Dictamen 14/2026 sobre los criterios de certificación de Europrivacy en lo que respecta a su aprobación por el Comité como Sello Europeo de Protección de Datos de conformidad con el artículo 42, apartado 5, 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 el artículo 42 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,

Considerando lo siguiente:

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 escala 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 por parte de los responsables y los encargados del tratamiento, teniendo en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas. 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.

2. 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 [artículo 42, apartado 5, y artículo 43, apartado 2, letra b), del RGPD] o, en el caso de un Sello Europeo de Protección de Datos, por parte del CEPD [artículo 42, apartado 5, y artículo 70, apartado 1, letra o), del RGPD].

3. 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.

4. 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, la evaluación del CEPD se lleva a cabo tomando como base 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* [«Guía para la evaluación de los criterios de certificación», documento en inglés] (el «Apéndice»), cuyo período de consulta pública finalizó el 26 de mayo de 2021.

[1] Las referencias a los «Estados miembros» en el presente documento deben entenderse como referencias a los «Estados miembros del EEE».

5. Por consiguiente, 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.

6. Los mecanismos de certificación deben permitir a los responsables y a los encargados del tratamiento demostrar el cumplimiento del RGPD. Por lo tanto, sus criterios deben reflejar adecuadamente los requisitos y principios relativos a la protección de datos personales establecidos en el RGPD y contribuir a su aplicación coherente.

7. 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.

8. Como resultado, las certificaciones deben aportar un valor añadido a los responsables y a los encargados del tratamiento, al ayudarles a poner en práctica medidas técnicas y organizativas normalizadas y específicas que puedan facilitar y mejorar de manera demostrable la conformidad con el RGPD de las operaciones de tratamiento, teniendo en cuenta las necesidades específicas del sector.

9. 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.

10. El CEPD recuerda que las certificaciones son herramientas voluntarias de rendición de cuentas y que la adhesión a un mecanismo de certificación no reduce la responsabilidad de los responsables o los encargados del tratamiento de cumplir el RGPD ni es óbice para que las autoridades de control ejerzan sus funciones y competencias a tenor del RGPD y la legislación nacional pertinente.

11. En este Dictamen, el CEPD aborda cuestiones como el ámbito de aplicación de los criterios y su aplicabilidad y pertinencia en todos los Estados miembros.

12. El presente 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.

13. En virtud del artículo 64, apartado 2, del RGPD, leído en conjunto con el artículo 10, apartado 2, del Reglamento interno del CEPD, el Dictamen del Comité se adoptará 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

14. De conformidad con el artículo 42, apartado 5, del RGPD y las Directrices, el Centro Europeo de Certificación y Privacidad (el «propietario del esquema») elaboró los criterios de certificación de Europrivacy (versión 82) (los «criterios de certificación»).

15. El 29 de enero de 2026, la autoridad de control de Luxemburgo presentó los criterios de certificación de Europrivacy (versión 82) al CEPD para su aprobación de conformidad con el artículo 64, apartado 2, del RGPD.

16. La decisión sobre la completitud del expediente se adoptó el 31 de marzo de 2026.

17. 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, como Sello Europeo de Protección de Datos de conformidad con el artículo 42, apartado 5, del RGPD («Dictamen anterior del CEPD»).

18. El presente Dictamen aborda la versión modificada de los criterios de certificación de Europrivacy (versión 82). En primer lugar, el Comité señala que, en esta versión de los criterios de certificación, actualmente presentada al CEPD, el ámbito de aplicación se ha ampliado para incluir a los solicitantes sujetos al artículo 3, apartado 2, del RGPD, para lo cual se ha introducido un criterio sobre posibles conflictos con la legislación de terceros países. Además, el Comité destaca que algunos de los criterios de certificación de Europrivacy aprobados por el CEPD en 2022 se han ajustado, perfeccionado o aclarado en su versión modificada (versión 82). Estas modificaciones se refieren, en particular, a: la designación de un representante en el EEE y la cooperación con las solicitudes presentadas por las autoridades de protección de datos competentes en el EEE; el informe de evaluación de cumplimiento de obligaciones nacionales («NOCAR»), el tratamiento ulterior, las garantías que acompañan al tratamiento de categorías especiales de datos personales, los derechos de los interesados, la participación de subencargados del tratamiento, la gestión de las violaciones de la seguridad de los datos, la evaluación de riesgos del tratamiento de datos y la política y los requisitos de seguridad.

