Dictamen conjunto [4/2026] del CEPD-SEPD

sobre la propuesta de Reglamento sobre la Ciberseguridad 2
y la propuesta de modificación de la Directiva SRI 2

Adoptado el 18 de marzo de 2026

Índice

Resumen

El 20 de enero de 2026, la Comisión Europea publicó una propuesta de Reglamento relativo a la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el marco europeo de certificación de la ciberseguridad y la seguridad de las cadenas de suministro de TIC y por el que se deroga el Reglamento (UE) 2019/881 («Reglamento sobre la Ciberseguridad 2») y una propuesta de Directiva por la que se modifica la Directiva (UE) 2022/2555 sobre medidas de simplificación y armonización con la [propuesta de Reglamento sobre la Ciberseguridad 2]. El 21 de enero de 2026, la Comisión consultó formalmente al Comité Europeo de Protección de Datos (CEPD) y al Supervisor Europeo de Protección de Datos (SEPD) de conformidad con el artículo 42, apartado 2, del Reglamento (UE) 2018/1725.

El CEPD y el SEPD recuerdan que la relación entre la protección de datos y la ciberseguridad es bidireccional. Por una parte, la ciberseguridad contribuye a la protección de los datos personales al limitar los riesgos de acceso no deseado, modificación o indisponibilidad de dichos datos. Por otra parte, algunas medidas de ciberseguridad pueden interferir con los derechos y las libertades de las personas, en particular los derechos a la privacidad y a la protección de datos. Por lo tanto, si bien la eficacia es un objetivo importante de las medidas de ciberseguridad, deben tenerse en cuenta la necesidad y la proporcionalidad.

El CEPD y el SEPD apoyan el objetivo general de las propuestas de reforzar el papel de ENISA y facilitar la adopción de la certificación de la ciberseguridad, conforme a las recomendaciones específicas formuladas en el presente Dictamen conjunto. También acogen con satisfacción el objetivo de establecer mecanismos y condiciones en la Directiva (UE) 2022/2555 para ayudar a facilitar el cumplimiento de los requisitos de ciberseguridad y, de este modo, hacer que su aplicación sea más coherente y eficaz, así como el objetivo de seguir abordando los diversos riesgos para las cadenas de suministro de TIC, incluidos los que no son técnicos. Asimismo, el CEPD y el SEPD apoyan firmemente el objetivo de establecer un punto de entrada único para la notificación de las violaciones de la seguridad de los datos personales, ya que reduciría la carga administrativa para las organizaciones sin afectar al nivel de protección de los interesados.

El CEPD y el SEPD también acogen con satisfacción que en la propuesta de Reglamento sobre la Ciberseguridad 2 se proporcionen más aclaraciones sobre las modalidades de la prestación de apoyo de ENISA a las distintas partes interesadas y recomiendan añadir también al SEPD como posible solicitante de asesoramiento de ENISA. El CEPD y el SEPD apoyan firmemente que dicho asesoramiento responda a una solicitud, lo que garantiza una coordinación y una división claras de las responsabilidades.

Por lo que se refiere a la cooperación entre ENISA y otras entidades de la Unión en general, el CEPD y el SEPD acogen con satisfacción las sinergias que esta cooperación puede permitir, en consonancia con sus respectivas tareas y mandatos. Recomiendan añadir una referencia explícita también al SEPD como organismo de la Unión, con el que cooperaría ENISA.

El CEPD y el SEPD consideran que, si las futuras tareas de ENISA como centro de información requieren un tratamiento sustancial de datos personales, esto debe especificarse explícitamente en las disposiciones del acto de base que regule las respectivas tareas, incluidos los elementos esenciales de cualquier tratamiento a gran escala y las garantías adecuadas. Por el contrario, si el objetivo es permitir que ENISA recopile y trate principalmente datos no personales agregados, esto también debe aclararse.

El CEPD y el SEPD recuerdan que, en principio, solo los detalles (prácticos) muy técnicos relacionados con el tratamiento de los datos personales deben decidirse en virtud de la autonomía administrativa del organismo de la UE de que se trate (en este caso, el Consejo de Administración de una agencia descentralizada). Además, el CEPD y el SEPD recomiendan establecer en el artículo 66 de la propuesta de Reglamento sobre la Ciberseguridad 2 una consulta previa con el SEPD antes de la adopción de dichas normas.

Por lo que se refiere al Marco Europeo de Capacidades en Ciberseguridad (ECSF, por sus siglas en inglés), el CEPD y el SEPD recomiendan a los colegisladores que modifiquen el artículo 19, apartado 2, de la propuesta de Reglamento sobre la Ciberseguridad 2 para que el ECSF no se limite exclusivamente a los «profesionales de la ciberseguridad», sino que también incluya perfiles para el personal en general.

Por lo que se refiere al marco europeo de certificación de la ciberseguridad, el CEPD y el SEPD recomiendan aclarar en mayor medida el ámbito de aplicación del artículo 80, apartado 1, letra w), del Reglamento sobre la Ciberseguridad 2 y la relación con la certificación del Reglamento General de Protección de Datos (RGPD). Además, el CEPD y el SEPD recomiendan que se exija a ENISA que consulte al CEPD antes de adoptar un esquema de certificación con arreglo al artículo 80, apartado 1, letra w), del Reglamento sobre la Ciberseguridad 2 para garantizar la coherencia.

El CEPD y el SEPD destacan la exigencia de tener en cuenta no solo la eficacia de las medidas de ciberseguridad, sino también su necesidad y proporcionalidad. El CEPD y el SEPD recomiendan aclarar que los esquemas de certificación deben tener en cuenta, en la medida de lo posible, los controles de seguridad que puedan ayudar a demostrar el cumplimiento de los requisitos del RGPD, en particular cuando los esquemas se apliquen a productos, servicios y procesos de TIC y a servicios de seguridad gestionados que puedan utilizarse en operaciones de tratamiento de datos.

El CEPD y el SEPD también acogen con satisfacción la medida propuesta destinada a garantizar un marco de confianza de las cadenas de suministro de TIC y a hacer frente a los riesgos no técnicos en sectores de alta criticidad.

