Dictamen 15/2020 sobre el proyecto de decisión de las autoridades de control competentes de Alemania 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.

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.

(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

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

«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 (CE) n.º 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. En comparación con las obligaciones relativas a la acreditación de los organismos de certificación por parte de 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 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). 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 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. Las autoridades de control alemanas de la Federación y de los Länder (en lo sucesivo, las «AC DE») han 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 Alemania, DAkkS, 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 las AC DE, una vez que estas los aprueben, 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/pokyny/guidelines-42018-accreditation-certification-bodies-under_es

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 las AC DE han decidido recurrir a una acreditación conjunta por su organismo nacional de acreditación, el DAkkS, y la AC competente, 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 las AC DE 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 las AC DE de manera tal que resulte posible su aplicación práctica y coherente, según requiera el contexto de las 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 y a las AC competentes, en su caso, 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 las AC DE, debe interpretarse que el Comité no tiene ningún comentario que realizar y no solicita a las AC DE que adopten nuevas medidas.

9. El presente dictamen no trata los aspectos presentados por las AC DE 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 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 RGPD 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 q), 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

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 AC considere adecuado.

2.2.2 TÉRMINOS Y DEFINICIONES

12. El Comité observa que el capítulo 3 («Definiciones») del proyecto de requisitos de acreditación de las AC DE define los tipos de esquemas de certificación permitidos, especificando que deben cumplir con los requisitos de la norma DIN EN ISO/IEC 17065. A este respecto, debe señalarse que las secciones 5.1 y 5.2 de las Directrices del CEPD ya definen qué puede certificarse en virtud del RGPD de forma global. Por lo tanto, el Comité reconoce que la intención de las AC DE no es limitar lo establecido en las Directrices y que las afirmaciones contenidas en el capítulo 3 del proyecto de requisitos de acreditación de las AC DE deben considerarse aplicables en el contexto de estos requisitos de acreditación.

2.2.3 OBSERVACIONES GENERALES

13. El Comité observa que la sección de «notas generales» del proyecto de requisitos de acreditación de las AC DE hace referencia a la «autorización» de los criterios de certificación por parte del CEPD «de conformidad con los artículos 63 y 64, apartado 1, letra c), del RGPD». El Comité observa que el RGPD no otorga al CEPD competencias para «autorizar» criterios de certificación. No obstante, en virtud de los artículos antes citados, el CEPD puede aprobar criterios de certificación. Por lo tanto, el Comité recomienda a las AC DE que eliminen la referencia a la «autorización del CEPD» con el fin de que el proyecto esté en consonancia con la redacción de RGPD.

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

14. En cuanto al requisito de responsabilidad jurídica (sección 4.1. del proyecto de requisitos de acreditación de las AC DE), el Comité observa que, en el documento justificativo, las AC DE explican que se espera que el organismo de certificación tenga procedimientos actualizados y, por lo tanto, no es necesario añadir requisitos adicionales al respecto. Sin embargo, el Comité considera que una expectativa no obliga a los organismos de certificación a tener tales procedimientos. Según queda establecido en la sección 4.1.1 del anexo de las Directrices, los organismos de certificación deberán contar con procedimientos actualizados que demuestren el cumplimiento de las responsabilidades jurídicas establecidas en las condiciones de acreditación. Igualmente, el organismo de certificación deberá ser capaz de demostrar que los procedimientos y las medidas cumplen con el RGPD, especialmente en lo relativo al control y manejo de los datos personales de la empresa cliente como parte del proceso de certificación. Por lo tanto, el Comité recomienda a las AC DE que modifiquen el proyecto de requisitos para que esté en consonancia con las Directrices.

15. En relación con el subapartado 4.1.2.2 del proyecto de requisitos de acreditación de las AC DE («acuerdo de certificación»), el Comité observa que el proyecto de requisitos de acreditación de las AC DE no incluye la obligación de permitir plena transparencia a la AC competente en relación con el

procedimiento de certificación, incluidos asuntos contractualmente confidenciales. Asimismo, no se hace referencia a la obligación por parte del solicitante de facilitar al organismo de certificación acceso a sus actividades de tratamiento. Por lo tanto, el Comité recomienda a las AC DE que incluyan dichas obligaciones en su proyecto.

