Asesorando empresas desde 1989

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

CE Consulting

Política de Protección de datos

Rev. 00

Documento de seguridad

Medidas de seguridad aplicadas al tratamiento de datos personales

Revisión	Fecha	Parte modificada o creada
00	22/03/2012	Creación del documento

I. OBJETO DEL DOCUMENTO DE SEGURIDAD

El presente documento responde a la obligación establecida en el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento y la libre circulación de datos personales, en adelante, RGPD y en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales en adelante LOPDGDD.

Será obligatorio el cumplimiento de los requerimientos y obligaciones para el responsable y el encargado de tratamiento que este incluye, entre las que destaca, la necesidad de llevar a cabo un análisis de riesgos con el fin de establecer medidas de seguridad y control para garantizar los derechos y libertades de las personas.

El modelo se ha redactado con el objeto de recopilar las exigencias establecidas por el Reglamento. Se presenta de forma sistemática las principales cuestiones que las organizaciones deberán tener en cuenta de cara a la aplicación del RGPD, para que resulte de ayuda a los responsables y a los encargados de tratamiento. Es posible y recomendable incorporar cualquier otra medida que se considere oportuna para aumentar la seguridad de los tratamientos, o incluso, adoptar las medidas exigidas para un nivel de seguridad superior al que por el tipo de información les corresponde, teniendo en cuenta la infraestructura y las circunstancias particulares de la organización.

Este documento contiene una guía para los responsables de tratamiento, que a su vez desarrolla las medidas adecuadas para adoptar en la organización para la correcta protección de los datos personales, así como las obligaciones legales para los responsables, el ejercicio de los derechos y la gestión de los riesgos. Asimismo, incluye anexos con las medidas adicionales en caso de tratar con centros sanitarios o educativos, en caso de realizar transferencias internacionales de datos personales, tratar con menores de edad, o la necesidad de Delegado de Protección de Datos en la organización.

El presente documento es de aplicación tanto a las actividades de tratamiento como a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad del Responsable del Tratamiento, tanto cuando actúa como tal o como Encargado del Tratamiento; incluyendo los sistemas de información, comunicación, soportes, equipos y resto de recursos empleados, entre los cuales queda incluido el personal, para el tratamiento de datos de carácter personal.

II. PRINCIPIOS GENERALES DE LA PROTECCIÓN DE DATOS PERSONALES

De conformidad con el artículo 5 del Reglamento General de Protección de Datos, los principios relativos al tratamiento de datos personales son los siguientes:

a) *Tratados de manera lícita, leal y transparente en relación con el interesado;*
b) *recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines;*
c) *adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados;*
d) *exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan;*
e) *mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos;*
f) *tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.*

El responsable del tratamiento será responsable del cumplimiento de lo dispuesto y capaz de demostrarlo

Por todo lo expuesto, es necesario tener en cuenta en relación a la protección de datos la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.
En términos prácticos, esta necesidad requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión. En síntesis, este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.

Las principales medidas dirigidas a garantizar su cumplimiento deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas. De acuerdo con este enfoque, algunas de las medidas que el RGPD establece se aplicarán sólo cuando exista un alto riesgo para los derechos y libertades, mientras que otras deberán modularse en función del nivel y tipo de riesgo que los tratamientos presenten. La aplicación de las medidas previstas por el RGPD debe adaptarse, por tanto, a las características de las organizaciones. Lo que puede ser adecuado para una organización que maneja datos de millones de interesados en tratamientos complejos que involucran información personal sensible o volúmenes importantes de datos sobre cada afectado no es necesario para una pequeña empresa que lleva a cabo un volumen limitado de tratamientos de datos no sensibles.

Asimismo, el Reglamento General de Protección de Datos mantiene el principio recogido en la Directiva 95/46 de que todo tratamiento de datos necesita apoyarse en una base que lo legitime. También recoge las mismas bases jurídicas que contenía la Directiva y que reproduce la LOPD:

- Consentimiento.
- Relación contractual.
- Intereses vitales del interesado o de otras personas.
- Obligación legal para el responsable.
- Interés público o ejercicio de poderes públicos.
- Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.

De este modo, en el caso de las bases jurídicas legitimadoras del tratamiento de datos personales por parte de las organizaciones privadas, podemos tener en cuenta, entre otras: relación contractual previa que contemple el tratamiento, consentimiento del ciudadano o interés legítimo que prevalezca sobre los derechos de las personas, entre otras.
Por tanto, en la actualidad, no resulta necesario que el particular consienta el tratamiento de sus datos personales si existe otra base jurídica que legitime el tratamiento.
En los casos en los que el consentimiento del ciudadano sea preciso por no existir otra base legitimadora, la Ley establece que debe ser una manifestación de voluntad libre, específica, informada e inequívoca por la que una persona acepta el tratamiento de sus datos personales, ya sea mediante una declaración o una clara acción afirmativa. Se excluye el consentimiento tácito o por omisión.
Además, cuando se pretenda que el consentimiento del ciudadano legitime un tratamiento para una variedad de finalidades, será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.
No podrá denegarse un contrato o la prestación de un servicio por el hecho de que la persona no consienta el tratamiento de sus datos personales para finalidades que no guarden relación con ese contrato o con la prestación de ese servicio.

III. GUÍA PARA RESPONSABLES DEL TRATAMIENTO

a. Medidas de protección de datos

El RGPD establece un catálogo de las medidas que los responsables, y en ocasiones los encargados, deben aplicar para garantizar que los tratamientos que realizan son conformes con el Reglamento y estar en condiciones de demostrarlo.

En primer lugar, vamos a mencionar la obligación relativa a todos los responsables de realizar una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo. El tipo de análisis variará en función de los tipos de tratamiento, la naturaleza de los datos, el número de interesados afectados y la cantidad y variedad de tratamientos que la organización lleve a cabo.

Por consiguiente, en el presente documento realizaremos una valoración de los riesgos inherentes a la organización.

Por otro lado, también se establece la obligación para los responsables y encargados de mantener un registro de operaciones de tratamiento en el que se contenga la información que establece el RGPD y que contenga las cuestiones básicas de: nombre y datos de contacto del responsable o corresponsable, finalidades de tratamiento, descripción de categorías de interesados y categorías de datos personales tratados, así como, entre otros, transferencias internacionales de datos. Esta obligación es exigible para aquellas organizaciones que empleen a más de 250 trabajadores, no obstante, es recomendable utilizar esta medida para prevenir los riesgos que puedan alcanzar a los derechos y libertades de los interesados.

Se debe considerar también la obligación de notificar las violaciones de seguridad de los datos. El RGPD define las violaciones de seguridad (o como también se las conoce “quiebras de seguridad”), de una forma muy amplia, que incluye todo incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

Cuando se produzca una violación de seguridad de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, a menos que, sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

Por último, debemos tener en cuenta la obligación para los responsables de tratamiento de realizar una evaluación de impacto sobre la protección de datos. Esta evaluación deberá hacerse con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados. La finalidad de realizar esta evaluación es determinar las necesidades adicionales en materia de protección de datos, pues si se llevan a cabo tratamientos de datos a gran escala o bien tratamiento de datos sensibles o que conlleven efectos jurídicos relevantes, supondría la necesidad de adoptar la figura en la organización de un Delegado de protección de datos.

b. Obligación de informar del tratamiento de datos y ejercicio de derechos

Todas las organizaciones quedan obligadas a informar a los ciudadanos de forma clara y sencilla sobre los aspectos más importantes del tratamiento de sus datos, identificando quién trata los datos, con qué base jurídica, para qué finalidad, y sobre la forma de ejercer los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición y decisiones automatizadas.

Las organizaciones no podrán denegar el ejercicio de estos derechos en el caso de que el ciudadano quiera ejercitarlos de un modo diferente al que se le ofrezca.

La obligación de informar a las personas interesadas sobre las circunstancias relativas al tratamiento de sus datos recae sobre el Responsable del Tratamiento.

La información se debe poner a disposición de los interesados en el momento en que se soliciten los datos, previamente a la recogida o registro, si es que los datos se obtienen directamente del interesado.

