

Dictamen del Comité (art. 64)



Dictamen 18/2018

sobre el proyecto de lista de la autoridad de control competente de Portugal

en lo que respecta a

**las operaciones de tratamiento que requieran una evaluación de impacto
relativa a la protección de datos (artículo 35, apartado 4, del RGPD)**

Adoptado el 25 de septiembre de 2018

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Índice

1.	Resumen de los hechos	5
2.	Evaluación	5
2.1	Razonamiento general del CEPD en relación con la lista presentada	5
2.2	Aplicación del mecanismo de coherencia al proyecto de lista	6
2.3	Análisis del proyecto de lista	6
	Referencia a las Directrices	6
	Datos biométricos	7
	Datos genéticos	7
	Datos de localización	7
	Tratamiento con fines científicos o históricos sin consentimiento	7
	Tratamiento ulterior	8
	Excepciones a la información que debe comunicarse a los interesados con arreglo al artículo 14, apartado 5, del RGPD	8
	Seguimiento de los trabajadores	8
	Tratamiento realizado con ayuda de un implante	8
	Interfaces de productos electrónicos personales no protegidos contra la lectura no autorizada	9
	Tratamiento utilizando tecnologías nuevas o innovadoras	9
3.	Conclusiones/recomendaciones	10
4.	Observaciones finales	12

El Comité Europeo de Protección de Datos

Vistos el artículo 63, el artículo 64, apartados 1 *bis* y 3 a 8, y el artículo 35, apartados 1, 3, 4 y 6, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en lo sucesivo, «RGPD»),

Visto el Acuerdo EEE, y en particular su anexo XI y su Protocolo 37, modificado por la Decisión n.º 154/2018 del Comité Mixto del EEE, de 6 de julio de 2018,

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 (RGPD) en todo el Espacio Económico Europeo. De conformidad con el artículo 64, apartado 1, del RGPD, el Comité tiene que emitir un dictamen siempre que una autoridad de control pretenda adoptar una lista de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos con arreglo a lo dispuesto en el artículo 35, apartado 4, del RGPD. El objetivo del presente dictamen es por tanto crear un enfoque armonizado con respecto al tratamiento que sea transfronterizo o que pueda afectar a la libre circulación de datos personales o de personas físicas a través de la Unión Europea. Aunque el RGPD no impone una lista única, sí fomenta la coherencia. El Comité pretende alcanzar este objetivo en sus dictámenes, en primer lugar, solicitando a las autoridades de control que incluyan algunos tipos de tratamiento en sus listas; en segundo lugar, solicitándoles que supriman algunos criterios que el Comité no considera que creen, necesariamente, grandes riesgos para los interesados; y por último, pidiéndoles que utilicen algunos criterios de manera armonizada.

(2) Con referencia al artículo 35, apartados 4 y 6, del RGPD, las autoridades de control competentes establecerán listas de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos (en lo sucesivo, «EIPD»). No obstante, aplicarán el mecanismo de coherencia si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

(3) Aunque los proyectos de listas de las autoridades de control competentes estén sujetos al mecanismo de coherencia, esto no significa que las listas deban ser idénticas. 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 de la evaluación/dictamen del Comité Europeo de Protección de Datos (CEPD) no es lograr una lista única de la UE, sino más bien evitar incoherencias significativas que puedan afectar a la equivalencia de la protección de los interesados.

(4) La realización de una EIPD es únicamente obligatoria para el responsable del tratamiento de conformidad con el artículo 35, apartado 1, del RGPD, cuando sea probable que el tratamiento «entrañe un alto riesgo para los derechos y libertades de las personas físicas». El artículo 35, apartado 3, del RGPD ilustra qué puede entrañar un alto riesgo. Se trata de una lista no exhaustiva. El Grupo de Trabajo del Artículo 29, en las Directrices sobre la evaluación de impacto relativa a la protección de datos¹, aprobadas por el CEPD², ha aclarado los criterios que pueden ayudar a identificar cuándo las operaciones de tratamiento están sujetas al requisito de una EIPD. Las Directrices WP248 del Grupo de Trabajo del Artículo 29 establecen que, en la mayoría de los casos, un responsable del tratamiento puede considerar que un tratamiento que cumpla dos criterios requerirá la realización de una EIPD; sin embargo, en algunos casos, un responsable del tratamiento puede considerar que un tratamiento que cumpla solo uno de estos criterios requiere una EIPD.

