RECOMENDACIONES

RECOMENDACIÓN DE LA COMISIÓN

de 1 de marzo de 2011

sobre directrices para la aplicación de las normas de protección de datos en el Sistema de Cooperación para la Protección del Consumidor (CPCS)

(2011/136/UE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 292,

Considerando lo siguiente:

(1) El Reglamento (CE) nº 2006/2004 del Parlamento Europeo y del Consejo, de 27 de octubre de 2004, sobre la cooperación entre las autoridades nacionales encargadas de la aplicación de la legislación de protección de los consumidores («Reglamento sobre la cooperación en materia de protección de los consumidores») [1] (denominado en lo sucesivo «el Reglamento CPC») pretende reforzar la cooperación para el cumplimiento de la legislación de protección de los consumidores en el mercado único, crea una red europea de autoridades públicas nacionales encargadas de la aplicación de la legislación (denominada en lo sucesivo «la red CPC»), y fija el marco y las condiciones generales según las cuales dichas autoridades deben cooperar para proteger el interés económico colectivo de los consumidores.

(2) La cooperación entre las autoridades nacionales encargadas de la aplicación de la legislación es esencial para que el mercado único funcione eficazmente, por lo que cada autoridad puede, en el marco de la red CPC, solicitar ayuda a otras autoridades para investigar posibles infracciones de la legislación europea de protección de los consumidores.

(3) El objetivo del Sistema de Cooperación para la Protección del Consumidor (denominado «CPCS» en sus siglas inglesas) es que las autoridades públicas encargadas de la aplicación de la legislación puedan intercambiar información sobre posibles infracciones de la legislación de protección de los consumidores en un entorno seguro y bien protegido.

(4) Es preciso que el intercambio electrónico de información entre Estados miembros se atenga a las normas sobre protección de datos personales establecidas en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos [2] (denominada en lo sucesivo «la Directiva de protección de datos») y en el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos [3] (denominado en lo sucesivo «el Reglamento de protección de datos»).

(5) El artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea reconoce el derecho a la protección de datos. El CPCS debe garantizar que las diversas obligaciones y responsabilidades que comparten la Comisión y los Estados miembros en lo que respecta a las normas sobre protección de datos sean claras, y que las personas a quienes se refieran tales datos dispongan de información y de mecanismos de fácil acceso para hacer valer sus derechos.

(6) Conviene fijar directrices para la aplicación de las normas de protección de datos en el CPCS (denominadas en lo sucesivo «las directrices») para garantizar que se respeten las normas de protección de datos al tratar datos en dicho sistema.

(7) Es preciso animar a los funcionarios responsables de hacer cumplir la legislación a que se pongan en contacto con sus autoridades nacionales de control de protección de datos para recibir orientación y ayuda sobre la mejor manera de aplicar las directrices de conformidad con la legislación nacional y, si es necesario, para asegurarse de que la notificación y los controles previos al procesamiento en el CPCS se realicen a nivel nacional.

(8) Debe fomentarse decididamente la participación en las sesiones de formación organizadas por la Comisión para ayudar a aplicar las directrices.

(9) Debe proporcionarse a la Comisión información sobre la aplicación de las directrices a más tardar dos años después de que se adopte la presente Recomendación. La Comisión debe volver a evaluar entonces el nivel de la protección de los datos en el CPCS y decidir si se necesitan instrumentos adicionales, incluidas medidas reglamentarias.

[1] DO L 364 de 9.12.2004, p. 1.

[2] DO L 281 de 23.11.1995, p. 31.

[3] DO L 8 de 12.1.2001, p. 1.

(10) Deben tomarse las medidas necesarias para facilitar la aplicación de las directrices a los actores y usuarios del CPCS. Las autoridades nacionales de protección de datos y el Supervisor Europeo de Protección de Datos deben vigilar de cerca la evolución y la aplicación de las garantías de protección de datos en relación con el CPCS.

(11) Las directrices complementan la Decisión 2007/76/EC de la Comisión [1] y tienen en cuenta el dictamen del Grupo de Trabajo sobre Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales, creado por el artículo 29 [2] de la Directiva de protección de datos, así como el dictamen del Supervisor Europeo de Protección de Datos [3], creado por el artículo 41 del Reglamento de protección de datos (denominado en lo sucesivo «SEPD»).

HA ADOPTADO LA PRESENTE RECOMENDACIÓN:

Los Estados miembros deben seguir las directrices que figuran en el anexo.

Hecho en Bruselas, el 1 de marzo de 2011.

Por la Comisión
John DALLI
Miembro de la Comisión

[1] DO L 32 de 6.2.2007, p. 192.
[2] Dictamen 6/2007 sobre aspectos de protección de datos relacionados con el sistema de cooperación de protección a los consumidores (CPCS), 01910/2007/EN (WP 130), adoptado el 21 de septiembre de 2007.
[3] Dictamen del SEPD, ref. 2010-0692.

