Dictamen 15/2026 sobre los criterios de certificación de Europrivacy en lo que respecta a su aprobación por el Comité como Sello Europeo de Protección de Datos destinado a su uso como herramienta para las transferencias de conformidad con los artículos 42 y 46 del RGPD

Adoptado el 15 de abril de 2026

Índice

El Comité Europeo de Protección de Datos

Vistos el artículo 63, el artículo 64, apartado 2, y los artículos 42 y 46 del 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 estos datos y por el que se deroga la Directiva 95/46/CE («RGPD»),

Visto el Acuerdo sobre el Espacio Económico Europeo (en lo sucesivo, «EEE»), y en particular su anexo XI y su Protocolo n.º 37, modificado por la Decisión del Comité Mixto del EEE n.º 154/2018, de 6 de julio de 2018[1],

Vistos los artículos 10 y 22 de su Reglamento interno,

1 Los Estados miembros, las autoridades de control, el Comité Europeo de Protección de Datos («CEPD» o «Comité») y la Comisión Europea promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos («mecanismos de certificación») y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el RGPD en las operaciones de tratamiento de los responsables y los encargados, teniendo en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas[2]. Además, el establecimiento de mecanismos de certificación puede reforzar la transparencia y permitir a los interesados evaluar el nivel de protección de datos de los productos y servicios correspondientes[3].

2 Además de la adhesión de los responsables o los encargados del tratamiento sujetos al RGPD, podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados de conformidad con el artículo 42, apartado 5, de dicho Reglamento con objeto de demostrar la existencia de garantías adecuadas ofrecidas por los responsables o los encargados no sujetos al RGPD con arreglo al artículo 3 en el marco de transferencias de datos personales a terceros países u organizaciones internacionales («importadores de datos») a tenor del artículo 46, apartado 2, letra f), del RGPD[4].

3 La certificación destinada a utilizarse como herramienta para las transferencias es un nuevo mecanismo de transferencia introducido por el artículo 46 del RGPD para garantizar que, en ausencia de una decisión con arreglo a su artículo 45, apartado 3, un responsable o un encargado del tratamiento en virtud de dicho Reglamento (el «exportador de datos del EEE») solo pueda transferir datos personales a un tercer país o a una organización internacional si se ofrecen garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. En particular, de conformidad con el artículo 46, apartado 2, letra f), del RGPD, un mecanismo de certificación aprobado con arreglo a su artículo 42 podrá aportar dichas garantías adecuadas si lo acompañan compromisos vinculantes y exigibles de los importadores de datos de aplicar garantías adecuadas, incluidas las relativas a los derechos de los interesados. Los criterios de certificación son parte integrante de un mecanismo de certificación. Por consiguiente, el RGPD exige la aprobación de los criterios de un mecanismo nacional de certificación por parte de la autoridad de control competente [artículos 42, apartado 5, y 43, apartado 2, letra b), del RGPD] o, en el caso de un Sello Europeo de Protección de Datos, por parte del CEPD [artículos 42, apartado 5, y 70, apartado 1, letra o), del RGPD].

[1] Las referencias a los «Estados miembros» en el presente dictamen deben entenderse como referencias a los «Estados miembros del EEE».
[2] Artículo 42, apartado 1, del RGPD.
[3] Considerando 100 del RGPD.
[4] Artículo 42, apartado 2, del RGPD.

4 Cuando una autoridad de control desee proponer la aprobación por parte del CEPD de un Sello Europeo de Protección de Datos conforme al artículo 42, apartado 5, del RGPD, dicha autoridad de control deberá confirmar la intención del propietario del esquema de ofrecer el mecanismo de certificación en todos los Estados miembros. En este caso, la función principal del CEPD es asegurar la aplicación coherente del RGPD a través del mecanismo de coherencia a que se refieren los artículos 63, 64 y 65 del RGPD. En este marco, con arreglo al artículo 64, apartado 2, del RGPD, el CEPD aprueba los criterios de certificación.

5 Un Sello Europeo de Protección de Datos aprobado de conformidad con el artículo 42, apartado 5, del RGPD, establecido con el fin de demostrar la existencia de garantías adecuadas proporcionadas por los importadores de datos junto con compromisos vinculantes y exigibles, sirve como herramienta para cubrir las transferencias de datos de todos los Estados miembros del EEE a terceros países u organizaciones internacionales5.

6 La evaluación del CEPD de una certificación destinada a su uso como herramienta para las transferencias se lleva a cabo sobre la base de las «Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento» (las «Directrices») y su apéndice, *Guidance on certification criteria assessment* [«Orientaciones sobre la evaluación de criterios de certificación», documento en inglés] (el «Apéndice»), así como de las «Directrices 07/2022 sobre la certificación como herramienta para las transferencias» (las «Directrices sobre la certificación como herramienta para las transferencias»).

