CENSOR CONSULTING

Régimen sancionador

para la vulneración de datos personales

Sujetos responsables

1. Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y la presente ley orgánica:

- Los responsables de los tratamientos.
- Los encargados de los tratamientos.
- Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.
- Las entidades de certificación.
- Las entidades acreditadas de supervisión de los códigos de conducta.

2. No será de aplicación al delegado de protección de datos el régimen sancionador establecido en este título.

Infracciones

Constituyen infracciones los actos y conductas que supongan una vulneración del contenido de los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 y de la presente ley orgánica.

PARA MÁS INFORMACIÓN:

CENSOR CONSULTING S.L.

Tel. 972 576 977
Móvil. 629 183 508

legal@censorconsulting.es
www.censorconsulting.es

Régimen sancionador
para la vulneración de datos personales

▶ Infracciones consideradas **muy graves**

1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquél, y en particular las siguientes:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679.

b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679.

c) El incumplimiento de los requisitos exigidos por el artículo 7 del Reglamento (UE) 2016/679 para la validez del consentimiento.

d) La utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello.

e) El tratamiento de datos personales de las categorías a las que se refiere el artículo 9 del Reglamento (UE) 2016/679, sin que concurra alguna de las circunstancias previstas en dicho precepto y en el artículo 9 de esta ley orgánica.

f) El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad fuera de los supuestos permitidos por el artículo 10 del Reglamento (UE) 2016/679 y en el artículo 10 de esta ley orgánica.

g) El tratamiento de datos de carácter personal relacionados con infracciones y sanciones administrativas fuera de los supuestos permitidos por el artículo 27 de esta ley orgánica.

h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos de carácter personal conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta ley orgánica.

i) La vulneración del deber de confidencialidad establecido en el artículo 5 de esta ley orgánica.

j) La exigencia del pago de un canon para facilitar al afectado la información a la que se refieren los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, fuera de los supuestos establecidos en su artículo 12.5.

k) El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

l) La transferencia internacional de datos de carácter personal a un destinatario que se encuentre en un tercer país o a una organización internacional, cuando no concurran las garantías, requisitos o excepciones establecidos en los artículos 44 a 49 del Reglamento (UE) 2016/679.

m) El incumplimiento de las resoluciones dictadas por la autoridad de protección de datos competente en ejercicio de los poderes que le confiere el artículo 58.2 del Reglamento (UE) 2016/679.

n) El incumplimiento de la obligación de bloqueo de los datos establecida en el artículo 32 de esta ley orgánica cuando la misma sea exigible.

ñ) No facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación.

o) La resistencia u obstrucción del ejercicio de la función inspectora por la autoridad de protección de datos competente.

2. Tendrán la misma consideración y también prescribirán a los tres años las infracciones a las que se refiere el artículo 83.6 del Reglamento (UE) 2016/679.

▶ Infracciones consideradas **graves**

En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquél, y en particular las siguientes:

a) El tratamiento de datos de carácter personal de un menor de edad sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela, conforme al artículo 8 del Reglamento (UE) 2016/679.

b) No acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por un menor de edad o por el titular de su patria potestad o tutela sobre el mismo, conforme a lo requerido por el artículo 8.2 del Reglamento (UE) 2016/679.

c) El impedimento o la obstaculización o la no atención reiterada de los derechos de acceso, rectificación, supresión, limitación del

▶ PARA MÁS INFORMACIÓN: CENSOR CONSULTING S.L. Tel. 972 576 977 Móvil. 629 183 508 legal@censorconsulting.es www.censorconsulting.es

Régimen sancionador
para la vulneración de datos personales

tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando éste, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación.

d) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño y por defecto e integrar las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25.1 del Reglamento (UE) 2016/679.