16. El Comité observa que la referencia explícita a las tareas y las facultades de la AC competente (tercer guion de la sección 4.1.2 del anexo) no está incluida en el subapartado 4.1.2.2 del proyecto de requisitos de acreditación de las AC DE. El Comité considera que se debe añadir esta referencia en el proyecto de requisitos y, por lo tanto, recomienda a las AC DE que modifiquen el proyecto en consecuencia.

17. Asimismo, el proyecto de requisitos de las AC DE relativo al acuerdo de certificación no incluye la obligación de permitir al organismo de certificación comunicar toda la información necesaria para conceder la certificación con arreglo al artículo 42, apartado 8, y el artículo 43, apartado 5, del RGPD (séptimo guion de la sección 4.1.2 del anexo). A pesar de que dicha obligación está incluida en la sección sobre la gestión de procesos del proyecto de requisitos de acreditación de las AC DE, el Comité considera que debe formar parte del acuerdo de certificación con el fin de consolidar su naturaleza vinculante. Por ende, el Comité recomienda a las AC DE que incluyan dicha obligación como parte de los componentes del acuerdo de certificación.

18. En virtud del anexo, el solicitante debe informar al organismo de certificación de los cambios significativos que se produzcan en su situación real y jurídica y en sus productos, procesos y servicios afectados por la certificación (décimo guion de la sección 4.1.2 del anexo). Sin embargo, el sexto guion del subapartado 4.1.2.2 del proyecto de requisitos de acreditación de las AC DE incluye únicamente la obligación de informar al organismo de certificación de los cambios significativos que se produzcan en circunstancias reales o jurídicas, pero no menciona explícitamente los productos, procesos y servicios. El Comité recomienda a las AC DE que incluyan dicha referencia, en consonancia con el anexo.

19. En lo que respecta al subapartado 4.2.7 del proyecto de requisitos de acreditación de las AC DE («gestión de la imparcialidad»), el Comité recomienda reforzar los criterios aplicables a los organismos de certificación que pertenezcan o estén controlados por una entidad jurídica independiente a fin de tener en cuenta que todo tipo de relación económica entre el organismo de certificación y la entidad jurídica, en función de sus características, puede afectar a la imparcialidad de sus actividades de certificación.

20. En lo que respecta a la sección 4.6 del proyecto de requisitos de acreditación de las AC DE («información de acceso público»), el Comité observa que no se hace referencia a la publicación de todas las versiones de los criterios aprobados y los procedimientos de certificación. Por lo tanto, el Comité anima a las AC DE a que modifiquen el proyecto de requisitos de acreditación con el fin hacer explícito que la publicación incluye todas las versiones de los criterios aprobados y los procedimientos de acreditación. Asimismo, el Comité observa que el segundo párrafo de la sección 4.6 declara que «los esquemas de certificación usados por el organismo de certificación los criterios aprobados conforme al artículo 42, apartado 5, del RGPD por los que se establece el periodo de aplicación permitido, *se publicarán de forma general*». Para evitar cualquier ambigüedad, el Comité anima a las AC DE a que eliminen la expresión «de forma general» e incluyan un «y» entre «organismo de certificación» y «los criterios aprobados».

2.2.5 REQUISITOS DE RECURSOS HUMANOS (capítulo 6 del proyecto de requisitos para la acreditación)

21. En cuanto a los requisitos de pericia y concretamente el subapartado 6.1.2.1 del proyecto de requisitos de acreditación de las AC DE («competencia de recursos humanos»), el Comité observa que los conocimientos exigidos en los ámbitos enumerados no especifican que dichos conocimientos deban ser relevantes y adecuados. Con el fin de garantizar la coherencia con el nivel de pericia exigido en el anexo, el Comité recomienda a las AC DE que pongan la redacción en consonancia con las Directrices exigiendo que los conocimientos sean relevantes y adecuados.