19. El CEPD subraya que la modificación de los criterios de certificación ya aprobados en 2022 afectará a las certificaciones expedidas hasta la fecha, así como a los procesos de certificación en curso. Por lo tanto, debe gestionarse de manera adecuada y transparente un período de transición entre los sellos europeos de protección de datos expedidos con arreglo a los criterios de certificación aprobados con el Dictamen anterior del CEPD (versión 60) y los expedidos con arreglo a los criterios de certificación (versión 82), evaluados en el presente Dictamen. A este respecto, el Comité entiende, sobre la base de la documentación facilitada por el propietario del esquema, que todos los procesos de certificación en curso deben haber concluido a finales de 2026 y que, a partir de entonces, los criterios de certificación aprobados con el Dictamen anterior del CEPD (versión 60) ya no podrán utilizarse para expedir nuevos certificados. Los certificados expedidos hasta la fecha seguirán siendo válidos hasta el final de su período de validez de tres años y se renovarán con arreglo a los criterios de certificación (versión 82). Por lo tanto, al finalizar el año 2029, los criterios de certificación aprobados con el Dictamen anterior del CEPD (versión 60) serán plenamente sustituidos por los criterios de certificación (versión 82). Además, el propietario del esquema pondrá a disposición del público la información relativa a este plan de transición. Puede que sea necesario realizar algunos ajustes en la acreditación de los organismos de certificación, pero el presente Dictamen no aborda esta cuestión, ya que no forma parte de las competencias del CEPD.

20. El esquema de certificación Europrivacy en general no está destinado a utilizarse como herramienta para las transferencias de conformidad con el artículo 42, apartado 2, y el

artículo 46, apartado 2, letra f), del RGPD. El 29 de enero de 2026, la autoridad de control de Luxemburgo también presentó al CEPD, para su aprobación de conformidad con el artículo 64, apartado 2, del RGPD, un conjunto adicional de criterios de certificación (*The Europrivacy Certification Scheme Extension for Certifying Data Importers under Article 46*) cuyo ámbito de aplicación abarca a los responsables y los encargados del tratamiento situados fuera del EEE que no están directamente sujetos al RGPD de conformidad con su artículo 3, apartado 2, pero que llevan a cabo el tratamiento de datos personales recibidos de otro responsable o encargado del tratamiento que sí está sujeto al RGPD. Sobre este conjunto de criterios de certificación destinados a utilizarse como herramienta para las transferencias de conformidad con el artículo 46, apartado 2, letra f), del RGPD, el CEPD ha adoptado el Dictamen 15/2026.

2 Evaluación

21. El CEPD ha llevado a cabo su evaluación de los criterios de certificación para su aprobación con arreglo al artículo 42, apartado 5, del RGPD, en consonancia con la estructura prevista en el anexo 2 de las Directrices (el «Anexo») y su Apéndice.

22. En el contexto del presente Dictamen y con el fin de aprobar los criterios de certificación de Europrivacy, el CEPD ha evaluado la solicitud y el objetivo de la evaluación - comprobaciones y controles preliminares [*Application and Target of Evaluation Preliminary Checks and Controls (A)]*; los criterios básicos del RGPD relativos a Europrivacy [*Europrivacy GDPR Core Criteria (G)*] y los controles y comprobaciones de las medidas tecnológicas y organizativas [*Technological and Organisational Measures Checks and Controls (T)*], facilitados junto con los criterios de certificación.