ANEXO

Directrices para la aplicación de las normas de protección de datos en el Sistema de Cooperación para la Protección del Consumidor (CPCS)

1. INTRODUCCIÓN

La cooperación entre las autoridades nacionales de protección de los consumidores es esencial para el buen funcionamiento del mercado interior, ya que los incumplimientos en casos transfronterizos socavan la confianza de los consumidores en las ofertas transfronterizas (y, por tanto, su confianza en el mercado interior), además de distorsionar la competencia.

El CPCS es una herramienta informática creada por el Reglamento CPC, que ofrece un mecanismo estructurado de intercambio de información a las autoridades nacionales de protección de los consumidores que forman parte de la red CPC. Permite que las autoridades públicas soliciten ayuda a sus homólogas de la red CPC para investigar y solucionar posibles infracciones de la legislación europea de protección de los consumidores, así como para tomar medidas a fin de hacer cumplir la legislación, deteniendo las prácticas comerciales ilegales de venta y prestación de servicios destinadas a consumidores de otros países de la UE. Las solicitudes de información y todas las comunicaciones entre las autoridades públicas competentes relativas a la aplicación del Reglamento CPC se canalizan a través del CPCS.

El objetivo del Reglamento CPC es mejorar el cumplimiento de la legislación de protección de los consumidores en todo el mercado interior mediante la creación, a escala de la UE, de una red de autoridades nacionales encargadas de la aplicación de la legislación, y establecer las condiciones bajo las cuales deben cooperar los Estados miembros entre sí. El Reglamento CPC establece que dichos intercambios de solicitud de información y ayuda mutua entre las autoridades nacionales encargadas de la aplicación de la legislación deben realizarse a través de una base de datos específica. El CPCS se elaboró para facilitar la cooperación administrativa y el intercambio de información con objeto de hacer cumplir la legislación europea de protección de los consumidores.

El ámbito de la cooperación se limita a las infracciones intracomunitarias de los actos jurídicos enumerados en el anexo del Reglamento CPC, que protege los intereses económicos colectivos de los consumidores.

2. ÁMBITO DE APLICACIÓN Y OBJETIVO DE LAS PRESENTES DIRECTRICES

Las presentes directrices pretenden abordar la cuestión esencial de garantizar un equilibrio en la cooperación entre las autoridades competentes de los Estados miembros para conseguir un cumplimiento eficaz y efectivo de la legislación, así como el respeto de los derechos fundamentales a la intimidad y a la protección de los datos personales.

La Directiva de protección de datos [1] define los datos personales como toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

Dado que los funcionarios nacionales encargados de hacer cumplir la legislación («los responsables de los casos»), que son los usuarios del CPCS, no siempre son expertos en protección de datos, y pueden no ser siempre suficientemente conscientes de los requisitos de protección de datos impuestos por su propia legislación nacional, es aconsejable facilitarles directrices que expliquen el funcionamiento del CPCS desde una perspectiva práctica de protección de datos, detallando las salvaguardias inherentes al sistema y los posibles riesgos que puede conllevar su uso.

El objetivo de las directrices es abordar las cuestiones más significativas que puede suscitar la protección de datos en el contexto del CPCS y ofrecer una explicación sencilla que puedan consultar todos los usuarios de dicho sistema. Sin embargo, no analizan exhaustivamente las implicaciones de la protección de datos en el CPCS.

Se recomienda encarecidamente que se consulte a las autoridades de protección de datos de los Estados miembros para garantizar que las directrices se complementan con las obligaciones específicas establecidas en las legislaciones nacionales de protección de datos. Los usuarios del CPCS también pueden obtener ayuda y orientación de dichas autoridades nacionales de protección de datos para garantizar que se cumplan los requisitos en la materia. Puede consultarse una relación de dichas autoridades, con los datos de contacto y la dirección de su sitio web, en:

http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/#eu

Cabe aclarar que el tratamiento de datos personales debe realizarse de conformidad con las condiciones y los principios específicos fijados en la Directiva de protección de datos. Los responsables de los casos están autorizados, en el marco del Reglamento, a intercambiar datos a través del CPCS, incluidos los datos personales, si la finalidad del tratamiento es detener una infracción de la legislación europea sobre consumidores que figura en el anexo del Reglamento CPC. Sin embargo, antes de tratar los datos, debe realizarse una evaluación minuciosa para garantizar que se cumplen los principios de protección de datos y que dicho tratamiento es estrictamente necesario para alcanzar los objetivos del Reglamento CPC.

[1] Artículo 2, letra a).

Teniendo esto en cuenta, los responsables de los casos que tengan acceso al CPCS deben realizar una evaluación caso por caso antes de efectuar cualquier tratamiento de datos personales [1]. La finalidad de las presentes directrices es ayudar a los responsables de los casos a realizar dicha evaluación presentando algunos principios rectores de protección de datos que es preciso tomar en consideración.

Las presentes directrices también pretenden aclarar algunas de las complejidades de la arquitectura del CPCS en lo que respecta a las operaciones conjuntas de tratamiento y control, clarificando las funciones de la Comisión y las de las autoridades competentes de los Estados miembros como «responsables conjuntos» de los intercambios de datos en el CPCS.