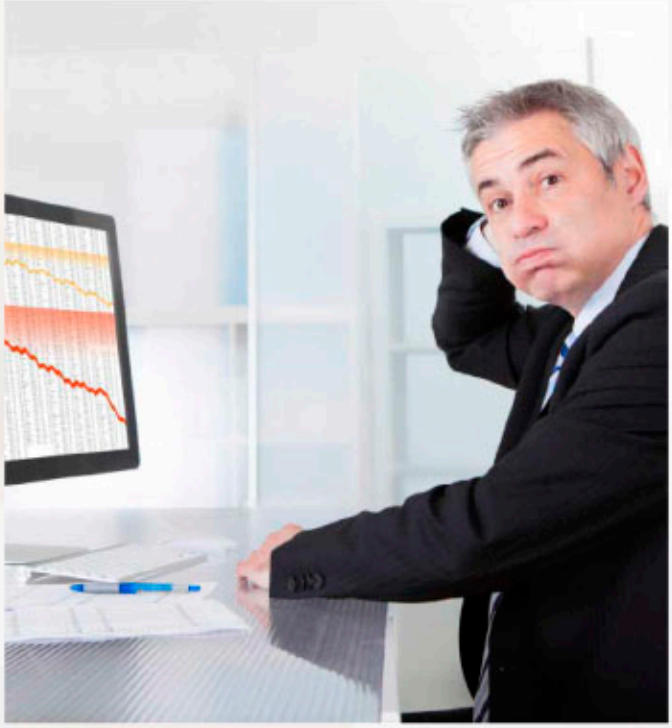
e) La falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, sólo se tratarán los datos personales necesarios para cada uno de los fines específicos del tratamiento, conforme a lo exigido por el artículo 25.2 del Reglamento (UE) 2016/679.

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679.

h) El incumplimiento de la obligación de designar un representante del responsable o encargado del tratamiento no establecido en el territorio de la Unión Europea, conforme a lo previsto en el artículo 27 del Reglamento (UE) 2016/679.

i) La falta de atención por el representante en la Unión del responsable o del encargado del tratamiento de las solicitudes efectuadas por la autoridad de protección de datos o por los afectados.



j) La contratación por el responsable del tratamiento de un encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas conforme a lo establecido en el Capítulo IV del Reglamento (UE) 2016/679.

k) Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

l) La contratación por un encargado del tratamiento de otros encargados sin contar con la autorización previa del responsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles.

m) La infracción por un encargado del tratamiento de lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, al determinar los fines y los medios del tratamiento, conforme a lo dispuesto en el artículo 28.10 del citado reglamento.

n) No disponer del registro de actividades de tratamiento establecido en el artículo 30 del Reglamento (UE) 2016/679.

ñ) No poner a disposición de la autoridad de protección de datos que lo haya solicitado, el registro de actividades de tratamiento, conforme al apartado 4 del artículo 30 del Reglamento (UE) 2016/679.

o) No cooperar con las autoridades de control en el desempeño de sus funciones en los supuestos no previstos en el artículo 72 de esta ley orgánica.

p) El tratamiento de datos de carácter personal sin llevar a cabo una previa valoración de los elementos mencionados en el artículo 28 de esta ley orgánica.

q) El incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento.

r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679. s) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 34 del Reglamento (UE) 2016/679 si el responsable del tratamiento hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación.

t) El tratamiento de datos de carácter personal sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.

u) El tratamiento de datos de carácter personal sin haber consultado previamente a la autoridad de protección de datos en los casos en que dicha consulta resulta preceptiva conforme al artículo 36 del Reglamento (UE) 2016/679 o cuando la ley establezca la obligación de llevar a cabo esa consulta.

v) El incumplimiento de la obligación de designar un delegado de protección de datos cuando sea exigible su nombramiento de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.

