REGIMEN SANCIONADOR

Reglamento Europeo (UE) 2016/679 (RGPD) y la ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPD)

ENTIDADES SUJETAS AL RÉGIMEN SANCIONADOR (art. 70 LOPDGDD)

-Los Responsables del tratamiento (RT)

-Los Encargados del tratamiento (ET)

-Los representantes de RT o ET no establecidos en el territorio de la UE

-Las entidades de certificación

-Las entidades acreditadas de supervisión de los códigos de conducta

No está sujeto al régimen sancionador:

-El Delegado de protección de datos (DPO)

SANCIONES (art. 83 GDPR y art. 76 de la LOPDGDD

La Autoridad de Control podrá imponer multas administrativas al Responsable del Tratamiento y el Encargado del Tratamiento por infringir el GDPR garantizando que serán efectivas, proporcionadas y disuasorias.

Las multas administrativas se impondrán en función de las circunstancias de cada caso individual, teniendo en cuenta las facultades investigadoras y correctoras conferidas a la Autoridad de Control.

La decisión de la Autoridad de Control para imponer una multa administrativa y calcular su importe tendrá en cuenta:

-La naturaleza, gravedad y duración de la infracción en relación con el fin del tratamiento.

-El número de interesados afectados.

-El nivel de los perjuicios sufridos por los interesados.

-La intencionalidad o negligencia de la infracción.

-Las categorías de datos afectados por la infracción.

-El grado de responsabilidad del Responsable del Tratamiento o Encargado del Tratamiento.

-La reiteración de infracciones del Responsable del Tratamiento o Encargado del Tratamiento.

-Las medidas tomadas por el Responsable del Tratamiento o Encargado del Tratamiento para paliar los perjuicios sufridos por los interesados.

-El grado de cooperación con la Autoridad de Control con el fin de remediar la infracción y mitigar sus posibles efectos adversos.

-La forma en que la Autoridad de Control ha tenido conocimiento de la infracción (si se ha notificado, o en la medida que se ha hecho).

-El cumplimiento de las medidas ordenadas previamente por la Autoridad de Control contra el Responsable del Tratamiento o Encargado del Tratamiento en relación con el asunto.

-La adhesión a códigos de conducta o a mecanismos de certificación aprobados por la Autoridad de Control.

Otros factores agravantes o atenuantes aplicables a las circunstancias de cada caso, como:

-Los beneficios financieros obtenidos o las pérdidas evitadas por la infracción.

-El carácter continuado de la infracción.

-La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

-La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.

-La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

-La afectación a los derechos de los menores.

-Disponer, cuando no fuere obligatorio, de un DPO.

El sometimiento por parte del Responsable del Tratamiento o Encargado del Tratamiento, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.

PRESCRIPCIÓN DE LAS SANCIONES (art. 78 de la LOPDGDD)

Las sanciones impuestas en aplicación del GDPR y la LOPDGDD prescriben en los siguientes plazos:

-3 años: infracciones consideradas muy graves o con un importe superior a 300.000 euros.

-2 años: infracciones consideradas graves o con un importe comprendido entre 40.001 y 300.000 euros.

-1 año: infracciones consideradas leves o con un importe igual o inferior a 40.000 euros.

-El plazo de prescripción 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.

-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 6 meses por causa no imputable al infractor.

INFRACCIONES CONSIDERADAS MUY GRAVES

Normativa	Artículo 83.5 y 83.6 del GDPR y 72 de la LOPDGDD

Prescripción	3 años
Multas administrativas	En función de las circunstancias de cada caso individual: Mínimo: 300.000 € Máximo: el importe más elevado entre 20.000.000 € y el 4% del total de la facturación mundial anual del ejercicio financiero anterior

PRINCIPIOS *(capítulo II GDPR)*	GDPR	LOPD GDD
Infringir las disposiciones relativas a los "Principios relativos al tratamiento"	5	
Vulneración del deber de confidencialidad	5.1.f	5
Infringir las disposiciones relativas a la "Licitud del tratamiento"	6	
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	6.4	
Infringir las disposiciones relativas a las "Condiciones para el consentimiento"	7	
Infringir las disposiciones relativas al "Tratamiento de categorías especiales de datos"	9	9
Infringir las disposiciones relativas al "Tratamiento de datos relativos a condenas e	10	10
La reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los interesados	Cdo. 75 y 85	

