COMISIÓN EUROPEA
DIRECCIÓN GENERAL XV
Mercado Interior y Servicios Financieros
Libre Circulación de la Información, Derecho de Sociedades e Información Financiera
**Libre circulación de la información, protección de datos y sus aspectos internacionales**

DG XV D/5057/97 final
**WP 7**

**Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales**

# Documento de Trabajo: Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos en un país tercero?

Adoptado por el Grupo de Trabajo el 14 de enero de 1998

**DOCUMENTO DE TRABAJO**

# EVALUACIÓN DE LA AUTORREGULACIÓN INDUSTRIAL: ¿EN QUÉ CASOS REALIZA UNA CONTRIBUCIÓN SIGNIFICATIVA AL NIVEL DE PROTECCIÓN DE DATOS EN UN PAÍS TERCERO?

## Introducción

El apartado 2 del artículo 25 de la Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (95/46/CE) establece que el nivel de protección que ofrece un país tercero se evaluará atendiendo a *todas las circunstancias* que concurran en una transferencia o en una categoría de transferencias de datos. Se hace referencia específica no sólo a las normas de Derecho, sino también a las "normas profesionales y las medidas de seguridad en vigor en dichos países."

El texto de la Directiva exige por lo tanto que se tengan en cuenta las normas no jurídicas que puedan existir en el país tercero en cuestión, siempre que estas normas *estén vigentes.* En este contexto debe evaluarse la función de la autorregulación industrial.

## ¿Qué es la autorregulación?

El término "autorregulación" puede significar cosas distintas para diferentes personas. A efectos del presente documento, deberá entenderse por código de autorregulación (u otro instrumento) cualquier conjunto de normas de protección de datos que se apliquen a una pluralidad de responsables del tratamiento que pertenezcan a la misma profesión o al mismo sector industrial, cuyo contenido haya sido determinado fundamentalmente por miembros del sector industrial o profesión en cuestión.

Esta es una definición amplia que abarcaría desde un código de protección de datos voluntario desarrollado por una pequeña asociación industrial con pocos miembros, hasta los detallados códigos de ética profesional aplicables a profesiones enteras, tales como médicos o banqueros, que suelen tener una fuerza cuasi jurídica.

## ¿Es el organismo responsable del código representante del sector?

Tal como sostendrá este documento, un importante criterio para juzgar el valor de un código es el grado hasta el cual pueden hacerse cumplir sus normas. En este contexto, la cuestión de si la asociación u organismo responsable del código representa a todos los operadores del sector o únicamente a un pequeño porcentaje de éstos, tiene probablemente menos importancia que la fuerza de la asociación en cuanto a su capacidad de, por ejemplo, imponer sanciones a sus miembros por incumplimiento del código. No obstante, existen diversas razones secundarias que hacen que los códigos que abarcan a todo un sector industrial o una profesión sean instrumentos de protección más útiles que los desarrollados por pequeñas agrupaciones de empresas dentro de un sector industrial. En primer lugar figura el hecho de que, desde el punto de vista del consumidor, un sector industrial fragmentado y caracterizado por diversas asociaciones rivales, cada una con su propio código para la protección de datos, es

algo confuso. La coexistencia de varios códigos diferentes crea un panorama opaco para las personas cuyos datos sean objeto de tratamiento. En segundo lugar, especialmente en sectores tales como el marketing directo, donde es práctica corriente transferir los datos personales entre diferentes empresas del mismo sector, pueden surgir situaciones en que la empresa que transmita datos personales no esté sujeta al mismo código de protección de datos que la empresa receptora. Esto supone una gran fuente de ambigüedad en cuanto a la naturaleza de las normas aplicables, y también puede dificultar en gran medida la investigación y resolución de las denuncias de los interesados.

**Evaluación de la autorregulación - el enfoque más adecuado**

Dada la gran variedad de instrumentos que entran dentro de la noción de autorregulación, está claro que existe una necesidad de diferenciar entre las diversas formas de autorregulación en términos de su impacto real en el nivel de protección de datos aplicable cuando se transfieren datos personales a un país tercero.