7 El CEPD constata que cada mecanismo de certificación debe abordarse individualmente y se entiende sin perjuicio de la evaluación de cualquier otro mecanismo de certificación.

8 Los mecanismos de certificación destinados a utilizarse como herramienta para las transferencias deben permitir a los importadores de datos demostrar la existencia de garantías adecuadas para asegurar que el nivel de protección de las personas físicas garantizado por el RGPD no se vea menoscabado cuando los datos personales transferidos sean objeto de tratamiento fuera del EEE 6 . Por lo tanto, sus criterios deben reflejar adecuadamente los requisitos y principios relativos a la protección de datos personales establecidos en el RGPD, a fin de garantizar que la protección conferida por dicho Reglamento se mantenga cuando se transfieran los datos personales7.

9 Al mismo tiempo, el propietario del esquema debe garantizar la conformidad y coherencia del mecanismo de certificación con cualquier norma ISO y práctica de certificación incluida o utilizada como base.

10 En consecuencia, las certificaciones deben aportar un valor añadido a los importadores de datos, al ayudarles a aplicar medidas organizativas y técnicas normalizadas y específicas para demostrar que existen las garantías adecuadas para el tratamiento de los datos personales recibidos por los exportadores de datos del EEE. En este sentido, el CEPD recuerda que el objeto de certificación, que coincide con el objetivo de evaluación durante la certificación, debe ser, en general, el tratamiento de los datos transferidos al importador de datos en el tercer país y el tránsito, en caso de que esté sometido al control del mismo importador8.

[5] Directrices 07/2022 del CEPD sobre la certificación como herramienta para las transferencias, versión 2.0, adoptadas el 14 de febrero de 2023, apartado 30.
[6] Artículo 44 del RGPD.
[7] Véase la Comunicación de la Comisión al Parlamento Europeo y al Consejo «Intercambio y protección de los datos personales en un mundo globalizado», COM(2017) 7 final, página 4.
[8] Véanse las Directrices 07/2022 del CEPD sobre la certificación como herramienta para las transferencias, versión 2.0, adoptadas el 14 de febrero de 2023, apartado 16.

11 Las certificaciones también tendrán un valor añadido para el exportador de datos, que podrá decidir basarse en la certificación obtenida por un importador de datos como herramienta para transferir datos personales de conformidad con el artículo 46, apartado 2, letra f), del RGPD y como elemento para demostrar el cumplimiento de obligaciones como las recogidas en el artículo 24, apartado 3, o el artículo 28, apartado 5, del RGPD9.

12 A este respecto, el CEPD recuerda que el exportador de datos que desee utilizar una certificación como garantía adecuada de conformidad con el artículo 46, apartado 2, letra f), del RGPD está obligado a comprobar si la certificación en la que pretende basarse es efectiva teniendo en cuenta las características del tratamiento previsto. A tal fin, el exportador de datos debe comprobar la certificación expedida para verificar si el certificado es válido y no ha expirado, si cubre la transferencia específica que debe llevarse a cabo y si el tránsito de datos personales entra en el alcance de la certificación, así como si se trata de transferencias ulteriores y se facilita la documentación adecuada al respecto10.

13 Además, el exportador de datos debe comprobar que el organismo de certificación que expide la certificación está acreditado por un organismo nacional de acreditación o una autoridad de control competente. Asimismo, el exportador de datos debe hacer referencia al uso de la certificación como herramienta para la transferencia en el contrato de tratamiento de datos de conformidad con el artículo 28 del RGPD en caso de transferencias del responsable al encargado del tratamiento o de un contrato de intercambio de datos con el importador de datos en caso de transferencias de responsable a responsable del tratamiento11. Por otro lado, debe cumplir las obligaciones específicas previstas en el artículo 13, apartado 1, letra f), del RGPD, en particular informar al interesado de las garantías adecuadas utilizadas, esto es, en caso de certificación conforme al artículo 46, apartado 2, letra f), del RGPD, el certificado recibido por el importador con arreglo a un mecanismo de certificación específico y los medios para obtener una copia del certificado y de las garantías contenidas en los criterios de certificación o donde se hayan proporcionado.

14 El CEPD acoge con satisfacción los esfuerzos realizados por los propietarios de esquemas para elaborar mecanismos de certificación que sean herramientas prácticas y puedan ser rentables para garantizar una mayor coherencia con el RGPD, así como promover el derecho a la privacidad y la protección de los datos de los interesados gracias a una mayor transparencia.

