las Libertades Civiles (“CLPO”) se refiere al Responsable de la Protección de las Libertades Civiles de la Oficina Director de Inteligencia Nacional (“ODNI CLPO”). [↑](#footnote-ref-16)
16. Sección 3(c)(i)(E) y Sección 3(d)(i)(H) de la O.E. 14086. [↑](#footnote-ref-17)
17. O.E. 14086, Sección 3 (c)(i)E. [↑](#footnote-ref-18)
18. O.E. 14086, Sección 3 (c)(i)E(1). [↑](#footnote-ref-19)
19. La respuesta normalizada indicará que la “*revisión del CLPO o bien no identificó ninguna infracción cubierta o bien el Tribunal de Revisión de Protección de Datos emitió una resolución que exigía una reparación adecuada*” (O.E. 14086, Sección 3 (c)(i)E). [↑](#footnote-ref-20)
20. Sección 3(c)(H)(ii) del O.E. 14086. [↑](#footnote-ref-21)
21. Las fechas que se tendrán en cuenta para evaluar si el recurso se presentó en el plazo de 60 días serán la fecha de notificación al reclamante, por parte de la APD, de la resolución de la CLPO, y la fecha de presentación, por parte del reclamante, de su recurso ante la APD. [↑](#footnote-ref-22)
22. Considerando 177 de la Decisión de Adecuación. [↑](#footnote-ref-23)
23. Sección 3(c)(i)(E) y sección 3(d)(i)(H) del O.E. 14086. [↑](#footnote-ref-24)
24. Considerando 189 de la Decisión de Adecuación y sección 3(d)(i)(D) O.E. 14086. [↑](#footnote-ref-25)
25. Considerando 189 de la Decisión de Adecuación; sección 3(d)(iii) O.E. 14086 and sección 201.9(b) Reglamento AG. [↑](#footnote-ref-26)
26. Considerando 190 de la Decisión de Adecuación y sección 3(d)(i)(E) O.E. 14086 y sección 201.9(c)-(e) Reglamento AG. De acuerdo con la definición de “reparación adecuada”, en la sección 4(a) O.E. 14086, el TRPD debe tener en cuenta “las formas en que habitualmente se ha abordado una infracción del tipo identificado” al decidir una medida correctora para subsanar plenamente una infracción, es decir, el TRPD considerará, entre otros factores, cómo se han solucionado problemas de cumplimiento similares en el pasado para asegurarse de que la solución es eficaz y adecuada. [↑](#footnote-ref-27)
27. Considerando 191 de la Decisión de Adecuación y sección 3(d)(ii) O.E. 14086 y sección 201.9(g) Reglamento AG. [↑](#footnote-ref-28)
28. De conformidad con la sección 3(d)(i)(B) del O.E. 14086, los elementos de la Comunidad de Inteligencia también pueden presentar solicitudes de revisión de la resolución llevada a cabo por el CLPO. [↑](#footnote-ref-29)
29. Considerando 192 de la Decisión de Adecuación y sección 3(d)(i)(H) O.E. 14086 y sección 201.9(h) Reglamento AG. Por lo que se refiere a la naturaleza de la notificación, véase la sección 201.9 (h)(3) del Reglamento AG. [↑](#footnote-ref-30)
30. Considerando 192 de la Decisión de Adecuación y sección 201.9(h) Reglamento AG. [↑](#footnote-ref-31)
31. sección 3(d)(v)(C) del O.E. 14086. [↑](#footnote-ref-32)
32. Para más información sobre la FOIA; véase [https://www.dni.gov/index.php/foia.](https://www.dni.gov/index.php/foia) [↑](#footnote-ref-33)
33. [https://www.dni.gov/index.php/make-a-records-request.](https://www.dni.gov/index.php/make-a-records-request) [↑](#footnote-ref-34)
34. [https://www.justice.gov/opcl/opcl-freedom-information-act.](https://www.justice.gov/opcl/opcl-freedom-information-act) [↑](#footnote-ref-35)