Dictamen del Comité (art. 64)

Dictamen 28/2022 sobre los criterios de certificación de Europrivacy en cuanto a su aprobación por el Comité como Sello Europeo de Protección de Datos conforme al artículo 42, apartado 5 (RGPD)

Adoptado el 10 de octubre de 2022

Translations proofread by EDPB Members.
This language version has not been proofread yet.

El Comité Europeo de Protección de Datos

Vistos el artículo 63, el artículo 64, apartado 2, y el artículo 42 del Reglamento 2016/679/UE 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 (en lo sucesivo, «RGPD»),

Visto el Acuerdo sobre el Espacio Económico Europeo (en lo sucesivo, el «EEE») y, en particular, su anexo XI y su protocolo 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 (en adelante «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 (en adelante «mecanismos de certificación») y de sellos y marcas de protección de datos, a fin de demostrar el cumplimiento del RGPD en las operaciones de tratamiento por parte de los responsables y encargados del tratamiento, teniendo en cuenta las necesidades 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) Los criterios de certificación son parte integrante de un mecanismo de certificación. En consecuencia, el RGPD exige la aprobación de los criterios de un mecanismo de certificación nacional 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].

(3) Cuando una autoridad de control (en lo sucesivo, «AC») quiera proponer la aprobación por parte del CEPD de un sello europeo de protección de datos conforme al artículo 42, apartado 5, del RGPD, la AC deberá confirmar la intención del titular del plan de ofrecer un mecanismo de certificación en todos los Estados miembros. En este caso, la función principal del CEPD es asegurar una aplicación coherente del RGPD a través del mecanismo de coherencia mencionado en 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) La finalidad del presente Dictamen es garantizar la aplicación coherente del RGPD, tanto por parte de las AC como de los responsables y encargados del tratamiento teniendo en cuenta los elementos básicos que los mecanismos de certificación deben desarrollar. 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» (en adelante,

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

las «Directrices») y su apéndice «Guidance on certification criteria assessment» [solo en inglés] (en adelante el «Apéndice»), cuyo período de consulta pública finalizó el 26 de mayo de 2021.

(5) En consecuencia, el CEPD reconoce que cada mecanismo de certificación debe abordarse de forma individual y sin perjuicio de la evaluación de cualquier otro mecanismo de certificación.

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

(7) Al mismo tiempo, el titular del plan debe garantizar la adaptación y conformidad del mecanismo de certificación con cualquier norma ISO y práctica de certificación incluida o utilizada como base.

(8) Por lo tanto, las certificaciones deben aportar valor a los responsables y encargados, ayudándoles a implementar medidas técnicas y de organización estandarizadas y específicas que se demuestre que pueden facilitar y mejorar la conformidad de las operaciones de tratamiento respecto al RGPD, teniendo en cuenta las necesidades específicas del sector.

(9) El CEPD acoge con satisfacción los esfuerzos realizados por los titulares de planes para elaborar mecanismos de certificación que sean herramientas prácticas y potencialmente rentables para garantizar una mayor coherencia con el RGPD y fomentar el derecho a la privacidad y la protección de los datos de los interesados mejorando la transparencia.

(10) El CEPD recuerda que las certificaciones son herramientas de rendición de cuentas voluntarias, y que el hecho de aplicar un mecanismo de certificación no reduce la responsabilidad de los responsables y encargados del tratamiento respecto al RGPD ni impide que las autoridades de control ejerzan sus tareas y poderes conforme al RGPD y la legislación nacional aplicable.

(11) En este Dictamen, el CEPD aborda cuestiones como el ámbito de aplicación de los criterios, la aplicabilidad y la relevancia de los criterios en todos los Estados miembros.

(12) Este Dictamen se centra en los criterios de certificación. En el caso de que el CEPD requiera información de alto nivel sobre los métodos de evaluación para poder evaluar a fondo la «auditabilidad» de los criterios en el contexto de su Dictamen al respecto, no se exigirá ningún tipo de aprobación de dichos métodos de evaluación.