3. EL CPCS: UNA HERRAMIENTA INFORMÁTICA DE COOPERACIÓN PARA EL CUMPLIMIENTO DE LA LEGISLACIÓN

El CPCS es una herramienta informática elaborada y mantenida por la Comisión en cooperación con los Estados miembros. El propósito del CPCS es ayudar a los Estados miembros en la aplicación práctica de la legislación europea de protección de los consumidores. Lo utiliza la red CPC, que está compuesta por autoridades públicas designadas por los Estados miembros y los países del EEE, para cooperar e intercambiar información sobre el cumplimiento de la legislación de protección de los consumidores, según lo previsto en el Reglamento CPC.

El artículo 10 del Reglamento CPC establece lo siguiente:

«La Comisión mantendrá actualizada una base de datos electrónica en la que registrará y tratará la información recibida con arreglo a los artículos 7, 8 y 9. Dicha base de datos podrá ser consultada solo por las autoridades competentes».

El artículo 12, apartado 3, del Reglamento CPC añade lo siguiente:

«Las solicitudes de asistencia y toda comunicación de información se presentarán por escrito en un formulario tipo y se comunicarán por vía electrónica mediante la base de datos establecida en el artículo 10».

El CPCS facilita la cooperación y los intercambios de información únicamente sobre infracciones intracomunitarias de las Directivas y de los Reglamentos enumerados en el anexo del Reglamento CPC, que aborda diversas cuestiones, entre otras las prácticas comerciales desleales, la venta a distancia, el crédito al consumo, los viajes organizados, las cláusulas contractuales abusivas, la utilización de inmuebles en régimen de tiempo compartido, el comercio electrónico, etc. El CPCS no puede utilizarse para intercambiar información sobre ámbitos legislativos que no figuren específicamente en dicho anexo.

Por ejemplo:

I. Un comerciante establecido en Bélgica impone cláusulas abusivas en sus transacciones con consumidores residentes en Francia, infringiendo lo dispuesto en la Directiva sobre cláusulas contractuales abusivas. La autoridad francesa responsable de los consumidores puede utilizar el CPCS para solicitar a su homóloga belga que tome todas las medidas ejecutivas necesarias disponibles en Bélgica contra el comerciante en cuestión, para que cese inmediatamente la infracción intracomunitaria.

II. La autoridad danesa responsable de los consumidores recibe denuncias acerca de un sitio web que utiliza prácticas comerciales fraudulentas y engañosas en perjuicio de los consumidores. El sitio web está hospedado en Suecia. La autoridad danesa responsable de los consumidores necesita información sobre el sitio web. Por lo tanto, puede utilizar el CPCS para solicitar información a su homóloga sueca, que está obligada a facilitar la información.

La información es introducida por los Estados miembros, almacenada en el CPCS para que pueden acceder a ellas los Estados miembros a los que se dirige, y suprimida por la Comisión [2]. El CPCS se utiliza como repertorio de información y como instrumento para intercambiar información a través de un sistema de comunicación eficaz y seguro.

Desde una perspectiva de protección de los datos, la creación de una base de datos de este tipo presenta siempre ciertos riesgos para el derecho fundamental de protección de datos personales: compartir más datos que los estrictamente necesarios para una cooperación eficaz, conservar datos que deberían haberse suprimido, mantener datos que ya no son exactos o correctos, que no se respeten los derechos de los interesados o que los responsables del tratamiento no cumplan sus obligaciones. Por lo tanto, es necesario abordar dichos riesgos garantizando que los usuarios del CPCS están bien informados y formados en lo que respecta a las normas de protección de datos y pueden asegurar el cumplimiento de la legislación aplicable en la materia.

4. MARCO JURÍDICO Y DE SUPERVISIÓN DE PROTECCIÓN DE DATOS

La Unión Europea tiene un marco jurídico bien establecido en materia de protección de datos desde 1995: la Directiva de protección de datos [3], que regula el tratamiento de los datos personales por parte de los Estados miembros, y el Reglamento de protección de datos [4], que regula el tratamiento de datos personales por parte de las instituciones y los organismos de la Unión Europea. La aplicación de la legislación sobre protección de datos depende actualmente de quién sea el agente o el usuario del CPCS.

---

[1] Cabe señalar que los principios de protección de datos se aplican tanto a los datos almacenados de forma física como electrónica.
[2] Las normas específicas sobre la supresión de datos pueden consultarse en la Decisión 2007/76/CE y en «La red de cooperación en materia de protección de los consumidores: Directrices operativas».
[3] Directiva 95/46/CE.
[4] Reglamento (CE) nº 45/2001.

El tratamiento por parte de la Comisión está regulado por el Reglamento de protección de datos, mientras que el tratamiento realizado por los responsables de los casos de las autoridades nacionales competentes encargadas de la aplicación de la legislación está regulado por las legislaciones nacionales que transponen la Directiva de protección de datos.

Siendo los dos actores principales con funciones específicas en el CPCS, la Comisión y las autoridades competentes designadas, como responsables conjuntos, tienen obligación de notificar y presentar sus respectivas operaciones de tratamiento para su comprobación previa por parte de las autoridades de control pertinentes, así como para garantizar que se cumplen las normas de protección de datos. Sin embargo, las legislaciones nacionales que transponen la Directiva de protección de datos pueden establecer excepciones a los requisitos de notificación y comprobación previa.