El punto de partida para la evaluación de cualquier conjunto específico de normas sobre protección de datos (tengan éstas categoría de autorregulación o de regulación) debe ser el enfoque general establecido en el documento de debate "Primeras orientaciones sobre las transferencias de datos personales a países terceros - Posibles formas de evaluar su adecuación". La piedra angular de este enfoque es el examen no sólo del contenido del instrumento (deberá contener una serie de principios básicos), sino también de su eficacia en cuanto a lograr:

- un buen nivel de obediencia general
- apoyo y ayuda a los individuos cuyos datos sean objeto de tratamiento
- una reparación adecuada (incluida la compensación, cuando corresponda).

**Evaluación del contenido de un instrumento de autorregulación**

Esta es una tarea relativamente sencilla. Se trata de garantizar que estén presentes los "principios de contenido" necesarios establecidos en el documento "Primeras orientaciones" (véase el extracto adjunto). Esta es una evaluación objetiva. Se trata de ver cual es el contenido del código, y no cómo se elaboró éste. El hecho de que un sector industrial o profesión haya desempeñado una función primordial en el desarrollo del contenido de un código no es relevante por sí mismo, aunque evidentemente, si en su desarrollo se han tenido en cuenta las opiniones de los individuos cuyos datos sean objeto de tratamiento y de las organizaciones de consumidores, es más probable que el código refleje más fielmente los principios básicos necesarios para la protección de datos.

La transparencia del código es un elemento crucial; en particular, el código debería redactarse en lenguaje sencillo y ofrecer ejemplos concretos que ilustren sus disposiciones.

Además, el código debería prohibir la transferencia de datos a empresas que no pertenezcan al sector y que no se rijan por el código, a menos que se prevean otras protecciones adecuadas.

**Evaluación de la eficacia de un instrumento de autorregulación**

La evaluación de la eficacia de un código o instrumento concreto de autorregulación es un ejercicio más difícil, que exige la comprensión de los métodos y formas por los que se garantiza la adhesión al código y por los que se resuelven los problemas de incumplimiento. Es necesario que se cumplan los tres criterios funcionales para juzgar la eficacia de la protección, para que pueda tenerse en cuenta un código de autorregulación en la evaluación de la adecuación de su protección.

*Un buen nivel de obediencia general*

Típicamente, un código profesional o industrial será desarrollado por un organismo representante del sector industrial o profesión en cuestión, y se aplicará a los miembros de dicho organismo representante específico. El nivel de cumplimiento del código dependerá del grado de conocimiento de la existencia del código y su contenido por parte de sus miembros, de las medidas que se adopten para garantizar la transparencia del código con el fin de permitir a las fuerzas del mercado realizar una contribución eficaz, de la existencia de un sistema de control externo (tal como la exigencia de una auditoría de su cumplimiento a intervalos periódicos) y, quizás lo más importante, de la naturaleza y la aplicación de las sanciones en caso de incumplimiento.
Por tanto, son importantes las siguientes preguntas:

- ¿Qué medidas adopta el organismo representante para asegurarse de que sus miembros conocen el código?
- ¿Exige el organismo representante a sus miembros pruebas de que aplican las disposiciones del código? ¿Con qué frecuencia?
- ¿Presentan dichas pruebas las propias empresas o proceden de una fuente externa (tal como un auditor acreditado)?
- ¿Investiga el organismo representante las supuestas o presuntas violaciones del código?
- ¿Es el cumplimiento del código una condición para formar parte del organismo representante o es dicho cumplimiento meramente “voluntario”?
- En caso de que un miembro viole el código, ¿con qué tipos de sanciones disciplinarias cuenta el organismo representante (expulsión u otras)?
- ¿Es posible para un individuo o empresa continuar trabajando en la profesión o sector industrial concreto, incluso después de haber sido expulsado del organismo representante?
- ¿Puede hacerse cumplir el código de otras maneras, por ejemplo en los tribunales o en un tribunal especializado? Los códigos profesionales tienen fuerza jurídica en algunos países. En algunas circunstancias, también puede ser posible aplicar las leyes generales relativas a prácticas comerciales correctas o incluso de competencia para aplicar los códigos de conducta de los sectores industriales.