22. Asimismo, el Comité observa que los requisitos para el personal con conocimientos técnicos responsable de adoptar las decisiones incluyen una experiencia profesional de, al menos, siete años o una experiencia profesional de cinco años en el campo de la protección de datos técnicos, en función de su nivel educativo, mientas que el personal responsable de las evaluaciones deberá contar con cuatro años de experiencia profesional o dos años de experiencia profesional en el campo de la protección de datos técnicos y experiencia en procedimientos de prueba, en función de su nivel educativo. De manera semejante, el personal con conocimientos jurídicos responsable de adoptar las decisiones debe contar con, al menos, cinco años de experiencia profesional en normativa sobre protección de datos, mientras que las personas a cargo de las evaluaciones precisan de dos años de experiencia en normativa sobre protección de datos y procedimientos de auditoría. 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 los requisitos en materia de competencias para evaluadores y responsables de la toma de decisiones deberán adaptarse teniendo en cuenta las diferentes funciones que realizan, en lugar de los años de experiencia. El Comité considera que 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 las AC DE a hacer más hincapié en la diferencia en los conocimientos sustantivos y/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.

23. Asimismo, el Comité considera que los conocimientos de los sistemas de gestión relativos al ámbito de certificación deberán ampliarse a la norma ISO/IEC 27701:2019 Técnicas de seguridad. Extensión para las normas ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la privacidad de la información. Requisitos y directrices, y anima a las AC DE a incluir dicha referencia.

24. Por último, en relación con los requisitos de educación para el personal técnico, el Comité considera que la lista de ámbitos ya está adaptada a la experiencia técnica exigida por el anexo. Por lo tanto, el Comité anima a las AC DE a eliminar la referencia a «ciencias naturales» de la lista de ámbitos relativa a la educación universitaria del personal técnico.

2.2.6 REQUISITOS DE LOS PROCESOS (capítulo 7 del proyecto de requisitos para la acreditación)

25. El Comité observa que el capítulo 7 del proyecto de requisitos de acreditación de las AC DE hace referencia en varias ocasiones al término «sus criterios» (p. ej., en las secciones 7.4, 7.6, 7.11 y 7.13). Para evitar cualquier ambigüedad, el Comité anima a las AC DE a aclarar el significado de dicho término, por ejemplo, añadiendo una explicación en el anexo 1 (Glosario).

26. En cuanto a la sección 7.1 del proyecto de requisitos de acreditación de las AC DE («información general»), el Comité observa que no se hace referencia expresa a la obligación del organismo de certificación a cumplir con los requisitos adicionales. A pesar de que dicha obligación puede deducirse del texto del proyecto de requisitos, el Comité considera que deberá incluirse una referencia explícita a dicha obligación. Por lo tanto, el Comité recomienda a las AC DE que modifiquen el proyecto en consecuencia.

27. El Comité observa que el proyecto de requisitos adicionales de las AC DE no incluye ninguna referencia a la operación de un Sello Europeo de Protección de Datos aprobado, de conformidad con la sección 7.1.2 del anexo. El Comité considera que se debe incluir esta referencia, especialmente teniendo en cuenta que la acreditación de un organismo de certificación que conceda Sellos Europeos de Protección de Datos debe llevarse a cabo en cada uno de los Estados miembros en los que esté establecido el organismo de certificación.[3] Por lo tanto, el Comité recomienda a las AC DE que incluyan la referencia anterior. Por ejemplo, el proyecto de requisitos podría incluir lo siguiente: *«Se notificará a la AC competente antes de que un organismo de certificación comience a operar un Sello Europeo de Protección de Datos aprobado en un nuevo Estado miembro en una oficina auxiliar».*

28. El Comité observa que en la sección 7.2 («solicitud»), el proyecto de requisitos de acreditación de las AC DE prevé la situación en la que intervengan los encargados en la realización de operaciones de tratamiento de datos, en consonancia con el anexo de las Directrices. Sin embargo, el Comité observa que, cuando intervengan los encargados, la solicitud contendrá los contratos relevantes del responsable/encargado, según queda establecido en el anexo. Por lo tanto, el Comité recomienda a las AC DE poner la redacción en consonancia con las directrices mediante la inclusión de la referencia a los contratos del responsable/encargado. Asimismo, el Comité anima a las AC DE a considerar si, para esta caso en concreto, también debe incluirse una referencia a los corresponsables del tratamiento y a los acuerdos específicos.

29. El Comité observa que en la sección 7.2 del proyecto de requisitos de acreditación de las AC DE se especifica que «el responsable y el encargado de los datos están facultados para presentar una solicitud de certificación». La posibilidad de que los encargados presenten una solicitud de certificación dependerá del esquema de certificación específico. Por lo tanto, para evitar cualquier confusión, el Comité anima a las AC DE a que eliminen dicha referencia o aclaren que la posibilidad de que los encargados reciban una certificación dependerá del ámbito de aplicación del esquema de certificación.