15 El CEPD recuerda que las certificaciones son herramientas voluntarias de rendición de cuentas y que la adhesión a un mecanismo de certificación no es óbice para que las autoridades de control ejerzan sus funciones y competencias a tenor del RGPD y la legislación nacional pertinente. Esto, en el contexto de las certificaciones que deben utilizarse como herramienta para las transferencias, también en lo que se refiere específicamente al respeto de las obligaciones asumidas como compromisos vinculantes y exigibles por los importadores de datos frente a los exportadores de datos, a través de instrumentos contractuales u otros instrumentos jurídicamente vinculantes, para aplicar las garantías adecuadas previstas por el mecanismo de certificación, entre otros, en lo que respecta a los derechos de los interesados.

16 El presente Dictamen tiene por objeto garantizar la aplicación coherente del RGPD, también por parte de las autoridades de control, los responsables y los encargados del tratamiento, a la luz de los elementos básicos que deben establecer los mecanismos de certificación. En particular, este Dictamen tiene por objeto evaluar los criterios de certificación destinados a

[9] Directrices 7/2022 sobre la certificación como herramienta para las transferencias, apartado 5.
[10] Directrices 7/2022 sobre la certificación como herramienta para las transferencias, apartado 20.
[11] *Ibid*.

ser utilizados como herramienta para las transferencias por parte de los importadores de datos. Por lo tanto, en el presente documento, el CEPD aborda cuestiones como el ámbito de aplicación, la aplicabilidad y la pertinencia de los criterios en caso de transferencias que tengan lugar desde todos los Estados miembros del EEE o desde cualquier exportador de datos incluido en el ámbito de aplicación del RGPD.

17 El dictamen del CEPD se centra únicamente en los criterios de certificación. El CEPD puede exigir información de alto nivel sobre los métodos de evaluación para poder evaluar exhaustivamente la posibilidad de auditoría de los criterios en el marco de su dictamen al respecto. Sin embargo, ello no conlleva ningún tipo de aprobación de dichos métodos de evaluación.

18 De conformidad con el artículo 64, apartado 2, del RGPD, en relación con el artículo 10, apartado 2, del Reglamento interno del CEPD, el dictamen del CEPD debe adoptarse en un plazo de ocho semanas a contar desde el primer día hábil posterior al momento en que la presidenta y la autoridad de control competente hayan decidido que el expediente está completo. Previa decisión de la presidenta, dicho plazo puede prorrogarse seis semanas más, teniendo en cuenta la complejidad del asunto. Si el dictamen del CEPD concluye que los criterios en cuestión no pueden aprobarse, la autoridad de control podrá volver a presentarlos para su aprobación cuando se aborden las cuestiones preocupantes expresadas en el Dictamen inicial del CEPD.

Ha aprobado el siguiente dictamen:

1 Resumen de los hechos

19 De conformidad con los artículos 42, apartado 2, y 46, apartado 2, letra f), del RGPD, las Directrices 1/2018 y las Directrices 7/2022 sobre la certificación como herramienta para las transferencias, el Centro Europeo para la Certificación y la Privacidad («el propietario del esquema») redactó la versión 82 de Europrivacy (los «criterios de certificación»).

20 El CEPD recuerda que ya había aprobado los criterios de certificación de Europrivacy (versión 60) el 10 de octubre de 2022, mediante la emisión de su Dictamen 28/2022, en que se aprueban como Sello Europeo de Protección de Datos de conformidad con el artículo 42, apartado 5, del RGPD, destinado a demostrar el cumplimiento del RGPD con arreglo al artículo 42, apartado 1, del RGPD. Este esquema no era una certificación sujeta al artículo 46, apartado 2, letra f), del RGPD destinada a las transferencias de datos.

21 El 29 de enero de 2026, la autoridad de control de Luxemburgo presentó al CEPD una versión actualizada de los criterios de certificación del Sello Europeo de Protección de Datos Europrivacy ya aprobados con un ámbito de aplicación ampliado que incluía, en particular, a los solicitantes sujetos al artículo 3, apartado 2, del RGPD, así como otras modificaciones relativas a los criterios básicos de certificación (versión 82). El CEPD ha adoptado el Dictamen 14/2026 sobre esta versión actualizada (versión 82) de los criterios de certificación de Europrivacy destinados a demostrar el cumplimiento del RGPD, de conformidad con el artículo 42, apartado 5.

22 En la misma fecha, la autoridad de control de Luxemburgo también presentó al CEPD un conjunto adicional de criterios de certificación (*The Europrivacy Certification Scheme Extension for Certifying Data Importers under Article 46*) destinado a utilizarse como herramienta para las transferencias con arreglo al artículo 46, apartado 2, letra f), del RGPD para su aprobación de conformidad con el artículo 64, apartado 2, del RGPD.