(5) Las listas elaboradas por las autoridades de control competentes apoyan el mismo objetivo de definir las operaciones de tratamiento que puedan entrañar un alto riesgo y las operaciones de tratamiento que, por tanto, requieren una EIPD. Así pues, los criterios desarrollados en las Directrices del Grupo de Trabajo del Artículo 29 deben aplicarse a la hora de evaluar si los proyectos de listas de las autoridades de control competentes no afectan a la aplicación coherente del RGPD.

(6) Veintidós autoridades de control competentes han presentado sus proyectos de listas al CEPD. Una evaluación global de estos proyectos de listas apoya el objetivo de una aplicación coherente del RGPD, a pesar de que aumenta la complejidad del asunto.

(7) El dictamen del CEPD será adoptado de conformidad con el artículo 64, apartado 3, del RGPD, leído en relación con el artículo 10, apartado 2, del reglamento interno del CEPD, en el plazo de ocho semanas a partir del primer día hábil después de que el presidente y la autoridad de control competente hayan decidido que el expediente está completo. Previa decisión del presidente, este plazo podrá prorrogarse seis semanas más, teniendo en cuenta la complejidad del asunto.

HA ADOPTADO EL DICTAMEN:

¹ Grupo de Trabajo del Artículo 29, Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679 (WP 248 rev. 01).

² CEPD, Aprobación 1/2018.

1. Resumen de los hechos

La *Comissão Nacional de Protecção de Dados* - CNPD (en lo sucesivo, autoridad de control portuguesa) ha presentado su proyecto de lista al CEPD. La decisión de que el expediente estaba completo se adoptó el 10 de julio de 2018. El plazo para la adopción del dictamen se amplió hasta el 25 de septiembre, teniendo en cuenta la complejidad del asunto derivada de que veintidós autoridades de control competentes presentaron al mismo tiempo los proyectos de listas, surgiendo por tanto la necesidad de una evaluación global.

2. Evaluación

2.1 Razonamiento general del CEPD en relación con la lista presentada

Se interpreta que toda lista presentada al CEPD especifica en mayor medida el artículo 35, apartado 1, que prevalecerá en cualquier caso. Por tanto, ninguna lista puede ser exhaustiva.

De conformidad con el artículo 35, apartado 10, del RGPD, el Comité opina que si ya se ha realizado una EIPD como parte de una evaluación de impacto general en el contexto de la adopción de la base jurídica, la obligación de realizar una EIPD de conformidad con el artículo 35, apartados 1 a 7, del RGPD no se aplica, a menos que el Estado miembro lo considere necesario.

Además, si el Comité solicita una EIPD para una determinada categoría de tratamiento, y la normativa nacional ya exige una medida equivalente, la autoridad de control portuguesa deberá añadir una referencia a esta medida.

El presente dictamen no trata puntos presentados por la autoridad de control portuguesa por considerarse que están fuera del ámbito de aplicación del artículo 35, apartado 6, del RGPD. Esto se refiere a elementos que no guarden relación «con la oferta de bienes o servicios a interesados» en varios Estados miembros ni con la observación del comportamiento de los interesados en varios Estados miembros. Además, no es probable que «puedan afectar sustancialmente a la libre circulación de datos personales en la Unión». Esto es especialmente cierto en el caso de elementos que guarden relación con la normativa nacional, y en particular cuando la obligación de realizar una EIPD se establezca en la normativa nacional. Además, todas las operaciones de tratamiento que guarden relación con la aplicación de la ley se consideraron fuera del ámbito de aplicación, ya que no entran en el alcance del RGPD.

El Comité ha observado que varias autoridades de control han incluido en sus listas algunos tipos de tratamiento que son necesariamente tratamiento nacional. Dado que solo el tratamiento que sea transfronterizo o que pueda afectar a la libre circulación de datos personales o de los interesados está afectado por el artículo 35, apartado 6, el Comité no se pronunciará sobre dichos tratamientos nacionales.

El dictamen tiene por objeto definir un núcleo coherente de operaciones de tratamiento de datos que se repitan en las listas proporcionadas por las autoridades de control.

Esto significa que, para un número limitado de tipos de operaciones de tratamiento, que se definirán de forma armonizada, todas las autoridades de control requerirán la realización de una EIPD y el Comité recomendará a las autoridades de control que modifiquen sus listas en consecuencia, a fin de garantizar la coherencia.

Cuando el presente dictamen no se pronuncie sobre alguna entrada de la lista para la EIPD, esto significa que el Comité no solicita a la autoridad de control portuguesa que tome nuevas medidas.