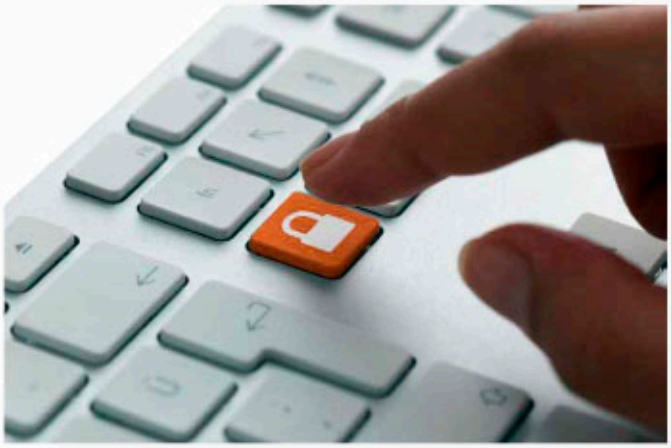
PARA MÁS INFORMACIÓN:
CENSOR CONSULTING S.L.
Tel. 972 576 977
Móvil. 629 183 508
legal@censorconsulting.es
www.censorconsulting.es

Régimen sancionador
para la vulneración de datos personales

w) No posibilitar la efectiva participación del delegado de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.
x) La utilización de un sello o certificación en materia de protección de datos que no haya sido otorgado por una entidad de certificación debidamente acreditada o en caso de que la vigencia del mismo hubiera expirado.
y) Obtener la acreditación como organismo de certificación presentando información inexacta sobre el cumplimiento de los requisitos exigidos por el artículo 43 del Reglamento (UE) 2016/679.
z) El desempeño de funciones que el Reglamento (UE) 2016/679 reserva a los organismos de certificación, sin haber sido debidamente acreditado conforme a lo establecido en el artículo 39 de esta ley orgánica.
aa) El incumplimiento por parte de un organismo de certificación de los principios y deberes a los que está sometido según lo previsto en los artículos 42 y 43 de Reglamento (UE) 2016/679.
ab) El desempeño de funciones que el artículo 41 del Reglamento (UE) 2016/679 reserva a los organismos de supervisión de códigos de conducta sin haber sido previamente acreditado por la autoridad de protección de datos competente.
ac) La falta de adopción por parte de los organismos acreditados de supervisión de un código de conducta de las medidas que resulten oportunas en caso que se hubiera producido una infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

▶ Infracciones consideradas **leves**

Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679 y, en particular, las siguientes:
a) El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679.
b) La exigencia del pago de un canon para facilitar al afectado la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, cuando así lo permita su artículo 12.5, si su cuantía excediese el importe de los costes afrontados para facilitar la información o realizar la actuación solicitada.
c) No atender las solicitudes de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, salvo que resultase de aplicación lo dispuesto en el artículo 73.1 k) de esta ley orgánica.
d) No atender los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando éste, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación, salvo que resultase de aplicación lo dispuesto en el artículo 73 c) de esta ley orgánica.
e) El incumplimiento de la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento exigida por el artículo 19 del Reglamento (UE) 2016/679.
f) El incumplimiento de la obligación de informar al afectado, cuando así lo haya solicitado, de los destinatarios a los que se hayan comunicado los datos personales rectificados, suprimidos o respecto de los que se ha limitado el tratamiento.
g) El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible conforme al artículo 3 de esta ley orgánica.
h) La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas con respecto al tratamiento de datos personales y sus relaciones con los afectados al que se refiere el artículo 26 del Reglamento (UE)



2016/679 o la inexactitud en la determinación de las mismas.
i) No poner a disposición de los afectados los aspectos esenciales del acuerdo formalizado entre los corresponsables del tratamiento, conforme exige el artículo 26.2 del Reglamento (UE) 2016/679.
j) La falta del cumplimiento de la obligación del encargado del tratamiento de informar al responsable del tratamiento acerca de la posible infracción por una instrucción recibida de éste de las disposiciones del Reglamento (UE)
k) El incumplimiento por encargado o subencargado de las estipulaciones impuestas en el contrato o acto jurídico que regula el tratamiento o las instrucciones del responsable del tratamiento, salvo que esté legalmente obligado a ello conforme al Reglamento (UE) 2016/679 y la presente ley orgánica o en los supuestos en que fuese necesario para evitar la infracción de la legislación en materia de protección de datos y se hubiese advertido de ello al responsable o al encargado del tratamiento.