23 La decisión sobre la completitud de este expediente se adoptó el 31 de marzo de 2026.

2 Evaluación

24 El CEPD ha llevado a cabo su evaluación de los criterios de certificación destinados a ser utilizados como herramienta para las transferencias por parte de los importadores de datos para su aprobación con arreglo al artículo 42, apartado 5, leído en conjunto con el artículo 46, apartado 2, letra f), del RGPD, en consonancia con la estructura prevista en el anexo 2 de las Directrices 1/2018 (el «anexo»), su apéndice y las «Directrices sobre la certificación como herramienta para las transferencias»12.

25 El Comité destaca que, en consonancia con las condiciones establecidas en los artículos 42, apartado 2, y 46, apartado 2, letra f), del RGPD, el esquema actual está destinado a utilizarse como herramienta para la transferencia y, por tanto, los exportadores de datos en el sentido del capítulo V del RGPD (es decir, el responsable o los encargados del tratamiento sujetos al RGPD para el tratamiento en cuestión13) podrían basarse en las certificaciones expedidas con arreglo al esquema para transferir datos personales a importadores de datos certificados no sujetos al RGPD a tenor del artículo 314. Esto significa que las transferencias de datos personales al importador de datos en el tercer país solo pueden tener lugar después de que el mismo importador haya sido certificado y haya suscrito compromisos vinculantes y exigibles con el exportador de datos del EEE para aplicar las garantías adecuadas previstas en los criterios de certificación al tratar los datos personales transferidos en el ámbito de aplicación del objetivo de evaluación, también en lo que respecta a los derechos de los interesados.

26 En el contexto del presente Dictamen y con el fin de aprobar los criterios de certificación de Europrivacy destinados a utilizarse como herramienta para las transferencias, el CEPD ha evaluado la solicitud y el objetivo de la evaluación - comprobaciones y controles preliminares para importadores de datos [*Application and Target of Evaluation - Preliminary Checks and Controls for Data Importers (ADI)]*; los criterios básicos del RGPD relativos a Europrivacy para importadores de datos *[Europrivacy GDPR Core Criteria for Data Importers (GI)]* y los controles y comprobaciones de las medidas tecnológicas y organizativas [*Technical and Organizational Measures Checks & Controls (T)]*.

27 Por lo que se refiere al proceso de certificación, teniendo en cuenta la particularidad de la certificación destinada a utilizarse como herramienta para las transferencias, el CEPD destaca la necesidad de un elevado nivel de transparencia y acoge con satisfacción las aclaraciones facilitadas a este respecto en el esquema de certificación Europrivacy, según el cual las transferencias no pueden comenzar antes de que se expida la certificación. A este respecto, el CEPD constata que, antes de que tenga lugar la transferencia de datos personales, la evaluación puede llevarse a cabo con datos personales no sujetos al RGPD o con datos no personales. En caso necesario, es posible utilizar datos ficticios para evaluar criterios específicos y, una vez iniciada la transferencia de datos, el auditor volverá a evaluar dichos criterios en la siguiente «auditoría de supervisión»15.

28 El CEPD recuerda que puede ser necesario realizar algunos ajustes en la acreditación de los organismos de certificación en relación con una certificación destinada a utilizarse como herramienta para las transferencias, en consonancia con las «Directrices sobre las

[12] Véanse, en particular: secciones 3 y 4 de las Directrices 07/2022.
[13] Véanse las Directrices 05/2021 del CEPD sobre la interacción entre la aplicación del artículo 3 y las disposiciones sobre transferencias internacionales de conformidad con el capítulo V del RGPD, versión 2.0, adoptadas el 14 de febrero de 2023, apartado 9.
[14] Artículo 42, apartado 2, del RGPD.
[15] Véase *Europrivacy™/® Certification Scheme Extension for Certifying Data Importers under Article 46 GDPR, EP-CS.1.DI*, apartado 6.1.

certificaciones como herramienta para las transferencias»[16]. Sin embargo, el presente Dictamen no aborda esta cuestión, ya que no pertenece a la competencia del CEPD.

29 El CEPD también recuerda la necesidad de que los criterios de certificación se pongan a disposición de los interesados cuyos datos personales vayan a transferirse en virtud de una certificación facilitada al importador de datos, de conformidad con el artículo 42, apartado 8, del RGPD y, en particular, cuando se trate de una certificación que vaya a utilizarse como herramienta para las transferencias, con arreglo al artículo 13, apartado 1, letra f), del RGPD.