DERECHOS DEL INTERESADO *(capítulo III GDPR)*	GDPR	LOPD GDD
Infringir las disposiciones relativas a los "Derechos del interesado"	12 a	
Exigir el pago de un canon para facilitar la información del tratamiento o por atender el ejercicio de los derechos del interesado, fuera de los supuestos establecidos en art. 12.5 del GDPR	12 y 15	
Atender las solicitudes de derechos fuera de los supuestos establecidos	12.5	
Omisión del deber de informar al interesado	13 y	12
Impedir, obstaculizar o no atender reiteradamente el ejercicio de derechos	15 a	

TRATAMIENTOS CONCRETOS (título IV LOPDGDD)	GDPR	LOPD GDD
Tratar datos personales relacionados con infracciones y sanciones administrativas fuera de los supuestos permitidos		27

RESPONSABLE Y ENCARGADO DEL TRATAMIENTO *(título V LOPDGDD)*	GDPR	LOPD GDD
Incumplir la obligación de bloqueo de los datos cuando la misma sea exigible		32

TRANSFERENCIAS INTERNACIONALES DE DATOS *(capítulo V GDPR)*	GDPR	LOPD GDD
Realizar transferencias internacionales de datos, cuando no concurran las garantías, requisitos o excepciones establecidas	44 a 49	

SITUACIONES ESPECÍFICAS DE TRATAMIENTO *(capítulo IX GDPR)*	GDPR	LOPD GDD
Infringir las disposiciones relativas al "Tratamiento y libertad de expresión y de	85	
Infringir las disposiciones relativas al "Tratamiento y acceso del público a documentos	86	
Infringir las disposiciones relativas al "Tratamiento del número nacional de	87	
Infringir las disposiciones relativas al "Tratamiento en el ámbito laboral"	88	
Infringir las disposiciones relativas a las "Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos"	89	
Infringir las disposiciones relativas a las "Obligaciones de secreto"	90	
Infringir las disposiciones relativas a las "Normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas"	91	

AUTORIDADES DE CONTROL (AC) *(capítulo VI GDPR)*	GDPR	LOPD GDD
No facilitar el acceso del personal de la Autoridad de Control 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	58.1	
La resistencia u obstrucción del ejercicio de la función inspectora por la AC	57	
Incumplir un requerimiento de la Autoridad de Control	58.2	
Incumplir las resoluciones dictadas por la Autoridad de Control	58.2	

INFRACCIONES CONSIDERADAS **GRAVES**

Normativa	Artículo 83.4 del GDPR y 73 de la LOPDGDD

Prescripción	A los 2 años
Multas administrativas	En función de las circunstancias de cada caso individual: Mínimo: entre 40.001 € y 300.000 Máximo: importe más elevado entre 10.000.000 € y el 2% del total de la facturación mundial anual del ejercicio financiero anterior

PRINCIPIOS *(capítulo II GDPR)*	GDPR	LOPD GDD
Condiciones aplicables al consentimiento del menor en relación con los servicios de la sociedad de la información	8	
El tratamiento de datos personales de un menor de edad sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela	8	7
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	8.2	7
Infringir las disposiciones relativas a los "Tratamientos que no requieren identificación"	11	
Impedir, obstaculizar o no atender reiteradamente el ejercicio de los derechos de acceso, rectificación, supresión, limitación o portabilidad en tratamientos en los que no se requiere la identificación del interesado, cuando este, para ejercer estos derechos, haya facilitado información adicional que permita su identificación	11.2 Cdo. 57	