23. Además, el Comité señala a este respecto que no aprobó las «comprobaciones y controles contextuales complementarios»[2], facilitados junto con los criterios de certificación aprobados en virtud del Dictamen anterior del CEPD (versión 60), destinados a garantizar que el tratamiento de datos incluidos en el objetivo de evaluación cumpla los requisitos específicos del ámbito y de la tecnología[3], y que dichas «comprobaciones y controles contextuales complementarios» ya no están presentes en la documentación actualizada facilitada en el contexto del presente Dictamen.

24. 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»[4].

25. Con respecto a las definiciones de «legislación de un tercer país», el Comité entiende que se refiere 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

[2] El CEPD no aprobó las «comprobaciones y controles contextuales complementarios» en su Dictamen anterior.
[3] Dictamen anterior del CEPD, apartados 7 y 8.
[4] Según la definición 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 hacer cumplir la normativa aplicable al tratamiento de los datos personales comprendidos en 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.

una sociedad democrática para salvaguardar uno de los objetivos enumerados en el artículo 23, apartado 1, del RGPD, sea proporcionada al objetivo perseguido, respete en lo esencial el derecho a la protección de datos y establezca medidas específicas para proteger los derechos e intereses fundamentales de los interesados.

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

26. El CEPD recuerda[5] que el esquema de certificación Europrivacy es de carácter general, en tanto en cuanto va dirigido a una amplia variedad de operaciones de tratamiento realizadas por responsables y encargados del tratamiento de diversos sectores de actividad.

27. El Comité acoge con satisfacción que, en la documentación relacionada con el ámbito de aplicación de este esquema de certificación facilitada por la autoridad de control de Luxemburgo, la versión modificada del esquema Europrivacy se aplique a: **i)** los responsables y los encargados del tratamiento establecidos en la Unión Europea (UE) o en el Espacio Económico Europeo (EEE); **ii)** los responsables y los encargados del tratamiento establecidos fuera del EEE que estén sujetos al RGPD de conformidad con su artículo 3, apartado 2, ya sea porque ofrecen bienes o servicios a interesados en el EEE o porque supervisan el comportamiento de los interesados en el EEE[6]. La aplicabilidad de los criterios se define atendiendo a la función y las responsabilidades del solicitante.

28. Con respecto a los solicitantes sujetos al artículo 3, apartado 2, del RGPD que se encuentren en un tercer país y no estén sujetos a una decisión de adecuación que abarque el objetivo de evaluación, el criterio A.2.1.6 determina las condiciones que deben cumplirse al definir el objetivo de evaluación durante la revisión de su solicitud de certificación. En particular, antes de proceder a una auditoría de certificación, este criterio exige al organismo de certificación comprobar que el solicitante puede demostrar que la legislación y la práctica del tercer país no obstaculizan el cumplimiento por parte del solicitante de los requisitos de certificación. De no ser así, el proceso de certificación se detendrá durante la fase de solicitud.

29. El Comité señala que un responsable del tratamiento puede presentar al proceso de certificación de Europrivacy un objetivo de evaluación que esté sujeto a la corresponsabilidad del tratamiento (criterio A.2.1.5). En caso de que el objetivo de evaluación esté sujeto a la corresponsabilidad del tratamiento, el Comité desea subrayar que el organismo de certificación acreditado tendrá que llevar a cabo con detenimiento el proceso de solicitud para garantizar que el objetivo de evaluación sea significativo y que el solicitante sea plenamente responsable de que dicho objetivo de evaluación cumpla todas las obligaciones en virtud del RGPD que el esquema de certificación pretende demostrar. En consecuencia, el acuerdo celebrado entre el solicitante y los demás corresponsables del tratamiento que participan en el objetivo de evaluación para definir sus respectivas responsabilidades en el cumplimiento de las obligaciones derivadas del RGPD podría, dependiendo del contexto de las actividades de tratamiento del objetivo de evaluación, impedir al solicitante cumplir los criterios de certificación.