En el caso de que los datos no se obtengan del propio interesado, por proceder de alguna cesión legítima, o de fuentes de acceso público, el Responsable informará a las personas interesadas dentro de un plazo razonable, pero, en cualquier caso: antes de un mes desde que se obtuvieron los datos personales; antes o en la primera comunicación con el interesado; o antes de que los datos, en su caso, se hayan comunicado a otros destinatarios. Esta obligación se debe cumplir sin necesidad de requerimiento alguno, y el responsable deberá poder acreditar con posterioridad que la obligación de informar ha sido satisfecha.

La información a las personas interesadas debe proporcionarse con un lenguaje claro y sencillo, de forma concisa, transparente, inteligible y de fácil acceso.

Se debe ofrecer la identidad del Responsable del Tratamiento, así como los datos de contacto del mismo, entendiéndose por éstos la dirección postal y la dirección electrónica.

Debe informarse también de los fines del tratamiento a que se destinan los datos personales, incluyendo el plazo durante el cual se conservarán dichos datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo. Debe tenerse en cuenta que, los fines deberán ser determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

Asimismo, se indicará la base jurídica en la cual se basa el tratamiento, según sea: por ejecución de un contrato, por cumplimiento de una obligación legal, o en interés público o ejercicio de Poderes Públicos, así como también por propio consentimiento del interesado.

Cuando se haya previsto ceder o comunicar, legítimamente, los datos personales que se recogen, se informará acerca de la identidad de los destinatarios, si están claramente determinados, o de las categorías de destinatarios, si estos no están determinados previamente.

El Responsable informará claramente sobre cómo podrá ejercer el interesado materialmente los derechos de acceso, rectificación o supresión, limitación, oposición o portabilidad del tratamiento de los datos personales. Deberá informar también de que

los interesados podrán presentar una reclamación ante la Autoridad de Control en materia de Protección de Datos competente.

Para el efectivo cumplimiento de estas previsiones legales, habilitamos una serie de instrumentos de los que debe hacer uso en su organización con la finalidad de evitar las posibles sanciones por incumplimiento.

i. Cartel informativo

En primer lugar, debe usted utilizar el presente cartel informativo, colocándolo en un lugar visible y accesible de su establecimiento o local para el público en general. En el mismo se establecen el aviso de recogida de datos personales por parte de la organización de forma lícita y ajustada a la legalidad vigente, incluyendo en el mismo la identificación del responsable del tratamiento de los datos, la finalidad del tratamiento, así como la posibilidad que ofrece la organización a los usuarios de la misma a que ejerzan sus derechos inherentes de conformidad con el RGPD y la LOPDDGG:

RECOGIDA DE DATOS PERSONALES DE ACUERDO CON EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS Y LA LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

RESPONSABLE DEL TRATAMIENTO:

MARTIN VECINO, S.L con CIF B81316101, domiciliada en CL LEON 80, FUENLABRADA - 28947 (MADRID) y contacto a través de: número de teléfono 916424471 | 620262226y correo electrónico agustin@martinvecino-sl.com

FINALIDAD DEL TRATAMIENTO:

Los datos de carácter personal facilitados serán tratados por la organización solo a efectos de gestionar y prestar el servicio solicitado. Así como, si es el caso, avisar al interesado/a de la recepción del producto encargado por el medio que nos facilite. Solo en el caso de contar con su consentimiento, recibirá información sobre los servicios ofrecidos y en los que podría estar interesado/a.

DERECHOS:

Acceso, rectificación, supresión y demás derechos reconocidos en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales, y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016. Para que pueda ejercer cualquiera de los derechos indicados deberá contactar con nosotros a través de la siguiente dirección CL LEON 80, FUENLABRADA - 28947 (MADRID) o mediante la dirección de correo electrónico agustin@martinvecino-sl.com, adjuntando copia de su DNI o pasaporte, a fin de acreditar su identidad.

Puede solicitar más información acerca de cómo tratamos sus datos dirigiéndose al correo electrónico mencionado.

ii. Firma en correo electrónico

En el caso de que se decida utilizar el correo electrónico como medio de comunicación con los usuarios de la organización, el Responsable de Tratamiento deberá incluir el texto que se prevé a continuación en la firma del correo electrónico.

El objetivo de esta medida es informar de la finalidad de este sistema como medio de comunicación, así como establecer la cláusula de confidencialidad que alude a la privacidad y el deber de secreto de los destinatarios.

De conformidad con lo dispuesto en la Ley Orgánica 3/2018, 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, informamos que los datos personales serán incluidos en un fichero titularidad y responsabilidad de MARTIN VECINO, S.L con la finalidad de posibilitar las comunicaciones a través del correo electrónico de la misma con los distintos contactos que ésta mantiene dentro del ejercicio de su actividad. Podrá ejercer los derechos de acceso, rectificación, supresión y demás derechos reconocidos en la normativa mencionada, en la siguiente dirección: CL LEON 80, FUENLABRADA - 28947 (MADRID), o a través de la siguiente dirección de correo electrónico: agustin@martinvecino-sl.com, adjuntando copia de su DNI o documento equivalente. Solicite más información al correo indicado.

En virtud de la Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y Correo Electrónico (LSSI-CE), este mensaje y sus archivos adjuntos pueden contener información confidencial, por lo que se informa de que su uso no autorizado está prohibido por la ley. Si ha recibido este mensaje por equivocación, por favor notifíquelo inmediatamente a través de esta misma vía y borre el mensaje original junto con sus ficheros adjuntos sin leerlo o grabarlo total o parcialmente. En caso de que sienta vulnerados sus derechos en lo concerniente a la protección de sus datos personales, especialmente cuando no haya obtenido satisfacción en el ejercicio de sus derechos, puede presentar una reclamación ante la Autoridad de Control en materia de Protección de Datos competente (Agencia Española de Protección de Datos), a través de su sitio web: www.agpd.es

Si usted no desea recibir más correos como este, puede darse de baja enviando un correo electrónico a la dirección: agustin@martinvecino-sl.com, con asunto "BAJAS"

c. Práctica de ejercicio de derechos

Los responsables deben facilitar a los interesados el ejercicio de sus derechos, y los procedimientos y las formas para ello deberán ser visibles, accesibles y sencillos.

El ejercicio de los derechos será gratuito para el interesado, excepto en los casos en los que se formulen solicitudes manifiestamente infundadas o excesivas, especialmente por repetitivas, el responsable podrá cobrar un canon que compense los costes administrativos de atender a la petición o negarse a actuar.

De modo que se establecen como obligaciones para los Responsables del Tratamiento:

- Articular procedimientos que permitan fácilmente que los interesados puedan acreditar que han ejercido sus derechos por medios electrónicos
- Demostrar el carácter infundado o excesivo de las solicitudes que tengan un coste para el interesado.
- Informar al interesado sobre las actuaciones derivadas de su petición en el plazo de un mes (podrá extenderse a dos meses más cuando se trate de solicitudes especialmente complejas y deberá notificar esta ampliación dentro del primer mes)
- Si decide no atender una solicitud, deberá informar de ello, motivando su negativa, dentro del plazo de un mes desde su presentación.
- Adoptar medidas para verificar la identidad de quienes soliciten el acceso y de quienes ejerzan los restantes derechos
- Podrá contar con la colaboración de los encargados para atender al ejercicio de derechos de los interesados, pudiendo incluir esta colaboración en el contrato de encargo de tratamiento.

Por todo lo expuesto, la normativa de protección de datos permite que se puedan ejercer los derechos de acceso, rectificación, oposición, supresión (“derecho al olvido”), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas.

DERECHO DE ACCESO

El derecho de acceso se define como el derecho que tiene toda persona a obtener información sobre el tratamiento de sus datos personales.

Se trata de un derecho personalísimo, pudiendo ejercerse solamente por el interesado, es decir, el titular de los datos personales.

El Responsable del tratamiento debe ofrecer en su política de privacidad la información sobre cómo pueden ejercer los interesados sus derechos ARCO (ARSULIPO) en general, y el derecho de acceso en particular.

A continuación, se facilita el formulario de solicitud de acceso a los datos personales y de denuncia ante la AEPD en caso de denegación de acceso en el Anexo 1. Así como un modelo con la posible respuesta del mismo, en el Anexo 2.

