El marco legal del *email marketing*

PID_00272862

Xavier Folguera

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

Xavier Folguera

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por las profesoras: Cintia Pla Garcia, Iviane Ramos de Luna (2020)

Primera edición: marzo 2020

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

Introducción

La actividad del *email marketing* ha tomado indiscutiblemente el relevo del marketing directo por su economía y rapidez, así como por su alta capacidad de segmentación, personalización y automatización. Esta disciplina publicitaria que antaño se canalizaba por medio del correo postal, hoy se realiza a través del correo electrónico. El cambio en la comunicación directa entre empresa y público ha sido tan radical que el marco legal que ampara los derechos de consumidores y empresas ha tenido que actualizarse profundizando en los aspectos de los derechos a la privacidad del individuo y las obligaciones de las organizaciones en el uso de datos personales.

El *email marketing* se basa fundamentalmente en la obtención y la gestión de datos, de la misma forma que antaño, aunque de una manera más profundamente segmentada, gracias al desarrollo de una sociedad cada vez más digitalizada. Por ello, cuando se plantea el estudio o conocimiento de la normativa que se debe cumplir, se puede comprender mejor si se enfoca desde dos actividades distintas:

1) Desde la captación de datos.

2) Desde la gestión de los datos y la emisión de mensajes, es decir, en la ejecución de campañas masivas publicitarias mediante el correo electrónico.

La norma actual ha puesto mucho énfasis en dotar al ciudadano de una herramienta que le otorgue la máxima seguridad en la protección de su privacidad, puesto que la circulación y el acceso a los datos personales es mucho más intensa y asequible que en la anterior era analógica.

Por ello, como veremos, la normativa se cierne especialmente en los principios de informar con gran transparencia por parte de las empresas en el momento de la captación de datos y del consentimiento del usuario para la recepción de mensajes.

1. Leyes fundamentales: RGPD, LOPDGDD y LSSI

El marco legal que ampara la actividad del *email marketing* abarca distintas leyes y normas, entre las cuales destaca el **Reglamento general de protección de datos (RGPD)**.

Esta norma constituye un punto de referencia clave para la actividad del marketing mediante el correo electrónico.

Con esta norma, el ciudadano cuenta con un marco legislativo que pretende restringir el uso de sus datos personales, al tiempo que se busca dotar a las empresas de la suficiente seguridad jurídica para realizar actividades de marketing que defiendan el derecho a la información de productos y servicios, todo ello en un entorno de libertad comercial y publicitaria.

El 25 de mayo de 2016 se aprobó en el Parlamento Europeo el nuevo RGPD, el **Reglamento (UE) 2016/679, general de protección de datos**, una nueva norma con el objetivo de proteger en el conjunto comunitario los derechos de los ciudadanos europeos con respecto a sus datos personales. Así pues, todos los países del entorno comunitario se vieron obligados a adaptar sus normas a lo aprobado en el Parlamento Europeo.

En España también se aprobó una ley complementaria al RGPD, después de su publicación en el *BOE* el 6 de diciembre de 2018, bajo el nombre de **Ley orgánica de protección de datos y garantía de los derechos digitales (LOPDGDD)**. El objetivo era adaptar la legislación española al RGPD y regular el derecho fundamental a la protección de datos.

A pesar de la preponderancia de estas leyes en el *email marketing*, en España también se debe tener en cuenta el papel de la **Ley de la sociedad de la información y del comercio electrónico (LSSI)**, ley que presenta artículos vinculados a la protección de datos y la actividad del *emailing*, relacionados con el derecho a la revocación del consentimiento para comunicaciones comerciales.

Ved también

La protección de datos y la actividad del *emailing* se trata en el apartado «Requerimientos legales del *email*: revocación del consentimiento» del presente módulo.

1.1. Qué es el RGPD: definición

El Reglamento general de protección de datos fue aprobado en el Parlamento de la Unión Europea con el fin de armonizar las anteriores normativas de privacidad de los países de la UE y crear un marco de confianza para el desarrollo

del mercado único digital. Esta confianza se entendía desde los derechos de protección de datos del ciudadano hasta la forma en que las compañías debían afrontar la denominada *ciberseguridad*, ya fuera a nivel técnico u organizativo.