La armonización de las normativas de protección de datos persigue garantizar un elevado nivel de protección a ese respecto y salvaguardar los derechos fundamentales de las personas, sin menoscabar la libre circulación de datos personales entre Estados miembros. Dado que las medidas nacionales de aplicación pueden dar lugar a normas divergentes, para garantizar el cumplimiento de la legislación de protección de datos se aconseja encarecidamente que los usuarios del CPCS analicen las presentes directrices con sus autoridades nacionales de protección de datos, puesto que pueden variar las normas, por ejemplo en cuanto a la información que debe facilitarse a los particulares o a la obligación de notificar determinadas operaciones de tratamiento a las autoridades de protección de datos.

Una característica significativa del marco jurídico de protección de datos de la UE es su supervisión por autoridades independientes de protección de datos. Los ciudadanos tienen derecho a presentar denuncias ante dichas autoridades y a resolver rápidamente sus problemas de protección de datos fuera de los tribunales. El tratamiento de los datos personales está supervisado, a nivel nacional, por las autoridades nacionales de protección de datos y, cuando dicho tratamiento lo realizan las instituciones europeas, por el Supervisor Europeo de Protección de Datos (SEPD) ([1]). Por tanto, la Comisión está sujeta a la supervisión del SEPD y los demás usuarios del CPCS están sujetos a la supervisión de las autoridades nacionales de protección de datos.

5. ¿QUIÉN SE ENCARGA DE QUÉ EN EL CPCS? RESPONSABILIDAD COMPARTIDA

El CPCS constituye un claro ejemplo de tratamiento conjunto y responsabilidad compartida. Si, por un lado, solo las autoridades competentes de los Estados miembros recogen, registran, revelan o intercambian datos de naturaleza personal, el almacenamiento y la supresión de dichos datos en sus servidores es responsabilidad de la Comisión. La Comisión no tiene acceso a estos datos personales, pero se considera que es el administrador y operador del sistema.

Por lo tanto, el reparto de las diferentes tareas y responsabilidades entre la Comisión y los Estados miembros puede resumirse del siguiente modo:

— cada autoridad competente es responsable de los datos en lo que respecta a sus propias actividades de tratamiento de datos,

— la Comisión no es usuaria, sino el operador del sistema, responsable principalmente del mantenimiento y la seguridad de la arquitectura del sistema. Sin embargo, la Comisión también tiene acceso a las alertas, a la información de retroalimentación y a otra información relacionada con el caso ([2]). El objetivo del acceso de la Comisión es supervisar la aplicación del Reglamento CPC y de la legislación de protección de los consumidores que figura en el anexo del Reglamento CPC, así como compilar información estadística relacionada con la realización de dichas tareas. En cambio, la Comisión no tiene acceso a la información que figura en las solicitudes de ayuda mutua y de cumplimiento de la legislación, ya que estas solamente se dirigen a las autoridades competentes de los Estados miembros que tratan el caso específico en cuestión. Sin embargo, el Reglamento CPC prevé que la Comisión pueda ayudar a las autoridades competentes en determinados litigios ([3]) y que sea invitada a participar en una investigación coordinada en la que estén involucrados más de dos Estados miembros ([4]),

— los agentes del CPCS comparten responsabilidad en cuanto a la legitimidad del tratamiento, el suministro de información y los derechos de acceso, rectificación y oposición,

— tanto la Comisión como las autoridades competentes, en sus funciones de controladores, son individualmente responsables de velar por que las normas sobre tratamiento de datos sean compatibles con las normas de protección de datos.

6. AGENTES Y USUARIOS DEL CPCS

En el CPCS existen diferentes perfiles de acceso: el acceso a la base de datos está restringido y asignado a un solo funcionario designado de la autoridad competente (usuario autenticado), y no es transferible. Las solicitudes de acceso al CPCS solo pueden concederse a funcionarios notificados a la Comisión por las autoridades competentes de los Estados miembros. Para acceder al sistema se necesita una identificación y una contraseña, que pueden obtenerse en la oficina de enlace única.

Solo los usuarios de la autoridad competente requerida y solicitante tienen acceso pleno a la información completa que se intercambia para un caso determinado, incluyendo también los anexos del expediente del caso del CPCS. Las oficinas de enlace únicas solo pueden leer la información más importante sobre un caso a fin de poder identificar a la autoridad competente a la que hay que transferir la correspondiente solicitud. No pueden leer documentos confidenciales adjuntos a una solicitud o a una alerta.

([1]) http://www.edps.europa.eu/EDPSWEB/edps/EDPS
([2]) Artículos 8, 9 y 15 del Reglamento (CE) nº 2006/2004 (Reglamento CPC).
([3]) Artículo 8, apartado 5, del Reglamento (CE) nº 2006/2004 (Reglamento CPC).
([4]) Artículo 9 del Reglamento (CE) nº 2006/2004 (Reglamento CPC).