30 El Comité señala, como se aclara en las definiciones del esquema, que las referencias a las «autoridades competentes en materia de protección de datos» en cualquier punto del esquema tendrán el significado de «autoridades de protección de datos del EEE»[17].

31 Del mismo modo, el Comité señala que las referencias a la «legislación aplicable» y a la «legislación de un tercer país» aluden a la legislación aplicable al solicitante o a los datos personales objeto de tratamiento en el objetivo de evaluación, siempre y cuando dicha legislación no imponga restricciones a los derechos de protección de datos que vayan más allá de lo necesario y proporcionado en una sociedad democrática para salvaguardar uno de los objetivos enumerados en el artículo 23, apartado 1, del RGPD, sea proporcionada al objetivo perseguido, respete la esencia del derecho a la protección de datosy establezca medidas específicas para proteger los derechos fundamentales e intereses de los interesados.

2.1 Ámbito de aplicación del mecanismo de certificación y objetivo de evaluación

32 La extensión del esquema de certificación Europrivacy para la certificación de importadores de datos de conformidad con el artículo 46 *(Europrivacy Certification Scheme Extension for Certifying Data Importers under Article 46)* está destinada a la utilización conforme al artículo 42, apartado 2, y al artículo 46, apartado 2, letra f), del RGPD por parte de importadores de datos situados fuera del EEE que no estén sujetos al RGPD de conformidad con el artículo 3, con el propósito de demostrar la existencia de garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales. Así pues, su ámbito de aplicación difiere del de la certificación Europrivacy sujeta al artículo 42, apartado 1, a que se hace referencia en el apartado 3 del presente Dictamen, ya que establece criterios específicos que deben aplicarse y respetarse cuando se entrega una certificación Europrivacy a solicitantes (responsables o encargados del tratamiento) situados fuera del EEE destinados a actuar como importadores de datos.

33 El esquema de certificación Europrivacy como herramienta para las transferencias está destinado a aplicarse tanto a una transferencia única como a un conjunto de transferencias, siempre que estén estrechamente relacionadas. El esquema de certificación contiene criterios de certificación para las operaciones de tratamiento en el marco del objetivo de evaluación

[16] Véanse las Directrices 07/2022, sección 2.

[17] Según la definición de «autoridad de control competente» recogida en los criterios de Europrivacy, «autoridad competente en materia de protección de datos» se refiere a las autoridades de protección de datos del EEE. En general, hace referencia a las autoridades nacionales de protección de datos con competencias para garantizar el cumplimiento de los datos personales tratados por el objetivo de evaluación. Cuando se trata de una certificación sujeta al RGPD entregada a un importador de datos en virtud del artículo 46 del RGPD, la autoridad competente en materia de protección de datos es la del exportador de datos en el EEE, excepto para la presentación de una reclamación, en cuyo caso cualquier autoridad del EEE es competente.

realizadas con datos personales transferidos al importador de datos, incluido el tránsito cuando esté bajo el control del mismo importador[18].

34 El CEPD toma nota de que el ámbito de aplicación de este esquema de certificación no abarca a los corresponsables del tratamiento y de que, cuando la corresponsabilidad del tratamiento esté contemplada en el objetivo de evaluación, el organismo de certificación se negará a expedir la certificación[19].

2.2 Operaciones de tratamiento

35 Los criterios de certificación abordan los componentes pertinentes de las operaciones de tratamiento de los datos personales transferidos en el ámbito de aplicación del objetivo de evaluación. En particular, los criterios de certificación prevén garantías para el tratamiento de categorías especiales de datos personales (sección GI.2 de los criterios sobre tratamiento de datos especiales). A este respecto, el Comité acoge con satisfacción que los criterios de certificación (criterio GI.2.1.3 sobre garantías adicionales para el tratamiento de categorías especiales de datos personales) también exijan que el solicitante disponga de restricciones y garantías adicionales, adaptadas a la naturaleza específica de los datos y a los riesgos correspondientes, cuando en el tratamiento se incluyan categorías especiales de datos personales.

2.3 Principios por los que se rige el tratamiento de datos

36 En la sección GI.1, los criterios de certificación abordan adecuadamente los principios de protección de datos, en consonancia con los previstos en el artículo 5 del RGPD, al objeto de garantizar que el tratamiento de datos en el objetivo de evaluación sea lícito y proporcionado.

37 En particular, en el marco del criterio de certificación GI.1.1.2, el principio de limitación de la finalidad y las obligaciones que debe cumplir el solicitante para su cumplimiento están debidamente desarrollados. El CEPD señala que los datos personales transferidos solo podrían tratarse para los fines para los que se han transferido. El criterio de certificación GI.1.1.3, en consonancia con las actuales cláusulas contractuales tipo adoptadas por la Comisión Europea[20], identifica las únicas exenciones en virtud de las cuales los datos pueden tratarse posteriormente para fines distintos de aquellos para los que se recabaron inicialmente (es decir, consentimiento con conocimiento de causa previo, obligación legal, intereses vitales de los interesados y reclamaciones).