El RGPD es considerado como la norma más importante de la Unión Europea en cuanto a la protección de datos personales. Con él se ha dotado de mayor seguridad y control a los datos de información personal, y es de obligado cumplimiento desde el 25 de mayo de 2018 (dos años después de su aprobación).

Como veremos, el RGPD es una norma que se rige por unos principios de transparencia, de limitación de uso, de minimización de datos, de limitación en los plazos de conservación, de integridad, seguridad y responsabilidad por parte de los gestores de datos.

1.2. Ámbito de aplicación

El RGPD se aplica a cualquier organización o empresa que procesa datos de carácter personal sobre residentes en la Unión Europea o que tiene su establecimiento permanente en la UE, o bien a empresas cuyos servicios o productos son comercializados a los ciudadanos que residen allí. Cuando hablamos de datos personales nos referimos a los de cualquier persona física, tanto en el rol de cliente o consumidor, como en el de trabajador de una empresa.

2. La captación de datos: principios y deberes del nuevo reglamento

En la captación de datos existen dos grandes principios en el cumplimiento de la ley: el **consentimiento explícito del usuario** y el **deber de informar**.

Ambos constituyen los factores diferenciales sobre las anteriores normativas y, por ello, las empresas han debido actualizar sus procedimientos para continuar realizando *email marketing*. Los datos conseguidos con los anteriores procedimientos, mediante permiso tácito y sin informar, no pueden utilizarse.

2.1. El consentimiento explícito

El primer concepto fundamental que distingue esta norma con respecto a las anteriores leyes es la obligación de poder demostrar de manera fehaciente y demostrable la captación de datos recabando el consentimiento del usuario, es decir, obteniendo su beneplácito explícito.

Las empresas deben disponer de la tecnología necesaria para poder demostrar a la Administración y a los titulares de los datos, en cualquier momento, que han captado esos datos de forma lícita (por lo que deben disponer de un archivo o documento acreditativo) y, al mismo tiempo, que ofrecen al usuario la revocación de dicho consentimiento de manera fácil y gratuita.

Por lo tanto, cualquier recopilación de datos debe obtenerse bajo la voluntad del usuario de forma expresa y libre, es decir, se excluye el consentimiento tácito, como sucedía anteriormente. Esa recopilación debe estar enfocada a una finalidad concreta y declarada previamente, y se impide su uso en cuestiones ajenas. El usuario podrá saber qué uso se está dando a sus datos, o sea, será verificable.

Hay que matizar que, en el caso de las comunicaciones a los clientes actuales, no es necesario el consentimiento explícito del destinatario para el envío de informaciones de productos o servicios que originaron la relación comercial existente. Esto es así puesto que el envío puede entrar dentro de las expectativas razonables del cliente, por lo que tiene la base legitimadora en el interés legítimo del responsable.

2.2. El deber de informar: información por capas

La ley obliga a las empresas a informar a los ciudadanos sobre el uso que se realizará de sus datos personales previamente a su cesión. En el *email marketing*, un dato personal fundamental es la dirección de correo electrónico, y se considera como tal tanto a nivel particular como a nivel profesional.

Esta obligación de transparencia en la captación de datos debe aplicarse a cualquier tipo de soporte, ya sea físico, digital u oral, o sea, en versión papel, versión en línea, versión telefónica, incluso a los nuevos soportes tecnológicos (IoT) y aplicaciones móviles.

En la antigua norma, ya se exigía que se informara sobre la existencia de un fichero, una finalidad, los destinatarios y la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición, pero el nuevo RGPD añade requisitos adicionales en cuanto a informar a las personas interesadas. Los nuevos requisitos principales son la obligación de informar sobre la base jurídica o legitimación para el tratamiento, los datos del delegado de protección de datos, los plazos y criterios de conservación de los datos y otros más detallados, que deben transmitirse en las denominadas *capas de información*.

El RGPD prevé la existencia del redactado de un documento, frecuentemente denominado *Política de privacidad*, que cualquier organización debe poseer para informar sobre los puntos antes mencionados, y que se debe presentar al usuario que cede los datos, mediante dos tipos de capas de información: una primera capa de epígrafes resumidos y una segunda capa con el documento completo.

Epígrafes

Los **epígrafes** son los conceptos fundamentales presentados de forma resumida que son desarrollados en un documento más extenso situado en el sitio web donde se captan los datos.

