Dictamen del Comité (art. 64)

Dictamen 14/2020 sobre el proyecto de decisión de la autoridad de control competente de Irlanda en relación con la aprobación de los requisitos para la acreditación de un organismo de certificación con arreglo al artículo 43, apartado 3, del RGPD

Adoptado el 25 de mayo de 2020

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

Adoptado

Índice

El Comité Europeo de Protección de Datos

Vistos el artículo 63; el artículo 64, apartado 1, letra c), y apartados 3 a 8; y el artículo 43, apartado 3, 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, el «Reglamento general de protección de datos», o «RGPD»),

Visto el Acuerdo sobre el Espacio Económico Europeo y, en particular, su anexo XI y su Protocolo 37, modificados 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, de 25 de mayo de 2018,

Considerando lo siguiente:

1) La principal función del Comité es velar por la aplicación coherente del Reglamento 2016/679 (en lo sucesivo, el «RGPD») en todo el Espacio Económico Europeo. De conformidad con el artículo 64, apartado 1, del RGPD, el Comité emitirá un dictamen cuando una autoridad de control (AC) tenga la intención de aprobar los requisitos de acreditación de organismos de certificación con arreglo al artículo 43. El objetivo del presente dictamen es, por tanto, crear un enfoque armonizado en relación con los requisitos que aplicará una autoridad de control para la protección de datos o el organismo nacional de acreditación para la acreditación de un organismo de certificación. Aunque el RGPD no impone un único conjunto de requisitos para la acreditación, sí promueve la coherencia. El Comité pretende alcanzar este objetivo en sus dictámenes, en primer lugar, animando a las autoridades de control a elaborar sus requisitos para la acreditación con arreglo a la estructura establecida en el anexo 1 de las Directrices 4/2018 del Comité Europeo de Protección de Datos (CEPD) sobre la acreditación de los organismos de certificación, y, en segundo lugar, analizándolos mediante un modelo proporcionado por el CEPD que permite la evaluación comparativa de los requisitos (con arreglo a la norma ISO 17065 y a las Directrices del CEPD sobre la acreditación de los organismos de certificación).

2) En relación con el artículo 43 del RGPD, las autoridades de control competentes adoptarán requisitos de acreditación. No obstante, aplicarán el mecanismo de coherencia a fin de permitir que se genere confianza en el mecanismo de certificación, en particular mediante el establecimiento de un alto nivel de requisitos.

3) Si bien los requisitos de acreditación están sujetos al mecanismo de coherencia, no significa que los requisitos deban ser idénticos. Las autoridades de control competentes disponen de un margen de discrecionalidad en lo que respecta al contexto nacional o regional, y deberán tener en cuenta su normativa nacional. El objetivo del dictamen del CEPD no es conseguir un conjunto único de requisitos de la UE, sino evitar incoherencias significativas que puedan afectar, por ejemplo, a la confianza en la independencia o el conocimiento de los organismos de certificación acreditados.

[1] Las referencias a la «Unión» realizadas en el presente dictamen deben entenderse como referencias al «EEE».

4) Las Directrices 4/2018 sobre la acreditación de los organismos de certificación en virtud del artículo 43 del Reglamento general de protección de datos (2016/679) (en lo sucesivo, las «Directrices») y las Directrices 1/2018 sobre la certificación e identificación de los criterios de certificación de acuerdo con los artículos 42 y 43 del Reglamento 2016/679 servirán como hilo conductor en el contexto del mecanismo de coherencia.