DERECHO DE RECTIFICACIÓN

El derecho de rectificación es el derecho a través del cual los ciudadanos pueden solicitar la modificación de aquella información falsa o inexacta sobre su persona.

Asimismo, la Ley Orgánica 2/1984, que en su artículo 1 dice que “Toda persona natural o jurídica tiene derecho a rectificar la información difundida por cualquier medio de comunicación social de hechos que le aludan, que considere inexactos y cuya divulgación pueda causarle perjuicio”.

La rectificación de datos personales inexactos o incompletos es también una obligación del Responsable del Tratamiento para garantizar el principio de exactitud de los datos, así como para garantizar la licitud del tratamiento.

A continuación, se facilita el formulario de solicitud de rectificación a los datos personales en el Anexo 3. Así como un modelo con la posible respuesta del mismo, en el Anexo 4.

DERECHO DE OPOSICIÓN

El Derecho de Oposición es aquel que permite a los interesados oponerse al tratamiento de sus datos personales. Se incluye en la lista de los Derechos ARCO (ARSULIPO).

Se encuentra regulado en el articulo 21 del RGPD y en el 18 de la LOPDGDD. Se trata de un derecho independiente (sin necesidad de ejercerse otro derecho previa o posteriormente) y personalísimo (solo puede ejercerlo el propio interesado, representantes legales o herederos).

A continuación, se facilita el formulario de solicitud de oposición a los datos personales en el Anexo 5. Así como un modelo con la posible respuesta del mismo, en el Anexo 6.

DERECHO DE SUPRESIÓN

El Derecho de Supresión es aquel que permite a los interesados revocar su propio consentimiento prestado anteriormente. A través del ejercicio del mismo se exige la eliminación de cualquier dato personal mediante petición directa al Responsable del Tratamiento.

Se trata de uno de los derechos ARCO (actuales ARSULIPO), recogido tanto en el Reglamento Europeo de Protección de Datos como en la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Dentro de este derecho se incluye también el derecho “al olvido”, el cual es la manifestación del derecho de supresión aplicado de forma concreta a los buscadores de Internet. Se traduce en el derecho a impedir la divulgación de los datos personales o información a través de Internet siempre y cuando su publicación no encaje con los principios de adecuación y pertinencia previstos en la norma.

A continuación, se facilita el formulario de solicitud de supresión a los datos personales en el Anexo 7. Así como un modelo con la posible respuesta del mismo, en el Anexo 8.

DERECHO DE LIMITACIÓN

El derecho a la limitación del tratamiento permite al interesado, cuyos datos personales son objeto de tratamiento, solicitar al responsable del tratamiento que aplique medidas sobre estos datos para, entre otras cosas, evitar su modificación o, en su caso, su borrado o supresión.

Para ejercer el derecho a la limitación de tratamiento de los datos personales, será necesario que la lleve a cabo el propio interesado, puesto que se trata de un derecho personalísimo, o sus representantes legales o herederos.

A continuación, se facilita el formulario de solicitud de limitación a los datos personales en el Anexo 9. Así como un modelo con la posible respuesta del mismo, en el Anexo 10.

DERECHO A LA PORTABILIDAD

El derecho a la portabilidad de los datos consiste en otorgar a cualquier ciudadano europeo el derecho a que cualquier empresa que trate sus datos personales de forma automatizada se los ceda o los transfiera a cualquier otra empresa que este les indique en un formato estructurado, inteligible y automatizado.

Es decir, el ciudadano puede exigir a las empresas que estén tratando sus datos, incluso aquellas que manejan Big Data que se los devuelvan o que los pasen a otra empresa.

se aplica en todos los Estados miembros de la Unión Europea, bajo el amparo del RGPD o Reglamento General de Protección de Datos.

A continuación, se facilita el formulario de solicitud de portabilidad a los datos personales en el Anexo 11. Así como un modelo con la posible respuesta del mismo, en el Anexo 12.

DERECHO A NO SER OBJETO DE DECISIONES INDIVIDUALES AUTOMATIZADAS

Este derecho pretende garantizar que los interesados no sean objeto de una decisión basada únicamente en el tratamiento de sus datos, incluida la elaboración de perfiles, que produzcan efectos jurídicos sobre ellos o les afecte de forma significativa.

No obstante, este derecho no será aplicable cuando sea necesario para la celebración o ejecución de un contrato entre el interesado y el responsable de tratamiento, cuando el tratamiento de los datos se fundamente en el consentimiento prestado de forma previa o bien, cuando esté autorizado por el Derecho de la Unión o de los Estados miembros y se establezcan medidas adecuadas para salvaguardar los derechos y libertades e intereses legítimos del interesado.

A continuación, se facilita el formulario de solicitud de no ser objeto de decisiones individuales automatizadas en el Anexo 13.

d. Gestión del riesgo y evaluación impacto protección de datos - MAPA DE RIESGOS

La gestión del riesgo es un elemento fundamental en los procesos de cualquier organización y es una parte inherente de la gestión de toda entidad, proyecto o actividad humana.

La gestión de riesgo está formada por un conjunto de acciones ordenadas y sistematizadas con el propósito de controlar las posibles consecuencias que una actividad puede tener sobre un conjunto de bienes o elementos que han de ser protegidos.

Precisa de un análisis, es decir, una reflexión crítica y objetiva de un tratamiento, requiere tomar decisiones que se han de plasmar en hechos concretos que minimicen el impacto sobre los activos hasta unos niveles tolerables. El RGPD demanda la identificación, evaluación y mitigación, realizadas de una forma objetiva, del riesgo para los derechos y libertades de las personas en los tratamientos de datos personales.

Por tanto, el RGPD establece la obligación de gestionar el riesgo que para los derechos y libertades de las personas supone un tratamiento.

El RGPD establece las obligaciones relativas a la evaluación de impacto relativa a la protección de datos (EIPD), fundamentalmente, en los artículos 35 y 36. Como establece el artículo 35:

Cuando sea probable que un tipo de tratamiento, …, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, …, una evaluación del impacto.

No es obligatorio que para cualquier tratamiento de datos personales sea necesario realizar una EIPD, pero sí que es obligatorio que se realice cuando hay una probabilidad de que entrañe un alto riesgo. La existencia de un grado razonable de presunción de que el tratamiento puede entrañar un alto riesgo hace imprescindible la realización de una EIPD. Podemos definir el EIPD como proceso que obliga a actuar, y de conformidad con lo previsto en el Reglamento, como un *proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos.*

Por todo lo expuesto, se extrae que es necesario realizar una previa identificación de los factores de riesgo que puedan propiciar un evento capaz de ocasionar un impacto den los derechos y libertades de los interesados.

Para dar respuesta a esta necesidad, el RGPD impone al Responsable de la obligación de realizar una evaluación del nivel de riesgo respecto de los tratamientos que realiza, teniendo en cuenta todos los aspectos del tratamiento, que se derivan de la naturaleza, ámbito, contexto y fines del tratamiento.

Por consiguiente, y con el fin de cumplir con la obligación impuesta, elaboramos la propia evaluación de impacto a través del **Mapa de Riesgos** que se adjunta a la presente documentación, en el cual se prevén cada uno de los puntos de mayor riesgo de la organización y sobre los cuales se van a adoptar una serie de medidas adicionales de control, adecuación y prevención.

e. Guía de actuación en caso de brechas de seguridad

El RGPD define, de un modo amplio, las "brechas de datos personales" como:

Todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

No tendrán consideración de brecha de datos personales sujetas a los artículos 33 y 34 del RGPD aquellos incidentes que:

- No afecten a datos personales, es decir, a datos que no sean de personas físicas identificadas o identificables.
- No afecten a tratamientos de datos personales llevados a cabo por un responsable o un encargado.
- Ocurran en tratamientos llevados a cabo por una persona física en el ámbito doméstico.

Recae sobre el Responsable del Tratamiento la obligación de notificar tanto a la Autoridad de Control como a los interesados las posibles brechas de datos personales que puedan darse.