(13) En virtud del artículo 64, apartado 2, del RGPD, conjuntamente con el artículo 10, apartado 2, del Reglamento interno del CEPD, el Dictamen del CEPD deberá adoptarse en un plazo de ocho semanas desde el primer día hábil posterior al momento en que la Presidencia y la autoridad de control competente hayan decidido que el expediente está completo. Por decisión de la Presidencia, dicho período podrá prorrogarse seis semanas más, teniendo en cuenta la complejidad del asunto. Si el Dictamen del CEPD concluye que los criterios en cuestión no se pueden aprobar, la AC podrá presentar de nuevo los criterios para su aprobación cuando haya abordado las preocupaciones expresadas en el Dictamen inicial del CEPD.

HA ADOPTADO EL SIGUIENTE DICTAMEN:

RESUMEN DE LOS HECHOS

1. De conformidad con el artículo 42, apartado 5, del RGPD y las Directrices, el Centro Europeo para la Certificación y la Privacidad (en adelante el «titular del plan») redactó los criterios Europrivacy v.60 (en adelante el «proyecto de criterios de certificación», los «criterios de certificación» o los «criterios»).

2. El 28 de septiembre de 2022, la autoridad de control de Luxemburgo (en adelante la «AC LU») presentó los criterios de certificación Europrivacy al CEPD para su aprobación conforme al artículo 64, apartado 2, del RGPD. La decisión sobre la integridad del expediente se adoptó el 28 de septiembre de 2022.

3. El mecanismo de certificación Europrivacy no es una certificación conforme al artículo 46, apartado 2, letra f), del RGPD pensada para las transferencias internacionales de datos personales, y, por lo tanto, no proporciona las salvaguardas adecuadas en el marco de las transferencias de datos personales a terceros países o a organizaciones internacionales en los términos que se mencionan en el artículo 46, apartado 2, letra f). Cabe recordar que las transferencias de datos personales a terceros países o a una organización internacional deben tener lugar solamente si se respetan las disposiciones del capítulo V del RGPD.

2 EVALUACIÓN

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

5. El CEPD observa que la orientación para la aplicación y los medios de verificación del mecanismo de certificación sugeridos que proporciona el titular del plan no siempre son coherentes en todo el catálogo de criterios. Por ejemplo, en la sección T.2.3.2 se exige la instauración de normas, políticas, procedimientos o mecanismos para detectar y denunciar intrusiones (p. ej., un sistema de detección de intrusiones que supervise el tráfico de la red para detectar actividades sospechosas y alertar cuando se descubra dicha actividad), mientras que el medio de verificación sugerido se refiere a una prueba de penetración e inspección (requerida en la sección T.2.3.1). Aunque dichas incoherencias no entran en el ámbito de aplicación de esta evaluación, el CEPD quiere destacar que pueden ser un obstáculo para la acreditación del organismo de certificación, a menos que el titular del plan las rectifique.

2.1 Ámbito de aplicación del mecanismo de certificación y Objetivo de Evaluación (OdE)

6. El mecanismo de certificación Europrivacy es un plan general, dado que está pensado para una amplia gama de diferentes operaciones de tratamiento realizadas por los responsables y encargados de varios sectores de actividad. Los principales criterios de este mecanismo de certificación consisten en unos «Criterios básicos» y «Comprobaciones y controles de las medidas técnicas y organizativas» sobre las medidas tecnológicas y organizativas puestas en marcha para proteger los datos personales tratados. Algunas de las «Comprobaciones y controles de las medidas técnicas y organizativas» solo son aplicables si el objetivo de evaluación (OdE) procesa categorías especiales de datos, datos relacionados con delitos o datos personales de un menor.

7. Además, los criterios incluyen también «comprobaciones y controles contextuales complementarios» pensados para garantizar que el tratamiento implicado en el OdE cumple los requisitos específicos del sector y de la tecnología. El titular del plan proporciona una matriz que describe a qué categorías de operaciones de tratamiento de datos se aplica cada grupo de «Comprobaciones y controles contextuales complementarios».

8. El CEPD acoge con satisfacción los planes generales que incluyen criterios específicos que los hacen más reproducibles y aplicables a operaciones de tratamiento específicas o a un sector de actividad determinado. No obstante, el CEPD también desea dejar claro que, en el contexto de un plan general, no se exige exhaustividad en los criterios relativos a operaciones de tratamiento específicas y, por lo tanto, no se ha evaluado en el contexto del presente Dictamen. Asimismo, el CEPD recuerda que cuando publica documentos relacionados con actividades de tratamiento específicas, el titular del plan y los organismos de certificación acreditados deben tener en cuenta dichos documentos.