Por lo que se refiere a la propuesta por la que se modifica la Directiva SRI 2, el CEPD y el SEPD acogen con satisfacción la designación de los proveedores de carteras europeas de identidad digital y de carteras europeas para empresas como «entidades esenciales», y apoyan plenamente el importante objetivo de prevenir futuros ataques con programas de secuestro y desarticular y desmantelar las organizaciones delictivas que están detrás de ellos.

El Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos

Visto el artículo 42, apartado 2, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE,

Han adoptado el siguiente Dictamen conjunto (el «Dictamen»)

1 ANTECEDENTES

1. El 20 de enero de 2026, la Comisión Europea publicó una propuesta de Reglamento relativo a la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el marco europeo de certificación de la ciberseguridad y la seguridad de las cadenas de suministro de TIC y por el que se deroga el Reglamento (UE) 2019/881 («el Reglamento sobre la Ciberseguridad 2»)[1] y una propuesta de Directiva por la que se modifica la Directiva (UE) 2022/2555 sobre medidas de simplificación y armonización con la [Propuesta de Reglamento sobre la Ciberseguridad 2[2]] (en lo sucesivo, «la propuesta de Reglamento sobre la Ciberseguridad 2», «la propuesta de modificación de la Directiva SRI 2» y, en conjunto, «las propuestas»). El 21 de enero de 2026, la Comisión consultó formalmente al CEPD y al SEPD de conformidad con el artículo 42, apartado 2, del Reglamento (UE) 2018/1725 («Reglamento de protección de datos para las instituciones, órganos y organismos de la UE» o EUDPR por sus siglas en inglés)[3].
2. La propuesta de Reglamento sobre la Ciberseguridad 2[4] tiene por objeto sustituir el actual Reglamento sobre la Ciberseguridad con el fin de 1) reforzar el papel de ENISA centrándose en las necesidades de las partes interesadas en un panorama de amenazas cada vez más hostil; 2) reactivar la aplicación del marco europeo de certificación de la ciberseguridad (ECCF, por sus siglas en inglés); 3) reducir la complejidad y la diversidad de las políticas relacionadas con la ciberseguridad; y 4) seguir abordando los riesgos de seguridad de las cadenas de suministro de TIC[5].

[1] COM(2026) 11 final.
[2] COM(2026) 13 final.
[3] Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).
[4] Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad») (DO L 151 de 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj, modificado por el Reglamento (UE) 2025/37 del Parlamento Europeo y del Consejo, de 19 de diciembre de 2024, por el que se modifica el Reglamento (UE) 2019/881 en lo que se refiere a los servicios de seguridad gestionados (DO L, 2025/37, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/37/oj).
[5] Exposición de motivos, COM(2026) 11 final, p. 1.

3. La propuesta de modificación de la Directiva SRI 2 se centra, en particular, en el tercer objetivo, introduciendo aclaraciones y facilitando el cumplimiento por parte de las entidades reguladas[6].

4. El objetivo del presente Dictamen conjunto es abordar los aspectos pertinentes de las propuestas que revisten especial importancia para la protección de los derechos y libertades de las personas en lo que respecta al tratamiento de datos personales.

2 OBSERVACIONES GENERALES

5. La propuesta de Reglamento sobre la Ciberseguridad 2 tiene por objeto ampliar el mandato de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y hacerla más operativa. El CEPD y el SEPD apoyan el refuerzo del papel de ENISA y el objetivo de facilitar la adopción de la certificación de la ciberseguridad, conforme a las recomendaciones específicas que figuran a continuación

6. También acogen con satisfacción el objetivo de establecer mecanismos y condiciones en la Directiva (UE) 2022/2555[7] (en lo sucesivo, «la Directiva SRI 2») para ayudar a facilitar el cumplimiento de los requisitos de ciberseguridad y, de este modo, hacer que su aplicación sea más coherente y eficaz, así como el objetivo de seguir abordando los diversos riesgos para las cadenas de suministro de TIC, incluidos los que no son técnicos.

7. Como ya señalaron en su dictamen conjunto sobre la propuesta «Ómnibus Digital»[8], el CEPD y el SEPD apoyan firmemente el objetivo de establecer un punto de entrada único para la notificación de las violaciones de la seguridad de los datos personales, ya que reduciría la carga administrativa para las organizaciones sin afectar al nivel de protección de los interesados.

8. El artículo 5, apartado 1, letra f), del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, RGPD) establece la seguridad como uno de los principios fundamentales relativos al tratamiento de datos personales. El artículo 32 del RGPD define con más detalle esta obligación, aplicable tanto a los responsables como a los encargados del tratamiento, para garantizar un nivel adecuado de seguridad. En ambas disposiciones se deja claro que la seguridad del tratamiento de datos personales es esencial para el cumplimiento del Derecho de la Unión en materia de protección de datos.

9. La relación entre la protección de datos y la ciberseguridad es doble. Por una parte, la ciberseguridad contribuye a la protección de los datos personales al limitar los riesgos de acceso no deseado, modificación o indisponibilidad de dichos datos. Por la otra parte, algunas medidas de ciberseguridad pueden interferir con los derechos y las libertades de las personas, en particular los derechos a la privacidad y a la protección de datos[9].

[6] COM(2026) 13 final.

[7] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

[8] Dictamen conjunto 2/2026 del CEPD-SEPD sobre la propuesta de Reglamento en lo que respecta a la simplificación del marco legislativo digital (Ómnibus Digital), adoptado el 10 de febrero de 2026.

[9] Véase el Dictamen 5/2021 del SEPD sobre la Estrategia de Ciberseguridad y la Directiva SRI 2.0, de 11 de marzo de 2021, apartados 10 y 11, el Dictamen 7/2022 del SEPD sobre la propuesta de Reglamento relativo a la seguridad de la información en las instituciones, órganos y organismos de la Unión, de 17 de mayo de 2022, apartados 9 y 10, y el Dictamen 2/2024 del SEPD sobre la propuesta de Reglamento por el que se modifica la Ley de Ciberseguridad en lo que respecta a los servicios de seguridad gestionados, de 10 de enero de 2024, apartado 5.