5) Si un Estado miembro estipula que los organismos de certificación deben estar acreditados por la autoridad de control, esta deberá establecer requisitos de acreditación, incluidos, entre otros, los requisitos enumerados en el artículo 43, apartado 2, del RGPD. Si se compara con las obligaciones relativas a la acreditación de los organismos de certificación por parte de los organismos nacionales de acreditación, el artículo 43 del RGPD ofrece menos información sobre los requisitos de acreditación cuando es la propia autoridad de control la que lleva a cabo la acreditación. Para contribuir a la adopción de un enfoque armonizado en la acreditación, los criterios de acreditación utilizados por la autoridad de control deben guiarse por la norma ISO/IEC 17065 y complementarse con los requisitos adicionales que establezca la autoridad de control de conformidad con el artículo 43, apartado 1, letra b), del RGPD. El CEPD señala que el artículo 43, apartado 2, letras a) a e), refleja y especifica los requisitos de la norma ISO 17065, lo cual contribuirá a una mayor coherencia.[2]

6) En virtud del artículo 64, apartado 1, letra c), y apartados 3 y 8, del RGPD, en combinación con el artículo 10, apartado 2, del Reglamento interno del CEPD, el dictamen del CEPD deberá adoptarse en un plazo de ocho semanas a contar desde el primer día hábil posterior al momento en que el presidente y la autoridad de control competente hayan decidido que el expediente está completo. Por decisión del presidente, dicho plazo podrá ampliarse otras seis semanas teniendo en cuenta la complejidad del asunto.

HA ADOPTADO EL SIGUIENTE DICTAMEN:

1 RESUMEN DE LOS HECHOS

1. La autoridad de control de Irlanda (en lo sucesivo, la «AC IE») ha presentado al CEPD su proyecto de requisitos de acreditación en virtud del artículo 43, apartado 1, letra b), del CEPD. El expediente se consideró completo el 13 de febrero de 2020. El organismo nacional de acreditación de Irlanda, INAB, llevará a cabo la acreditación de los organismos de certificación para certificar el uso de los criterios de certificación del RGPD. Esto significa que el INAB utilizará la norma ISO 17065 y los requisitos adicionales establecidos por la AC IE, una vez que esta los apruebe tras un dictamen del Comité sobre el proyecto de requisitos, para acreditar a los organismos de certificación.

2. De conformidad con el artículo 10, apartado 2, del Reglamento interno del Comité, debido a la complejidad del asunto en cuestión, la presidenta decidió prorrogar otras seis semanas el período de adopción inicial de ocho semanas.

[2] Directrices 4/2018 sobre la acreditación de los organismos de certificación en virtud del artículo 43 del Reglamento general de protección de datos (párr. 39). Disponible en: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

2 EVALUACIÓN

2.1 Razonamiento general del CEPD sobre el proyecto de decisión presentado

3. La finalidad del presente dictamen es evaluar los requisitos de acreditación elaborados por una AC, ya sea en relación con la norma ISO 17065 o con un conjunto completo de requisitos, a los efectos de permitir que un organismo nacional de acreditación o una AC, de conformidad con el artículo 43, apartado 1, del RGPD, acrediten a un organismo de certificación responsable de expedir y renovar la certificación de conformidad con el artículo 42 del RGPD. Esto se entiende sin perjuicio de las funciones y competencias de la AC competente. En este caso concreto, el Comité observa que la AC IE ha decidido recurrir a su organismo nacional de acreditación para la expedición de la acreditación, tras establecer unos requisitos adicionales de conformidad con las Directrices, que dicho organismo debe seguir al expedir la acreditación.

4. Esta evaluación de los requisitos adicionales de acreditación de la AC IE tiene por objeto examinar las variaciones (adiciones o supresiones) de las Directrices y, en particular, del anexo 1. Además, el dictamen del CEPD también se centra en todos los aspectos que pueden repercutir en un enfoque coherente en relación con la acreditación de los organismos de certificación.

5. Cabe señalar que el objetivo de las Directrices sobre la acreditación de los organismos de certificación es ayudar a las AC a definir sus requisitos de acreditación. El anexo de las Directrices no incluye requisitos de acreditación como tales. Por lo tanto, los requisitos de acreditación para los organismos de certificación deben ser definidos por la AC de manera tal que resulte posible su aplicación práctica y coherente, según requiera el contexto de la AC.

