Dictamen 4/2020 sobre el proyecto de decisión de la autoridad de control competente del Reino Unido relativa a la aprobación de los requisitos para la acreditación de un organismo de certificación con arreglo al artículo 43, apartado 3 (RGPD)

Adoptado el 29 de enero 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), incisos 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 «RGPD»),

Visto el artículo 51, apartado 1, letra b), de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (en lo sucesivo, «la Directiva sobre la policía»)

Visto el Acuerdo sobre el Espacio Económico Europeo 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, 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. Con arreglo a lo dispuesto en el artículo 64, apartado 1, del RGPD, el Comité emitirá un dictamen siempre que una autoridad de control (AC) prevea adoptar los requisitos para la acreditación de los organismos de certificación de acuerdo con lo dispuesto en el artículo 43. Por consiguiente, el objetivo del presente dictamen es crear un enfoque armonizado en relación con los requisitos que una autoridad de control competente en materia de protección de datos o el organismo nacional de acreditación aplicarán a la acreditación de un organismo de certificación. Aunque el Reglamento general de protección de datos 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 redactar sus requisitos de acreditación siguiendo la estructura establecida en el anexo de las directrices del Comité Europeo de Protección de Datos (CEPD) sobre la acreditación de los organismos de certificación y, en segundo lugar, analizándolos y utilizando para ello 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) Con referencia al artículo 43 del RGPD, las autoridades de control competentes adoptarán requisitos de acreditación. No obstante, aplicarán el mecanismo de coherencia para permitir que se genere confianza en el mecanismo de certificación, en particular mediante el establecimiento de un nivel de requisitos elevado.

(3) Si bien los requisitos para la acreditación están sujetos al mecanismo de coherencia, ello no significa que los requisitos deban ser idénticos. Las autoridades de control competentes disponene de un margen de apreciación en relación con el contexto nacional o regional y deben tener en cuenta su legislación local. El objetivo del dictamen del CEPD no es alcanzar un único conjunto de requisitos de

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

la UE, sino más bien evitar incoherencias importantes que puedan afectar, por ejemplo, a la confianza en la independencia o a la pericia de los organismos de certificación acreditados.

(4) Las «Directrices 4/2018 sobre la acreditación de los organismos de certificación con arreglo al artículo 43 del Reglamento General de Protección de Datos (2016/679)» (en lo sucesivo, las «Directrices»), y las «Directrices 1/2018 sobre la certificación y la identificación de los criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento 2016/679» servirán de 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, pero sin ánimo limitativo, los requisitos enumerados en el artículo 43, apartado 2. En comparación con las obligaciones relativas a la acreditación de los organismos de certificación por los organismos nacionales de acreditación, el artículo 43 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 de la acreditación, los requisitos 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). El CEPD señala que el artículo 43, apartado 2, letras a) a e), refleja y especifica los requisitos de la norma ISO 17065, lo que contribuirá a la coherencia.[2]

(6) En virtud del artículo 64, apartado 1, letra c) y el artículo 64, apartados 3 y 8, del RGPD, en combinación con el artículo 10, apartado 2, del Reglamento interno del CEPD, el dictamen del Comité 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 de la Presidenta, dicho plazo podrá prorrogarse seis semanas más, teniendo en cuenta la complejidad del asunto.

HA ADOPTADO EL SIGUIENTE DICTAMEN:

1 RESUMEN DE LOS HECHOS

1. La AC del Reino Unido ha presentado al CEPD su proyecto de requisitos de acreditación en virtud del artículo 43, apartado 1, letra b). Consiguientemente a una decisión que tiene en cuenta el expediente completo, se emitió el 25 de octubre de 2019. El organismo nacional de acreditación del Reino Unido, UKAS, 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 organismo nacional de acreditación utilizará la norma ISO 17065 y los requisitos adicionales establecidos por la AC, una vez que esta los apruebe, tras un dictamen del Comité sobre el proyecto de requisitos, para acreditar a los organismos de certificación.