Por último, el Comité recuerda que la transparencia es fundamental para los responsables del tratamiento y los encargados del tratamiento. Con el fin de aclarar las entradas de la lista, el Comité opina que una referencia explícita en las listas, para cada tipo de tratamiento, a los criterios establecidos en las Directrices podría mejorar la transparencia. Por tanto, el Comité considera que podría añadirse una explicación sobre los criterios que ha tenido en cuenta la autoridad de control portuguesa para crear su lista.

2.2 Aplicación del mecanismo de coherencia al proyecto de lista

El proyecto de lista presentada por la autoridad de control portuguesa se refiere a la oferta de bienes o servicios a los interesados, se refiere al seguimiento de su comportamiento en varios Estados miembros y/o puede afectar sustancialmente a la libre circulación de datos personales en la Unión debido principalmente a que las operaciones de tratamiento que figuran en el proyecto de lista no se limitan a interesados de este país.

2.3 Análisis del proyecto de lista

Teniendo en cuenta que:

- a. El artículo 35, apartado 1, del RGPD requiere una EIPD cuando sea probable que el tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas; y
- b. el artículo 35, apartado 3, del RGPD establece una lista no exhaustiva de tipos de operaciones de tratamiento que requieren una EIPD,

el Comité opina que:

REFERENCIA A LAS DIRECTRICES

El Comité opina que el análisis realizado en las Directrices WP248 del Grupo de Trabajo del Artículo 29 es un elemento esencial para garantizar la coherencia en toda la Unión. Por tanto, solicita a las diferentes autoridades de control que incluyan una declaración en el documento que contenga su lista por el que se aclare que la lista se basa en esas Directrices y que complementa y especifica las mismas.

Dado que el documento de la autoridad de control portuguesa no contiene tal declaración, el Comité recomienda a dicha autoridad que modifique el documento en consecuencia.

DATOS BIOMÉTRICOS

La lista presentada por la autoridad de control portuguesa para un dictamen del Comité prevé que el tratamiento de los datos biométricos, por sí mismo, requiere una EIPD. El Comité opina que el tratamiento de los datos biométricos, por sí mismo, no entraña necesariamente un alto riesgo. No obstante, el tratamiento de datos biométricos dirigido a identificar de manera unívoca a una persona física, en combinación con al menos otro criterio, requiere la realización de una EIPD. Así pues, el Comité pide a la autoridad de control portuguesa que modifique su lista en consecuencia, añadiendo que el elemento que establece el tratamiento de datos biométricos dirigido a identificar de manera unívoca a una persona física requiere la realización de una EIPD cuando se haga en combinación con al menos otro criterio, que deberá aplicarse sin perjuicio de lo dispuesto en el artículo 35, apartado 3, del RGPD.

DATOS GENÉTICOS

La lista presentada por la autoridad de control portuguesa para un dictamen del Comité no exige actualmente la realización de una EIPD para el tratamiento de los datos genéticos. El Comité opina que el tratamiento de datos genéticos, por sí mismo, no entraña necesariamente un alto riesgo. No obstante, el tratamiento de datos genéticos en combinación con al menos otro criterio requiere la realización de una EIPD. Así pues, el Comité pide a la autoridad de control portuguesa que modifique su lista en consecuencia, añadiendo explícitamente a la misma el tratamiento de datos genéticos en combinación con al menos otro criterio, que deberá aplicarse sin perjuicio de lo dispuesto en el artículo 35, apartado 3, del RGPD.

DATOS DE LOCALIZACIÓN

El Comité opina que el tratamiento de los datos de localización, por sí mismo, no entraña necesariamente un alto riesgo. No obstante, el tratamiento de datos de localización en combinación con al menos otro criterio requiere la realización de una EIPD. La lista presentada por la autoridad de control portuguesa para un dictamen del Comité no exige la realización de una EIPD para el tratamiento de los datos de localización por sí solo. El Comité pide a la autoridad de control portuguesa que modifique su lista en consecuencia, añadiendo que el elemento que establece el tratamiento de los datos de localización requiere la realización de una EIPD cuando se haga en combinación con al menos otro criterio.