10. El CEPD y el SEPD recuerdan que el considerando 49 del RGPD reconoce que las medidas de ciberseguridad que implican el tratamiento de datos personales constituyen un interés legítimo del responsable del tratamiento de que se trate, subrayando al mismo tiempo que las medidas deben ser estrictamente necesarias y proporcionadas para garantizar la seguridad de las redes y de la información. En consecuencia, las medidas de ciberseguridad no solo deben guiarse por consideraciones de eficacia, sino también tener en cuenta si sus repercusiones en los derechos fundamentales se limitan a lo necesario y proporcionado.

3 APOYO DE ENISA A LA EJECUCIÓN DE LA POLÍTICA Y DEL DERECHO DE LA UNIÓN Y COOPERACIÓN CON OTRAS ENTIDADES DE LA UNIÓN

11. De conformidad con el artículo 5, apartado 1, de la propuesta de Reglamento sobre la Ciberseguridad 2, ENISA contribuirá a la ejecución de la política y del Derecho de la Unión en diversos ámbitos, prestando apoyo a las distintas partes interesadas enumeradas en dicho artículo.

12. Entre ellos, de conformidad con el artículo 5, apartado 1, letra h), de la propuesta de Reglamento sobre la Ciberseguridad 2, ENISA proporcionaría, a petición del Comité Europeo de Protección de Datos, asesoramiento sobre la aplicación de aspectos específicos de ciberseguridad de la política y el Derecho de la Unión en materia de protección de datos y privacidad. El CEPD y el SEPD observan que el artículo 5, apartado 1, letra h), de la propuesta de Reglamento sobre la Ciberseguridad 2 no es una disposición completamente nueva. En el artículo 5, apartado 5, letra c), del actual Reglamento sobre la Ciberseguridad ya se establece que ENISA puede asistir «a los Estados miembros en la ejecución de aspectos específicos de ciberseguridad de la política y el Derecho de la Unión en materia de protección de los datos y la privacidad, así como la emisión, previa solicitud de un dictamen para el Comité Europeo de Protección de Datos».

13. El CEPD y el SEPD acogen con satisfacción que la propuesta de Reglamento sobre la Ciberseguridad 2 aporte más aclaraciones sobre las modalidades de cooperación, manteniendo al mismo tiempo los elementos fundamentales del artículo 5, apartado 5, letra c), del Reglamento sobre la Ciberseguridad. En el nuevo artículo 5, apartado 1, letra h), se aclararía que el CEPD, como organismo de la Unión, tiene derecho a solicitar directamente el asesoramiento de ENISA (sin estar vinculado a la aplicación por parte de los Estados miembros de aspectos específicos de ciberseguridad de la política y el Derecho de la Unión en materia de protección de datos y privacidad).

14. Al mismo tiempo, el CEPD y el SEPD recomiendan añadir también al SEPD como posible solicitante en el artículo 5, apartado 1, letra h), del Reglamento sobre la Ciberseguridad 2, habida cuenta del papel de este último como autoridad de control para el tratamiento de datos personales por parte de las instituciones, los órganos y los organismos de la Unión Europea. Permitir que tanto el CEPD como el SEPD recurran a la competencia técnica de ENISA en el ámbito de la ciberseguridad puede contribuir a garantizar que sus orientaciones y decisiones en el ámbito de la protección de datos se basen en los conocimientos más avanzados en materia de ciberseguridad. Podría haber varios temas para los que el asesoramiento y la cooperación pueden ser beneficiosos, incluidas las normas y prácticas operativas en materia de ciberseguridad, así como el uso de tecnologías de protección de la privacidad (PETs, por sus siglas en inglés) en el contexto de la ciberseguridad.

15. El CEPD y el SEPD apoyan firmemente que el asesoramiento mencionado en el artículo 5, apartado 1, letra h), del Reglamento sobre la Ciberseguridad 2 solo se preste previa solicitud del CEPD o, como aquí se propone, del SEPD. Al disponer que ENISA solo actúe a petición del CEPD o del SEPD, el artículo 5, apartado 1, letra h) garantizaría una coordinación y una división de responsabilidades claras[10].

16. El CEPD y el SEPD observan que el artículo 5, apartado 1, letra h), de la propuesta de Reglamento sobre la Ciberseguridad 2 resulta una manifestación específica de la obligación de cooperación más general consagrada en el artículo 68 de la propuesta de Reglamento sobre la Ciberseguridad 2, que regula la cooperación de ENISA con otras entidades de la Unión. De conformidad con el artículo 68, ENISA cooperará en asuntos relacionados con la ciberseguridad con otros organismos de la UE, incluido el Comité Europeo de Protección de Datos, para garantizar la coherencia, crear sinergias y abordar cuestiones de interés común. Esta cooperación podrá garantizarse mediante el intercambio de conocimientos técnicos y mejores prácticas, la prestación de asesoramiento y directrices sobre cuestiones de interés relacionadas con la ciberseguridad y el establecimiento de disposiciones prácticas para la ejecución de tareas específicas previa consulta a la Comisión.

17. El CEPD y el SEPD acogen con satisfacción la cooperación y las sinergias entre ENISA y otras entidades de la Unión, en consonancia con sus respectivas tareas y mandatos. En este contexto, en aras de la claridad jurídica, el CEPD y el SEPD recomiendan modificar el artículo 68 de la propuesta de Reglamento sobre la Ciberseguridad 2 añadiendo una referencia explícita también al SEPD como organismo de la Unión, con el que ENISA cooperaría[11].

4 COOPERACIÓN OPERATIVA, CONOCIMIENTO COMPARTIDO DE LA SITUACIÓN EN MATERIA DE CIBERSEGURIDAD Y PROTECCIÓN DE LOS DATOS PERSONALES

[10] Al condicionar la participación de ENISA a la solicitud de las autoridades de control, se mantiene un proceso de consulta estructurado, en el que ENISA proporciona conocimientos técnicos, mientras que dichas autoridades conservan el pleno control sobre las decisiones relacionadas con la protección de datos. También garantiza que se coordine cualquier intervención de la ENISA, con el CEPD o el SEPD tomando la iniciativa y determinando la línea de actuación adecuada. Este respeto de las funciones establecidas promueve la coherencia, evita la fragmentación normativa y refuerza la rendición de cuentas de los organismos de protección de datos en su función de supervisión.