En primer lugar, respecto de la obligación de notificar a la **Autoridad de Control**, se establece en el artículo 33 del RGPD, que tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de datos personales debe efectuar la correspondiente notificación a la Autoridad de Control competente, cuando sea probable que la brecha constituya un riesgo para los derechos y libertades de las personas. En su caso, debe realizarse sin dilación y a más tardar en las 72 horas siguientes, computando también las horas trascurridas durante fines de semana y festivos.

El criterio para determinar si un incidente ha producido "una brecha de datos personales" se recoge en el propio RGPD: "toda violación de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."

Con carácter general, en el ámbito privado, los responsables del tratamiento afectado por la brecha deberán notificar a la Agencia Española de Protección de Datos:

- Cuando su único establecimiento esté localizado en España.
- Si tienen varios establecimientos en la Unión Europea, únicamente cuando el establecimiento principal esté localizado en España.
- Si no tienen establecimiento principal en la Unión Europea, sólo en el caso de que hayan designado un representante en España.
- Si no tienen establecimiento ni representante en la Unión Europea, en el caso de que la brecha de datos personales cuente con afectados en España.

Los responsables de tratamiento con establecimiento principal en otro Estado Miembro de la Unión Europea, o que no tengan un establecimiento en la Unión, pero hayan nombrado un representante en otro Estado Miembro, deberán notificar a la Autoridad de Control de dicho Estado Miembro.

El artículo 33 del RGPD establece que la notificación de brechas de datos personales a la Autoridad de Control deberá como mínimo:

- "Describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;"
- "Comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto del que pueda obtenerse más información;"
- "Describir las posibles consecuencias de la violación de la seguridad de los datos personales;"
- "Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos."

Por otro lado, también se prevé la obligación de notificar las brechas de seguridad a los **interesados** que hayan resultado afectados. Se tarta de las personas físicas cuyos datos personales se han visto afectados por una brecha comprometiendo la confidencialidad, integridad y/o disponibilidad de esos datos, y quienes pueden sufrir las consecuencias.

El artículo 34 del RGPD establece que cuando sea probable que la brecha de datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable de tratamiento comunicará la brecha de datos personales a los afectados sin dilación indebida (en el RGPD no se establece un plazo concreto)

Por tanto, tan pronto como el responsable de tratamiento tenga constancia de la brecha de datos personales deberá valorar el riesgo para las personas afectadas y determinar la necesidad de comunicar la brecha a los afectados. En caso de que el riesgo se determine como alto, la comunicación a los afectados deberá realizarse a la mayor brevedad posible.

De conformidad con el artículo 34 del RGPD, la comunicación a las personas afectadas se realizará en un lenguaje claro y sencillo, con el siguiente contenido mínimo:

- Datos de contacto del Delegado de Protección de Datos, o en su caso, del punto de contacto en el que pueda obtenerse más información.
- Descripción general del incidente y momento en que se ha producido.
- Las posibles consecuencias de la brecha de datos personales.
- Descripción de los datos e información personal afectados.
- Resumen de las medidas implantadas hasta el momento para controlar los posibles daños.
- Otras informaciones útiles a los afectados para que puedan proteger sus datos o prevenir posibles daños.

La comunicación preferentemente se deberá realizar de forma directa al afectado, ya sea por teléfono, correo electrónico, SMS, a través de correo postal, o a través de cualquier otro medio dirigido al afectado que el responsable considere adecuado.

f. Encargado de tratamiento

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste.

El encargado puede realizar todos los tratamientos, automatizados o no, que el responsable del tratamiento le haya encomendado formalmente.

El responsable del tratamiento debe elegir un encargado del tratamiento que ofrezca garantías suficientes respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas, de acuerdo con lo establecido en el RGPD, y que garantice la protección de los derechos de las personas afectadas. Existe, por tanto, un deber de diligencia en la elección del responsable.

La regulación de la relación entre el responsable y el encargado del tratamiento debe establecerse a través de un contrato o de un acto jurídico similar que los vincule. El contrato o acto jurídico debe constar por escrito, inclusive en formato electrónico.

En el caso de designar un encargado de tratamiento, deberá formalizar el contrato vinculante de la relación. Disponen de un modelo en el Anexo 14

IV. MEDIDAS ADICIONALES PARA CENTROS EDUCATIVOS

La protección de datos en un centro educativo es fundamental, ya que se están tratando datos de menores de edad. Para el desarrollo de sus actividades, los centros docentes recaban información sobre los alumnos que es necesario proteger y tratar con la debida diligencia y cumpliendo los requisitos de la LOPD y el reglamento de protección de datos.

“Los centros educativos deben adoptar una serie de medidas de seguridad en relación a los sistemas de información a través de los que se tratan los datos personales del alumnado y personal del centro”.

Los datos personales que permiten identificar a una persona directa o indirectamente dentro del contexto de tratamiento de datos realizado en un centro educativo son:

- Datos identificativos
- Datos académicos, financieros o profesionales
- Las imágenes captadas de los alumnos
- Categorías especiales de datos: por ejemplo, aquellos relativos a la salud de los alumnos, cuyo tratamiento se hace para prestar los correspondientes servicios médicos, conocer alergias y/o intolerancias de los alumnos respecto a los servicios de comedor escolar y para adaptar la docencia en función de posibles discapacidades físicas o psíquicas.

Los centros educativos pueden recoger datos personales de sus alumnos de diversas maneras, por ejemplo, a través de los formularios de inscripción en el colegio o escuela.

Sea cual sea el caso, la condición imprescindible para recabar datos personales de los alumnos es obtener consentimiento expreso. Además, en el caso de los alumnos menores de 14 años este consentimiento RGPD ha de ser otorgado por sus padres o tutores.

Esto incluye a la información de cualquier tipo, incluyendo las categorías especiales de datos que hagan referencia al origen ético o racial, o a la salud de los alumnos.

La protección de datos en colegios y escuelas también está supeditado al deber de información. Las instituciones educativas tienen el deber de informar acerca de:

- El tratamiento de datos.
- Identidad de responsables y encargados del tratamiento.
- Finalidad del tratamiento.
- Plazo de conservación de los datos
- Si los datos se van a ceder a terceros
- Vías para ejercer los derechos de Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad y Oposición.

Las principales obligaciones para los centros educativos tienen que ver con el registro de actividades de tratamiento, la realización de análisis de riesgos y evaluaciones de impacto, la definición de responsabilidad ante el tratamiento, la obtención de consentimiento y la notificación de brechas de seguridad.

V. MEDIDAS ADICIONALES PARA CENTROS SANITARIOS

Ente los principales pilares de la protección de datos en sanidad está el respeto de la confidencialidad de los datos médicos, la obtención de consentimiento por parte del paciente o el tratamiento de datos de acuerdo al RGPD, la LOPDGDD y la Ley de autonomía del paciente.

El centro sanitario público o privado que trate al paciente y que tenga su historia clínica ejercerá como responsable del tratamiento de los datos. Como tal, tienen la obligación de implantar las medidas técnicas y organizativas necesarias para su correcta custodia, así como evitar que la información se extravíe o caiga en manos de terceros no autorizados.

La ley de protección de datos sanitarios señala que el tratamiento debe hacerse según los siguientes principios:

- Transparencia, licitud y lealtad.
- Limitación de la finalidad, esto es, se recogerán con fines concretos y explícitos y no se usarán posteriormente con otras finalidades.
- Minimización de los datos. Se limitará el uso de los datos del paciente a aquellos que sean pertinentes, adecuados y limitados a las necesidades para el cumplimiento de la finalidad.
- Exactitud. Los datos han de ser exactos, veraces y estar actualizados.
- Limitación del plazo de conservación al cumplimiento del fin para el que fueron recabados
- Integridad y confidencialidad. Se protegerán los datos frente a la pérdida, destrucción, acceso no autorizado o daño accidental.

Las menciones del RGPD en sanidad establecen que los datos médicos forman parte de las categorías especiales de datos, es decir, que son datos sensibles.

Los datos relativos a la salud, al igual que los referentes a la raza, orientación sexual o creencias religiosas, están considerados por el RGPD y la LOPDGDD como datos personales sensibles.

