Dictamen del Comité (art. 64)

Dictamen 19/2024 sobre los criterios de certificación de EuroPrise en relación con su aprobación por el Comité como Sello Europeo de Protección de Datos conforme al artículo 42, apartado 5 (RGPD)

Adoptado el 16 de julio de 2024

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

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 (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 lo sucesivo «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 podrá 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 (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 (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 sistema de ofrecer un 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 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) Como resultado, las certificaciones deben aportar valor a los responsables y encargados del tratamiento, ayudándoles a poner en práctica medidas técnicas y de organización estandarizadas y específicas que puedan facilitar y mejorar demostrablemente la conformidad de las operaciones de tratamiento con el RGPD, teniendo en cuenta las necesidades específicas del sector.

(9) El CEPD acoge con satisfacción los esfuerzos realizados por los titulares de sistemas 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 en relación con el RGPD ni impide que las autoridades de control ejerzan sus tareas y competencias conforme al RGPD y la legislación nacional aplicable.

(11) En este Dictamen, el CEPD aborda cuestiones tales 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 exhaustivamente 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 otras seis semanas, 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:

1. RESUMEN DE LOS HECHOS

1. De conformidad con el artículo 42, apartado 5, del RGPD y las Directrices, el proyecto de «Catálogo de criterios EuroPriSe para la certificación de las operaciones de tratamiento por parte de los encargados del tratamiento» (ámbito de aplicación: EU) v1.5» (en lo sucesivo, «el proyecto de criterios de certificación», «criterios de certificación» o «criterios») fue redactado por EuroPriSe Cert GmbH (en

lo sucesivo, el «titular del sistema»), una entidad jurídica radicada en Alemania, y se presentó a l Landesbeauftragte für datenschutz und Informationsfreiheit Nordrhein-Westfalen, la autoridad de supervisión alemana competente en Renania del Norte-Westfalia (*Landesbeauftragte für datenschutz und Informationsfreiheit Nordrhein-Westfalen*), en lo sucesivo, «DE-NRW SA».

2. El 29 de abril de 2024, la autoridad de control de Alemania (en lo sucesiva la «DE SA») presentó el proyecto de los criterios de certificación al CEPD para su aprobación, conforme al artículo 64, apartado 2, del RGPD. La decisión sobre la integridad del expediente se adoptó el 29 de mayo de 2024.

3. El mecanismo de certificación EuroPrise 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 a los que se refiere el artículo 46, apartado 2, letra f). Cabe recordar que las transferencias de datos personales a terceros países o a una organización internacional sólo tendrán lugar 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 consonancia con la estructura prevista en el Anexo 2 de las Directrices (en adelante el «Anexo») y su adenda.

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

5. El mecanismo de certificación EuroPrise contiene criterios de certificación de un régimen de certificación a escala de la UE para la certificación del tratamiento por parte de los encargados del tratamiento. El objeto de las certificaciones a las que se aplica el catálogo de criterios son las operaciones de tratamiento realizadas en productos, procesos y servicios o con la ayuda de (también aquí varios) productos y servicios y en relación con las cuales el solicitante de la certificación actúa como encargado del tratamiento. Los principales criterios de este mecanismo de certificación se dividen en tres conjuntos de requisitos, a saber: desde una perspectiva jurídica (conjunto 1), desde la perspectiva de las medidas técnicas y organizativas (conjunto 2) y desde la perspectiva de los derechos de los interesados (conjunto 3).

6. Los solicitantes de certificación en virtud de este sistema deben ser encargados del tratamiento. Esto incluye a los encargados del tratamiento a los que un responsable del tratamiento encomiende directamente el tratamiento de datos personales en el sentido del artículo 4, apartado 7, del RGPD. Sin embargo, los solicitantes de certificación también pueden ser encargados del tratamiento en el sentido del artículo 28, apartados 2) y 4) del RGPD (subencargados del tratamiento).

7. Cuando un encargado del tratamiento -certificado en virtud del sistema de certificación EuroPrise- utiliza un sub-encargado del tratamiento, este último no puede alegar que se haya certificado con arreglo al sistema de certificación EuroPrise. En tal caso, sólo las operaciones de tratamiento realizadas por el encargado de tratamiento inicial y certificado están cubiertas por la certificación. Sin embargo, los sub-encargados del tratamiento también pueden solicitar la certificación, lo que daría lugar a un procedimiento autónomo e independiente.

8. El Comité observa en la documentación relacionada con el ámbito de aplicación del mecanismo de certificación proporcionado por la DE SA que el sistema EuroPriSe se aplica a los encargados del tratamiento establecidos en la Unión Europea (UE) o en el Espacio Económico Europeo (EEE).

2.2 Operaciones de tratamiento

9. El alcance de estos criterios no se limita a determinados tipos de operaciones de tratamiento. Es más bien la metodología subyacente a una evaluación EuroPrise, que permite la certificación de cualquier operación de tratamiento por parte de los encargados del tratamiento. Se trata, por tanto, de un enfoque metodológico universal sobre cuya base puede certificarse un gran número de operaciones de tratamiento muy diferentes. Por lo tanto, es de fundamental importancia que se respeten los requisitos metodológicos, ya que esta es la única manera de garantizar una aplicación uniforme de los criterios de certificación y un nivel comparable de ensayos en los diferentes procedimientos de certificación. El objetivo es garantizar la comparabilidad y reproducibilidad de las certificaciones emitidas y sus resultados.