38 El CEPD también señala que el solicitante está obligado a presentar una evaluación por escrito para garantizar que la legislación y la práctica del tercer país no le impidan cumplir los criterios de Europrivacy y respetan en lo esencial los derechos y libertades fundamentales de los interesados y no exceden de lo necesario y proporcionado en una sociedad democrática para salvaguardar uno de los objetivos enumerados en el artículo 23, apartado 1, del RGPD. La entidad certificada debe revisar la evaluación siempre que los cambios normativos u organizativos puedan obstaculizar el cumplimiento de los criterios o afectar al objetivo de evaluación o a los derechos de los interesados y debe informarse al organismo de certificación (criterio GI.1.1.1).

[18] Véanse los criterios de certificación GI.11.1.5 y GI.11.1.6.
[19] *Europrivacy™/® Certification Scheme Extension for Certifying Data Importers under Article 46 GDPR, EP-CS.1.DI*, apartado 3.2.2., que también dispone claramente que la corresponsabilidad del tratamiento queda excluida del ámbito de aplicación de este esquema para los solicitantes sujetos al artículo 46.
[20] Decisión de Ejecución (UE) 2021/914 de la Comisión, de 4 de junio de 2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

2.4 Obligaciones generales de los responsables y los encargados del tratamiento

39 Los criterios de certificación reflejan las obligaciones del responsable del tratamiento de conformidad con el artículo 24 del RGPD (sección GI.4 de los criterios) y exigen la evaluación de los acuerdos contractuales entre el encargado del tratamiento y el responsable del tratamiento de conformidad con el artículo 28 del RGPD (sección GI.5 de los criterios de certificación relativa a los encargados o subencargados del tratamiento) con el objetivo de asegurar que los encargados del tratamiento de datos que participen en el tratamiento de los datos del objetivo de evaluación garanticen el mismo nivel de protección de datos que el exigido por los criterios de Europrivacy. A este respecto, el CEPD acoge con satisfacción los diferentes criterios de certificación relacionados con la participación de subencargados del tratamiento para los solicitantes que actúan como responsables o encargados del tratamiento, ya que esta distinción permite reflejar mejor la separación de funciones y responsabilidades entre los distintos agentes de la cadena de tratamiento (sección GI.5.1).

40 Los criterios de certificación exigen que todos los solicitantes designen un delegado de protección de datos, aun cuando el solicitante no esté obligado a designarlo de conformidad con el artículo 37 del RGPD. Los criterios de certificación comprueban que el delegado de protección de datos cumple los mismos requisitos que los previstos en los artículos 37 a 39 (sección GI.9 de los criterios de certificación relativa a la designación del delegado de protección de datos), a fin de garantizar que la función, las competencias y la cualificación del delegado de protección de datos que supervisa la conformidad del tratamiento de datos en el objetivo de evaluación cumplan los requisitos necesarios. Sobre este particular, el Comité señala que el nombramiento del delegado de protección de datos no es una obligación imperativa de los responsables y encargados del tratamiento en virtud del RGPD, a menos que se cumplan las condiciones previstas en el artículo 37, apartado 1, del RGPD.

41 Los criterios de certificación exigen comprobar el contenido de los registros de las actividades de tratamiento de conformidad con el artículo 30 del RGPD (sección GI.5.3 de los criterios sobre registro de las actividades de tratamiento). En relación con este extremo, el Comité acoge con satisfacción que los criterios de certificación exijan claramente que los solicitantes cooperen con las solicitudes presentadas por las autoridades de protección de datos del EEE competentes respecto de los exportadores y pongan a su disposición, previa solicitud, el registro de las actividades de tratamiento (criterio GI.5.3.5).

2.5 Derechos de los interesados

42 Los criterios de certificación abordan los derechos de los interesados en consonancia con el capítulo III del RGPD y exigen que se adopten las medidas correspondientes con el objetivo de garantizar que el tratamiento en el objetivo de evaluación respete y permita el ejercicio efectivo de los derechos de los interesados. La sección GI.3 de los criterios de certificación en materia de transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado prevé, entre otras garantías, que los interesados tengan derecho a ser informados sobre el tratamiento de los datos y sobre cómo pueden ejercer sus derechos. El CEPD acoge con satisfacción, en particular, que los criterios de certificación prevean que el solicitante disponga de procedimientos o de un mecanismo para tramitar las solicitudes de los interesados y, en caso de inacción ante la solicitud de los interesados, informe a estos de los motivos para no adoptar medidas, del derecho a presentar una reclamación ante una autoridad de protección de datos del EEE y de interponer un recurso judicial.