[11] El CEPD y el SEPD consideran que el artículo 7, apartado 2, del actual Reglamento sobre la Ciberseguridad, que obliga a ENISA a cooperar a nivel operativo y a establecer sinergias con las instituciones, órganos y organismos de la Unión, entre otros con las autoridades de control que se ocupan de la protección de la privacidad y los datos personales, con vistas a abordar cuestiones de interés común, ya se extiende al SEPD.

18. En virtud de los artículos 10 y 11 de la propuesta de Reglamento sobre la Ciberseguridad 2, que constituiría un nuevo desarrollo del artículo 7 actual del Reglamento sobre la Ciberseguridad, ENISA ampliaría su papel como centro de cooperación operativa, que incluiría el tratamiento de cantidades sustanciales de información de inteligencia sobre amenazas[12]. Como consecuencia de ello, podría deducirse que la información tratada por ENISA como parte de su función puede incluir datos personales, como direcciones IP, credenciales de usuario, registros de usuarios, intercambios financieros o datos de cuentas comprometidas.

19. Tras las aclaraciones facilitadas por la Comisión Europea[13], el CEPD y el SEPD entienden que no se pretende que el Reglamento sobre la Ciberseguridad 2 imponga ni autorice ningún tratamiento a gran escala de datos personales por parte de ENISA[14].

    Si bien toman nota de que ENISA recopilaría y trataría principalmente datos no personales agregados, el CEPD y el SEPD recuerdan, no obstante, que si las futuras tareas de ENISA como centro de información requieren un tratamiento sustancial de datos personales, esto debe especificarse explícitamente en las disposiciones del acto de base que regule las respectivas tareas, incluidos los elementos esenciales de cualquier tratamiento a gran escala y las garantías adecuadas. Por el contrario, si el objetivo es permitir que ENISA recopile y trate principalmente datos no personales agregados, esto también debe aclararse, al menos mediante un considerando.

20. El CEPD y el SEPD observan que ENISA seguiría tratando datos personales con fines administrativos[15]. El artículo 66, apartado 1, de la propuesta de Reglamento sobre la Ciberseguridad 2, al igual que el Reglamento sobre la Ciberseguridad actual[16], contiene una referencia general a la legislación aplicable en materia de protección de datos, el Reglamento de protección de datos para las instituciones, órganos y organismos de la UE, sin establecer ninguna otra norma específica.

[12] Véase COM(2026) 11 final, ficha legislativa de financiación y digital, p. 19: «Los nuevos elementos y tareas de la propuesta aportarán valor añadido a las partes interesadas europeas, que se beneficiarían de que ENISA actúe como centro de información, contribuya al intercambio de información y facilite notificaciones de alerta a las entidades afectadas», y p. 95: «En los últimos años, ENISA se ha convertido en un centro de información procedente de diversas fuentes. En este sentido, muchas de las tareas de ENISA están asociadas a la reutilización y el reciclado de información a efectos de diversos análisis».

[13] Tal como se expuso durante una reunión *ad hoc* del Subgrupo de Expertos en Tecnología del CEPD celebrada el 27 de febrero de 2026.

[14] La Comisión ha aclarado que ENISA no tiene mandato para llevar a cabo análisis operativos de incidentes y no tiene acceso a los datos de los propios incidentes. En su lugar, los datos que se traten serán datos agregados. Las alertas de los equipos de respuesta a incidentes de seguridad informática (CSIRTs, por sus siglas en inglés) nacionales no suelen incluir datos personales operativos, sino datos administrativos, como la información de contacto. En la misma línea, las empresas que se suscriban para recibir alertas tempranas también podrían facilitar sus datos de contacto. Según la Comisión Europea, en el improbable caso de que la información agregada sobre amenazas o incidentes facilitada a ENISA contenga direcciones IP, ENISA no tendría ninguna necesidad operativa y, por consiguiente, ninguna posibilidad jurídica y fáctica de investigar al abonado que está detrás de la dirección IP. La Comisión Europea aclara además que el servicio de asistencia previsto en el artículo 13 es de carácter consultivo y proporciona, por ejemplo, información sobre la autoridad competente del Estado miembro a la que dirigirse.

[15] Por ejemplo, en el proceso de examen de las solicitudes de autorización como prestador de declaraciones en el marco del esquema europeo individual de declaración de las capacidades en materia de ciberseguridad (artículo 22), durante el proceso de recurso contra las decisiones adoptadas (artículos 36 y siguientes), al tramitar reclamaciones presentadas por personas físicas o jurídicas en relación con la certificación o las declaraciones de conformidad UE [artículo 88, apartado 6, letra h)] o en relación con las certificaciones de la ciberseguridad (artículo 96).

[16] Véase el artículo 41, apartado1, del Reglamento (UE) 2019/881.

21. En la misma línea, el artículo 66, apartado 2, de la propuesta de Reglamento sobre la Ciberseguridad 2 reproduce el actual artículo 41, apartado 2, del Reglamento sobre la Ciberseguridad, que establece la posibilidad de que el Consejo de Administración de ENISA adopte las «medidas suplementarias necesarias para la aplicación del Reglamento (UE) 2018/1725» por parte de la Agencia[17], sin obligación de que el Consejo de Administración adopte ninguna medida específica. La disposición del artículo 66, apartado 2, de la propuesta de Reglamento sobre la Ciberseguridad 2 no especifica el alcance y el tipo de dichas medidas suplementarias de protección de datos, ni el procedimiento aplicable para su adopción. Tampoco aclara el papel del SEPD en el proceso[18].

22. El CEPD y el SEPD entienden que, si el Consejo de Administración de ENISA procede a aplicar el artículo 66, apartado 2, de la propuesta de Reglamento sobre la Ciberseguridad 2, su decisión o decisiones deben proporcionar detalles adicionales sobre la manera en que ENISA lleva a cabo el tratamiento de datos personales.