Desde la publicación del RGPD esta información es considerada como una categoría especial de datos, la de los datos especialmente protegidos.

Nadie está obligado a revelar estos datos sobre su persona, y solo se pueden tratar bajo consentimiento expreso y por escrito del afectado. Además, las entidades que traten estas categorías especiales de datos, sobre todo si lo hacen a gran escala, han de realizar una evaluación de impacto y contar con un Delegado de Protección de Datos.

VI. MENORES DE EDAD

El tratamiento de datos de menores de edad requiere de una vigilancia especial, ya que por parte de la Agencia Española de Protección de Datos (AEPD) se exige un mayor rigor cuando el consentimiento se obtiene de un menor, debido a que va dirigido a una persona más vulnerable que aún no está totalmente formada.

El RGPD se refiere en varios lugares a los tratamientos de los datos de los menores:

- En la regulación de los intereses legítimos del responsable como base legal para el tratamiento, señalándose que no será aplicable cuando prevalezcan los derechos, libertades o intereses de los interesados que requieran protección de datos personales, especialmente cuando esos interesados sean niños.
- Al señalar que la información que se ofrece a los interesados en relación con el tratamiento o con el ejercicio de derechos deberá ser especialmente concisa, transparente, inteligible y proporcionada con lenguaje claro y sencillo cuando los interesados sean niños.
- En el contexto del derecho al borrado de los datos personales.
- Al establecer que las actividades de formación y sensibilización dirigidas a los niños deberán estar entre las prioridades de las autoridades de protección de datos.
- En el contexto de las explicaciones que ofrecen los Considerandos del RGPD cuando se refieren a la realización de perfiles.

La Agencia Española de Protección de Datos considera, al amparo de la legislación vigente, que los mayores de catorce años, en principio pueden otorgar el consentimiento para el tratamiento de sus datos personales.

En el caso de los menores de catorce años, el consentimiento para el tratamiento de datos será otorgado por sus padres o tutores legales, de acuerdo con el artículo 7.1 de la LOPDGDD.

Asimismo, el responsable del tratamiento hará esfuerzos razonables para verificar que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

Los menores entre 14 y 18 años, como se ha mencionado, podrán otorgar su consentimiento, salvo en el caso en que la Ley prevea otra situación distinta.

Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquellos.

En ningún caso podrá recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo. No obstante, podrán recabarse datos de identidad y dirección del padre, madre o tutor.

VII. TRANSFERENCIAS INTERNACIONALES

Las transferencias internacionales de datos suponen un flujo de datos personales desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega).

Los datos solo podrán ser comunicados fuera del Espacio Económico Europeo:

- A países, territorios o sectores específicos (el RGPD incluye también organizaciones internacionales sobre los que la Comisión haya adoptado una decisión reconociendo que ofrecen un nivel de protección adecuado).

  Se añade una excepción al listado que en su momento estableció la Directiva 95/46. Se trata de la posibilidad de que el responsable pueda transferir datos a un país sin nivel adecuado de protección cuando esa transferencia sea necesaria para satisfacer intereses legítimos imperiosos del responsable y la transferencia no es repetitiva y afecta sólo a un número limitado de interesados. En todo caso, la transferencia solo será posible si no prevalecen los derechos, libertades e intereses de los afectados y deberá comunicarse a la autoridad de protección de datos.

- Cuando se hayan ofrecido garantías adecuadas sobre la protección que los datos recibirán en su destino

- Cuando se aplique alguna de las excepciones que permiten transferir los datos sin garantías de protección adecuada por razones de necesidad vinculadas al propio interés del titular de los datos o a intereses generales.

A falta de decisión de adecuación y de garantías adecuadas únicamente se podrán realizar si se cumple alguna de las condiciones siguientes:

- La persona interesada haya dado explícitamente su consentimiento, después de haber sido informada de los posibles riesgos
- La transferencia sea necesaria para la ejecución de un contrato entre la persona interesada y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud de la persona interesada
- La transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica
- La transferencia sea necesaria por razones importantes de interés público
- La transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones
- La transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando la persona interesada esté física o jurídicamente incapacitada para dar su consentimiento

- La transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta

Si no resultase aplicable ninguna de estas excepciones, solo se podrá llevar a cabo una transferencia si no es repetitiva, afecta solo a un número limitado de personas interesadas, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades de la persona interesada, y el responsable del tratamiento evalué todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofrezca garantías apropiadas con respecto a la protección de datos personales.

En este supuesto el responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14 del RGPD, el responsable del tratamiento informará a la persona interesada de la transferencia y de los intereses legítimos imperiosos perseguidos.

VIII. DELEGADO DE PROTECCIÓN DE DATOS

El RGPD establece la figura del Delegado de Protección de Datos (DPD), que será obligatorio en:

- Autoridades y organismos públicos
- Responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala
- Responsables o encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos sensibles

El DPD ha de ser nombrado atendiendo a sus cualificaciones profesionales y, en particular, a su conocimiento de la legislación y la práctica de la protección de datos. Aunque no debe tener una titulación específica, en la medida en que entre las funciones del DPD se incluya el asesoramiento al responsable o encargado en todo lo relativo a la normativa sobre protección de datos, los conocimientos jurídicos en la materia son sin duda necesarios, pero también es necesario contar con conocimientos ajenos a lo estrictamente jurídico, como por ejemplo en materia de tecnología aplicada al tratamiento de datos o en relación con el ámbito de actividad de la organización en la que el DPD desempeña su tarea.

La designación del DPD y sus datos de contacto deben hacerse públicos por los responsables y encargados y deberán ser comunicados a las autoridades de supervisión competentes.

La posición del DPD en las organizaciones tiene que cumplir los requisitos establecidos, entre los que se encuentran:

- total autonomía en el ejercicio de sus funciones
- necesidad de que se relacione con el nivel superior de la dirección
- obligación de que el responsable o el encargado faciliten al DPD todos los recursos necesarios para desarrollar su actividad

Se permite nombrar un solo DPD para un grupo empresarial siempre que sea accesible desde cada establecimiento del grupo. La accesibilidad debe entenderse en un sentido amplio. Incluye la accesibilidad física para el propio personal del grupo y también la posibilidad de que los interesados contacten con el DPD en su lengua, aun cuando el DPD esté adscrito a un establecimiento en otro Estado Miembro.

La AEPD ha optado por promover un sistema de certificación de profesionales de protección de datos como herramienta útil a la hora de evaluar que los candidatos a ocupar el puesto de DPD reúnen las cualificaciones profesionales y los conocimientos requeridos. Las certificaciones serán otorgadas por entidades certificadoras debidamente acreditadas por la Entidad Nacional de Acreditación, siguiendo criterios de acreditación y certificación elaborados por la AEPD en colaboración con los sectores afectados.

La certificación no será un requisito indispensable para el acceso a la profesión, será sólo una opción a disposición de responsables y encargados para facilitar su selección de los profesionales llamados a ocupar el puesto de DPD. Pero responsables y encargados pueden tomar en consideración otras cuestiones u otros medios para demostrar la competencia de los DPD.

Se permite que el DPD mantenga con responsables o encargados una relación laboral o mediante un contrato de servicios. Es decir, permite que pueda contratarse el servicio de DPD con personas físicas o jurídicas ajenas a la organización.

Está permitido que el DPD desarrolle sus funciones a tiempo completo o parcial. En este último caso, es preciso evitar que existan conflictos de intereses. Estos conflictos pueden surgir cuando el DPD, en su tarea de supervisión de las actividades de tratamiento de datos llevadas a cabo por la organización, debe valorar su propio trabajo dentro de ella, como sucede si se designa DPD al responsable de tecnologías de la información (cuando estas tecnologías se emplean para el tratamiento de datos) o al responsable de un área de negocio que decide sobre determinados tratamientos.

ANEXO 1

DERECHOS ARCO

EJERCICIO DEL DERECHO DE ACCESO

DATOS DEL RESPONSABLE DEL FICHERO

Nombre/Razón social: MARTIN VECINO, S.L, DNI/CIF: B81316101.

Dirección en la que se ejercita el derecho de acceso: CL LEON 80, FUENLABRADA - 28947 (MADRID).