En casos relacionados con el cumplimiento de la legislación, se comparte información general entre los usuarios de todas las autoridades competentes notificadas como responsables de los actos jurídicos que se hayan infringido. Este intercambio se produce a través de las notificaciones. Dichas notificaciones deben ofrecer una descripción general del caso y evitar incluir datos personales. Pueden existir excepciones, como el nombre del comerciante o proveedor (si es una persona física).

La Comisión no tiene acceso a las solicitudes de información y cumplimiento de la legislación ni a documentos confidenciales, pero recibe notificaciones y alertas.

7. PRINCIPIOS DE PROTECCIÓN DE DATOS APLICABLES AL INTERCAMBIO DE INFORMACIÓN

Los usuarios del CPCS de los Estados miembros solo pueden tratar datos personales en las condiciones y de conformidad con los principios que fija la Directiva de protección de datos. Al tratar datos personales en el CPCS, el responsable del tratamiento debe garantizar que se cumplan los principios de protección de datos.

Cabe también señalar que las normas de confidencialidad y de protección de datos se aplican al CPCS. Las normas de confidencialidad y de secreto profesional pueden aplicarse a los datos en general, pero las normas de protección de datos se limitan a los datos personales.

No debe olvidarse que los usuarios del CPCS de los Estados miembros son también responsables de muchas otras operaciones de tratamiento, y puede que no sean especialistas en protección de datos. El cumplimiento de las normas de protección de datos en el CPCS no tiene que ser innecesariamente complicado ni representar una carga administrativa excesiva. Tampoco tiene por qué haber una sola forma de lograrlo. Las presentes directrices son recomendaciones para el tratamiento de datos personales, y cabe recordar que no todos los datos intercambiados en el CPCS son personales.

Antes de introducir información en el CPCS, los funcionarios responsables de hacer cumplir la legislación deben verificar si los datos personales que van a enviar son estrictamente necesarios para una cooperación eficaz y tomar en consideración a quién van a enviarlos. Dichos funcionarios deben preguntarse si el receptor de los datos necesita realmente recibir dicha información a efectos de la alerta o la solicitud de ayuda mutua.

La siguiente lista de principios fundamentales de protección de datos pretende ayudar a los funcionarios responsables de hacer cumplir la legislación que acceden al CPCS a evaluar caso por caso si se cumplen las normas de protección de datos relacionadas con el tratamiento de datos personales cada vez que tratan datos personales en el sistema. Dichos funcionarios también deben tener en cuenta que, a nivel nacional, pueden existir excepciones y limitaciones a la aplicación de los principios de protección de datos descritos a continuación, por lo que se aconseja que consulten a sus autoridades nacionales de protección de datos ([1]).

¿Qué principios de protección de datos deben respetarse?

Los principios generales de protección de datos que deben tenerse en cuenta antes de tratar datos personales se han extraído de la Directiva de protección de datos. Dado que esta Directiva se ha transpuesto a la legislación nacional, se recuerda a los responsables de los casos que deben consultar a sus autoridades nacionales de control de protección de datos sobre la aplicación de los principios descritos a continuación, y se aconseja que comprueben si existen excepciones o limitaciones a su aplicación.

Principio de transparencia

Según la Directiva de protección de datos, los interesados tienen derecho a ser informados si se tratan sus datos personales. El responsable del tratamiento debe indicar su nombre y dirección, los fines del tratamiento, los destinatarios de los datos y cualquier otra información necesaria para garantizar la lealtad del tratamiento de datos ([2]).

Los datos solo pueden tratarse en las circunstancias siguientes ([3]):

— si el interesado ha dado su consentimiento,

— si el tratamiento es necesario para la ejecución de un contrato o para la aplicación de medidas precontractuales,

— si el tratamiento es necesario para el cumplimiento de una obligación jurídica,

— si el tratamiento es necesario para proteger los intereses esenciales del interesado,

([1]) Artículo 11, apartado 2, y artículo 13 de la Directiva 95/46/CE.
([2]) Artículos 10 y 11 de la Directiva 95/46/CE.
([3]) Artículo 7 de la Directiva 95/46/CE.

— si el tratamiento es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos,

— si el tratamiento es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o los terceros a los que se comuniquen los datos.

Principio de licitud y lealtad

Los datos personales no pueden recogerse ni tratarse de forma desleal o ilícita ni utilizarse para fines no compatibles con los establecidos en el Reglamento CPC. Para que el tratamiento sea lícito, los responsables de los casos deben asegurarse de tener razones inequívocas que justifiquen el tratamiento. El tratamiento debe realizarse con fines determinados, explícitos y legítimos. No debe realizarse un tratamiento posterior de manera incompatible con dichos fines ([1]). Esto solo puede preverse en el Reglamento CPC.

Para que el tratamiento sea leal, es preciso informar a los interesados de los fines para los cuales se tratarán sus datos, así como de la existencia del derecho de acceso, rectificación y oposición.