23. El CEPD y el SEPD recuerdan que, en principio, solo los detalles (prácticos) muy técnicos relacionados con el tratamiento de datos personales deben decidirse en virtud de la autonomía administrativa del organismo de la UE de que se trate, en este caso, el Consejo de Administración de una agencia descentralizada. Esto se debe a que la autorización de interferencias con los derechos fundamentales debería reservarse al legislador y, a lo sumo, a la Comisión mediante actos de ejecución o delegados[19]. Por lo tanto, lo que se entiende exactamente con la segunda frase del proyecto de artículo 66, apartado 2, por «medidas suplementarias necesarias para la aplicación del Reglamento (UE) 2018/1725 por parte de ENISA», debe aclararse explícitamente en la parte dispositiva del Reglamento.

24. No obstante, si se considera necesario que el Consejo de Administración adopte medidas que vayan más allá de los detalles técnicos (prácticos) del tratamiento ya previstos en la legislación o en los actos delegados o de ejecución, además de delimitar más claramente su ámbito de aplicación, las medidas que adopte el Consejo de Administración deben ser claras y precisas, y su aplicación debe ser previsible para las personas afectadas. Esto incluye que dichas normas reciban la publicidad adecuada. Además, deben ofrecer las salvaguardias necesarias para garantizar el cumplimiento de los principios y las salvaguardias clave en materia de protección de datos, como la limitación de la finalidad, la limitación del plazo de conservación y la protección de datos desde el diseño y por defecto. Asimismo, como salvaguardia adicional importante en tales casos, el CEPD y el SEPD recomiendan que el artículo 66 de la propuesta de Reglamento sobre la Ciberseguridad 2 prevea una consulta previa al SEPD antes de la adopción de dichas normas[20].

[17] El 21 de noviembre de 2019, el Consejo de Administración de ENISA adoptó una Decisión sobre las normas internas relativas a la limitación de determinados derechos de los interesados en relación con el tratamiento de datos personales en el marco del funcionamiento de ENISA, de conformidad con el artículo 25 del Reglamento de protección de datos para las instituciones, órganos y organismos de la UE.

[18] Por ejemplo, el artículo 18 *bis*, apartado 5, del Reglamento (UE) 2016/794 (Reglamento Europol) establece que el Consejo de Administración de Europol, a propuesta del director ejecutivo **y previa consulta al SEPD**, especificará las condiciones relativas al suministro y tratamiento de datos personales […] (la negrita es nuestra).

[19] Véase el documento de orientación del SEPD para los colegisladores sobre los elementos clave de las propuestas legislativas, disponible en https://www.edps.europa.eu/system/files/2025-05/EDPS_Publication_Guidance_for_co-legislators_EN.pdf, apartado 76.

[20] De forma similar a lo previsto en el artículo 18 *bis*, apartado 5, del Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo (Reglamento Europol) (DO L 135 de 24.5.2016, p. 53).

5 PUNTO DE ENTRADA ÚNICO PARA LA NOTIFICACIÓN DE INCIDENTES (ARTÍCULO 15 DEL REGLAMENTO SOBRE LA CIBERSEGURIDAD 2)

25. De conformidad con el artículo 15 de la propuesta de Reglamento sobre la Ciberseguridad 2, la ENISA debe establecer, proporcionar, gestionar, mantener y actualizar, según sea necesario, entre otras cosas, la plataforma única de notificación establecida de conformidad con el artículo 16, apartado 1, del Reglamento (UE) 2024/2847 y el punto de entrada único para la notificación de incidentes establecido de conformidad con el artículo 23 *bis* de la Directiva (UE) 2022/2555. Estas herramientas tienen por objeto simplificar las diferentes obligaciones de notificación relacionadas con la ciberseguridad[21].

26. Como ya señalaron en su dictamen conjunto sobre la propuesta «Ómnibus Digital»[22], el CEPD y el SEPD apoyan firmemente el objetivo de establecer un punto de entrada único para la notificación de las violaciones de la seguridad de los datos personales, ya que reduciría la carga administrativa para las organizaciones sin afectar al nivel de protección de los interesados. En su Declaración de Helsinki[23], el CEPD ya subrayó su apoyo a una posible solución europea de notificación que abarque todas las normativas, ya que esto ayudaría a facilitar el cumplimiento del RGPD. El CEPD y el SEPD también recuerdan la importancia de garantizar la seguridad de las notificaciones presentadas y transmitidas a través del punto de entrada único, ya que las notificaciones de violación de la seguridad de los datos a menudo incluyen información delicada[24].

6 MARCO EUROPEO DE CAPACIDADES EN CIBERSEGURIDAD (ARTÍCULO 19 DEL REGLAMENTO SOBRE LA CIBERSEGURIDAD 2)

27. El artículo 19 de la propuesta de Reglamento sobre la Ciberseguridad 2 exigirá que ENISA desarrolle y ponga a disposición del público un Marco Europeo de Capacidades en Ciberseguridad (ECSF). El ECSF contribuirá a garantizar que los profesionales de la ciberseguridad, los empleadores, los proveedores de formación y las autoridades públicas de los Estados miembros se basen en un entendimiento común de lo que requieren determinados puestos de trabajo en el ámbito de la ciberseguridad. Apoyará perfiles laborales claros, requisitos de cualificación transparentes y una mejor armonización entre la educación y las necesidades del mercado laboral. ENISA utilizará el ECSF como base para impartir formación, en particular para apoyar la aplicación de la legislación de la UE en materia de ciberseguridad, la cooperación operativa entre los Estados miembros y las actividades de sensibilización. Esto significa que el ECSF funciona como base para programas estructurados de formación en ciberseguridad, especialmente para las autoridades públicas y las entidades cubiertas por la legislación de la UE en materia de ciberseguridad.