2.2 Operaciones de tratamiento

30. Como señaló el CEPD en su Dictamen anterior, los criterios de certificación abordan los componentes pertinentes de las operaciones de tratamiento (datos, sistemas y tratamiento)

[5] Dictamen anterior del CEPD, apartado 6.
[6] Véanse las Directrices 3/2018 del CEPD relativas al ámbito territorial del RGPD (artículo 3), versión 2.1, adoptadas el 12 de noviembre de 2019, sección 2.

con respecto al ámbito general del esquema de certificación. En particular, los criterios de certificación permiten identificar categorías especiales de datos, tal como se definen en el artículo 9 del RGPD (sección G.2 relativa a los criterios sobre tratamiento de datos especiales).

2.3 Licitud del tratamiento

31. Como declaró el CEPD en su Dictamen anterior sobre los criterios de certificación ya aprobados (versión 60), estos exigen que se comprueben tanto la licitud del tratamiento de datos para cada operación de tratamiento individual en el objetivo de evaluación como los requisitos de una base jurídica, tal como se define en el artículo 6 del RGPD (sección G.1 de los criterios sobre la licitud del tratamiento de datos). En particular, el Comité acoge con satisfacción que los criterios de certificación actualizados exijan que el consentimiento de los interesados abarque cada uno de los fines para los que se lleva a cabo el tratamiento y que la retirada del consentimiento no dé lugar a un perjuicio para el interesado.

32. Asimismo, como se señala en el Dictamen anterior del CEPD, los criterios de certificación exigen comprobar los requisitos específicos de las condiciones en las que, de conformidad con el artículo 9, apartado 2, del RGPD, se permite el tratamiento de categorías especiales de datos personales (sección G.2.1 de los criterios sobre tratamiento de datos especiales), así como proporcionar limitaciones y garantías adicionales para los derechos y libertades del interesado. Los criterios de certificación también exigen comprobar los requisitos de las condiciones definidas en el artículo 10 del RGPD para el tratamiento de datos personales relativos a condenas e infracciones penales (sección G.2.2 de los criterios), cuando proceda. A este respecto, el Comité también acoge con satisfacción que los criterios de certificación actualizados (criterio G.2.1.3 sobre garantías adicionales para el tratamiento de categorías especiales de datos personales) también exijan que el solicitante disponga de restricciones y salvaguardias adicionales, adaptadas a la naturaleza específica de los datos y a los riesgos correspondientes, cuando el tratamiento afecte a categorías especiales de datos personales.

33. Además, en lo que respecta a los solicitantes sujetos al artículo 3, apartado 2, del RGPD establecidos en un tercer país que no estén sujetos a una decisión de adecuación que abarque el objetivo de evaluación, los criterios de certificación actualizados exigen que el solicitante presente un informe de evaluación elaborado por un experto jurídico que indique que la legislación y la práctica nacionales del tercer país no impiden el cumplimiento de sus obligaciones en materia de protección de datos en virtud del RGPD. Del mismo modo, la evaluación debe confirmar que la legislación nacional del tercer país no impone 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, es proporcionada al objetivo perseguido, respeta en lo esencial el derecho a la protección de datos y establece medidas específicas para proteger los derechos e intereses fundamentales de los interesados. También debe revisarse cuando 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 G.1.1.5).

34. En este contexto, los criterios de certificación actualizados aclaran en sus orientaciones que, cuando un solicitante esté establecido fuera del EEE y se beneficie de una decisión de adecuación pertinente para el tratamiento realizado en el objetivo de evaluación, el cumplimiento de este requisito podrá demostrarse mediante un informe simplificado. Según estos criterios, dicho informe debería haber evaluado si la decisión de adecuación está en vigor y documentar las razones por las que el objetivo de evaluación entra en el ámbito de aplicación de la decisión de adecuación (criterio G.1.1.5, letra F).