[2] Apartado 39 de las Directrices: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf

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 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. Ello se entiende sin perjuicio de las tareas y las facultades de la AC competente. En este caso concreto, el Comité observa que la AC del Reino Unido ha decidido recurrir a su organismo nacional de acreditación para la expedición de la acreditación, habiendo establecido requisitos adicionales de conformidad con las Directrices, que dicho organismo debe utilizar al expedir la acreditación.

4. Esta evaluación de los requisitos adicionales de acreditación de la AC del Reino Unido tiene por objeto examinar las variaciones (adiciones o supresiones) de las Directrices y, en particular, del anexo. 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 autoridades de control a definir sus requisitos de acreditación. El anexo a las Directrices no constituye un requisito de acreditación como tal. Por lo tanto, los requisitos de acreditación de los organismos de certificación deben ser definidos por la AC de manera que permitan su aplicación práctica y coherente, según lo requiera el contexto de dicha autoridad.

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 asociado al presente dictamen. En consecuencia, el Comité decidió, cuando procediera, señalar secciones específicas de la norma ISO, sin reproducir, no obstante, el texto.

8. Por último, el Comité ha realizado su evaluación de conformidad con la estructura prevista en el anexo 1 a las Directrices. En los casos en que el presente dictamen guarde silencio sobre una sección específica del proyecto de requisitos de acreditación de la AC del Reino Unido, debe interpretarse que el Comité no tiene ningún comentario y no pide a la AC del Reino Unido que adopte nuevas medidas.

9. El presente dictamen no trata los aspectos presentados por la AC del Reino Unido que están fuera 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 enfoque de la evaluación (art. 43, apartado 2, del RGPD y el Anexo 1 de las Directrices del CEPD) que los requisitos de acreditación prevén para que se evalúe de manera coherente lo siguiente:

a. abordar todos los ámbitos clave, como se destaca en el anexo a las Directrices, y considerar cualquier desviación a lo dispuesto en el mismo;

b. la independencia del organismo de certificación;

c. los conflictos de intereses del organismo de certificación;

d. la pericia del organismo de certificación;

e. las garantías adecuadas para garantizar que el organismo de certificación aplique de forma adecuada los criterios de certificación del RGPD;

f. los procedimientos para la expedición, la revisión periódica y la retirada de la certificación del RGPD; y

g. la tramitación transparente de las reclamaciones relativas a las 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 considera lo siguiente:

2.2.1 PREÁMBULO (Sección 0 del proyecto de requisitos de acreditación adicionales)

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 de la protección de datos, no son un requisito para la acreditación de los organismos de certificación propiamente dichos. Sin embargo, por razones de exhaustividad y transparencia, el Comité considera que esas condiciones de cooperación, cuando existan, se harán públicas en un formato que la autoridad de control considere adecuado.

12. El Comité toma nota del hecho de que la AC del Reino Unido está estableciendo esas condiciones de cooperación con su organismo nacional de acreditación y que dichos términos se publicarán en el sitio web de la autoridad de control británica una vez finalizados.

2.2.2 REQUISITOS GENERALES DE ACREDITACIÓN (Sección 4 del proyecto de requisitos de acreditación adicionales)

13. En cuanto al requisito de responsabilidad jurídica (subsección 4.1.1), el Comité toma nota del hecho de que la AC del Reino Unido exige que el organismo de certificación que se acredite «*debería poder aportar pruebas del cumplimiento, según se requiera, durante el proceso de acreditación*» del RGPD y la Ley de protección de datos del Reino Unido de 2018. A fin de asegurar una evaluación y aplicación adecuadas de este requisito, el Comité anima a la AC del Reino Unido a que sustituya «*debería poder aportar pruebas*» por «deberá aportar pruebas». Por lo tanto, el Comité recomienda que la AC del Reino Unido modifique el proyecto en consecuencia.

14. En lo que respecta al acuerdo de certificación (subsección 4.1.2) y, en particular, al requisito número 8 (número 9 del anexo), el Comité toma nota del hecho de que la AC del Reino Unido creó una versión reformulada de parte del requisito previsto en el anexo 1 a las Directrices. Sin embargo, la AC del Reino Unido omitió una referencia a [cuando proceda] «las consecuencias para el cliente también deben abordarse». Por consiguiente, el Comité recomienda a la AC del Reino Unido que añada la parte que falta del requisito mencionado anteriormente.