Al examinar los tipos de sanciones existentes, es importante distinguir entre una sanción “reparadora” que únicamente exige que un responsable del tratamiento, en caso de incumplimiento, modifique sus prácticas con el fin de adecuarlas a lo establecido en el código, y una sanción que vaya más lejos, castigando al responsable por su incumplimiento. Sólo la segunda categoría de sanción “punitiva” tiene repercusión en el comportamiento futuro de los responsables del tratamiento, proporcionando un incentivo para que se cumpla sistemáticamente el código.

La falta de sanciones auténticamente disuasorias y punitivas es por tanto un fallo esencial en un código. Sin dichas sanciones, es difícil entender cómo puede lograse un nivel satisfactorio de obediencia global, a no ser que se establezca un sistema riguroso de control externo (tal como una autoridad pública o privada competente para intervenir en caso de incumplimiento del código, o una exigencia obligatoria de realizar auditorías externas a intervalos periódicos).

*Apoyo y ayuda a los individuos cuyos datos sean objeto de tratamiento*

Un requisito esencial para un sistema de protección de datos adecuado y eficaz es que no se abandone a los individuos que se enfrentan a un problema relativo a sus datos personales, sino que se les proporcione un apoyo institucional que permita hacer frente a sus dificultades. Este apoyo institucional debería, idealmente, ser imparcial, independiente y poseer los poderes necesarios para investigar cualquier denuncia de un interesado. A este respecto, las preguntas que deben formularse respecto de la autorregulación son las siguientes:

- ¿Existe un sistema que permita la investigación de las denuncias de los interesados?
- ¿Cómo se da a conocer a los interesados este sistema y las decisiones adoptadas en cada caso concreto?
- ¿Conlleva el sistema costes para el interesado?
- ¿Quién realiza la investigación? ¿Tiene los poderes necesarios?
- ¿Quién juzga sobre una supuesta violación del código? ¿Es independiente e imparcial?

La imparcialidad del árbitro o juez sobre una supuesta violación de un código es un punto clave. Claramente, dicha persona u organismo deberá ser independiente respecto al responsable del tratamiento. No obstante, esto por sí mismo no basta para garantizar la imparcialidad. Idealmente, el árbitro debería asimismo no pertenecer a la profesión o sector en cuestión, por la razón de que los miembros de una misma profesión o sector tienen una clara comunidad de intereses con el responsable del tratamiento que supuestamente haya violado el código. A falta de esto, la neutralidad del órgano de decisión podría garantizarse incluyendo a representantes de los consumidores (en igual número) junto a los representantes del sector.

*Reparación adecuada*

Si el código de autorregulación resulta violado, deberá existir un recurso para el interesado. Este recurso deberá solucionar el problema (p. ej. corregir o suprimir datos incorrectos, o garantizar que cese el tratamiento con objetivos incompatibles) y, si se ha producido un perjuicio al interesado, permitir el pago de una compensación adecuada. Hay que tener en cuenta que "perjuicio" en el sentido de la Directiva sobre protección de datos incluye no sólo el daño físico y la pérdida financiera, sino también cualquier daño psicológico o moral que se cause (llamado "distress" en el Derecho del Reino Unido y de EEUU).

Muchas de las cuestiones relativas a las sanciones que se han enumerado en la sección "Un buen nivel de obediencia general" son pertinentes aquí. Tal y como se ha

explicado anteriormente, las sanciones tienen una doble función: castigar al infractor (y fomentar así el cumplimiento de las normas por parte del infractor y de los demás), y remediar una violación de las normas. Nos ocuparemos ahora de la segunda función. Por lo tanto, podrían plantearse también las siguientes preguntas:

- ¿Es posible comprobar que un miembro que manifiestamente haya violado el código, ha modificado sus prácticas y solucionado el problema?
- ¿Pueden los interesados obtener compensación con arreglo al código, y en caso afirmativo, de qué manera?
- ¿Equivale la violación del código a una violación de contrato, o puede hacerse cumplir en virtud del Derecho público (p. ej. protección de los consumidores, competencia desleal), y puede la jurisdicción competente conceder indemnización por daños y perjuicios sobre dicha base?