6. El Comité reconoce el hecho de que, habida cuenta de su pericia, se debe dar libertad de acción a los organismos nacionales de acreditación al definir determinadas disposiciones específicas dentro de los requisitos de acreditación aplicables. No obstante, el Comité considera necesario subrayar que, cuando se establezcan requisitos adicionales, estos deben definirse de manera que permitan su aplicación práctica y coherente y su revisión cuando sea necesario.

7. El Comité observa que las normas de la ISO, en particular la norma ISO 17065, están sujetas a derechos de propiedad intelectual y, por lo tanto, no hará referencia al texto del documento correspondiente en el presente dictamen. En consecuencia, el Comité ha decidido, cuando proceda, señalar secciones específicas de la norma ISO, pero sin reproducir el texto.

8. Por último, el Comité ha realizado su evaluación siguiendo la estructura prevista en el anexo 1 de las Directrices (en lo sucesivo, el «anexo»). En los casos en que el presente dictamen guarde silencio sobre una sección específica del proyecto de requisitos de acreditación de la AC IE, debe interpretarse que el Comité no tiene ningún comentario que realizar y no solicita a la AC IE que adopte nuevas medidas.

9. El presente dictamen no trata los aspectos presentados por la AC IE que quedan excluidos del ámbito de aplicación del artículo 43, apartado 2, del RGPD, como las referencias a la legislación nacional. No obstante, el Comité observa que la legislación nacional debe estar en consonancia con el RGPD, cuando sea necesario.

2.2 Principales puntos de interés para la evaluación (artículo 43.2 del RGPD y anexo 1 de las directrices del CEPD) proporcionados por los requisitos de acreditación para la evaluación coherente de los siguientes puntos:

1) abordar todos los ámbitos clave que figuran en el anexo de las Directrices y considerar toda desviación del anexo;

2) independencia del órgano de certificación;

3) conflictos de intereses del organismo de certificación;

4) conocimientos técnicos del organismo de certificación;

5) salvaguardias adecuadas para garantizar que el organismo de certificación aplique los criterios de certificación del RGPD adecuadamente;

6) procedimientos para la expedición, revisión periódica y retirada de la certificación del RGPD; y

7) tramitación transparente de las reclamaciones sobre infracciones de la certificación.

10. Considerando que:

a. el artículo 43, apartado 2, del Reglamento general de protección de datos proporciona una lista de ámbitos de acreditación que un organismo de certificación debe abordar para ser acreditado,

b. el artículo 43, apartado 3, del RGPD dispone que los requisitos para la acreditación de los organismos de certificación serán aprobados por la autoridad de control competente;

c. el artículo 57, apartado 1, letras p) y g), del RGPD establece que una autoridad de control competente debe elaborar y publicar los requisitos para la acreditación de organismos de certificación y puede decidir efectuar la acreditación de los propios organismos de certificación;

d. el artículo 64, apartado 1, letra c), del RGPD establece que el Comité emitirá un dictamen cuando una autoridad de control proyecte adoptar los requisitos aplicables a la acreditación de un organismo de certificación conforme al artículo 43, apartado 3;

e. si el organismo nacional de acreditación es el que realiza la acreditación de conformidad con lo dispuesto en la norma ISO/IEC 17065/2012, deberán aplicarse también los requisitos adicionales establecidos por la autoridad de control competente;

f. el anexo 1 a las Directrices para la acreditación de la certificación prevé sugerencias de requisitos que una autoridad de control de la protección de datos elaborará y que aplicará durante la acreditación de un organismo de certificación por el organismo nacional de acreditación;

el Comité opina lo siguiente:

2.2.1 INTRODUCCIÓN (sección 0 del proyecto de requisitos de acreditación de la AC IE)

11. El Comité reconoce el hecho de que las condiciones de cooperación, que regulan la relación entre un organismo nacional de acreditación y su autoridad de control encargada de la protección de datos, no son un requisito para la acreditación de los organismos de certificación propiamente dicho. Sin embargo, por razones de exhaustividad y transparencia, el Comité considera que dichas condiciones de cooperación, cuando existan, se harán públicas en un formato que la AC considere adecuado.