15. En cuanto al uso de sellos y marcas de protección de datos (subsección 4.1.3), el Comité observa que la AC del Reino Unido solicita que se facilite una copia «*del sello, marca o logotipo a la ICO para sus registros*.». Dado que los sellos, marcas y logotipos son gestionados no solo por el organismo de certificación, sino también por el propietario del sistema, el Comité anima a la AC del Reino Unido a que se refiera también a todos los sellos, marcas y logotipos previstos en cualquier sistema de certificado aprobado por dicha autoridad.

2.2.3 REQUISITOS DE LOS RECURSOS (Sección 6 del proyecto de requisitos de acreditación adicionales)

16. En cuanto al personal del organismo de certificación (subsección 6.1) y, en particular, el punto 6, el Comité toma nota del hecho de que la AC del Reino Unido ha previsto que «*el personal responsable de las decisiones de certificación debe tener una experiencia profesional significativa en la identificación y la aplicación de medidas de protección de datos*». Sin embargo, el Comité considera que, si bien el personal que toma decisiones de certificación puede no contar por sí mismo con «*una experiencia profesional significativa en la identificación y la aplicación de medidas de protección de*

datos», debe tener acceso por lo menos a alguien que cuente con dicha experiencia para poder tomar una decisión fundada. La experiencia profesional significativa en la aplicación de esas medidas, al menos en las primeras etapas, probablemente no estaría tan extendida en este sector. Por lo tanto, el Comité anima a la AC del Reino Unido a que exija que el organismo de certificación defina y explique el requisito de experiencia profesional que es adecuado para el sistema de certificación.

2.2.4 REQUISITOS DEL PROCESO, ARTÍCULO 43, APARTADO 2, LETRAS C Y D) (Sección 7 del proyecto de requisitos de acreditación adicionales)

17. Por lo que respecta a la subsección general sobre los requisitos del proceso (subsección 7.1) y, en particular, el apartado 4, el Comité toma nota del requisito adicional de que un organismo de acreditación garantice que el organismo de certificación realiza una investigación o una auditoría en los casos en que se cuestione el cumplimiento de la protección de datos. El Comité entiende que el cumplimiento de la protección de datos se refiere al titular de la certificación. Sin embargo, esto debe especificarse claramente en los requisitos. Además, el Comité considera que la AC del Reino Unido debe detallar que esa investigación debe vincularse con el alcance de la certificación y el objetivo de la evaluación. Por consiguiente, el Comité recomienda que la AC del Reino Unido modifique su requisito como corresponda, estableciendo claramente que el cumplimiento de la protección de datos se refiere al titular de la certificación y especificando que la investigación debe vincularse con el alcance de la certificación y el objeto de la evaluación.

18. En lo que respecta a la aplicación de los requisitos del proceso (subsección 7.2), el Comité toma nota de la necesidad de que el organismo de certificación especifique «*si se utilizan encargados del tratamiento y, en los casos en que el encargado sea el solicitante, se describirán sus responsabilidades y tareas, y en la solicitud figurará el contrato o contratos de responsable o encargado del tratamiento pertinentes.*». Si bien reconoce que la AC del Reino Unido ha utilizado la redacción del anexo 1, el Comité anima a esta a que considere la posibilidad de mencionar también en este caso una referencia a los responsables conjuntos y sus medidas específicas.

19. En lo que respecta a los métodos de evaluación (subsección 7.4), el Comité toma nota del requisito adicional previsto por la AC del Reino Unido en virtud del cual «*Además del punto 7.4.5 de la norma ISO17065, se dispondrá que la certificación existente, que se refiere al mismo objeto de certificación, podrá tenerse en cuenta como parte de una nueva evaluación […]».* En este sentido, el Comité considera que es necesario aclarar además que, en los casos en que la certificación existente se tenga en cuenta como parte de una nueva evaluación, el alcance de dicha certificación también debe evaluarse en detalle con respecto a su cumplimiento de los criterios de certificación pertinentes. Por lo tanto, el Comité anima a la AC del Reino Unido a que aclare la redacción en consecuencia.