2.6 Medidas técnicas y organizativas y evaluación de los riesgos para los derechos y libertades de los interesados

43 Los criterios de certificación exigen la aplicación de medidas técnicas y organizativas que demuestren un nivel de seguridad adecuado al riesgo del tratamiento e incorporen la protección de datos desde el diseño y por defecto, de conformidad con los artículos 25 y 32 del RGPD (sección GI.6 de los criterios de certificación sobre protección de datos desde el diseño y por defecto, y seguridad del tratamiento) con el fin de garantizar que los datos tratados en el objetivo de evaluación gocen de la seguridad adecuada y de la protección de datos desde el diseño y por defecto. Además, los criterios de certificación constan de una sección (los criterios T sobre medidas tecnológicas y organizativas, comprobaciones y controles), en la que se abordan exhaustivamente las medidas técnicas y organizativas.

44 Los criterios de certificación exigen la aplicación de medidas para garantizar que las obligaciones de notificación de violaciones de la seguridad de los datos personales se lleven a cabo de manera oportuna y su ámbito de aplicación se ajuste a lo estipulado en los artículos 33 y 34 del RGPD (sección GI.7 de los criterios de certificación sobre gestión de violaciones de la seguridad de los datos personales).

45 A este respecto, el Comité señala que los criterios de certificación incluyen una lista detallada (criterio GI.7.1.1. sobre la obligación de documentar las violaciones de la seguridad de los datos personales) de la información que el solicitante debe documentar cuando se produzca una violación de la seguridad de los datos personales (que incluye las categorías de datos personales que se vean o puedan verse afectadas; el número aproximado de interesados que se vean o puedan verse afectados; las categorías y el número aproximado de registros de datos personales a los que se refiera o pueda referirse y las consecuencias probables de dicha violación). Además, el CEPD acoge con satisfacción que los criterios de certificación prevean claramente que, cuando sea probable que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y libertades de las personas físicas, el solicitante deberá disponer de normas, un procedimiento o un mecanismo para informar a la autoridad competente en materia de protección de datos del EEE respecto del exportador o exportadores y los interesados, en consonancia con los requisitos de los artículos 33 y 34 del RGPD (criterio GI.7.1.2 sobre la obligación del responsable del tratamiento de notificar y comunicar las violaciones de la seguridad de los datos personales y criterio GI 7.2 relativo a la comunicación de una violación de la seguridad de los datos personales al interesado).

46 El CEPD también acoge con satisfacción que los criterios de certificación exijan evaluar el riesgo para los derechos y libertades de las personas físicas del tratamiento de datos cubierto por el objetivo de evaluación, previendo la participación de la autoridad competente en materia de protección de datos en el EEE respecto del exportador o exportadores, de conformidad con el artículo 35 del RGPD (sección GI.8 de los criterios de certificación sobre la obligación de evaluar si se requiere una evaluación de impacto relativa a la protección de datos).

2.7 Criterios para demostrar la existencia de garantías adecuadas para las transferencias de datos personales

47 Los criterios de certificación exigen identificar todas las transferencias de datos personales a terceros países y a organizaciones internacionales incluidas en el objetivo de evaluación y justificar la elección de un mecanismo de transferencia de datos que ofrezca garantías adecuadas y acordes con las previstas en el capítulo V del RGPD (sección GI.10 de los criterios sobre transferencias de datos personales a terceros países u organizaciones

internacionales). El CEPD constata que estos criterios de certificación se aplicarán en caso de «transferencias ulteriores» de los datos personales incluidos en el objetivo de evaluación, ya sea al mismo tercer país en el que esté situado el solicitante o a otro tercer país. El Comité acoge con satisfacción que estos criterios de certificación exijan específicamente que el solicitante cuente con una descripción o un registro claros de todos los flujos de datos personales incluidos en el ámbito de aplicación del objetivo de evaluación y las transferencias identificadas a terceros países y a organizaciones internacionales, y que adopte el motivo adecuado para la transferencia de datos personales en consonancia con los recogidos en el capítulo V del RGPD, teniendo en cuenta la obligación de no socavar el nivel de protección de los datos personales previsto en el EEE.

48 El CEPD también señala que los criterios de certificación requieren que el solicitante haya realizado una evaluación de impacto de la transferencia y, en caso necesario, haya adoptado medidas complementarias para garantizar que no se menoscabe el nivel de protección de los datos transferidos (criterio GI.10.1.5).