2.2.2 TÉRMINOS Y DEFINICIONES

12. El Comité observa que la referencia a las Directrices sobre la acreditación como «WP 261» no se encuentra actualizada. El CEPD adoptó las Directrices 4/2018 sobre la acreditación de los organismos de certificación en virtud del artículo 43 del Reglamento general de protección de datos (2016/679). Por tanto, el Comité recomienda a la AC IE que modifique la redacción y haga referencia a las Directrices 4/2018.

2.2.3 OBSERVACIONES GENERALES

13. El Comité observa que el proyecto de requisitos de la AC IE hace referencia de manera reiterada a la «autoridad de control competente». Puesto que la AC competente es en este caso la AC IE, el Comité aconseja a la AC IE que sustituya la referencia citada por «DPC» o la «AC IE», a fin de evitar confusiones.

14. El Comité toma nota de que el proyecto de requisitos de la AC IE incluye una sección sobre términos y definiciones. Sin embargo, algunos de los términos no se usan de un modo sistemático a lo largo del documento (p. ej., «objeto de evaluación» y «objetivo de evaluación»). A fin de evitar confusiones, el Comité recomienda a la AC IE que utilice una terminología coherente en el proyecto de requisitos.

2.2.4 REQUISITOS GENERALES PARA LA ACREDITACIÓN (sección 4 del proyecto de requisitos para la acreditación)

15. Por lo que respecta a la cláusula 7 del subapartado 4.1.2 del proyecto de requisitos para la acreditación de la AC IE, el Comité considera que la redacción es ligeramente confusa en lo referente a quién se ofrecen las razones para aprobar la certificación. Tampoco queda clara la referencia a «facilitar» el registro. Por tanto, el Comité recomienda a la AC IE que reformule estas cuestiones para garantizar una mayor claridad.

2.2.5 REQUISITOS ESTRUCTURALES (sección 5 del proyecto de requisitos para la acreditación)

16. El Comité observa que el proyecto de requisitos para la acreditación de la AC IE hace referencia al nombramiento de una «persona con una antigüedad suficiente y responsabilidad para velar por el cumplimiento de las normas sobre protección de datos y la administración de la información». Resulta necesario aclarar la referencia a la antigüedad suficiente en lo que se refiere a la experiencia y el alcance de las funciones. Además, las atribuciones de este cargo parecen similares a las de un delegado de protección de datos. El Comité aconseja a la AC IE que establezca claramente las funciones de este cargo y que especifique la experiencia pertinente.

2.2.6 REQUISITOS DE RECURSOS HUMANOS (sección 6 del proyecto de requisitos para la acreditación)

17. Por lo que respecta al personal del organismo de certificación (subapartado 6.1), el Comité observa que, entre los requisitos mínimos exigidos al personal con conocimientos técnicos responsable de tomar decisiones, se incluye tener al menos cinco años de experiencia profesional relacionada con el objeto de la certificación, mientras que el personal responsable de las evaluaciones debe contar con, al menos, dos años de experiencia profesional. De manera semejante, el personal con conocimientos jurídicos responsable de adoptar las decisiones debe contar con, al menos, cinco años de experiencia profesional, mientras que las personas a cargo de las evaluaciones precisan de dos años de experiencia. El Comité observa que el número mínimo de años de experiencia profesional exigido al personal responsable de la toma de decisiones es significativamente diferente del que debe reunir el personal a cargo de la evaluación. A este respecto, el Comité considera que debería hacerse hincapié en el tipo de conocimientos diferentes en lugar de en el número de años de experiencia profesional. En opinión del Comité, los evaluadores deben contar con unos conocimientos más especializados y experiencia profesional en los procedimientos técnicos (p. ej., auditorías y certificaciones), mientras que los responsables de la toma de decisiones deben tener unos conocimientos más generales y amplios, además, de experiencia profesional en el campo de la protección de datos. Teniendo esto en cuenta, el Comité anima a la AC IE a hacer más hincapié en la diferencia en los conocimientos sustantivos o la experiencia de los evaluadores y los responsables de la toma de decisiones, y a reducir la discrepancia en los años de experiencia exigidos.