▶ PARA MÁS INFORMACIÓN:
CENSOR CONSULTING S.L.
Tel. 972 576 977
Móvil. 629 183 508
legal@censorconsulting.es
www.censorconsulting.es

Régimen sancionador
para la vulneración de datos personales

l) Disponer de un Registro de actividades de tratamiento que no incorpore toda la información exigida por el artículo 30 del Reglamento (UE) 2016/679.
m) La notificación incompleta o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.
n) El incumplimiento de la obligación de documentación de cualquier violación de seguridad, exigida por el artículo 33.5 del Reglamento (UE) 2016/679.
ñ) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 34 del Reglamento (UE) 2016/679, salvo que resulte de aplicación lo previsto en el artículo 73 s) de esta ley orgánica.
o) Facilitar información inexacta a la Autoridad de protección de datos, en los supuestos en los que el responsable del tratamiento deba elevarle una consulta previa, conforme al artículo 36 del Reglamento (UE) 2016/679.
p) No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.
q) El incumplimiento por los organismos de certificación de la obligación de informar a la autoridad de protección de datos de la expedición, renovación o retirada de una certificación, conforme a lo exigido por los apartados 1 y 5 del artículo 43 del Reglamento (UE) 2016/679.
r) El incumplimiento por parte de los organismos acreditados de supervisión de un código de conducta de la obligación de informar a las autoridades de protección de datos acerca de las medidas que resulten oportunas en caso de infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

▶ Interrupción de la prescripción

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor. Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679 interrumpirá la prescripción el conocimiento formal por el interesado del proyecto de acuerdo de inicio que sea sometido a las autoridades de control interesadas.

▶ Sanciones y medidas correctivas

1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.
2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:
a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
3. Será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 83.2 del Reglamento (UE) 2016/679.
4. Será objeto de publicación en el Boletín Oficial del Estado la información que identifique al infractor, la infracción cometida y el importe de la sanción impuesta cuando la autoridad competente sea la Agencia Española de Protección de Datos, la sanción fuese superior a un millón de euros y el infractor sea una persona jurídica.

▶ Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento

1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:
a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
b) Los órganos jurisdiccionales.
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
e) Las autoridades administrativas independientes.
f) El Banco de España.
g) Las corporaciones de Derecho público cuando las finalidades

▶ PARA MÁS INFORMACIÓN: CENSOR CONSULTING S.L. Tel. 972 576 977 Móvil. 629 183 508 legal@censorconsulting.es www.censorconsulting.es

Régimen sancionador
para la vulneración de datos personales

del tratamiento se relacionen con el ejercicio de potestades de derecho público.

h) Las fundaciones del sector público. i) Las Universidades Públicas.

j) Los consorcios.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 73 a 75 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido. La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos podrá proponer también la iniciación de actuaciones disciplinarias. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, ésta publicará en su página web con la debida separación las resoluciones en que se imponga una sanción a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

▶ Prescripción de las sanciones

1. Las sanciones impuestas en aplicación del Reglamento (UE) 2016/679 y de esta ley orgánica prescriben en los siguientes plazos:

a) Las sanciones por importe inferior a 40.000 euros, prescriben en el plazo de un año.

b) Las sanciones por importe comprendido entre 40.001 y 300.000 euros prescriben a los dos años.

c) Las sanciones por un importe superior a 300.000 euros prescriben a los tres años.

2. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla.

3. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

▶ PARA MÁS INFORMACIÓN: CENSOR CONSULTING S.L. Tel. 972 576 977 Móvil. 629 183 508 legal@censorconsulting.es www.censorconsulting.es