2.2.1. Primera capa: epígrafes básicos

El objetivo de la norma es que el usuario pueda leer fácilmente una información básica sobre el uso que se realizará de sus datos en el momento de cederlos, y obliga a las empresas que desean obtenerlos a que informen en una primera «capa de información» –por medio de una tabla con un resumen en forma de epígrafes básicos– del conjunto de las informaciones requeridas por la ley.

Estos epígrafes se refieren al responsable, la finalidad, la legitimación, el destinatario y los derechos.

Este pequeño resumen informativo debe acompañarse de una casilla de aceptación (*check box*), que el usuario debe marcar antes de ceder los datos, lo cual confirma la aceptación de la cesión de datos y la empresa que los capta consi-

gue seguridad jurídica por la aceptación explícita del usuario. De este modo, se resuelve el primer principio expuesto sobre el consentimiento explícito del cedente de datos.

Al mismo tiempo, además del *check box* antes mencionado, debe existir un enlace (hipervínculo) dirigido al grueso de la información, la denominada «segunda capa» de información, más detallada y completa. El usuario debe declarar que ha leído tal documento y ha sido informado previamente a su cesión. Todo ello dota al concepto **tratamiento de datos** de un sentido mucho mayor al que se le otorgaba anteriormente.

Imagen 1. Ejemplo de epígrafes básicos

Responsable. Se denomina responsable del tratamiento de datos a la entidad o empresa propietaria de la base datos. Se deberá exponer el nombre de la empresa que es responsable de la base de datos. Esta empresa puede cederlos a un «encargado» y puede tener un delegado, como veremos más adelante.

Finalidad. Se deben exponer con transparencia los fines del tratamiento, es decir, para qué se utilizará la base de datos. También se explicitarán plazos y criterios de conservación, además de la existencia de mensajes automatizados y de perfiles segmentados de usuarios.

Legitimación. Se debe detallar la base jurídica del tratamiento, esto es, si existe obligación o voluntariedad en la cesión de datos. Habitualmente, se manifiesta el simple consentimiento voluntario del usuario.

Destinatarios. Este punto se refiere a la intención de posibles cesiones o transferencias de datos a terceros. Por ejemplo, si la empresa forma parte de un grupo de empresas con actividades distintas, debe quedar explicitado si cederá los datos o no.

Derechos. Se expone el ejercicio de los derechos de acceso, supresión, portabilidad y oposición. También debe concretarse la forma de poder ejercer tales derechos.

2.2.2. Segunda capa: documento detallado

El documento que desarrolla los epígrafes se denomina habitualmente *Política de privacidad*, y expresa la forma en que cada empresa u organización cuida y procesa los datos del usuario, manteniendo con garantías la información obtenida.

Cada organización tiene su propio documento, ya que no existe un modelo prefijado con exactitud. Es responsabilidad del usuario leerla antes de aceptarla para asegurarse de que no haya condiciones que incluyan el riesgo de intercambio de información o cualquier otra cláusula que pueda interpretarse como una violación de su privacidad.

2.3. El consentimiento asegurado: el doble *opt-in*

Una de las herramientas recomendadas en la captación segura de datos es el uso del **doble *opt-in***. Este mecanismo consiste en el envío de un mensaje a la bandeja de entrada del titular de los datos después de haber dado su dirección de correo y aceptado su registro en la base de datos. Este mensaje incluye un enlace que debe ser pulsado por el usuario para dar validez a su registro en la base de datos.

Si bien es cierto que cuando un usuario introduce su dirección de correo en un formulario, con un *opt-in* simple puede quedar constancia de que se ha registrado, puede darse la circunstancia de que la dirección sea errónea o de otro usuario, lo cual imposibilite que el usuario confirme su dirección y, por tanto, no queda realmente registrado en la base. Por ello, la vía más segura es el doble *opt-in*.

Así pues, la empresa podría disponer de un archivo informático de doble *opt-in* con los datos del registro, así como del correo remitido por el usuario, lo que la dotaría de una completa documentación que, en caso de litigio, avalaría a la empresa ante un organismo competente, que siempre se regirá bajo el principio de la demostración.

2.4. Los perfiles segmentados

El éxito del *email marketing* se basa en la segmentación de los perfiles personales con los datos obtenidos. Esta segmentación se puede realizar o bien procesando datos y agrupándolos según los intereses del usuario, o bien desde los intereses de la empresa. Con ello, las empresas pueden crear perfiles de personas y usarlos para evaluar determinados aspectos vinculados con ellas.