30. En relación con la sección 7.3 del proyecto de requisitos de acreditación de las AC DE («solicitudes de evaluación»), el Comité observa que el proyecto de requisitos de acreditación de las AC DE establece que «los métodos de evaluación previstos están estipulados contractualmente [...]». Con el fin de aclarar que se trata de un requisito, el Comité anima a las AC DE a que redacten de nuevo el primer

[3] A este respecto, véase las Directrices 1/2018, párrafo 44.

párrafo para aclarar que los métodos de evaluación deberán incluirse en el acuerdo de certificación, esto es, volver a redactar el requisito como «los métodos de evaluación previstos deberán estar estipulados contractualmente [...]». Asimismo, el Comité anima a las AC DE a que sustituyan la referencia a la sección 7.3.1.b de la norma ISO 17065 por la sección 7.3 de la norma ISO 17065 para poner la redacción en consonancia con el anexo. Además, el Comité observa que el cuarto párrafo hace referencia a competencias técnicas y jurídicas adecuadas. En aras de la claridad, el Comité anima a las AC DE a que añadan «en materia de protección de datos».

31. El Comité observa que la sección 7.4 del proyecto de requisitos de acreditación de las AC DE («métodos de evaluación») no obliga al organismo de certificación a describir métodos de evaluación suficientes para evaluar el cumplimiento de los criterios de certificación por parte de las operaciones de tratamiento. El Comité recomienda a las AC DE que modifiquen el proyecto de requisitos para incluir dicha referencia. Un ejemplo podría ser añadir lo siguiente: *«El organismo de certificación deberá garantizar que los mecanismos usados para conceder una certificación describan métodos de evaluación suficientes para evaluar el cumplimiento de los criterios de certificación por parte de las operaciones de tratamiento»*. Asimismo, en lo que respecta al primer ámbito que se abordará en los métodos de evaluación, el Comité considera que la necesidad y la proporcionalidad también se evaluarán en relación con los interesados afectados, cuando proceda. Por último, el Comité observa que no se hace ninguna referencia a la documentación de los métodos y las conclusiones. Por lo tanto, el Comité anima a las AC DE a que modifiquen el proyecto y que incluyan de manera explícita dichas referencias.

32. En relación con las certificaciones existentes (sección 7.4 del proyecto de requisitos de acreditación de las AC DE), el Comité considera que el cuarto guion de la página 13 crea confusión, puesto que no queda clara la relación entre los periodos de validez de certificaciones vigentes y de certificaciones previas, y cómo se encajarían la una con la otra. Además, no parece posible cuestionar la validez de la certificación previamente emitida por un organismo de certificación acreditado diferente. En resumen, convendría aclarar un poco el párrafo sobre la relación entre la mención de los diferentes elementos. El Comité recomienda a las AC DE que modifiquen el proyecto en particular aclarando que el periodo de validez de la certificación del RGPD no debe depender de la validez de otros tipos de certificaciones.

33. En cuanto a la sección 7.5 («valoración») del proyecto de requisitos de acreditación de las AC DE, el Comité anima a las AC DE a que cambien el título de la sección por «revisión».

34. En relación con las modificaciones que afectan a la certificación (sección 7.10 del proyecto de requisitos de acreditación de las AC DE), el Comité observa que el proyecto de requisitos de acreditación de las AC DE establece que «se informa al cliente de manera oportuna de las modificaciones en el marco legal que le afecten». Teniendo en mente la necesidad de preservar la imparcialidad del organismo de certificación, el Comité anima a las AC DE a que reformulen la frase para dejar claro que el cliente recibirá, de manera oportuna, la información general sobre modificaciones que puedan afectarle. Asimismo, 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 las AC DE a que aclaren la referencia. Un ejemplo podría ser la referencia a los «documentos adoptados por el Comité Europeo de Protección de Datos».

35. El Comité observa que la sección 7.11 del proyecto de requisitos de acreditación de las AC DE («cancelación, limitación, suspensión o retirada de la certificación») no obliga al organismo de certificación a aceptar decisiones y órdenes de las AC DE 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 las AC DE que incluyan dicha obligación. Además, el Comité anima a las AC DE a que sustituyan la palabra «limitación» por «reducción» del título de la sección, de acuerdo con el anexo de las Directrices.