---

[21] Véase el artículo 16, apartado 1, del Reglamento (UE) 2024/2847 y COM(2025) 837 final, p. 8.
[22] Dictamen conjunto 2/2026 del CEPD-SEPD sobre la propuesta de Reglamento en lo que respecta a la simplificación del marco legislativo digital (Ómnibus Digital), adoptado el 10 de febrero de 2026.
[23] CEPD, Declaración de Helsinki sobre una mayor claridad, apoyo y compromiso. Un enfoque basado en los derechos fundamentales para la innovación y la competitividad, adoptada el 2 de julio de 2025.
[24] Véase el capítulo 8.3 del Dictamen conjunto 2/2026 del CEPD-SEPD sobre la propuesta de Reglamento en lo que respecta a la simplificación del marco legislativo digital (Ómnibus Digital), adoptado el 10 de febrero de 2026.

28. El CEPD y el SEPD acogen con satisfacción el objetivo de reforzar el personal en el ámbito de la ciberseguridad de la UE y subrayan que hacer que las competencias sean más transferibles y reconocibles a través de las fronteras es importante para el funcionamiento del mercado único digital.

29. Al mismo tiempo, observan que los perfiles definidos en el artículo 19, apartado 2, de la propuesta de Reglamento sobre la Ciberseguridad 2 se limitan actualmente a los profesionales de la ciberseguridad. La propuesta no incluye un perfil de las capacidades necesarias para los ciudadanos, los funcionarios o el personal no especializado. Como se reconoce en el considerando 21 de la propuesta de Reglamento sobre la Ciberseguridad 2, la alfabetización digital es esencial para el empoderamiento de unos ciudadanos resilientes; sin embargo, casi la mitad de la población adulta no tiene capacidades digitales básicas, a pesar de que más del 90 % de los puestos de trabajo las requieren. Por lo tanto, el ECSF debe incluir un perfil de «ciberseguridad para generalistas», que abarque las capacidades mínimas que debe poseer cada residente en la UE en edad de trabajar para interactuar de forma segura en el mercado único digital, protegiéndose no solo a sí mismo, sino también a su organización y a terceros, en particular frente a la captación ilegítima de datos confidenciales (phising) asistida por inteligencia artificial (IA), los contenidos sintéticos manipulados (deepfakes), las suplantaciones de identidad y los ataques de ingeniería social. Este perfil podría ser utilizado por organizaciones públicas o privadas para la formación de su personal a fin de minimizar los riesgos derivados del factor humano, lo que reduciría el riesgo general de violaciones de la seguridad de los datos.

30. El CEPD y el SEPD observan que el considerando 45 de la propuesta distingue explícitamente el ECSF del Marco Europeo de Competencias Digitales (DigComp 3.0), y se aclara que este último es para la vida cotidiana, la participación en la sociedad, el trabajo y el aprendizaje, y puede ser utilizado tanto por adultos como por niños[25], mientras que el Marco Europeo de Capacidades en Ciberseguridad está destinado a un público especializado, ya que ofrece un marco sencillo que determina las funciones y tareas asociadas en materia de ciberseguridad, los conocimientos y las capacidades necesarios para desempeñarlas.

31. El CEPD y el SEPD apoyan todas las iniciativas mencionadas, ya sean ejecutadas por ENISA o, en el caso del Marco Europeo de Competencias Digitales, por el Centro Común de Investigación (JRC) de la Comisión Europea, ya que, siempre que exista una aceptación suficiente, reducirían el riesgo de violaciones de la seguridad de los datos. Por lo tanto, animan a todas las partes implicadas a explorar formas de aumentar la repercusión de los marcos.

---

[25] El CEPD y el SEPD recuerdan además que, entre 2022 y 2024, la Comisión Europea estudió la elaboración de un Certificado Europeo de Capacidades Digitales (EDSC, por sus siglas en inglés), basado en el Marco Europeo de Competencias Digitales. Dicho certificado debía facilitar y acelerar el reconocimiento de las competencias digitales de las personas por parte de los empleadores, los proveedores de formación u otros agentes. Esta iniciativa tenía por objeto ofrecer un sello de calidad para la certificación de las capacidades digitales en toda Europa. Tras un estudio de viabilidad [véase Centeno, C., Cosgrove, J., Cachia, R., Mora, T., Di Legge, A., *et al.*, *European Digital Skills Certificate (EDSC) Feasibility Study* [«Estudio de viabilidad del Certificado Europeo de Capacidades Digitales», documento en inglés], Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2024, doi:10.2760/958195, JRC138344, https://publications.jrc.ec.europa.eu/repository/handle/JRC138344], y un proyecto piloto con varios países de la UE, la Comisión Europea llegó a la conclusión de que dicho sello de calidad no aportaría suficiente valor añadido a los ciudadanos europeos. Sin embargo, el Marco Europeo de Competencias Digitales, publicado por primera vez en 2013, sigue existiendo [Cosgrove, J. y Cachia, R., *DigComp 3.0: European Digital Competence Framework* [«DigComp 3.0: Marco Europeo de Competencias Digitales», documento en inglés], quinta edición, Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2025, https://data.europa.eu/doi/10.2760/0001149, JRC144121]. Describe lo que se necesita para ser digitalmente competente en la sociedad actual y apoya el desarrollo de la competencia digital entre personas de todas las edades. Abarca una amplia gama de niveles de capacidades, desde las básicas hasta las muy avanzadas. Varias competencias del Marco Europeo de Competencias Digitales se refieren explícitamente a la ciberseguridad, como 4.1. Dispositivos de protección, 4.2. Protección de los datos personales y la privacidad, e incluso 4.4. Protección del medio ambiente (prevención de fugas de datos de los equipos desechados). Otros ámbitos también se refieren a las capacidades pertinentes, por lo que contiene capacidades del ámbito 1 cruciales para la defensa contra la ingeniería social, reduce los riesgos de amenaza interna del ámbito 2 y evita la divulgación accidental de información, y mejora la velocidad de detección de incidentes del ámbito 5.

32. Al mismo tiempo, el CEPD y el SEPD consideran que el Marco Europeo de Competencias Digitales no sustituye a un esquema de ciberseguridad específico para los generalistas[26] y recomienda a los colegisladores que modifiquen el artículo 19, apartado 2, de la propuesta de Reglamento sobre la Ciberseguridad 2 para que el ECSF no se limite exclusivamente a los «profesionales de la ciberseguridad», sino que también incluya perfiles para el personal en general o los ciudadanos. Esto debe ir acompañado de la correspondiente modificación del considerando 45.