20. En relación con la frase «*Puede considerarse el informe de evaluación completo o la información que permita una evaluación de la actividad de certificación anterior y sus resultados.*», el Comité recomienda a la AC del Reino Unido que se sustituya «puede» por «debe» cuando el organismo de certificación decida tener en cuenta la certificación existente. Además, el Comité considera que sería más claro referirse simplemente a la «certificación» en lugar de a la «actividad de certificación» y recomienda a la AC del Reino Unido que modifique el proyecto en consecuencia. Por otra parte, la referencia a la «certificación previa» podría ser engañosa, ya que no se refiere claramente a la certificación existente que el organismo de certificación desea tener en cuenta como parte de su propia evaluación. El Comité anima a la AC del Reino Unido a que modifique la redacción, a fin de

aclarar que la referencia se refiere a la certificación existente. Por último, el Comité observa que el organismo de certificación debe poder acceder al informe de evaluación y a cualquier otra información pertinente que permita evaluar la actividad de certificación, a fin de poder adoptar una decisión fundada. Por lo tanto, el Comité anima a la AC del Reino Unido a que aclare la redacción en consecuencia.

21. Además, en el párrafo que comienza con «*además del punto 7.4.6 de la norma ISO 17065*», el Comité considera que, cuando la AC del Reino Unido se refiere a «su mecanismo de certificación», en realidad se refiere al «sistema de certificación». Por lo tanto, el Comité anima a la AC del Reino Unido a que sustituya la redacción en consecuencia.

22. En lo que respecta a los cambios que afectan a la certificación (subsección 7.10) y, en particular, el cuarto punto («decisiones del Comité Europeo de Protección de Datos»), el Comité reconoce que la AC del Reino Unido ha utilizado la redacción prevista en el anexo 1. Sin embargo, a fin de asegurar una clara comprensión de lo que se entiende por «decisiones del Comité Europeo de Protección de Datos», el Comité anima a la AC del Reino Unido a que aclare la referencia. Un ejemplo podría ser la referencia a los «documentos adoptados por el Comité Europeo de Protección de Datos».

3 CONCLUSIONES Y RECOMENDACIONES

23. Los requisitos del proyecto de acreditación de la autoridad de control del Reino Unido pueden dar lugar a una aplicación incoherente de la acreditación de los organismos de certificación y deben introducirse los siguientes cambios:

24. Por lo que respecta a los «requisitos generales para la acreditación», el Comité recomienda a la AC del Reino Unido que:

    1. sustituya, en la subsección 4.1.1, la frase «debería poder aportar pruebas» por «deberá poder aportar pruebas»,

    2. incluya en la subsección 4.1.2 la parte que falta del requisito, para alinearlo con el texto del anexo 1 de las Directrices.

25. Por lo que se refiere a los «requisitos del proceso», el Comité recomienda a la AC del Reino Unido que:

    1. modifique la subsección 7.1, para establecer claramente que el cumplimiento de la protección de datos se refiere al titular de la certificación y que la investigación debe vincularse al alcance de la certificación y al objeto de la evaluación

    2. modifique la subsección 7.4 sustituyendo «puede» por «debe» y «actividad de certificación» por «certificación».

    3. sustituya la referencia al «mecanismo de certificación» por «sistema de certificación».

4 OBSERVACIONES FINALES

26. Este dictamen se dirige a la AC del Reino Unido y se hará público de conformidad con el artículo 64, apartado 5, letra b), del RGPD.

27. En virtud del artículo 64, apartados 7 y 8, del RGPD, la autoridad de control, en el plazo de dos semanas desde la recepción del dictamen, debe comunicar por medios electrónicos al presidente si va a mantener o modificar su proyecto de listado. Dentro del mismo periodo, deberá proporcionar 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 seguir este dictamen, en su totalidad o en parte.

Por el Comité Europeo de Protección de Datos

La Presidenta

(Andrea Jelinek)