2.4 Principios por los que se rige el tratamiento de datos

35. El CEPD recuerda que los criterios de certificación abordan adecuadamente los principios de protección de datos de conformidad con el artículo 5 del RGPD. En particular, los criterios de certificación actualizados amplían y desarrollan el principio de limitación de la finalidad, ya que incorporan un criterio específico que exige demostrar que los datos personales no son objeto de un tratamiento ulterior incompatible con dicha finalidad, que la licitud de cualquier tratamiento ulterior debe evaluarse por separado y que la compatibilidad de la finalidad debe evaluarse y documentarse debidamente para efectuar un tratamiento ulterior de los datos (criterio G.1.1.6).

2.5 Obligaciones generales de los responsables y los encargados del tratamiento

36. El CEPD recuerda que los criterios de certificación[7] reflejan las obligaciones del responsable del tratamiento de conformidad con el artículo 24 del RGPD (G.4 sobre la responsabilidad del responsable del tratamiento) 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 G.5 de los criterios relativa a los encargados o subencargados del tratamiento).

37. Además, el Comité acoge con satisfacción que se haya añadido a los criterios de certificación la obligación del solicitante sujeto al artículo 3, apartado 2, del RGPD de designar una oficina o un representante en el EEE de conformidad con el artículo 27 del RGPD cuyos datos de contacto estén disponibles en el sitio web del solicitante (criterio G.4.1.4). El Comité toma nota de estos criterios de certificación y recuerda que no siempre se trata de una obligación imperativa para los responsables y los encargados del tratamiento de conformidad con el RGPD, por lo que deben tenerse en cuenta las condiciones establecidas en el artículo 27 de dicho Reglamento.

38. Asimismo, el CEPD señala que, como se indica en su Dictamen anterior, 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 comprueban que el delegado de protección de datos cumple los requisitos establecidos en los artículos 37 a 39 (sección G.9 de los criterios relativos al delegado de protección de datos).

39. Del mismo modo, 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 G.5.3 de los criterios sobre registro de las actividades de tratamiento). A este respecto, el Comité acoge con satisfacción que los criterios de certificación actualizados exijan a los solicitantes sujetos al artículo 3, apartado 2, del RGPD su cooperación con las solicitudes presentadas por las autoridades de protección de datos competentes del EEE y que pongan a disposición de estas el registro de las actividades de tratamiento cuando así se lo soliciten (criterio G.5.3.5).

40. En este mismo orden de cosas, el CEPD señala que se han incluido algunos criterios de certificación adicionales en relación con la contratación de subencargados del tratamiento para los solicitantes que actúan como responsables o encargados del tratamiento (sección

[7] Dictamen anterior del CEPD, apartado 15.

G.5.1.2 sobre la contratación de subencargados del tratamiento). Esta distinción permite reflejar mejor la separación de funciones y responsabilidades entre los agentes de la cadena de tratamiento.

2.6 Derechos de los interesados

41. Al igual que en su Dictamen anterior, el CEPD recuerda que los criterios de certificación abordan adecuadamente el derecho del interesado a la información de conformidad con el capítulo III del RGPD y exigen que se adopten las medidas correspondientes[8]. Los criterios de certificación también exigen el establecimiento de medidas que prevean la posibilidad de intervenir en la operación de tratamiento con el fin de garantizar los derechos de los interesados y permitir correcciones, supresiones o restricciones (sección G.3 de los criterios sobre los derechos de los interesados).