El objetivo final de la segmentación es intentar predecir el comportamiento humano y tomar decisiones estratégicas y tácticas, lo que implica frecuentemente el tratamiento automatizado de datos. Con los perfiles segmentados, cualquier empresa puede decidir a qué grupos puede o debe hacer envíos con mensajes específicos para aumentar la eficacia de cada campaña.

La normativa actual permite todo tipo de creación de perfiles, pero las empresas deben asegurar derechos importantes a las personas que forman parte de estas bases.

- Solicitar el consentimiento previo y explícito para llevar a cabo las operaciones de perfilado de usuarios.

- El derecho al olvido. Si el usuario desea que se borren datos concretos, la empresa debe llevar a cabo dicha supresión.

- El derecho a ser informado y a poseer una copia de sus datos personales.

- El derecho de oposición y de interrupción del tratamiento.

2.4.1. La protección de datos de menores de 14 años

Los perfiles humanos segmentados que incluyen a menores requieren una especial atención. Las empresas que venden productos enfocados a menores, como juguetes, aplicaciones o videojuegos, deberán obtener el consentimiento de alguno de los progenitores si desean recabar datos sobre sus preferencias, intereses o gustos. Para ello, deberán ofrecer una información más clara, sencilla y transparente.

Al igual que con el resto de los segmentos de población, las empresas están obligadas a almacenar pruebas que cuenten con el consentimiento de los padres y, en definitiva, de todos los contactos incluidos en la base de datos.

2.4.2. La compra o cesión de bases de datos

El RGPD permite teóricamente la adquisición de listas de contactos, siempre y cuando el consentimiento se haya dado de manera clara y sea demostrable, pero en España, la actual Ley orgánica de protección de datos impide la transferencia del consentimiento y, en consecuencia, no es legal adquirir o usar listas de otros.

Dicho en otras palabras, aunque podamos obtener de terceros correos electrónicos de usuarios, no por ello hemos adquirido el consentimiento del usuario para remitirle correos que no ha autorizado explícitamente.

3. La gestión de datos en el *email marketing*

El *email marketing* es la herramienta de marketing digital más antigua de las existentes y ha sido utilizada por las empresas desde el inicio de internet. Durante mucho tiempo y en general, las organizaciones han recabado datos de forma tácita, o sea, sin obtener un consentimiento expreso del usuario, pero el nuevo marco normativo ha obligado a la revisión de los procesos; procesos donde intervienen no solo empresas y usuarios, sino también agencias de marketing digital o empresas externas.

Por ello, la nueva ley ha descrito nuevos actores en la práctica profesional del *email marketing*, que sirven para elevar el nivel de control en la protección de datos del ciudadano y para repartirse las responsabilidades en el cumplimiento de la ley.

3.1. Los roles en la gestión

La nueva ley describe con claridad los tres roles que intervienen en esta práctica profesional, y exige a cada uno de ellos unas responsabilidades específicas que no pueden pasarse por alto.

1) Responsable

El **responsable del tratamiento** descrito en el RGPD es la persona física o jurídica que determina los fines y medios del tratamiento de datos.

Podemos hablar de la empresa, el autónomo o la persona física que lleva a cabo actividades comerciales y que dará cuenta a las autoridades y al usuario en caso de conflictos.

El responsable decide el uso que se va a hacer de los datos, su conservación, su cesión o si se van a eliminar. En resumen, estará obligado al deber de informar, guardar secreto, comprobar que los datos sean correctos y auténticos, que se han obtenido de forma lícita y comprobable, atendiendo a los ciudadanos en su derecho de acceso, rectificación y cancelación, adoptando todas las medidas de seguridad organizativa posibles.

2) Encargado

Las empresas confían en terceros para gestionar muchas actividades que suponen la transmisión de datos personales, como pueden ser asesorías laborales o mutuas médicas; en lo que al *email marketing* concierne, pueden intervenir agencias digitales que realicen campañas de *email marketing*. Este rol se denomina *encargado*.