## Conclusiones

- La autorregulación debería evaluarse utilizando el enfoque funcional y objetivo establecido en el documento "Primeras orientaciones".
- Para que un instrumento de autorregulación pueda considerarse un elemento válido para una "protección adecuada" debe ser vinculante para todos los miembros a quienes se transfieran los datos personales y proporcionar una protección adecuada si los datos se transfieren a terceros.
- El instrumento debe ser transparente e incluir el contenido básico de los principios esenciales de la protección de datos.
- El instrumento debe tener mecanismos que garanticen de forma eficaz un nivel satisfactorio de cumplimiento general. Una forma de lograr esto es el establecimiento de un sistema de sanciones disuasorias y punitivas. Otro sistema son las auditorías externas obligatorias.
- El instrumento debe proporcionar apoyo y ayuda a los interesados que se enfrenten a un problema relativo al tratamiento de sus datos personales. Por ello, debe existir un órgano independiente, imparcial y de fácil acceso que acoja las denuncias de los interesados y resuelva sobre las violaciones del código.
- El instrumento deberá garantizar una reparación adecuada en caso de incumplimiento. Los interesados deberán poder obtener una reparación de su problema y una compensación adecuada.

COMISIÓN EUROPEA
DIRECCIÓN GENERAL XV
Mercado Interior y Servicios Financieros
Libre Circulación de la Información, Derecho de Sociedades e Información Financiera
**Libre circulación de la información, protección de datos y sus aspectos internacionales**

XV D/5020/97- final
**WP4**

**ANEXO**

GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

# Primeras orientaciones sobre las transferencias de datos personales a países terceros - Posibles formas de evaluar su adecuación

Documento de debate adoptado por el Grupo de trabajo el 26 de junio de 1997

***(i) Principios de contenido***

Se sugiere la inclusión de los siguientes principios básicos:

1) **Principio de limitación de objetivos** - los datos deberán tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia. Las únicas excepciones a esta norma serían las necesarias en una sociedad democrática por una de las razones expuestas en el artículo 13 de la Directiva.

2) **Principio de proporcionalidad y de calidad de los datos -** los datos deberán ser exactos y, cuando sea necesario, estar actualizados. Los datos deberán ser adecuados, relevantes y no excesivos en relación al objetivo por el que se han transferido o por el que han sido nuevamente tratados.

3) **Principio de transparencia -** deberá informarse a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el país tercero, y de cualquier otra cuestión siempre que resulte necesario para garantizar la equidad. Las únicas excepciones permitidas deberán corresponder a los artículos 11(2) y 13 de la Directiva.

4) **Principio de seguridad -** el responsable del tratamiento deberá adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento. Toda persona que actúe bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, no deberá tratar los datos salvo por instrucción del responsable del tratamiento.

5) **Derechos de acceso, rectificación y oposición -** el interesado deberá tener derecho a obtener una copia de todos los datos a él relativos, y derecho a rectificar aquellos datos que resulten ser inexactos. En determinadas situaciones, el interesado deberá también ser capaz de oponerse al tratamiento de los datos a él relativos. Las únicas excepciones a estos derechos deberán estar en línea con el artículo 13 de la Directiva.

6) **Restricciones respecto a transferencias sucesivas a otros países terceros -** únicamente deberán permitirse transferencias sucesivas de datos personales del país tercero de destino a otro país tercero en el caso de que este último país tercero garantice asimismo un nivel de protección adecuado. Las únicas excepciones permitidas deberán estar en línea con el artículo 26 de la Directiva.

A continuación figuran ejemplos de principios adicionales que deberán aplicarse a tipos específicos de tratamientos:

1) **Datos sensibles -** cuando se trate de categorías de datos "sensibles" (las incluidas en el artículo 8), deberán establecerse protecciones adicionales, tales como la exigencia de que el interesado otorgue su consentimiento explícito para el tratamiento.

2) **Marketing directo -** en el caso de que el objetivo de la transferencia de datos sea el marketing directo, el interesado deberá tener en cualquier momento la posibilidad de negarse a que sus datos sean utilizados con dicho propósito.

3) **Decisión individual automatizada -** cuando el objetivo de la transferencia sea la adopción de una decisión automatizada en el sentido del artículo 15 de la Directiva, el interesado deberá tener el derecho a conocer la lógica aplicada a dicha decisión, y deberán adoptarse otras medidas para proteger el interés legítimo del individuo.