33. Además, el CEPD y el SEPD consideran que es necesario que los perfiles profesionales del ECSF integren un módulo sobre la necesidad de garantizar la conformidad de las medidas de ciberseguridad con el Derecho de la Unión en materia de protección de datos, en particular en lo que respecta a la aplicación práctica del principio de protección de datos desde el diseño y por defecto (artículo 25 del RGPD), e invitan al colegislador a añadir un considerando con este objetivo.

7 MARCO EUROPEO DE CERTIFICACIÓN DE LA CIBERSEGURIDAD (TÍTULO III)

34. En el artículo 71 y el artículo 80, apartado 1, letra w), de la propuesta de Reglamento sobre la Ciberseguridad 2 se regula el ámbito de aplicación de la certificación de la ciberseguridad. En el artículo 80, apartado 1, letra w), se añade, como objetivo de seguridad de los esquemas europeos de certificación de la ciberseguridad, «asegurar que la entidad sea capaz de garantizar la seguridad del tratamiento de los datos personales».

35. El CEPD y el SEPD observan que la redacción del artículo 80, apartado 1, letra w), de la propuesta de Reglamento sobre la Ciberseguridad 2 se aproxima mucho a los requisitos de seguridad del tratamiento del RGPD[27]. En este sentido, el ámbito de aplicación del nuevo esquema de certificación podría interpretarse en el sentido de que incluye requisitos establecidos en el RGPD. Sin embargo, el ámbito de aplicación jurídico y operativo no está del todo claro, ya que la disposición no remite a las disposiciones del RGPD [por ejemplo, el artículo 5, apartado 1, letra f), el artículo 32 y el artículo 25 del RGPD] y se incluye en una lista de «objetivos de seguridad» (artículo 80, apartado 1, primera frase).

36. El CEPD y el SEPD recuerdan que la seguridad en virtud del RGPD está relacionada con los riesgos para los derechos y libertades fundamentales de las personas. Si bien la definición jurídica de ciberseguridad contemplada en el Derecho de la Unión incluye en líneas generales la protección de los usuarios y otras personas[28], el ámbito de aplicación de las medidas de ciberseguridad suele abarcar todo tipo de riesgos para la organización de que se trate. Sigue existiendo la oportunidad de establecer sinergias para que la evaluación de riesgos pueda integrar la protección de los derechos y libertades de las personas.

---

[26] En el Marco Europeo de Competencias Digitales, el contenido de seguridad se difunde entre veintiuna competencias, carece de modelos de amenaza explícitos, no traduce en términos operativos los riesgos de seguridad de las organizaciones y no se refiere directamente a las obligaciones de cumplimiento. Si bien el ECSF, en su forma actual, se aplicaría a las capacidades de los profesionales de la ciberseguridad, no existe un marco estructurado a escala de la UE para los empleados que no trabajan en el ámbito de la ciberseguridad. El CEPD y el SEPD recuerdan que la mayoría de las violaciones de la seguridad tienen su origen en la captación ilegítima de datos confidenciales (phising), la ingeniería social, el uso indebido de las credenciales, la mala configuración y el uso de «tecnología de la información en la sombra». Estos son comportamientos generalistas. Un marco de ciberseguridad generalista podría concretar los riesgos, proporcionar expectativas sensibles a las funciones (por ejemplo, para los recursos humanos o las finanzas) y apoyar resultados medibles.

[27] Véanse los artículos 5, apartado 1, letra f), y 32 del RGPD.

[28] Véase el artículo 2, apartado 1, de la propuesta de Reglamento sobre la Ciberseguridad 2, que es una disposición heredada y reza como sigue: «ciberseguridad»: todas las actividades necesarias para la protección de las redes y los sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas.

37. El CEPD y el SEPD recuerdan además que el RGPD tiene su propio mecanismo de certificación (artículos 42 y 43 del RGPD), y consideran que la certificación de la ciberseguridad es distinta de la certificación de la protección de datos con arreglo al artículo 42 del RGPD.

38. Dicho esto, el CEPD y el SEPD consideran que puede haber sinergias entre la ciberseguridad y la certificación de la protección de datos. Por ejemplo, la certificación del Reglamento sobre la Ciberseguridad 2 podría utilizarse como prueba justificativa para demostrar que se cumplen algunos requisitos de una certificación del RGPD, en lo que respecta a la ciberseguridad. Sin embargo, el CEPD y el SEPD observan que el artículo 80, apartado 1, letra w), de la propuesta de Reglamento sobre la Ciberseguridad 2 no articula claramente la relación con la certificación de los artículos 42 y 43, del RGPD. En aras de la seguridad jurídica, el CEPD y el SEPD recomiendan aclarar en mayor medida el ámbito de aplicación del artículo 80, apartado 1, letra w), del Reglamento sobre la Ciberseguridad 2 y la relación con la certificación del RGPD. Además, el CEPD y el SEPD recomiendan que se exija a ENISA que consulte al CEPD antes de adoptar un esquema de certificación con arreglo al artículo 80, apartado 1, letra w), del Reglamento sobre la Ciberseguridad 2 para garantizar la coherencia.

39. El CEPD y el SEPD destacan la exigencia de tener en cuenta no solo la eficacia de las medidas de ciberseguridad, sino también su necesidad y proporcionalidad. Determinados controles de ciberseguridad crean riesgos específicos para la protección de datos. Este puede ser el caso del seguimiento y el registro, la inspección profunda de paquetes o el análisis del comportamiento de los usuarios. Un sistema de certificación bien diseñado para la seguridad del tratamiento podría incluir controles para garantizar que las medidas de seguridad puedan aplicarse de manera que se cumplan las normas de protección de datos (por ejemplo, determinados aspectos deben ser configurables. Este podría ser el caso, por ejemplo, de la granularidad de los datos registrados con fines de seguridad, ya que esto puede permitir o facilitar el cumplimiento por parte del responsable del tratamiento de los principios de seguridad y minimización de datos del RGPD. En la misma línea, los períodos de conservación deben poder configurarse de modo que el responsable del tratamiento pueda decidir, en el contexto del tratamiento que está llevando a cabo, cuánto tiempo deben conservarse los datos personales antes de ser suprimidos o anonimizados utilizando técnicas certificadas).