2.2.7 REQUISITOS DE LOS PROCESOS (sección 7 del proyecto de requisitos para la acreditación)

18. Por cuanto hace al subapartado 7.10 del proyecto de requisitos para la acreditación de la AC IE («Cambios que afectan a la certificación»), el Comité observa que no se hace ninguna referencia a los procedimientos que deben acordarse para los cambios conforme a la sección 7.10 del anexo. El Comité recomienda a la AC IE que incluya dicha referencia y una mención a algunos de los procedimientos que podrían adoptarse (p. ej., períodos de transición, proceso de aprobaciones con la AC competente, etc.). Además, el Comité considera que los cambios en el estado de la técnica también son relevantes y pueden afectar a la certificación. Por tanto, sugiere a la AC IE que incluya esta posibilidad en la lista de cambios que afectan a la certificación. Por último, el Comité acoge de buen grado la inclusión de las violaciones de la seguridad de los datos personales y las infracciones del RGPD en la lista de cambios que pueden afectar a la certificación. No obstante, a fin de garantizar la claridad, el Comité recomienda a la AC IE especificar que las violaciones de la seguridad de los datos o las infracciones del RGPD solo se tendrán en cuenta en la medida en que se encuentren relacionadas con la certificación.

19. En relación con los cambios que afectan a la certificación (subapartado 7.10 del proyecto de requisitos de la AC IE) y, en particular, con el quinto punto, el Comité toma nota de que la AC IE hace referencia a las «decisiones vinculantes aplicables del Comité Europeo de Protección de Datos» y también al artículo 39 del Reglamento interno del CEPD, que incluye «todos los documentos finales adoptados por el CEPD». Sin embargo, con vistas a asegurar una clara comprensión del alcance de la fórmula «decisiones del Comité Europeo de Protección de Datos», el Comité anima a la AC IE a que aclare la referencia. Por ejemplo, podría hacerse referencia a los «documentos adoptados por el Comité Europeo de Protección de Datos».

20. El Comité observa que el subapartado 7.11 del proyecto de requisitos de la AC IE (cancelación, limitación, suspensión o retirada de la certificación) no obliga al organismo de certificación a aceptar decisiones y órdenes de la AC IE por las que se retire o no se expida una certificación a un solicitante si dejan de satisfacerse los requisitos de la certificación. Por lo tanto, el Comité recomienda a la AC IE que incluya dicha obligación.

3 CONCLUSIONES Y RECOMENDACIONES

21. El proyecto de requisitos de acreditación de la AC IE puede dar lugar a una aplicación incoherente de la acreditación de los organismos de certificación. Por tanto, deben realizarse los siguientes cambios:

22. En cuanto a los «requisitos de los procesos», el Comité recomienda a la AC IE que:

1) incluya, en el subapartado 7.11, la obligación del organismo de certificación de aceptar las decisiones y órdenes de la AC IE por las que se retire o no se expida una certificación a un solicitante si dejan de satisfacerse los requisitos de la certificación.

4 OBSERVACIONES FINALES

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

24. En virtud del artículo 64, apartados 7 y 8, del RGPD, la AC IE deberá comunicar por medios electrónicos a la presidenta, en el plazo de dos semanas desde la recepción del dictamen, si va a mantener o modificar su proyecto de lista. Dentro del mismo período, deberá presentar el proyecto de lista modificado o, cuando no tenga la intención de seguir el dictamen del Comité, deberá indicar los motivos pertinentes por los cuales no tiene intención de seguirlo, en todo o en parte.

25. La AC IE deberá comunicar la decisión final al Comité para su inclusión en el registro de decisiones que hayan sido objeto del mecanismo de coherencia, de conformidad con el artículo 70, apartado 1, letra y), del RGPD.

Por el Comité Europeo de Protección de Datos

La Presidenta

(Andrea Jelinek)