Cuando una compañía encarga a terceros la realización de tratamientos, esta relación debe quedar regulada en un contrato escrito en el que conste que el encargado cumplirá un conjunto de requisitos:

- Se limitará a utilizar los datos exclusivamente para el fin descrito y no para otros fines.
- Mantendrá absoluto secreto sobre los contenidos de la base de datos.
- Tratará los datos conforme a las instrucciones del responsable de tratamiento.
- Expondrá las medidas de seguridad que el encargado estará obligado a cumplir.

La existencia de este contrato permite al encargado el acceso de los datos de los usuarios sin el permiso de estos, ya que se supone que el responsable ha cedido tal derecho. Finalmente, el encargado del tratamiento debe devolver los datos o eliminarlos cuando ha finalizado el servicio contratado.

3) Delegado

La nueva ley incorpora una nueva figura en el tratamiento de datos, denominada *delegado de protección de datos*. La existencia de esta figura solo es obligada o bien en empresas cuyas actividades principales requieran un control o una observación frecuente y sistemática de datos de personas a gran escala, o bien que incluyan en el tratamiento datos de categorías especiales.

Algunos de los tipos de empresas obligadas a nombrar a un delegado son las empresas prestadoras de servicios de la sociedad de la información que elaboren perfiles, las que desarrollen publicidad y prospección comercial, o sea, agencias digitales que gestionan datos de consumidores en nombre de un anunciante. Existen muchas más empresas obligadas, como las vinculadas a la docencia, inversión, sanidad y juego en línea, entre otras.

Entre las funciones del **delegado**, destacan la supervisión de lo marcado en el RGPD, el asesoramiento al responsable o encargado y su cooperación con la autoridad de control (Agencia Española de Protección de Datos) en caso necesario.

4. Requerimientos legales del *email*: revocación del consentimiento

En cualquier campaña de *email marketing*, es imperativo legal que todos los mensajes incluyan enlaces para la fácil revocación del consentimiento del usuario para la recepción de comunicaciones comerciales.

El artículo 22.1 de la Ley de servicios de la sociedad de la información regula esta obligación.

«[...] los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el **consentimiento** que hubieran prestado. Cuando las comunicaciones hubieran sido remitidas por **correo electrónico** dicho medio deberá consistir necesariamente en la inclusión de una dirección de correo electrónico u otra dirección electrónica válida donde pueda ejercitarse este derecho quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.»

Artículo 22.1 de la Ley de servicios de la sociedad de la información.

Dicho de otro modo, el usuario debe poder **revocar su consentimiento** para recibir **comunicaciones comerciales** utilizando la misma comunicación, por ejemplo, mediante un enlace al pie del mensaje, mencionando «darse de baja» o «desuscripción».

5. Los derechos ARCO y su ampliación con el RGPD

Existen cuatro derechos en la LOPDGDD que cualquier usuario puede ejercer para proteger sus datos de carácter personal: el derecho de acceso, el derecho de rectificación, el derecho de cancelación y el derecho de oposición (ARCO). Cada derecho resuelve una necesidad distinta:

- **Derecho de acceso**. Permite al interesado conocer los datos que se están procesando y la finalidad, el origen y las comunicaciones en las que está presente.

- **Derecho de rectificación**. El usuario puede exigir cambios por errores.

- **Derecho de cancelación**. Permite la exigencia de retirada y archivo de datos, si el interesado lo considera inapropiado.

- **Derecho de oposición**. Siempre y cuando alguna norma legal no diga lo contrario, el usuario tiene el derecho a oponerse al tratamiento de sus datos cuando no sea necesario su consentimiento.

Con la entrada en vigor del RGPD, a estos cuatro derechos se le han sumado otros tres, que ciertamente pueden ser más circunstanciales que los anteriores desde el punto de vista del *email marketing*:

- **Derecho de olvido**. Permite al interesado exigir no solo la retirada de permiso y archivo de datos, sino directamente la supresión de datos. Este derecho se puede ejercer en múltiples casos, como, por ejemplo, la retirada de su consentimiento o el cumplimiento de una obligación legal.
  Se da la circunstancia de que las empresas también podrían negarse a eliminar esos datos en ciertos casos, como por ejemplo cuando está protegido por el derecho a la libertad de expresión o cuando esos datos son usados para fines de archivo de interés público o estadísticos.