Principios de proporcionalidad y exactitud, y período de conservación

La información debe ser proporcional, adecuada, pertinente y no excesiva con relación a los fines para los que se recoge o trata. Los datos deben ser exactos y, si procede, estar actualizados. Se tomarán todas las medidas razonables para suprimir o rectificar los datos inexactos o incompletos en relación con los fines para los que fueron recogidos o para los que son tratados posteriormente. Los datos de carácter personal deben conservarse de forma que permitan la identificación de los interesados durante un período no superior al necesario para los fines para los que se recogieron o trataron. Deben establecerse garantías apropiadas para los datos personales archivados por un período más largo con fines históricos, estadísticos o científicos.

Los responsables de los casos deben considerar si la información que están tratando es estrictamente necesaria para conseguir los objetivos fijados.

Principio de limitación de la finalidad

Los datos personales deben recogerse con fines determinados, explícitos y legítimos. No deben tratarse posteriormente de manera incompatible con dichos fines, y es preciso informar a los interesados. Los responsables de los casos solo deben tratar datos personales si existe un motivo inequívoco para ello, es decir, si existe un fundamento jurídico en el Reglamento CPC que justifique la transmisión.

Derechos de acceso

Los interesados tienen derecho, según la Directiva de protección de datos ([2]), a ser informados si se tratan sus datos personales, así como de los fines del tratamiento, de los destinatarios de los datos y de sus derechos específicos, es decir, los derechos de información y rectificación. El interesado tiene derecho de acceso a todos los datos tratados sobre su persona. También tiene derecho a solicitar la rectificación, la supresión o el bloqueo de los datos incompletos, inexactos o cuyo tratamiento no se ajuste a las normas de protección de datos ([3]).

Datos sensibles

Está prohibido tratar datos que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, el estado de salud, la orientación sexual y las condenas penales. Sin embargo, la Directiva de protección de datos ([4]) establece excepciones a esta norma, según las cuales pueden tratarse datos sensibles en determinadas condiciones ([5]). Los usuarios del CPCS deben adoptar una actitud de prudencia al manejar datos sensibles ([6]). Se recomienda a los usuarios del CPCS que verifiquen con su autoridad nacional de protección de datos si se aplican excepciones al tratamiento de datos sensibles.

Excepciones

La Directiva de protección de datos autoriza determinadas excepciones en el marco de la prevención, investigación, detección y persecución de infracciones. Se aconseja a los responsables de los casos que consulten la legislación nacional para evaluar si dichas excepciones son posibles y en qué condiciones ([7]). Si existen esas excepciones, se recomienda que estén claramente indicadas en las declaraciones de confidencialidad de cada autoridad competente.

([1]) Artículo 6, apartado 1, letra b), de la Directiva 95/46/CE.
([2]) Artículos 10, 11 y 12 de la Directiva 95/46/CE.
([3]) Artículo 12 de la Directiva 95/46/CE.
([4]) Artículo 8, apartado 2, de la Directiva 95/46/CE.
([5]) Artículo 8 de la Directiva 95/46/CE.
([6]) Capítulo 4 del anexo de la Decisión 2007/76/CE.
([7]) Dictamen 6/2007 sobre aspectos de protección de datos relacionados con el sistema de cooperación de protección a los consumidores (CPCS), 01910/2007/EN (WP 130), adoptado el 21 de septiembre de 2007, p. 24-26.

Aplicación de los principios de protección de datos

La aplicación de estos principios de protección de datos al funcionamiento del CPCS lleva a formular las siguientes recomendaciones:

1) El uso del CPCS debe limitarse estrictamente a los fines establecidos en el Reglamento CPC. El artículo 13, apartado 1, del Reglamento CPC establece que la información comunicada solo puede utilizarse para asegurar el respeto de la legislación protectora de los intereses de los consumidores. Estos actos legislativos figuran en el anexo de dicho Reglamento.

2) Se recomienda a los funcionarios responsables de hacer cumplir la legislación que solo utilicen la información obtenida de una solicitud o de una alerta de ayuda mutua para fines relativos a ese caso concreto, cumpliendo estrictamente los requisitos jurídicos de protección de datos y evaluando previamente la necesidad del tratamiento en el marco de investigaciones realizadas en interés general público.

3) Al transmitir datos, los funcionarios responsables de hacer cumplir la legislación deben evaluar caso por caso quién debe ser el destinatario de la información que va a tratarse.

4) Los usuarios del CPCS deben escoger cuidadosamente las preguntas que hacen en la solicitud de ayuda mutua y solo solicitar los datos necesarios. No se trata solo de cumplir los principios de calidad de los datos, sino también de reducir la carga administrativa.

5) La Directiva de protección de datos [1] exige que los datos personales sean exactos y estén actualizados. Se recomienda que la autoridad competente que ha facilitado la información ayude a garantizar la exactitud de los datos almacenados en el CPCS. En este sistema se han incorporado mensajes que recuerdan periódicamente a los responsables de los casos que deben comprobar si los datos personales son exactos y si están actualizados.