RESPONSABLE Y ENCARGADO DEL TRATAMIENTO *(capítulo IV GDPR)*	GDPR	LOPD GDD
Infringir las disposiciones relativas a la "Protección de datos desde el diseño y por defecto"	25	
No adoptar medidas técnicas y organizativas apropiadas para aplicar la protección de datos desde el diseño incluyendo las garantías necesarias en el tratamiento	25	
No adoptar medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratarán los datos necesarios para cada fin del tratamiento	25.2	

Infringir las disposiciones relativas a los "Corresponsables del tratamiento (CoRT)"	26	
Infringir las disposiciones relativas a los "Representantes de los RT no establecidos en la	27	
No designar un representante del RT o ET no establecido en la UE	27	
Falta de atención del representante en la UE de las solicitudes efectuadas por la AC o por los interesados	27.4	
Infringir las disposiciones relativas a los "Encargados del tratamiento (ET)"	28	
Contratar un ET que no ofrezca suficientes garantías para aplicar las medidas técnicas y organizativas apropiadas conforme a lo establecido en el Capítulo IV del GDPR	28.1	
Contratar por parte de un ET, otros SubET sin contar con la autorización previa del RT, o sin informarle de los cambios en la subcontratación cuando estos sean exigibles	28.2	
Encargar el tratamiento a un ET sin la previa formalización de un contrato o acto jurídico que contenga lo dispuesto en el GDPR	28.3	
La infracción de un ET al determinar por su cuenta los fines y los medios del tratamiento	28.10	
No adoptar medidas para que cualquier persona que actúe bajo la autoridad del RT o ET y tenga acceso a datos personales, los trate siguiendo las instrucciones del RT	29	
No disponer del Registro de actividades de tratamiento	30	
No poner a disposición de la AC el Registro de actividades de tratamiento	30.4	
No cooperar con la AC	31	
No cooperar con la AC en el desempeño de sus funciones en los supuestos no previstos en el artículo 72 de la LOPDGDD (infracciones consideradas muy graves)	31	
Infringir las disposiciones relativas a la "Seguridad del tratamiento"	32	
No adoptar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento	32.1	

Quebrantar, como consecuencia de la falta de la debida diligencia, las medidas técnicas y organizativas que se hubiesen implantado	32.1	
No notificar una violación de seguridad a la AC	33	
Incumplir el deber del ET de notificar al RT las violaciones de seguridad de las que tuviera	33	
No comunicar una violación seguridad al interesado	34	
Incumplir el deber de comunicación al interesado de una violación de la seguridad cuando sea requerido por la AC	34	
Infringir las disposiciones relativas a la "Evaluación de impacto"	35	
Tratar datos sin llevar a cabo una previa valoración de si procede la realización de una evaluación de impacto y la consulta previa a la AC		28

Tratar datos personales sin haber llevado a cabo una DPIA de las operaciones de tratamiento en los supuestos en que la misma sea exigible	35.3	
Infringir las disposiciones relativas a la "Consulta previa"	36	
Tratar datos personales sin realizar una consulta previa a la AC en los casos en que resulte preceptiva o cuando la ley establezca la obligación de llevarla a cabo	36	
Infringir las disposiciones relativas a la "Designación, funciones y cometidos del DPO"	37 a	
Incumplir la obligación de designar un DPO cuando sea exigible	37	34
No posibilitar la participación del DPO en todas las cuestiones relativas a la protección de datos, no respaldarlo o interferir en el desempeño de sus funciones	38	
Desempeñar funciones reservadas a los organismos de supervisión de códigos de conducta sin haber sido previamente acreditado por la Autoridad de Control	41	
No adoptar, por parte de los organismos acreditados de supervisión de un código de conducta, las medidas oportunas en caso de producirse una infracción del código	41.4	
Infringir las disposiciones relativas a las "Garantías de certificación"	42	
Utilizar un sello o certificado de protección de datos que no haya sido otorgado por una entidad de certificación acreditada o cuando la vigencia hubiera expirado	42	
Incumplir, por parte de un organismo de certificación, los principios y deberes a los que está sometido	42 y 43	
Infringir las disposiciones relativas a los "Organismos y procedimientos de certificación"	43	
Obtener la acreditación como organismo de certificación presentando información inexacta sobre el cumplimiento de los requisitos exigidos	43	
Desempeñar funciones que el GDPR reserva a los organismos de certificación, sin haber sido debidamente acreditado	43.1	39