2.3 Legalidad y principios del tratamiento de datos

10. Los criterios requieren examinar si las operaciones de tratamiento que se van a certificar cumplen los principios de protección de datos desde el diseño y por defecto (apartado 1.5 de los criterios), lo que implica la participación del solicitante en la asistencia al responsable del tratamiento en la aplicación de estos principios. Esto permite evaluar el cumplimiento del artículo 25 del RGPD, interpretado en conjunción con el artículo 5 del RGPD. Si bien no existen criterios destinados directamente al cumplimiento del artículo 6 del RGPD —dado que el responsable del tratamiento es responsable de la legalidad del tratamiento-, los criterios tienen por objeto garantizar que los encargados-solicitantes diseñen las operaciones de tratamiento que deben certificarse de manera que se facilite la aplicación por parte de los responsables del tratamiento de los principios de protección de datos contemplado en el artículo 5 del RGPD, incluido el principio de la legalidad del tratamiento.

2.4 Obligaciones generales de los responsables y los encargados del tratamiento

11. Los criterios reflejan la relación entre el encargado del tratamiento y el responsable del tratamiento. En particular, los criterios establecen la obligación del encargado del tratamiento de disponer de un modelo de acuerdo de tratamiento de datos con el responsable del tratamiento, que incluye todos los requisitos contemplados en el artículo 28 del RGPD (sección 1.2 de los criterios).

12. Los criterios exigen que los solicitantes designen un delegado de protección de datos (DPD) de conformidad con el artículo 37 del RGPD y que aporten una prueba del nombramiento del DPD (por ejemplo, certificado de nombramiento). Con los criterios se verifica que el DPD cumple los requisitos establecidos en los artículos 37 a 39 (conjunto 1, sección 1.1 de los criterios).

13. Los criterios comprueban el contenido de los registros de tratamiento de las actividades de conformidad con el artículo 30 del RGPD (conjunto 1, sección 1.1 de los criterios).

2.5 Derechos de los interesados

14. Los criterios abordan de manera adecuada el derecho de los interesados a la información de conformidad con el 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 las limitaciones (conjunto 3 de los criterios).

2.6 Riesgos para los derechos y las libertades

15. Los criterios exigen que el encargado del tratamiento sea consciente de los posibles riesgos para los derechos y libertades de las personas físicas en relación con el tratamiento de datos incluido en el objetivo de evaluación. Si es probable que el tratamiento de datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, varios criterios garantizan que el solicitante demuestre que se cumplen los requisitos del artículo 35 del RGPD, de conformidad con el artículo 35 del RGPD (sección 1.2.2 de los criterios, requisito n.º 6, sección 1.3.2 de los criterios, sección 1.3.3 de los criterios, sección 2.1.5.1 de los criterios, sección 2.1.5.9 de los criterios).

2.7 Medidas técnicas y organizativas que garantizan la protección

16. 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 exigen la aplicación de medidas técnicas para implementar la protección de datos desde el diseño y por defecto, de conformidad con el artículo 25 y el artículo 32 del RGPD (sección 1.5 de los criterios, sección 2.1 de los criterios/otros documentos).

17. Los criterios exigen la aplicación de medidas para garantizar que las obligaciones de notificación de violación de los datos personales se cumplan en su debido momento y correspondan al ámbito de aplicación del 33 y 34 del RGPD (sección 1.2.2 de los criterios, requisito n.º 6).

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

18. Los criterios requieren la identificación de todas las transferencias de datos personales a terceros países y a organizaciones internacionales implicadas en el objetivo de evaluación 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 1.4 de los criterios).

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

19. 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 4 de los criterios exige que el solicitante cumpla la legislación nacional aplicable y la legislación sectorial pertinente en materia de protección de datos. Además, la Junta entiende que un "informe de conformidad con la legislación nacional" -que evalúe, en particular, la conformidad del objetivo de la evaluación con los requisitos de la legislación nacional aplicable en materia de protección de datos- deberá ser elaborado por expertos jurídicos, siempre que dichos expertos hayan demostrado el nivel necesario de conocimientos sobre la legislación nacional aplicable.

CONCLUSIONES Y RECOMENDACIONES

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

21. El CEPD registrará el mecanismo de certificación del «Catálogo de Criterios EuroPrise para la certificación de las operaciones de tratamiento por encargados del tratamiento» en el registro público de mecanismos de certificación y sellos de protección de datos, de conformidad con el artículo 42, apartado 8.

OBSERVACIONES FINALES

22. Este dictamen se dirige a la Autoridad de Control de Alemania y Renania del Norte-Westafalia y se hará público de conformidad con el artículo 64, apartado 5, letra b), del RGPD.

Por el Comité Europeo de Protección de Datos

La Presidenta
Anu Talus