6) Una forma práctica de informar a los interesados de sus derechos es mediante una declaración completa de confidencialidad en internet. Se recomienda que cada autoridad competente incluya una declaración de confidencialidad en su sitio web. Dicha declaración debe cumplir todos los requisitos de información fijados en la Directiva de protección de datos, incluir un enlace al sitio web en el que figura la declaración de confidencialidad de la Comisión, así como información adicional, como la información de contacto de la autoridad competente en cuestión y las limitaciones nacionales a los derechos de acceso o información. Todos los responsables de los datos involucrados tienen la responsabilidad de garantizar que se publiquen las declaraciones de confidencialidad.

7) Los interesados pueden pedir el acceso, la rectificación y la supresión de sus datos personales en relación con más de una fuente. Aunque cada autoridad competente asume la responsabilidad de sus propias operaciones de tratamiento de datos, como responsable del tratamiento, es deseable ofrecer una respuesta coordinada a las solicitudes relativas a asuntos transfronterizos. En estos casos, se recomienda que las autoridades competentes informen de la recepción de la solicitud a las demás autoridades competentes afectadas.

   Cuando una autoridad competente considere que la aceptación de una solicitud puede afectar al procedimiento de investigación o de cumplimiento de la legislación que lleven a cabo otras autoridades competentes, la citada autoridad debe solicitar la opinión de sus homólogas antes de aceptar la solicitud.

   Los interesados pueden también dirigir su solicitud a la Comisión. La Comisión solo puede aceptar solicitudes en relación con los datos a los que tiene acceso. Al recibir una solicitud, la Comisión debe consultar a la autoridad competente que ha facilitado la información. Si no se formula ninguna objeción o la autoridad competente no responde en un plazo razonable, la Comisión puede decidir si es o no oportuno dar curso favorable a la solicitud sobre la base de lo dispuesto en el Reglamento de protección de datos. La Comisión también debe solicitar la opinión de las autoridades competentes cuyas actividades de investigación o de cumplimiento de la legislación pueden resultar comprometidas si se da curso favorable a la solicitud. La Comisión debe analizar si es posible facilitar dichos intercambios mediante la incorporación de características técnicas adicionales en el CPCS.

8) La Decisión 2007/76/CE de aplicación de la CPC prevé la introducción de campos de datos en el CPCS con los nombres de los directores de empresa. Los funcionarios responsables de hacer cumplir la legislación deben evaluar si es necesario incluir este tipo de datos personales para solucionar el caso. Antes de introducir la información en el CPCS o de enviar una alerta o una solicitud de ayuda mutua a otra autoridad competente, debe evaluarse caso por caso si es necesario incluir el nombre de un director de empresa en los campos previstos al efecto.

9) La Decisión 2007/76/CE de aplicación de la CPC exige que la autoridad competente que introduzca información, alertas o solicitudes de cumplimiento de la legislación indique si la información debe tratarse de forma confidencial. Esto debe hacerse caso por caso. Del mismo modo, al enviar la información solicitada, la autoridad requerida debe indicar si dicha información debe tratarse de forma confidencial. El CPCS incluye un parámetro por defecto en el que los usuarios del sistema deben conceder explícitamente el acceso a los documentos desactivando el icono de indicación de confidencialidad.

[1] Artículo 6, apartado 1, letra d), de la Directiva 95/46/CE.

8. CPCS Y PROTECCIÓN DE DATOS

Entorno favorable para la protección de datos

El CPCS se ha elaborado teniendo en cuenta los requisitos de la legislación de protección de datos:

— el CPCS utiliza s-TESTA, que son las siglas de *secured Trans European Services for Telematics between Administrations* (Servicios transeuropeos seguros de telemática entre administraciones). Ofrece una plataforma paneuropea gestionada, fiable y segura de comunicación para las administraciones europeas y nacionales. La red s-TESTA está basada en una infraestructura privada dedicada y totalmente independiente de internet. El diseño del sistema incluye medidas de seguridad apropiadas para garantizar la mejor protección posible de la red. La red tiene una acreditación de seguridad que la hace apropiada para transmitir información clasificada «EU Restricted» («Restringido UE»),

— se han introducido varias características técnicas: contraseñas seguras y personalizadas para los funcionarios competentes notificados de las autoridades designadas, el uso de la red segura s-TESTA, mensajes que recuerdan a los responsables de los casos que deben tener en cuenta las normas de protección de datos al tratar datos personales, la creación de diversos perfiles de usuario que modulan el acceso a la información según la función del usuario (autoridad competente, oficina de enlace única o la Comisión), la posibilidad de limitar el acceso a documentos definiéndolos como confidenciales y el mensaje de la página de inicio del CPCS sobre las normas de protección de datos,

— normas de aplicación [1] que cubren aspectos importantes para garantizar el cumplimiento de la legislación sobre protección de datos: normas claras sobre supresión (qué información; cómo y cuándo suprimir datos); principios que especifican los tipos de acceso a la información (solo las autoridades competentes directamente afectadas tienen acceso completo y los demás solo tienen acceso a información general),

— directrices operativas [2] que clarifican los aspectos que es preciso tener en cuenta al cumplimentar los diferentes campos de datos, así como la integración de las presentes directrices [3],

— revisiones anuales para asegurar que las autoridades competentes verifiquen la exactitud de los datos personales (está previsto un marcado, pero aún no está implementado) y también que los casos están cerrados y/o suprimidos según lo previsto por las normas, para garantizar que no se olviden. La Comisión organiza periódicamente con los Estados miembros una revisión sistemática de los casos que han estado abiertos durante un período sustancialmente superior al período medio de tratamiento,

— supresión automática de los casos de ayuda mutua cinco años después del cierre del caso de acuerdo con el Reglamento CPC,

— el CPCS es una herramienta informática en proceso de evolución que pretende ofrecer un entorno favorable para la protección de datos. Se han incorporado numerosas salvaguardias en la arquitectura del sistema, que se han descrito anteriormente. La Comisión tiene intención de continuar incorporando mejoras según sea necesario.