INFRACCIONES CONSIDERADAS **LEVES**

Normativa	Las restantes infracciones de carácter meramente formal de los artículos 83.4 y 83.5 del GDPR y 74 de la LOPDGDD
Prescripción	1 año
Multas administrativas	En función de las circunstancias de cada caso individual, con un máximo de 40.000 €

PRINCIPIOS *(capítulo II GDPR)*	GDPR	LOPD GDD
No atender el ejercicio de los derechos de acceso, rectificación, supresión, limitación o portabilidad en tratamientos en los que no se requiere la identificación del interesado, cuando este, para ejercer estos derechos, haya facilitado información adicional que permita su identificación, salvo que resultase de aplicación lo dispuesto en el artículo 73.c de la LOPDGDD	11.2 Cdo. 57	

DERECHOS DEL INTERESADO *(capítulo III GDPR)*	GDPR	LOPD GDD
Exigir el pago de un canon para facilitar la información del tratamiento o por atender el ejercicio de los derechos del interesado, cuando lo permita el art. 12.5 del GDPR pero su cuantía exceda el importe de los costes afrontados para facilitar la información o realizar la actuación solicitada	12 y 15	
Incumplir el principio de transparencia de la información o el derecho de información del interesado por no facilitar toda la información exigida en el GDPR	13 y 14	
No atender las solicitudes de ejercicio de los derechos del interesado, salvo que resultase de aplicación lo dispuesto en el artículo 72.1.k de la LOPDGDD	15 a 22	
No notificar la rectificación o supresión de datos o la limitación del tratamiento a cada uno de los destinatarios a los que se hayan comunicado los datos, salvo que sea imposible o exija un esfuerzo desproporcionado	19	
No informar al interesado, cuando 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	19	

DISPOSICIONES GENERALES *(título I LOPDGDD)*	GDPR	LOPD GDD

No suprimir los datos referidos a una persona fallecida cuando ello fuera exigible		3

RESPONSABLE Y ENCARGADO DEL TRATAMIENTO *(título V LOPDGDD)*	GDPR	LOPD GDD
No formalizar un acuerdo con corresponsables del tratamiento (CoRT) que determine las obligaciones, funciones y responsabilidades y sus relaciones con los interesados, o la inexactitud en la determinación de las mismas	26	
No poner a disposición de los interesados los aspectos esenciales del acuerdo formalizado entre los CoRT	26.2	
Incumplir, por parte del Encargado del Tratamiento, las estipulaciones impuestas en el contrato o acto jurídico que regula el tratamiento o las instrucciones del RT, salvo que esté legalmente obligado a ello conforme el GDPR y la LOPDGDD, o en los supuestos en que fuese necesario para evitar la infracción y se hubiese advertido de ello al RT o ET	28.3	
Incumplir, por parte del ET, el informar al RT acerca de la posible infracción por recibir una instrucción que incumple el GDPR o la LOPDGDD	28.3.h	
Disponer de un Registro de actividades de tratamiento que no incorpore toda la información	30	
La notificación incompleta, tardía o defectuosa a la AC relacionada con una violación de seguridad	33	
No documentar cualquier violación de seguridad en los términos exigidos en el GDPR	33.5	
No comunicar al interesado una violación de la seguridad que entrañe un alto riesgo para sus derechos y libertades	34	
Facilitar información inexacta a la AC, en los supuestos en los que el RT deba elevarle una consulta previa	36	
No publicar los datos de contacto del DPO, o no comunicarlos a la AC, cuando su nombramiento sea exigible	37	34
Incumplir, por parte de los organismos acreditados de supervisión de un código de conducta, la obligación de informar a la AC acerca de las medidas que resulten oportunas en caso de infracción del código	41.4	
Incumplir, por parte de los organismos de certificación, la obligación de informar a la AC de la expedición, renovación o retirada de una certificación	43.1 y 43.5	