9. Los criterios aplicables a la especificación del OdE se definen en los requisitos que se pueden consultar en A.2.1.1. Las reglas específicas aplicables al proceso que deben seguir el solicitante y el organismo de certificación para definir el OdE se especifican en el plan de Europrivacy (10.2 «Actividades previas a la certificación»).

10. El Comité observa en la documentación relacionada con el ámbito de aplicación del mecanismo de certificación proporcionado por la AC LU que el plan Europrivacy se aplica a los responsables y encargados establecidos en la Unión Europea (UE) o en el Espacio Económico Europeo (EEE). La aplicabilidad de los criterios se define en función del papel y las responsabilidades del solicitante.

11. El Comité observa que el responsable de los datos puede presentar al proceso de certificación de Europrivacy un OdE sujeto a un control conjunto (criterios A.2.7.1). El Comité desea destacar que, cuando el OdE esté sujeto a un control conjunto, el organismo de certificación acreditado tendrá que aplicar el proceso con mucho cuidado para garantizar que el OdE sea significativo y que el solicitante sea completamente responsable del cumplimiento del OdE con todas las obligaciones en virtud del RGPD que el mecanismo de certificación pretende demostrar. En consecuencia, el acuerdo celebrado entre el solicitante y los demás corresponsables del tratamiento implicados en el OdE en relación con sus respectivas responsabilidades de cumplimiento del RGPD[4] podrían —según el contexto de las actividades de tratamiento del OdE— impedir al solicitante cumplir los criterios de certificación.

12. El Comité observa que el tratamiento de datos genéticos queda excluido del ámbito de aplicación del mecanismo de certificación Europrivacy. En consecuencia, la evaluación de los criterios realizada por el Comité no aborda la idoneidad de los criterios cuando el OdE incluye el tratamiento de este tipo de datos.

2.2 Operaciones de tratamiento

13. Los criterios abordan los componentes relevantes de las operaciones de tratamiento (datos, sistemas y tratamiento) en relación con el ámbito de aplicación general del mecanismo de certificación. En particular, los criterios permiten identificar categorías especiales de datos según se definen en el artículo 9 del RGPD (sección G.2 de los criterios «Tratamiento de datos especiales»).

[4] *La determinación de sus responsabilidades respectivas debe abordar, en particular, el ejercicio de los derechos de los interesados y las obligaciones de suministro de información. Además de esto, la distribución de las responsabilidades debe abarcar otras obligaciones del responsable del tratamiento relacionadas, por ejemplo, con los principios generales de protección de datos, la base jurídica, las medidas de seguridad, la obligación de notificar las violaciones de la seguridad de los datos, las evaluaciones de impacto relativas a la protección de datos, el recurso a encargados del tratamiento, las transferencias a terceros países, y los contactos con los interesados y las autoridades de control.* (Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD).

2.3 Legalidad del tratamiento

14. Los criterios exigen que se compruebe la legalidad del tratamiento de datos para cada una de las operaciones de tratamiento del OdE, y que se comprueben los requisitos de la base jurídica tal como se define en el artículo 6 del RGPD (sección G.1 de los criterios «Legalidad del tratamiento de datos»).

2.4 Principios del tratamiento

15. Los criterios abordan de forma adecuada los principios de protección de datos con arreglo al artículo 5 del RGPD. En particular, los criterios requieren al solicitante que demuestre que los datos personales son idóneos, relevantes y se limitan a lo que es necesario en relación con los fines para los que se tratan (minimización de datos).

2.5 Obligaciones generales de los responsables y los encargados del tratamiento

16. Los criterios reflejan las obligaciones del responsable del tratamiento conforme al artículo 24 del RGPD (G.4 - «Responsabilidad del responsable del tratamiento de datos») y exigen la evaluación de los acuerdos contractuales del responsable-encargado conforme al artículo 28 del RGPD (sección G.5 de los criterios «Encargados y subencargados del tratamiento de datos»).

17. Los criterios exigen a todos los solicitantes que nombren a un responsable de protección de datos (RPD), incluso cuando el solicitante no esté obligado a designar un RPD según el artículo 37 del RGPD. Con los criterios se verifica que el RPD cumpla los requisitos de los artículos 37 a 39 (sección G.9 de los criterios «Responsable de protección de datos»).