42. Además, el CEPD acoge con satisfacción las mejoras que se han introducido en los criterios de certificación en lo que respecta a la información que debe facilitarse a los interesados (sección G.3.2 sobre la información que debe facilitarse cuando los datos personales se han obtenido del interesado y sección G.3.3 sobre la información que debe facilitarse cuando los datos personales no se han obtenido del interesado); las modalidades de comunicación a los interesados [9] y para el ejercicio de sus derechos [10] (sección G.3.1 sobre información transparente, comunicación y modalidades para el ejercicio de los derechos de los interesados); el derecho de acceso (sección G.3.4 sobre el derecho de acceso del interesado), a la supresión [sección G.3.6 sobre el derecho de supresión («derecho al olvido»)], a la limitación del tratamiento (criterio G.3.7.1 sobre el derecho a la limitación del tratamiento); la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento (criterio G.3.8.2 sobre la obligación de informar a los interesados sobre los destinatarios cuando se solicite); el derecho de oposición (sección G.3.10 sobre el derecho de oposición) y el derecho a no ser objeto de una decisión individual automatizada, incluida la elaboración de perfiles (sección G.3.11 sobre el derecho a no ser objeto de una decisión individual automatizada, incluida la elaboración de perfiles).

2.7 Riesgos para los derechos y las libertades

43. El CEPD ya ha señalado en su Dictamen anterior que los criterios de certificación requieren la evaluación del riesgo que supone para los derechos y libertades de las personas físicas el tratamiento de datos del objetivo de evaluación, de conformidad con el artículo 35 del RGPD (sección G.8 de los criterios sobre la obligación de evaluar si se requiere una evaluación de impacto relativa a la protección de datos)[11].

44. El CEPD acoge con satisfacción los cambios introducidos en los criterios de certificación con el fin de establecer que el solicitante debe haber evaluado, con una metodología repetible,

[8] Dictamen anterior del CEPD, apartado 19.
[9] Por ejemplo, el criterio G.3.1.1 sobre la obligación de informar en un lenguaje claro profundiza en la información sobre el tratamiento de datos facilitada por el solicitante al interesado, que ahora incluye que i) debe facilitarse por escrito o por otros medios, ii) debe estar disponible en la lengua o lenguas oficiales del solicitante y iii) debe estar disponible en la lengua de los interesados destinatarios.
[10] Así, el criterio G.3.1.3 sobre la garantía de una gestión y un registro adecuados de los derechos de los interesados exige ahora que el solicitante disponga de un procedimiento o un mecanismo para confirmar también la recepción de la solicitud al interesado y conservar registros de las solicitudes del interesado con la fecha de recepción.
[11] Dictamen anterior del CEPD, apartado 20.

los riesgos que plantea el tratamiento, que pueden afectar a los derechos y libertades de las personas físicas (sección G.6.2.4 sobre la evaluación de riesgos para el tratamiento de datos).

45. Además, el CEPD acoge con satisfacción las adiciones y los detalles adicionales que se introducen en los criterios de certificación. Por ejemplo, el CEPD toma nota de la adición realizada al proceso de evaluación de impacto relativa a la protección de datos en aquellas situaciones en las que el solicitante no está obligado a realizar dicha evaluación (sección G.8.2.1 sobre los requisitos del proceso de evaluación de impacto relativa a la protección de datos).

2.8 Medidas técnicas y organizativas que garantizan la protección

46. Como se señala en el Dictamen anterior del CEPD, los criterios de certificación exigen la aplicación de medidas técnicas y organizativas que garanticen la confidencialidad, la integridad y la disponibilidad de las operaciones de tratamiento. Los criterios también exigen la introducción de medidas técnicas para aplicar la protección de datos desde el diseño y por defecto, de conformidad con los artículos 25 y 32 del RGPD (sección G.6 de los criterios sobre protección de datos desde el diseño y por defecto y seguridad del tratamiento, sección G.6.2 de los criterios sobre seguridad del tratamiento y sección sobre criterios T)[12]. A este respecto, el Comité acoge con satisfacción que los criterios de certificación modificados aborden en mayor profundidad (sección G.6.1.2 sobre minimización de datos por defecto) las normas y procedimientos que el solicitante ha de aplicar para cumplir estos criterios.

47. Como se subraya en el Dictamen anterior del CEPD, los criterios de certificación requieren 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 G.7 de los criterios sobre gestión de violaciones de la seguridad de los datos personales).