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

_____, mayor de edad, con domicilio en _____ _____, Localidad_____, Provincia_____, con DNI _____, del que acompaña copia, por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y en consecuencia,

SOLICITA,

Que se le facilite gratuitamente el derecho de acceso a sus ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, y que se remita por correo la información a la dirección arriba indicada en el plazo de diez días a contar desde la resolución estimatoria de la solicitud de acceso.

Asimismo, se solicita que dicha información comprenda, de modo legible e inteligible, los datos de base que sobre mi persona están incluidos en sus ficheros, los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los mismos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

En _____ a _____ de _____ de 20___

Firmado

(Este derecho también podrá ejercerse a través del representante legal, en cuyo caso, además del DNI del interesado, habrá que aportar el DNI y documento acreditativo de la representación de tercero)

ANEXO 2

RESOLUCIÓN A LA SOLICITUD DE ACCESO DE DATOS

Muy Sr./a. nuestro/a,

Recibida su solicitud de acceso a los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos de lo siguiente:

Datos sobre su persona (Indicar los datos obrantes en el fichero)

Origen de los datos (Indicar si son datos obtenidos directamente del interesado o por comunicación de un tercero)

Comunicaciones realizadas (Indicar, en su caso, a qué terceros se han comunicado los datos)

Sin otro particular,

En _____ , a ___ de _____ de 20___

_____ (Firma y sello de la empresa)

ANEXO 3

DERECHOS ARCO

EJERCICIO DEL DERECHO DE RECTIFICACIÓN

DATOS DEL RESPONSABLE DEL FICHERO

Nombre/Razón social: MARTIN VECINO, S.L, DNI/CIF: B81316101.

Dirección en la que se ejercita el derecho de acceso: CL LEON 80, FUENLABRADA - 28947 (MADRID)

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

_____, mayor de edad, con domicilio en _____ _____, Localidad_____, Provincia_____, con DNI _____, del que acompaña copia, por medio del presente escrito ejerce el derecho de rectificación, de conformidad con lo previsto en el artículo 16 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y en consecuencia,

SOLICITA,

Que se proceda a acordar la rectificación de los datos personales sobre los cuales se ejercita el derecho, que se realice en el plazo de diez días a contar desde la recogida de esta solicitud, y que se me notifique de forma escrita el resultado de la rectificación practicada.

Que en caso de que se acuerde, dentro del plazo de diez días hábiles, que no procede acceder a practicar total o parcialmente las rectificaciones propuestas, se me comunique motivadamente a fin de, en su caso, solicitar la tutela de la Agencia Española de Protección de Datos, al amparo del citado Reglamento.

Que si los datos rectificados hubieran sido comunicados previamente se notifique al responsable del fichero la rectificación practicada, con el fin de que también éste proceda a hacer las correcciones oportunas para que se respete el deber de calidad de los datos a que se refiere el artículo 5 del mencionado Reglamento (UE) 2016/679.

En _____ a _____ de _____ de 20___

Firmado

ANEXO 4

RESOLUCIÓN A LA SOLICITUD DE RECTIFICACIÓN DE DATOS

Muy Sr./a. nuestro/a,

Recibida su solicitud de rectificación de los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos de lo siguiente:

Datos sobre su persona (Indicar los datos obrantes en el fichero)

Origen de los datos (Indicar si son datos obtenidos directamente del interesado o por comunicación de un tercero)

Comunicaciones realizadas (Indicar, en su caso, a qué terceros se han comunicado los datos)

Sin otro particular,

En _____ , a ___ de _____ de 20___

_____ (Firma y sello de la empresa)

ANEXO 5

DERECHOS ARCO

EJERCICIO DEL DERECHO DE OPOSICIÓN

DATOS DEL RESPONSABLE DEL FICHERO

Nombre/Razón social: MARTIN VECINO, S.L, DNI/CIF: B81316101.

Dirección en la que se ejercita el derecho de acceso: CL LEON 80, FUENLABRADA - 28947 (MADRID).

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

_____, mayor de edad, con domicilio en _____ _____, Localidad_____, Provincia_____, con DNI _____, del que acompaña copia, por medio del presente escrito ejerce el derecho de oposición, de conformidad con lo previsto en el artículo 21 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y en consecuencia,

EXPOGO,

(describir la situación en la que se produce el tratamiento de sus datos personales y enumerar los motivos por los que se opone al mismo)

Para acreditar la situación descrita, acompaño una copia de los siguientes documentos: (enumerar los documentos que adjunta con esta solicitud para acreditar la situación que ha descrito)

SOLICITO,

Que sea atendido mi ejercicio del derecho de oposición en los términos anteriormente expuestos.

En _____ a _____ de _____ de 20___

Firmado

ANEXO 6

RESOLUCIÓN A LA SOLICITUD DE OPOSICIÓN DE DATOS

Muy Sr./a. nuestro/a,

Recibida su solicitud de oposición respecto a la cesión de los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos que no se ha procedido a la cesión de los mismos.

Sin otro particular,

En _____ , a ___ de _____ de 20___

_____ (Firma y sello de la empresa)

ANEXO 7

DERECHOS ARCO

EJERCICIO DEL DERECHO DE SUPRESIÓN

DATOS DEL RESPONSABLE DEL FICHERO

Nombre/Razón social: MARTIN VECINO, S.L, DNI/CIF: B81316101.

Dirección en la que se ejercita el derecho de acceso: CL LEON 80, FUENLABRADA - 28947 (MADRID).

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

_____, mayor de edad, con domicilio en _____ _____, Localidad_____, Provincia_____, con DNI _____, del que acompaña copia, por medio del presente escrito ejerce el derecho de supresión, de conformidad con lo previsto en el artículo 16 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y en consecuencia,

SOLICITA,

1. Que se proceda, sin dilación indebida y de manera gratuita, a la supresión de sus datos de carácter personales del solicitante que estén en posesión del Responsable en el plazo máximo de diez días a contar desde la recepción de esta solicitud.

2. Que se comunique al solicitante de forma escrita a la dirección arriba indicada la cancelación de los datos una vez realizada.

3. Que, en el caso de que el responsable del fichero considere que dicha cancelación no procede, lo comunique igualmente, de forma motivada y dentro del mismo plazo de diez días. Si el Responsable se niega a atender la presenta solicitud, se interpondrá la oportuna reclamación ante la Agencia de Protección de Datos para iniciar el procedimiento de tutela de derechos.

En _____ , a ___ de _____ de 20___

Firmado

ANEXO 8

RESOLUCIÓN A LA SOLICITUD DE SUPRESIÓN DE DATOS

Muy Sr./a. nuestro/a,

Recibida su solicitud de cancelación a los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos se ha procedido a su destrucción, cancelación o, en su defecto, al bloqueo por las causas legalmente establecidas.

Sin otro particular,

En _____ , a ___ de _____ de 20___

_____ (Firma y sello de la empresa)

ANEXO 9

DERECHOS ARCO

EJERCICIO DEL DERECHO DE LIMITACIÓN

DATOS DEL RESPONSABLE DEL FICHERO

Nombre/Razón social: MARTIN VECINO, S.L, DNI/CIF: B81316101.

Dirección en la que se ejercita el derecho de acceso: CL LEON 80, FUENLABRADA - 28947 (MADRID).

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

_____, mayor de edad, con domicilio en _____ _____, Localidad_____, Provincia_____, con DNI _____, del que acompaña copia, por medio del presente escrito ejerce el derecho de limitación, de conformidad con lo previsto en el artículo 18 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y en consecuencia,

SOLICITA,

Que se proceda, de manera gratuita y en el plazo de diez días a la limitación del tratamiento de los datos por parte del Responsable debido a que:

(SELECCIONE LA OPCIÓN CORRESPONDIENTE)

- Se debe verificar la exactitud de los datos mientras el solicitante se encuentra en un procedimiento de rectificación.
- El solicitante se opone a la supresión de datos personales que están siendo tratados de manera ilícita y en su lugar se solicita la limitación de su uso;
- El solicitante se opone a la supresión de datos personales que el responsable ya no necesite para los fines del tratamiento y en su lugar se solicita la limitación de su uso;
- El solicitante se opone al tratamiento mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Que se comunique al solicitante de forma escrita a la dirección arriba indicada tanto la limitación realizada como el levantamiento de la misma antes de ambas acciones se lleven a cabo.