18. Los criterios comprueban el contenido de los registros de actividades de tratamiento conforme al artículo 30 del RGPD (sección G.5.3 de los criterios «Registros de las actividades de tratamiento»).

2.6 Derechos de los interesados

19. Los criterios abordan de forma adecuada el derecho de los interesados a la información conforme al capítulo III del RGPD y requieren la puesta en práctica de las correspondientes medidas. Los criterios también requieren la puesta en práctica de medidas que permitan intervenir en la operación de tratamiento a fin de garantizar los derechos de los interesados y permitir la rectificación, la supresión o limitaciones (sección G.3 de los criterios «Derechos de los interesados»).

2.7 Riesgos para los derechos y las libertades

20. Los criterios exigen que se evalúen los riesgos para los derechos y las libertades de las personas naturales a las que concierne el tratamiento de datos del OdE conforme al artículo 35 del RGPD (sección G.8 de los criterios «Evaluación de impacto relativa a la protección de datos»).

2.8 Medidas técnicas y organizativas que garantizan la protección

21. Los criterios requieren la aplicación de medidas técnicas y organizativas que faciliten la confidencialidad, la integridad y la disponibilidad de las operaciones de tratamiento. Los criterios también requieren la aplicación de medidas técnicas para implementar la protección de datos desde el diseño y por defecto conforme al artículo 25 y el artículo 32 del RGPD (sección G.6 de los criterios «Seguridad del tratamiento y protección de datos desde el diseño» y sección T.1/T.2 de los criterios «Requisitos de seguridad básica/Requisitos de seguridad ampliada»).

22. Los criterios exigen la aplicación de medidas para garantizar que las obligaciones de notificación de violación de datos se cumplan en su debido momento y correspondan al ámbito de aplicación de los artículos 33 y 34 del RGPD (sección G.7 de los criterios «Gestión de las violaciones de datos»).

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

23. Los criterios requieren que se identifiquen todas las transferencias de datos personales a terceros países y a organizaciones internacionales implicadas en el OdE y que se argumente la opción elegida en cuanto al mecanismo de transferencia de datos elegido por las salvaguardias adecuadas, conforme al capítulo V del RGPD (sección G.10 de los criterios «Transferencias de datos personales a terceros países y organizaciones internacionales»).

3. CRITERIOS ADICIONALES PARA UN SELLO EUROPEO DE PROTECCIÓN DE DATOS

24. Según las Directrices, la evaluación debe incluir la cuestión de «si los criterios son capaces de tener en cuenta la legislación o los supuestos en materia de protección de datos de los Estados miembros». La sección G.1.1.3 de los criterios requiere que el solicitante proporcione dicha evaluación en un informe de evaluación de cumplimiento de las obligaciones nacionales o NOCAR (acrónimo inglés de «National Obligations Compliance Assessment Report»). El Comité observa que dicho informe debe incluir una evaluación de las obligaciones nacionales aplicables al OdE y documentar las medidas que ha tomado el solicitante para cumplir la normativa aplicable y, probablemente, medidas correctoras continuadas. El solicitante no utilizará la lista de requisitos nacionales complementaria que proporciona el titular del plan para cada país como una lista exhaustiva de obligaciones nacionales relevantes para el OdE. La lista indicativa de comprobaciones y controles complementarios mínimos que proporciona el titular del plan no son criterios de certificación que entren en el ámbito de aplicación del presente Dictamen.

CONCLUSIONES Y RECOMENDACIONES

25. A modo de conclusión, el CEPD considera que los criterios de certificación Europrivacy son coherentes con el RGPD y los aprueba con arreglo a la función del Comité que se define en el artículo 70, apartado 1, letra o), del RGPD, a fin de obtener una certificación común (Sello Europeo de Protección de Datos).

26. El CEPD registrará el mecanismo de certificación de Europrivacy en el registro público de mecanismos de certificación y sellos y marcas de protección de datos conforme al artículo 42, apartado 8.

OBSERVACIONES FINALES

27. Este Dictamen se dirige a la AC LU y se publicará de conformidad con lo dispuesto en el artículo 64, apartado 5, letra b), del RGPD.

Por el Comité Europeo de Protección de Datos

La Presidenta