3 Criterios adicionales para un Sello Europeo de Protección de Datos destinado a utilizarse como herramienta para las transferencias

49 De conformidad con las Directrices sobre la certificación como herramienta para las transferencias, el esquema de certificación debe garantizar que el importador de datos «haya evaluado las normas y prácticas del tercer país en el que opera y si impiden al importador cumplir sus compromisos en el marco de la certificación». A este respecto, el Comité señala que el criterio ADI.2.1.5 define las condiciones que deben cumplir los solicitantes a la hora de definir el objetivo de evaluación durante la revisión de su solicitud de certificación. En particular, exige al organismo de certificación que, antes de proceder a una auditoría de certificación, compruebe que el solicitante puede demostrar que la legislación y la práctica del tercer país no obstaculizan el cumplimiento de los requisitos de certificación. De no ser así, el proceso de certificación se detendrá durante la fase de solicitud.

50 El Comité también señala que, en virtud del criterio GI.11.1.3, el solicitante debe analizar las leyes y prácticas del tercer país e identificar el posible impacto en los derechos y libertades del interesado cuyos datos puedan importarse y disponer de normas, procedimientos o políticas para poner su análisis escrito de las leyes y prácticas locales a disposición del organismo de certificación y de las autoridades competentes en materia de protección de datos que así lo soliciten.

51 Además, de conformidad con las Directrices sobre la certificación como herramienta para las transferencias, los criterios de certificación establecen que, en caso necesario, el solicitante deberá haber adoptado medidas complementarias para garantizar que no se menoscabe el nivel de protección de los datos personales transferidos y que, cuando esto no sea posible, el importador de datos deberá informar al exportador de datos y la transferencia de datos personales habrá de suspenderse o interrumpirse (criterio GI.11.1.3).

52 Asimismo, el Comité señala que el esquema Europrivacy, de conformidad con el artículo 42, apartado 2, del RGPD, prevé que el importador y el exportador de datos suscriban un contrato que recoja los compromisos vinculantes y exigibles pertinentes antes de que tenga lugar cualquier transferencia y establece un modelo de dicho contrato. Sobre este particular, el CEPD toma nota de que, en consonancia con las Directrices sobre la certificación como herramienta para las transferencias, los criterios de certificación incluyen una lista detallada

del contenido de los compromisos vinculantes y exigibles que debe adoptar el solicitante frente a cada exportador del EEE, entre ellos, la obligación de reconocer el derecho de los interesados como terceros beneficiarios a hacer cumplir frente al importador de datos titular de una certificación las normas de la certificación, a cooperar con las autoridades de protección de datos del EEE competentes respecto de los exportadores de datos (lo que implica, en particular, aceptar sus auditorías e inspecciones, tener en cuenta su asesoramiento y cumplir sus decisiones), a acatar cualquier decisión vinculante en materia de certificación emitida en la jurisdicción y los órganos jurisdiccionales de los Estados miembros del EEE, a tratar los datos recibidos únicamente mientras el certificado sea válido y a devolver o suprimir los datos recibidos si se retira el certificado. Los criterios de certificación también prevén la obligación del solicitante de garantizar que carece de motivos para creer que las leyes y prácticas del tercer país aplicables al tratamiento en el objetivo de evaluación, incluidos los requisitos de divulgación de datos personales o las medidas que autoricen el acceso por parte de las autoridades públicas, le impiden cumplir los compromisos contraídos en virtud de la certificación y que informará al exportador de datos de cualquier cambio pertinente en la legislación o la práctica a este respecto (criterio GI.11.1.1 sobre compromisos vinculantes y exigibles para los importadores de datos).

4 Conclusiones/recomendaciones

53 En conclusión, el CEPD considera que los criterios de certificación de Europrivacy destinados a utilizarse como herramienta para las transferencias son coherentes con el RGPD y los aprueba en virtud de la función del Comité definida en el artículo 70, apartado 1, letra o), del RGPD, lo que da lugar a una certificación común (Sello Europeo de Protección de Datos) destinada a utilizarse como herramienta para las transferencias.

54 El CEPD considera que los criterios de certificación forman parte integrante del esquema de certificación, incluirá el esquema de certificación Europrivacy en el registro público de mecanismos de certificación y sellos y marcas de protección de datos y pondrá los criterios a disposición del público de conformidad con el artículo 42, apartado 8, del RGPD.

5 Observaciones finales

55 El presente Dictamen se dirige a la autoridad de control de Luxemburgo y se hará público, como dispone el artículo 64, apartado 5, letra b), del RGPD.

Por el Comité Europeo de Protección de Datos

La Presidenta

Anu Talus