2.2.7 OTROS REQUISITOS ADICIONALES

36. En relación con el subapartado 8.11.3 de los requisitos de acreditación de las AC DE («tramitación de reclamaciones»), el Comité anima a las AC DE a sustituir la referencia a «reclamaciones justificadas» por «reclamaciones fundamentadas» para una mayor claridad.

3 CONCLUSIONES / RECOMENDACIONES

37. El proyecto de requisitos de acreditación de las autoridades de control alemanas de la Federación y de los Länder puede dar lugar a una aplicación incoherente de la acreditación de los organismos de certificación, y deben realizarse los siguientes cambios:

38. Por lo que respecta a las «observaciones generales», el Comité recomienda a las AC DE que:

    1) eliminen la referencia a la «autorización del CEPD» con el fin de que el proyecto esté en consonancia con la redacción de RGPD.

39. Por lo que respecta a los «requisitos generales para la acreditación», el Comité recomienda a las AC DE:

    1) Modificar los requisitos en cuanto a la responsabilidad jurídica (subapartado 4.1) con el fin de que estén en consonancia con las directrices.

    2) Modificar el subapartado 4.1.2.2 para incluir, en el acuerdo de certificación, la obligación de permitir plena transparencia de las AC DE en relación con el procedimiento de certificación y dar acceso al organismo de certificación a las actividades de tratamiento del solicitante.

    3) Incluir, en el subapartado 4.1.2.2, una referencia explícita a las tareas y las facultades de la AC competente, conforme al anexo.

    4) Incluir, entre los componentes del acuerdo de certificación, la obligación de permitir al organismo de certificación comunicar toda la información necesaria para conceder la certificación con arreglo al artículo 42, apartado 8, y el artículo 43, apartado 5, del RGPD.

    5) Incluir una referencia explícita a los «productos, procesos y servicios afectados por la certificación» en el sexto guion del subapartado 4.1.2.2.

    6) Reforzar, en el subapartado 4.2.7, los criterios aplicables a los organismos de certificación que pertenezcan o estén controlados por una entidad jurídica independiente a fin de tener en cuenta que todo tipo de relación económica entre el organismo de certificación y la entidad jurídica, en función de sus características, puede afectar a la imparcialidad de sus actividades de certificación.

40. En cuanto a los «requisitos en materia de recursos», el Comité recomienda a las AC DE:

1) Redactar el subapartado 6.1.2.1 en consonancia con las directrices exigiendo que los conocimientos sean relevantes y adecuados.

41. En cuanto a los «requisitos de los procesos», el Comité recomienda a las AC DE:

1) Modificar la sección 7.1 para que haga referencia explícita a la obligación del organismo de certificación a cumplir con los requisitos adicionales.

2) Incluir una referencia a la operación de un Sello Europeo de Protección de Datos aprobado.

3) Redactar la sección 7.2 en consonancia con las directrices mediante la inclusión de la referencia a los contratos del responsable/encargado.

4) Incluir en la sección 7.4 la obligación del organismo de certificación de describir métodos de evaluación suficientes para evaluar el cumplimiento de los criterios de certificación por parte de las operaciones de tratamiento.

5) Aclarar, en la sección 7.4, que el periodo de validez de la certificación del RGPD no debe depender de la validez de otros tipos de certificaciones.

6) Incluir, en la sección 7.11, la obligación del organismo de certificación de aceptar las decisiones y órdenes de las AC DE 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

42. El presente dictamen se dirige a las autoridades de control alemanas de la Federación y de los Länder y se publicará de conformidad con el artículo 64, apartado 5, letra b), del RGPD.

43. De conformidad con el artículo 64, apartados 7 y 8, del RGPD, las AC DE deberán comunicar por medios electrónicos a la presidenta, en el plazo de dos semanas desde la recepción del dictamen, si van a mantener o modificar su proyecto de decisión. Dentro del mismo periodo, deberán proporcionar el proyecto de decisión enmendado o, cuando no tengan la intención de seguir el dictamen del Comité, deberán indicar los motivos pertinentes por los cuales no tienen intención de seguir este dictamen, en su totalidad o en parte.

44. Las AC DE deberán 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)

Adoptado