48. A este respecto, el Comité señala que los criterios de certificación se han mejorado y desarrollado en mayor detalle. Más en particular, los criterios de certificación incluyen ahora una relación más detallada (sección G.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).

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

49. Tal y como se afirma en el Dictamen anterior del CEPD, los criterios de certificación exigen identificar todas las transferencias de datos personales a terceros países y a organizaciones

[12] Dictamen anterior del CEPD, apartado 21.

internacionales incluidas en el objetivo de evaluación y justificar la elección de un mecanismo de transferencia de datos que ofrezca garantías adecuadas a tenor del capítulo V del RGPD (sección G.10 sobre transferencias de datos personales a terceros países u organizaciones internacionales).

50. El CEPD constata que, en el caso de los solicitantes sujetos al artículo 3, apartado 2, del RGPD, estos criterios de certificación se aplicarán tanto en caso de transferencias de datos personales incluidos en el objetivo de evaluación a entidades situadas en el mismo tercer país en que se encuentre el solicitante como a entidades situadas en otro tercer país..

51. Además, el Comité acoge con satisfacción que los criterios de certificación relativos a las transferencias de datos personales se hayan desarrollado en más detalle y establezcan con mayor claridad las obligaciones del solicitante en lo que respecta a este asunto (sección G.10.1 sobre las obligaciones generales para las transferencias internacionales de datos personales a terceros países u organizaciones internacionales).

3 Criterios adicionales para un Sello Europeo de Protección de Datos

52. Según las Directrices, la evaluación debe incluir la cuestión de si los criterios permiten tener en cuenta la legislación o los supuestos en materia de protección de datos de los Estados miembros. Como se afirma en el Dictamen anterior del CEPD, la sección G.1.1.3 de los criterios de certificación requiere que el solicitante facilite dicha evaluación en un informe de evaluación de cumplimiento de obligaciones nacionales. Dicho informe incluirá una evaluación de las obligaciones nacionales aplicables al objetivo de evaluación y documentará las medidas adoptadas por el solicitante para cumplir las normas aplicables y, posiblemente, las medidas correctoras en curso. El solicitante no utilizará la lista de requisitos clave complementarios nacionales que proporciona el propietario del esquema para cada país como si fuese una relación exhaustiva de obligaciones nacionales pertinentes para el objetivo de evaluación. La lista indicativa de los requisitos mínimos de comprobaciones y controles complementarios facilitada por el propietario del esquema no constituye un criterio de certificación en el ámbito del presente Dictamen.

53. El Comité acoge con satisfacción los ajustes realizados en el informe de evaluación de cumplimiento de obligaciones nacionales, en los criterios actualizados (sección G.1.1.3 sobre la evaluación del cumplimiento de obligaciones nacionales). En particular, ahora se aclara que el solicitante debe documentar en un informe de evaluación de cumplimiento de obligaciones nacionales la evaluación realizada sobre la conformidad del tratamiento de datos con las obligaciones nacionales complementarias del EEE en materia de protección de datos personales aplicables al solicitante. Concretamente, este informe debe contener, entre otros, una identificación clara del objetivo de evaluación que se ha evaluado, la lista de obligaciones complementarias nacionales del EEE en materia de protección de datos identificadas aplicables al objetivo de evaluación, así como la evaluación de la conformidad del objetivo de evaluación con las obligaciones complementarias nacionales del EEE en materia de protección de datos identificadas. El Comité considera que, en caso de que el solicitante esté establecido fuera del EEE y esté sujeto al artículo 3, apartado 2, del RGPD, las obligaciones nacionales de protección de datos del EEE aplicables al objetivo de evaluación deben determinarse en función de la ubicación de los interesados a los que el solicitante ofrezca bienes o servicios o cuyo comportamiento esté siendo supervisado.

4 Conclusiones/recomendaciones

54. En conclusión, el CEPD considera que los criterios de certificación de Europrivacy 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). 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