- **Derecho de portabilidad**. En virtud de lo dispuesto en el citado artículo 20 del RGPD, el interesado tiene derecho a «recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado».
  Se puede decir que se aplica el derecho de portabilidad en telefonía al terreno de los datos personales. En definitiva, el derecho a la portabilidad tiene por objeto atribuir al interesado un mayor control sobre sus datos

personales y favorecer el libre flujo de datos personales en la UE con el fin de fomentar la competencia.

- **Derecho de limitación del tratamiento** (art. 18 RGPD). El RGPD aumenta la capacidad de decisión y control de los ciudadanos sobre sus datos personales. Limitar el tratamiento significa que, si el interesado quiere borrar sus datos personales pero algún motivo legal lo impide, este puede solicitar la limitación de sus datos al responsable del tratamiento. De este modo, los datos pueden ser conservados, pero no utilizados para otros fines.

6. Transferencia internacional de datos: herramientas de envíos

Con la entrada en vigor del RGPD, el legislador europeo también ha querido proteger el derecho a la protección de datos personales más allá de la Unión Europea. En este sentido, muchas de las herramientas *cloud* (en la nube) que utiliza el *email marketing* están alojadas en servidores de fuera del entorno europeo, por lo que podría estar incumpliendo la ley.

Los países que se encuentran fuera de las fronteras europeas deben garantizar niveles de garantía o adecuación en materia de protección de datos equivalentes a los establecidos en la Unión Europea. En el caso de las compañías americanas, si están adheridas al acuerdo EU-US Privacy Shield, es suficiente, y este es el caso de Mailchimp.

Con el RGPD, las transferencias internacionales de datos deben estar bajo control.

> Se define como **transferencia internacional** cualquier comunicación de datos personales que se produce entre un responsable o encargado situado en un país miembro de la UE, y un encargado o responsable ubicado fuera de ella.

Con la entrada en vigor del RGPD, quien pudiera exportar los datos, ya fuera el encargado o el responsable del tratamiento (por ejemplo, una agencia digital o el propio anunciante), asumiría responsabilidades en caso de conflicto. Por lo tanto, la nueva ley atribuye responsabilidad a los proveedores de las empresas como encargados y a las propias compañías propietarias de las bases de datos como responsables de ellas.

En general, el RGPD no exige aprobación de la autoridad de control (Administración) para realizar legítimamente una transferencia internacional de datos, excepto en algunos casos especiales incluidos en el art. 43 LOPDGDD. En otras palabras, se puede utilizar cualquier herramienta de *email marketing*, siempre y cuando en el país de recepción se ofrezcan garantías adecuadas, mediante la aprobación de las denominadas *normas corporativas vinculantes*. Estas normas son el modelo de referencia de la UE sobre la privacidad de datos.

7. Régimen sancionador por incumplimiento de la ley

Las infracciones de protección de datos se dividen en leves, graves y muy graves.

Tabla 1. Ejemplos de infracciones

Leves	Graves	Muy graves
• La falta de transparencia de la información. • El incumplimiento de informar al afectado cuando lo haya solicitado. • El incumplimiento de las obligaciones del encargado.	Las infracciones graves son la que vulneran sustancialmente el tratamiento, y están relacionadas con: • La obtención o el uso de datos de un menor de edad recabados sin consentimiento. • La falta de adopción de medidas técnicas y organizativas necesarias para la efectiva protección de datos. • El incumplimiento de nombrar responsable o encargado de tratamiento de datos.	Las infracciones muy graves suponen un incumplimiento sustancial del tratamiento: • El uso de los datos para una finalidad diferente a la pactada. • La omisión del deber de correcta información al afectado. • La exigencia de un pago para poder acceder a los datos propios almacenados. • La transferencia internacional de información sin garantías.

Los **infractores** pueden ser:

1) Los responsables de los tratamientos.
2) Los encargados de los tratamientos.
3) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.
4) Las entidades de certificación.
5) Las entidades acreditadas de supervisión de los códigos de conducta.

7.1. Sanciones

El importe marcado en el RGPD por el incumplimiento de la norma abarca las infracciones graves y muy graves:

- Las **infracciones graves** se sancionarán con multas administrativas que pueden ascender hasta los diez millones de euros o, si se trata de una empresa, una cuantía máxima del 2 % de la facturación.

- Las **infracciones muy graves** se sancionarán con multas administrativas que pueden alcanzar los veinte millones de euros o, tratándose de una empresa, de una cuantía equivalente al 4 % de la facturación.