TRATAMIENTO CON FINES CIENTÍFICOS O HISTÓRICOS SIN CONSENTIMIENTO

El Comité opina que el tratamiento de los datos personales con fines científicos o históricos, por sí mismo, no entraña necesariamente un alto riesgo. No obstante, el tratamiento de datos personales con fines científicos o históricos, en combinación con al menos otro criterio, requiere la realización de una EIPD. La lista presentada por la autoridad de control portuguesa para un dictamen del Comité prevé que este tipo de tratamiento, en combinación con al menos otro criterio, requiere una EIPD. El Comité toma nota de la inclusión de este criterio en la lista.

TRATAMIENTO ULTERIOR

El Comité opina que el tratamiento ulterior de datos personales no debe ser un criterio que dé lugar a la obligación de realizar una EIPD, por sí solo o en combinación con otro criterio. La lista presentada por la autoridad de control portuguesa para un dictamen del Comité exige actualmente la realización de una EIPD para el tratamiento ulterior de los datos personales. El Comité pide a la autoridad de control portuguesa que modifique su lista en consecuencia, suprimiendo este criterio.

EXCEPCIONES A LA INFORMACIÓN QUE DEBE COMUNICARSE A LOS INTERESADOS CON ARREGLO AL ARTÍCULO 14, APARTADO 5, DEL RGPD

El Comité opina que los tipos de actividades de tratamiento que podrían privar a los interesados de sus derechos, por sí mismos, no entrañan un alto riesgo. Por tanto, una actividad de tratamiento realizada por el responsable del tratamiento con arreglo al artículo 14 del RGPD y cuando la información que deba comunicarse a los interesados esté sujeta a una exención en virtud del artículo 14, apartado 5, letras b) a d), podría requerir la realización de una EIPD solo cuando se haga en combinación con al menos otro criterio. La lista presentada por la autoridad de control portuguesa para un dictamen del Comité exige actualmente la realización de una EIPD para el tratamiento de datos cuando el artículo 14, apartado 5, letras b), c) y d), se aplique por sí solo. El Comité pide a la autoridad de control portuguesa que modifique su lista en consecuencia, añadiendo que requiere la realización de una EIPD cuando se haga en combinación con al menos otro criterio.

SEGUIMIENTO DE LOS TRABAJADORES

El Comité considera que, debido a su naturaleza específica, el tratamiento del seguimiento de los trabajadores que cumpla el criterio de interesados vulnerables y de seguimiento sistemático contemplado en las Directrices podría exigir una EIPD. Dado que la lista presentada por la autoridad de control portuguesa para un dictamen del Comité ya contempla que este tipo de tratamiento requiere una evaluación de impacto relativa a la protección de datos, el Comité únicamente recomienda hacer referencia explícita a los dos criterios que figuran en las Directrices WP248 del GT29. Además, el Comité opina que las Directrices WP249 del GT29 siguen siendo válidas a la hora de definir el concepto de tratamiento sistemático de los datos de los trabajadores.

TRATAMIENTO REALIZADO CON AYUDA DE UN IMPLANTE

El Comité opina que el tratamiento de datos que no sean de salud, con ayuda de un implante, no exige la realización de una EIPD en todos los casos. La lista presentada por la autoridad de control portuguesa para un dictamen del Comité no aclara actualmente que debe realizarse una EIPD para el tratamiento de datos de salud con ayuda de un implante. Así pues, el Comité pide a la autoridad de control portuguesa que modifique su lista en consecuencia, indicando que en cualquier caso el tratamiento de datos de salud con ayuda de un implante exige la realización de una EIPD.

INTERFACES DE PRODUCTOS ELECTRÓNICOS PERSONALES NO PROTEGIDOS CONTRA LA LECTURA NO AUTORIZADA

El Comité opina que el tratamiento realizado en el contexto de la recogida de datos personales a través de interfaces de productos electrónicos personales que no estén protegidos contra la lectura no autorizada, no debe ser un criterio que dé lugar a la obligación de realizar una EIPD, por sí solo o en combinación con otro criterio. Dado que la lista presentada por la autoridad de control portuguesa para un dictamen del Comité prevé que este tipo de tratamiento requiere una evaluación de impacto relativa a la protección de datos en su elemento 2, el Comité solicita a dicha autoridad que modifique su lista en consecuencia.