Y que, en el caso de que el responsable del fichero considere que la limitación del tratamiento no procede, lo comunique al solicitante de forma motivada y dentro del plazo de un mes. Si el responsable se niega a atender la presenta solicitud, se interpondrá la oportuna reclamación ante la Agencia Española de Protección de Datos para iniciar el procedimiento de tutela de derechos.

En _____ , a ___ de _____ de 20___

Firmado

ANEXO 10

RESOLUCIÓN A LA SOLICITUD DE LIMITACIÓN DE DATOS

Muy Sr./a. nuestro/a,

Recibida su solicitud de limitación respecto al tratamiento de los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos que hemos procedido a restringir el acceso a los mismos, así como a adoptar las medidas necesarias para evitar su tratamiento y cesión.

Sin otro particular,

En _____ , a ___ de _____ de 20___

_____ (Firma y sello de la empresa)

ANEXO 11

DERECHOS ARCO

EJERCICIO DEL DERECHO DE PORTABILIDAD

DATOS DEL RESPONSABLE DEL FICHERO

Nombre/Razón social: MARTIN VECINO, S.L, DNI/CIF: B81316101.

Dirección en la que se ejercita el derecho de acceso: CL LEON 80, FUENLABRADA - 28947 (MADRID).

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

_____, mayor de edad, con domicilio en _____ _____, Localidad_____, Provincia_____, con DNI _____, del que acompaña copia, por medio del presente escrito ejerce el derecho de portabilidad, de conformidad con lo previsto en el artículo 20 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y en consecuencia,

SOLICITA,

1. Que se proceda, sin dilación indebida y de manera gratuita, a la portabilidad de datos de carácter personal del solicitante que estén en posesión del Responsable en el plazo máximo de un mes a contar desde la recepción de esta solicitud.
2. Que se comunique al solicitante de forma escrita a la dirección arriba indicada, la portabilidad de dichos datos, una vez que esta haya sido realizada.
3. Que, en caso de que el responsable del fichero considere que dicha portabilidad no procede, lo comunique igualmente, de forma motivada y dentro del mismo plazo de un mes. Si el Responsable se niega a atender la presente solicitud, se interpondrá la oportuna reclamación ante la Agencia de Protección de Datos para iniciar el procedimiento de tutela de susodichos derechos.

En _____ , a ___ de _____ de 20___

Firmado

ANEXO 12

RESOLUCIÓN A LA SOLICITUD DE PORTABILIDAD DE DATOS

Muy Sr./a. nuestro/a,

Recibida su solicitud de portabilidad respecto a los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos de que se ha procedido a la portabilidad de todos sus datos.

Sin otro particular,

En _____ , a ___ de _____ de 20___

_____ (Firma y sello de la empresa)

ANEXO 13

DERECHOS ARCO

EJERCICIO DEL DERECHO A NO SER OBJETO DE DECISIONES INDIVIDUALES AUTOMATIZADAS

DATOS DEL RESPONSABLE DEL FICHERO

Nombre/Razón social: MARTIN VECINO, S.L, DNI/CIF: B81316101.

Dirección en la que se ejercita el derecho de acceso: CL LEON 80, FUENLABRADA - 28947 (MADRID).

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

_____, mayor de edad, con domicilio en _____ _____, Localidad_____, Provincia_____, con DNI _____, del que acompaña copia, por medio del presente escrito ejerce el derecho a no ser objeto de decisiones individuales automatizadas, de conformidad con lo previsto en el artículo 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y en consecuencia,

SOLICITA,

No ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que me produzca efectos jurídicos o me afecte significativamente de modo similar, en particular en los siguientes aspectos:

Que se adopten las medidas necesarias para salvaguardar mis derechos y libertades, así como mis intereses legítimos, el derecho a la intervención humana y que pueda exponer mi punto de vista e impugnar la decisión, todo ello en el supuesto de que el tratamiento de mis datos personales se fundamente en la celebración o ejecución de un contrato, o bien en mi consentimiento explícito.

Que sea atendida mi solicitud en los términos anteriormente expuestos en el plazo de un mes.

En _____ , a ___ de _____ de 20___

Firmado

ANEXO 14

CONTRATO PARA ENCARGADO DE TRATAMIENTO

REUNIDOS

De una parte, _____ con DNI nº _____actuando como representante legal de _____con domicilio en _____ y CIF nº _____ en adelante RESPONSABLE DEL FICHERO.

De otra parte, _____ con DNI nº _____actuando como legal representante de_____, con domicilio en _____ y CIF nº _____ en adelante ENCARGADO DEL TRATAMIENTO.

Ambas partes se reconocen mutuamente la capacidad legal suficiente para suscribir este contrato de encargo de tratamiento de datos personales y para quedar obligadas en la representación en que respectivamente actúan, en los términos convenidos en él. A tal fin,

MANIFIESTAN

1. Que ambas partes se encuentran vinculadas por una relación contractual de carácter mercantil para la prestación de _____ (en adelante SERVICIO).
2. Que para la prestación de dicho servicio es necesario que el ENCARGADO DEL TRATAMIENTO tenga acceso y realice tratamientos de datos de carácter personal de los _____ responsabilidad del RESPONSABLE DEL FICHERO, por lo que asume las funciones y obligaciones que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, estipula para los Encargados de Tratamiento
3. Ambas partes reconocen cumplir con todas las obligaciones derivadas de la normativa comunitaria y nacional en materia de protección de datos, en especial las relativas al derecho de información, consentimiento y deber de secreto, y a la adopción de las medidas de seguridad técnicas y organizativas que garanticen la seguridad de los datos personales
4. Que, en cumplimiento del artículo 28 del RGPD, ambas partes de forma libre y espontánea voluntad acuerdan regular este acceso y tratamiento de datos de carácter personal de conformidad con las siguientes:

ESTIPULACIONES

PRIMERO: OBJETO DEL CONTRATO

Mediante las presentes cláusulas se habilita a la entidad ENCARGADA DE TRATAMIENTO, para tratar por cuenta del, RESPONSABLE DEL TRATAMIENTO, los datos de carácter personal necesarios para prestar el servicio anteriormente descrito.

SEGUNDO: IDENTIFICACIÓN DE LA INFORMACIÓN AFECTADA

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el RESPONSABLE DEL TRATAMIENTO, pone a disposición del ENCARGADO DEL TRATAMIENTO, la información que se describe a continuación:

- …
- …

TERCERO: DURACIÓN

El presente acuerdo tiene una duración de _____

Una vez finalice el presente contrato, el ENCARGADO DE TRATAMIENTO debe suprimir/devolver al RESPONSABLE, o devolver a otro encargado que designe el RESPONSABLE los datos personales y suprimir cualquier copia que esté en su poder.

CUARTO: OBLIGACIONES DEL ENCARGADO DE TRATAMIENTO

El ENCARGADO DEL TRATAMIENTO y todo su personal se obliga a:

1-. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

2-. Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento. Si el ENCARGADO DEL TRATAMIENTO considera que alguna de las instrucciones infringe el Reglamento (UE) 2016/679 o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.

3-. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:

- El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.
- Las categorías de tratamientos efectuados por cuenta de cada responsable.
- En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del Reglamento (UE) 2016/679, la documentación de garantías adecuadas.
- Una descripción general de las medidas técnicas y organizativas de seguridad relativas a: la seudoanimización y el cifrado de datos personales, la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento, la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico y el proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

4-. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles. El

encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación. Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

5. Subcontratación. (Escoger una de las opciones)

Opción A No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del ENCARGADO. Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de 72 horas, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido. El subcontratista, que también tendrá la condición de ENCARGADO DEL TRATAMIENTO, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el ENCARGADO DEL TRATAMIENTO y las instrucciones que dicte el responsable.

Corresponde al ENCARGADO inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

Opción B Se autoriza al ENCARGADO a subcontratar con la empresa _____ las prestaciones que comporten los tratamientos siguientes: _____.