40. Por lo tanto, el CEPD y el SEPD recomiendan explicar en un considerando que los esquemas de certificación deben, en la medida de lo posible, diseñarse, aplicarse y mantenerse de manera que tengan en cuenta los controles de seguridad que puedan ayudar a demostrar el cumplimiento de los requisitos del RGPD, en particular cuando los esquemas se apliquen a productos, servicios y procesos de TIC y a servicios de seguridad gestionados que puedan utilizarse en operaciones de tratamiento de datos. También cabe señalar que algunos controles pueden ser facilitadores de la privacidad y la protección de datos desde el diseño y por defecto.

8 MARCO DE CONFIANZA DE LAS CADENAS DE SUMINISTRO DE TIC (TÍTULO IV)

41. La propuesta de Reglamento sobre la Ciberseguridad 2 añade medidas para la seguridad de las cadenas de suministro de TIC y se abordan, en particular, los riesgos no técnicos, como los factores geopolíticos, jurídicos, de propiedad, de dependencia y de interferencia estratégica que afectan a las cadenas de suministro de TIC en sectores de alta criticidad y otros sectores críticos. Si bien estas medidas de seguridad de las cadenas de suministro tienen principalmente por objeto abordar riesgos que no están directamente relacionados con la protección de datos, también pueden tener un efecto beneficioso en la protección de los derechos fundamentales al limitar la injerencia extranjera en los datos de los interesados de la UE a través de actividades como el espionaje y la vigilancia.

42. El CEPD y el SEPD acogen con satisfacción la medida propuesta destinada a garantizar un marco de confianza de las cadenas de suministro de TIC y a abordar los riesgos no técnicos en sectores de alta criticidad.

9 ENTIDADES ESENCIALES ADICIONALES EN EL MARCO DE LA PROPUESTA DE MODIFICACIÓN DE LA DIRECTIVA SRI 2

43. La propuesta por la que se modifica la Directiva SRI 2 incluiría las carteras europeas de identidad digital y los proveedores de carteras europeas para empresas, como «entidades esenciales», independientemente de su tamaño. Las entidades clasificadas como «esenciales» están sujetas plenamente a las obligaciones de gestión de riesgos de ciberseguridad de la Directiva SRI 2 y deben aplicar las medidas de seguridad exigidas en virtud de su artículo 21, incluyendo el análisis de riesgos y las políticas de seguridad, la gestión de incidentes, la continuidad de las actividades y la gestión de crisis, la seguridad de las cadenas de suministro, la gestión de vulnerabilidades, las políticas en materia de criptografía y cifrado, y el control de acceso y la gestión de activos.

44. El CEPD y el SEPD acogen con satisfacción la designación de las carteras europeas de identidad digital y los proveedores de carteras europeas para empresas como «entidades esenciales». El CEPD y el SEPD consideran que las carteras de identidad digital son un componente fundamental de la infraestructura digital de la UE, de modo que los incidentes que les afecten podrían tener una gran repercusión transfronteriza. Sustentan la identificación, la autenticación y las declaraciones electrónicas seguras. Para la economía digital, las carteras para empresas son igual de críticas que las carteras europeas de identidad digital. Por consiguiente, ambos tipos de proveedores de carteras reciben un trato similar al de los proveedores de servicios de confianza, que ya han sido designados como «entidades esenciales» en virtud de la Directiva SRI 2, y otros operadores de infraestructuras altamente críticas.

10 RECOGIDA DE DATOS SOBRE ATAQUES CON PROGRAMAS DE SECUESTRO

45. De conformidad con el artículo 5, apartado 8, de la propuesta de modificación de la Directiva SRI 2, en el que se propone añadir nuevos apartados 12 y 13 al artículo 23 de la Directiva SRI 2, en caso de ataque con programas de secuestro, se puede solicitar a las entidades afectadas que presenten determinada información sobre incidentes con programas de secuestro de archivos a los equipos de respuesta a incidentes de seguridad informática (CSIRTs, por sus siglas en inglés), incluido si una entidad ha pagado un rescate y, en caso afirmativo, qué cantidad y a quién (criptoactivos / proveedores de servicios) y la identidad de la persona que actúa como punto de contacto.

46. De conformidad con el artículo 23, apartado 11, de la Directiva SRI 2, la Comisión está facultada para adoptar actos de ejecución que especifiquen en mayor medida el tipo de información, el formato y el procedimiento de las obligaciones de notificación. El ámbito de aplicación de este acto de ejecución se ampliaría para abarcar también las nuevas obligaciones de notificación en caso de ataques con programas de secuestro.

47. El CEPD y el SEPD apoyan plenamente el importante objetivo de prevenir futuros ataques con programas de secuestro y desarticular y desmantelar las organizaciones delictivas que están detrás de ellos. El CEPD y el SEPD señalan que la información que debe compartirse en relación con los ataques con programas de secuestro podría ser de carácter potencialmente sensible, como explica la Comisión en el considerando 10 de la propuesta de modificación de la Directiva SRI 2. Además, dicha notificación puede implicar el tratamiento de datos personales. El CEPD y el SEPD acogen con satisfacción el enfoque escalonado elegido en los apartados 12 y 13, según el cual la información más sensible del apartado 13 solo se comunicará previa solicitud.

48. Al mismo tiempo, en vista de la sensibilidad de los datos notificados y en consonancia con los principios de necesidad y proporcionalidad, en caso de que la notificación de ataques con programas de secuestro implique el tratamiento de datos personales, el CEPD y el SEPD recomiendan especificar en el acto de ejecución con arreglo al artículo 23, apartado 11, de la Directiva SRI 2 las garantías aplicables en materia de protección de datos. A este respecto, también recuerdan el requisito de que la Comisión, de conformidad con el artículo 42, apartado 1, del Reglamento de protección de datos para las instituciones, órganos y organismos de la UE, consulte al SEPD sobre los proyectos de actos delegados y de ejecución cuando repercutan en la protección de los derechos y libertades de las personas en lo que respecta al tratamiento de datos personales.