Directrices adicionales

¿Cuánto tiempo debe conservarse un caso y cuándo debe cerrarse y suprimirse?

Solo la Comisión puede suprimir información del CPCS [4], y normalmente lo hace a solicitud de una autoridad competente. Al solicitar una supresión, la autoridad competente debe especificar los motivos. La única excepción son las solicitudes de cumplimiento de la legislación. Estas son suprimidas automáticamente por la Comisión cinco años después de que la autoridad solicitante cierre el caso.

Se han fijado normas con plazos específicos para garantizar la supresión de los datos que ya no se necesitan, que sean inexactos o infundados, o que han sido conservados durante los plazos máximos autorizados.

¿Por qué el período de conservación es de cinco años?

El propósito del período de conservación es facilitar la cooperación entre las autoridades públicas encargadas de hacer cumplir la legislación protectora de los intereses de los consumidores durante el examen de las infracciones intracomunitarias, así como contribuir al buen funcionamiento del mercado interior, a la calidad y coherencia del cumplimiento de la legislación protectora de los intereses de los consumidores, al control de la protección de los intereses económicos de estos y a elevar los niveles y la coherencia del cumplimiento de la legislación. Durante el período de conservación, los funcionarios autorizados encargados de hacer cumplir la legislación que trabajen para una autoridad competente que ha tratado originalmente un caso pueden consultar el expediente para establecer vínculos con infracciones posiblemente repetidas, a fin de contribuir a un cumplimiento mejor y más eficaz.

[1] Decisión 2007/76/CE.
[2] «La red de cooperación en materia de protección de los consumidores: Directrices operativas», documento aprobado por el Comité CPC el 8 de junio de 2010.
[3] El contenido de las presentes directrices se integrará en las futuras formaciones sobre el CPCS.
[4] Artículo 10 del Reglamento (CE) nº 2006/2004 (Reglamento CPC) y capítulo 2 del anexo de la Decisión 2007/76/CE de aplicación de la CPC.

¿Qué información puede incluirse en el foro de debate?

El foro de debate anexo al sistema es una herramienta destinada a intercambiar información sobre cuestiones tales como nuevas facultades para hacer cumplir la legislación y mejores prácticas. En general, aunque los funcionarios encargados de hacer cumplir la legislación no utilizan frecuentemente el foro de debate, este no debe servir para intercambiar datos relacionados con los casos ni debe hacer referencia a datos personales.

¿Qué tipo de datos puede incluirse en los resúmenes breves y en los documentos adjuntos?

La Decisión 2007/76/CE de implementación de la CPC prevé un campo de datos «documentos adjuntos» en las alertas y en las solicitudes de información y de cumplimiento de la legislación. Los resúmenes breves son campos en los que debe describirse la infracción. Se recomienda que no se incluyan datos personales en los resúmenes breves, dado que el propósito de este campo es facilitar una descripción general sobre la infracción. Deben suprimirse los datos personales de los documentos adjuntos que no sean estrictamente necesarios.

¿Qué se entiende por «sospecha razonable» de que se ha producido una infracción?

El término «sospecha razonable» debe interpretarse con arreglo a la legislación nacional. Sin embargo, se recomienda que las supuestas infracciones solo se incluyan en el CPCS si existen pruebas de que se ha producido o puede haberse producido una infracción.

¿Cómo deben tratarse las transmisiones a terceros países?

El Reglamento CPC ([1]) establece que un Estado miembro que tenga un acuerdo bilateral de asistencia mutua puede también transmitir a una autoridad de un tercer país información notificada en virtud del Reglamento CPC, siempre que la autoridad competente que envió inicialmente la información haya dado su consentimiento y que se cumplan las disposiciones de protección de datos.

Se recomienda que, en ausencia de un acuerdo internacional de la Unión Europea sobre medidas de asistencia mutua ([2]) con un tercer país, los acuerdos bilaterales de asistencia con un tercer país concreto establezcan garantías adecuadas de protección de los datos y se notifiquen a las autoridades pertinentes de control de protección de datos para que realicen un control previo, a menos que la Comisión haya constatado que el tercer país en cuestión garantiza un nivel adecuado de protección de los datos personales transmitidos por la Unión de conformidad con el artículo 25 de la Directiva de protección de datos.

([1]) Artículo 14, apartado 2, del Reglamento (CE) nº 2006/2004 (Reglamento CPC).
([2]) Artículo 18 del Reglamento (CE) nº 2006/2004 (Reglamento CPC).