Para subcontratar con otras empresas, el encargado debe comunicarlo por escrito al responsable, identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo de 72 horas.

El subcontratista, que también tiene la condición de ENCARGADO DEL TRATAMIENTO, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el ENCARGADO DEL TRATAMIENTO y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación, de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el

encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

6-. El ENCARGADO DEL TRATAMIENTO deberá observar en todo momento, y en relación con los ficheros de datos de carácter personal a los que tuviera acceso o le pudieren ser entregados por el Responsable, para la realización en cada caso de los trabajos y servicios que pudieren acordarse, el deber de confidencialidad y secreto profesional que, de conformidad con lo dispuesto en la normativa de Protección de Datos, subsistirá aun después de finalizar la relación de los trabajos encargados en relación con cualquier fichero así como, en su caso, tras la finalización por cualquier causa del presente contrato.

7-. Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente

8-. Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

9-. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

10-. Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:

- Acceso, rectificación, supresión y oposición
- Limitación del tratamiento
- Portabilidad de datos
- A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

El ENCARGADO DEL TRATAMIENTO debe resolver, por cuenta del responsable, y dentro del plazo establecido, las solicitudes de ejercicio de los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, en relación con los datos objeto del encargo.

11-. Derecho de información

El ENCARGADO DEL TRATAMIENTO, en el momento de la recogida de los datos, debe facilitar la información relativa a los tratamientos de datos que se van a realizar. La redacción y el formato en que se facilitará la información se debe consensuar con el responsable antes del inicio de la recogida de los datos.

12-. Notificación de violaciones de la seguridad de los datos

El ENCARGADO DEL TRATAMIENTO notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 72 horas, y a través de correo electrónico con confirmación de lectura, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia. No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

- Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
- El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
- Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

(Escoger alguna o las dos opciones)

Opción A

- Corresponde al RESPONSABLE DEL TRATAMIENTO comunicar las violaciones de la seguridad de los datos a la Autoridad de Protección de Datos y a los interesados.
  La comunicación contendrá, como mínimo, la información siguiente:
  Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
  Nombre y datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
  Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
  Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos. Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

Opción B

Corresponde al ENCARGADO DEL TRATAMIENTO comunicar en el menor tiempo posible las violaciones de la seguridad de los datos a los interesados, cuando sea probable que la violación suponga un alto riesgo para los derechos y las libertades de las personas físicas.

La comunicación debe realizarse en un lenguaje claro y sencillo y deberá, como mínimo:

- Explicar la naturaleza de la violación de datos.
- Indicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- Describir las posibles consecuencias de la violación de la seguridad de los datos personales.

- Describir las medidas adoptadas o propuestas por el RESPONSABLE DEL TRATAMIENTO para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

13-. Dar apoyo al RESPONSABLE DEL TRATAMIENTO en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

14-. Dar apoyo al RESPONSABLE DEL TRATAMIENTO en la realización de las consultas previas a la autoridad de control, cuando proceda.

15-. Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

16-. Implantar las medidas de seguridad siguientes: Todas aquellas necesarias para:

- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
- Seudonimizar y cifrar los datos personales, en su caso.

17-. Designar un delegado de protección de datos y comunicar su identidad y datos de contacto al responsable.

18-. Destino de los datos: (Escoger una de las 3 opciones siguientes)

Opción A

Devolver al RESPONSABLE DEL TRATAMIENTO los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación. La devolución debe comporta el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado. No obstante, el ENCARGADO puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

Opción B

Devolver al ENCARGADO que designe por escrito el RESPONSABLE DEL TRATAMIENTO, los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida prestación. La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado. No obstante, el ENCARGADO puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

Opción C

Destruir los datos, una vez cumplida la prestación. Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado al RESPONSABLE DEL TRATAMIENTO. No obstante, el ENCARGADO puede conservar una copia, con los datos debidamente boqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

QUINTO: OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

Corresponde al RESPONSABLE DEL TRATAMIENTO:

1-. Entregar al encargado los datos a los que se refiere la cláusula 2 de este documento.

2-. Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.

3-. Realizar las consultas previas que corresponda.

4-. Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del Reglamento (UE) 2016/679 por parte del encargado.

5-. Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

SEXTO: RESPONSABILIDAD DEL ENCARGADO DE TRATAMIENTO

1-. El ENCARGADO DEL TRATAMIENTO será considerado responsable del tratamiento en el caso de que destine los datos a otra finalidad, los comunique o los utilice incumpliendo el presente contrato. En estos casos, el ENCARGADO DEL TRATAMIENTO responderá de las infracciones en que hubiera incurrido personalmente.

2.- El ENCARGADO DEL TRATAMIENTO indemnizará al RESPONSABLE DEL TRATAMIENTO por los daños y perjuicios, de cualquier naturaleza, que pudieran resultar del incumplimiento de las obligaciones contraídas en virtud del presente contrato.

3.- A título enunciativo, y no limitativo, dicha indemnización incluirá los daños morales e imagen, costes publicitarios o de cualquier otra índole que pudieran resultar para su reparación. El ENCARGADO DEL TRATAMIENTO, asimismo, deberá responder de cualquier indemnización que a resultas de su incumplimiento tuviera que satisfacer a terceros.

4.- La responsabilidad del ENCARGADO DEL TRATAMIENTO incluirá, además, el importe de cualquier sanción administrativa y/o resolución judicial condenatoria que pudiera resultar contra el RESPONSABLE DEL TRATAMIENTO, como resultado del incumplimiento del ENCARGADO DEL TRATAMIENTO de la normativa y de las obligaciones exigidas en el presente contrato. La indemnización comprenderá, además del importe de la sanción y/o resolución judicial, el de los intereses de demora, costas judiciales y el importe de la defensa del RESPONSABLE DEL TRATAMIENTO en cualquier proceso en el que pudiera resultar demandada por cualquiera de las causas anteriormente expuestas.

SÉPTIMO: CONTROLES Y AUDITORÍA

El RESPONSABLE DEL TRATAMIENTO, en su condición, se reserva el derecho de efectuar en cualquier momento los controles y auditorías que estime oportunos para comprobar el correcto cumplimiento por parte del ENCARGADO DEL TRATAMIENTO del presente contrato. Por su parte, el Encargado deberá facilitar al RESPONSABLE

DEL TRATAMIENTO cuantos datos o documentos le requiera para el adecuado cumplimiento de dichos controles y auditorías.

OCHO: NOTIFICACIONES

1.- Cualquier notificación que se efectúe entre las partes se hará por escrito y será entregada personalmente o de cualquier otra forma que certifique la recepción por la parte notificada.

2.- Cualquier cambio de domicilio de una de las partes deberá ser notificado a la otra de forma inmediata y por un medio que garantice la recepción del mensaje.

NUEVE: CLÁUSULAS GENERALES

1.- La no exigencia por cualquiera de las partes de cualquiera de sus derechos, de conformidad con el presente Contrato, no se considerará que constituye una renuncia a dichos derechos en el futuro.

2.- La relación jurídica que se constituye entre las partes se rige por este único Contrato, siendo el único válido existente entre las partes y sustituye a cualquier tipo de acuerdo o compromiso anterior acerca del mismo objeto, ya sea escrito o verbal, y sólo podrá ser modificado por un acuerdo firmado por ambas partes.

3.- Si se llegara a demostrar que alguna de las estipulaciones contenidas en este Contrato es nula, ilegal o inexigible, la validez, legalidad y exigibilidad del resto de las estipulaciones no se verán afectadas o perjudicadas por aquélla.

4.- El presente Contrato y las relaciones entre el RESPONSABLE DEL TRATAMIENTO y el ENCARGADO DEL TRATAMIENTO no constituyen en ningún caso sociedad, empresa conjunta, agencia o contrato de trabajo entre las partes.

5.-Los encabezamientos de las distintas cláusulas son sólo a efectos informativos, y no afectarán, calificarán o ampliarán la interpretación de este Contrato.

En testimonio de lo cual formalizan el presente contrato, por duplicado, en el lugar y fecha indicados en el encabezamiento.

En nombre de «EL RESPONSABLE» En nombre de «EL ENCARGADO»