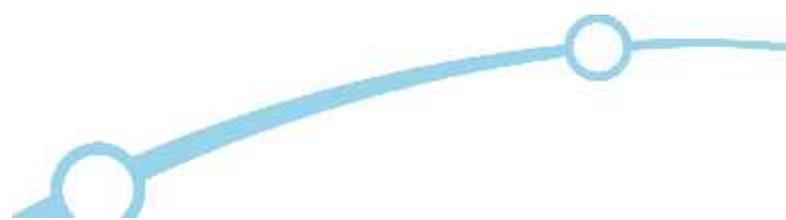
TRATAMIENTO UTILIZANDO TECNOLOGÍAS NUEVAS O INNOVADORAS

La lista presentada por la autoridad de control portuguesa para un dictamen del Comité prevé que el uso de tecnologías nuevas o innovadoras, por sí mismo, requiere una EIPD. El Comité opina que el uso de tecnologías innovadoras, por sí mismo, no entraña necesariamente un alto riesgo. No obstante, el uso de tecnologías innovadoras en combinación con al menos otro criterio requiere la realización de una EIPD. Por consiguiente, el Comité solicita a la autoridad de control portuguesa que modifique su lista en consecuencia, en primer lugar haciendo referencia en dicha lista a las tecnologías innovadoras, y en segundo lugar añadiendo que el elemento requiere la realización de una EIPD cuando se haga en combinación con al menos otro criterio.

3. Conclusiones/recomendaciones

El proyecto de lista de la autoridad de control portuguesa puede dar lugar a una aplicación incoherente de la exigencia de una EIPD, y es preciso introducir los siguientes cambios:

-) En cuanto a la referencia a las Directrices: el Comité pide a la autoridad de control portuguesa que modifique su documento en consecuencia.
-) En cuanto a los datos biométricos: el Comité pide a la autoridad de control portuguesa que modifique su lista, añadiendo que el elemento que establece el tratamiento de datos biométricos dirigido a identificar de manera unívoca a una persona física requiere la realización de una EIPD cuando se haga en combinación con al menos otro criterio.
-) En cuanto a los datos genéticos: el Comité pide a la autoridad de control portuguesa que modifique su lista, añadiendo explícitamente a la misma el tratamiento de datos genéticos en combinación con al menos otro criterio.
-) En cuanto a los datos de localización: el Comité pide a la autoridad de control portuguesa que modifique su lista, añadiendo que el elemento que establece el tratamiento de los datos de localización requiere la realización de una EIPD cuando se haga en combinación con al menos otro criterio.
-) En cuanto al tratamiento ulterior: el Comité pide a la autoridad de control portuguesa que modifique su lista en consecuencia, suprimiendo este criterio.
-) En cuanto a las excepciones a la información que debe darse a los interesados con arreglo al artículo 14, apartado 5, del RGPD: el Comité pide a la autoridad de control portuguesa que modifique su lista, añadiendo que requiere la realización de una EIPD cuando se haga en combinación con al menos otro criterio.
-) En cuanto al seguimiento de los trabajadores: el Comité únicamente recomienda hacer referencia explícita a los dos criterios que figuran en las Directrices WP248 del GT29.
-) En cuanto al tratamiento realizado con ayuda de un implante: el Comité pide a la autoridad de control portuguesa que modifique su lista, indicando que únicamente el tratamiento de datos de salud con ayuda de un implante exige la realización de una EIPD.
-) En cuanto a las interfaces de productos electrónicos personales no protegidos contra la lectura no autorizada: el Comité pide a la autoridad de control portuguesa que modifique su lista suprimiendo de la misma la referencia a la recogida de datos personales a través de interfaces de productos electrónicos personales que no estén protegidos contra la lectura no autorizada.
-) En cuanto al tratamiento utilizando tecnologías nuevas o innovadoras: el Comité solicita a la autoridad de control portuguesa que modifique su lista, en primer lugar haciendo referencia en dicha lista a las tecnologías innovadoras, y en segundo lugar añadiendo que el elemento requiere la realización de una EIPD cuando se haga en combinación con al menos otro criterio.



4. Observaciones finales

El presente dictamen se dirige a la *Comissão Nacional de Protecção de Dados* - CNPD (autoridad de control portuguesa) y se publicará con arreglo a lo dispuesto en el artículo 64, apartado 5, letra b), del RGPD.

De conformidad con el artículo 64, apartados 7 y 8 del RGPD, la autoridad de control comunicará a la presidencia por medios electrónicos, en el plazo de dos semanas a partir de la recepción del dictamen, si va a mantener o modificar su proyecto de lista. En el mismo plazo, presentará el proyecto de lista modificado o, cuando no tenga intención de seguir el dictamen de dicho Comité, indicará los motivos para no atenerse a este dictamen, en su totalidad o en parte.

Por el Comité Europeo de Protección de Datos

La presidenta

(Andrea Jelinek)